Fall 2020 Course Notes

Niven Achenjang

November 7, 2022

These are my course notes for the Fall 2020 academic semester. Each class[1] gets its own "chapter" and each lecture gets its own "section." These are live-texed or whatever, so there is likely to be some (but hopefully not too much) content missing from me typing more slowly than one lectures. It also, of course, reflects my understanding (or lack thereof) of the material, so it is far from perfect. Two classes (number theory and class groups) overlapped once a week, so expect some shenanigans in those notes. Finally, this document contains many typos, but ideally not enough to distract from the mathematics. With all that taken care of, enjoy and happy mathing.

Contents

[1] After writing all this, I think I now understand why people usually only include one class per document. This thing is absurdly long

List of Figures

List of Tables

1 18.745 (Lie Groups and Lie Algebras, I)

Instructor: Pavel Etingof

Course site: I think here (may require MIT credentials and/or stop existing when this class ends).

Lecture notes: Here (same caveats as above).

1.1 Lecture 1 (9/1)

1.1.1 Course/Administrative Stuff

All lectures will be recorded.

This class used to be Lie algebras first and then Lie groups after that, but this year we're trying both at once. The syllabus is online. There is no exam, but homework every week assigned on Tuesday (including today). Upload solutions to the Stellar site. The textbook is also on the website (restricted use, do not share the file). Lecture notes also on the site. Ask questions by unmuting and talking or typing into the chat.

This is a "hybrid" course, so there will be some in-person events for the people in Cambridge/-Boston/wherever this school is.

There are office hours in the same zoom room. One right after Tuesday lecture, and one right before Thursday lecture.

Brief Intro The purpose of group theory is to give a mathematical treatment of symmetries. Likewise, the theory of Lie groups is meant to give a mathematical treatment of *continuous* symmetries, i.e. families of symmetries continuously depending on several real parameters. The theory was founded in the second half of the 19th century by Norwegian mathematician Sophus Lie who was studying symmetries of differential equations.

A prototypical example of a Lie group is SO(3), the rotational symmetries of the 2-dimensional sphere. It is 3 dimensional, with parameters sometimes called "Euler angles" φ, θ, ψ.

Unlike ordinary parametrized curves and surfaces, Lie groups are determined by their linear approximation at the identity element. This leads to the notion of the Lie algebra of a Lie group which allows one to reformulate the theory of continuous symmetries in purely algebraic terms. The goal of this course is to get a detailed study of Lie groups/algebras, potentially even over fields other than $\mathbb{R}$ or $\mathbb{C}$.

1.1.2 Topological groups

Recall that continuity described by topology and symmetry described by group theory, so "continuous symmetry" should be described by topological groups.

Etingof spends a bit of time reviewing basic topology (topological space, product topology, subspace/induced topology, continuous maps, etc.)...

Definition 1.1.1. A **topological group** is a group G which is also a topological space, so that the multiplication map $m : G \times G \to G$ and the inversion map $\iota : G \to G$ are both continuous. $\diamond$

Note 1. In this course, algebra will be more important than geometry/topology. Geometry/topology/-analysis will play a bigger role in the second semester.

Example. The group $(\mathbb{R}, +)$ is topological. $\triangle$

Example. Any subgroup of a topological group is itself a topological group. e.g. $(\mathbb{Q}, +)$ is a topological group. $\triangle$

The previous example shows that general topological groups may be too general. Is $(\mathbb{Q}, +)$ really a good model for continuous symmetries? To remedy this, we restrict our focus.

1.1.3 Lie Groups

We will want to look at topological groups which are also topological manifolds.

He spends a bit of time recalling neighborhoods, bases, Hausdorff, convergence, and homeomorphism... (Importantly, neighborhoods in this class are automatically open, as they should be).

Definition 1.1.2. A Hausdorff topological space X is said to be an n**-dimensional topological manifold** if it has a countable base (second-countable) and is locally homeomorphic to $\mathbb{R}^n$; namely, for every $x \in X$, there is a neighborhood $U \subset X$ of x and a continuous map $\varphi : U \to \mathbb{R}^n$ such that $\varphi : U \to \varphi(U)$ is a homeomorphism with $\varphi(U) \subset \mathbb{R}^n$ open. $\diamond$

Remark 1.1.3. It is true (but non-obvious) that if a nonempty open set in $\mathbb{R}^n$ is homeomorphic to one in $\mathbb{R}^m$, then $n = m$. In particular, the number n above is uniquely determined by X as long as $X \neq \emptyset$. This number is called the **dimension** of X. $\circ$

Remark 1.1.4. We adopt the convention that $\emptyset$ is a manifold of any integer dimension. $\circ$

Example. $X = \mathbb{R}^n$ is an n-dimensional topological manifold. Take $U = X$ and $\varphi = \mathrm{Id}$. $\triangle$

Example. An open subset of a topological manifold is itself a topological manifold of the same dimension. $\triangle$

Example. The circle $S^1 \subset \mathbb{R}^2$ defined by $x^2 + y^2 = 1$ is a topological manifold. For example, the point $(1, 0)$ has a neighborhood $U = S^1 \setminus \{(-1, 0)\}$ and a map $\varphi : U \to \mathbb{R}$ given by the stereographic projection:

$$\varphi(\theta) = \tan(\theta/2) \ \text{ with } \ -\pi < \theta < \pi.$$

similarly for any other point (S^1 is homogeneous or whatever).

More generally, the n-sphere $S^n \subset \mathbb{R}^{n+1}$ defined by $x_0^2 + \cdots + x_n^2 = 1$ is a topological manifold for the same reason (stereographically project). $\triangle$

Example. The figure-8 curve ∞ is not a manifold, since it is not locally homeomorphic to $\mathbb{R}$ at the self-intersection point (can split into 4 parts by removing a single point whereas remove a point in $\mathbb{R}$ splits into only 2 components). $\triangle$

Definition 1.1.5. A pair (U, φ) with the above properties is called a **local chart**. An **atlas** of local charts is a collection of charts $(U_\alpha, \varphi_\alpha)_{\alpha \in A}$ such that

$$\bigcup_{\alpha \in A} U_\alpha = X.$$

$\diamond$

By definition, any topological manifold admits an atlas labeled by the points of X. "Such an atlas, one cannot print... as a book... because it's uncountable."

There are usually much smaller atlases. For example, $\mathbb{R}^n$ has an atlas with just one chart, and S^n has an atlas with two charts. Very often, X we care about admit atlases with finitely many charts. For example, if X is compact, then there is a finite atlas (often even if X is non-compact). Moreover, there is always a countable atlas.

Now let (U, φ) and (V, ψ) with overlapping charts (i.e. $V \cap U = \emptyset$). Then we get **transition maps**

$$\varphi \circ \psi^{-1} : \psi(U \cap V) \to \varphi(U \cap V),$$

which is a homeomorphism between open subsets in $\mathbb{R}^n$.

Example. Consider the two chart atlas for the circle S^1, one missing $(-1, 0)$ and the other missing $(1, 0)$. Then,

$$\varphi(\theta) = \tan(\theta/2) \text{ and } \psi(\theta) = \cot(\theta/2).$$

Hence, $\varphi(U \cap V) = \mathbb{R} \setminus 0 = \psi(U \cap V)$ with

$$(\varphi \circ \psi^{-1})(x) = \frac{1}{x}$$

(since $\cot = 1/\tan$). △

1.1.4 C^k, real analytic and complex analytic manifolds

The notion of topological manifold is not convenient for us, since continuous functions in general do not admit linear approximations (i.e. derivatives).

Definition 1.1.6. An atlas on X is said to be **of regularity class** C^k, $1 \leq k \leq \infty$, if all transition maps between its charts are of class C^k (k times continuously differentiable). An atlas of class C^∞ is called **smooth**. Also an atlas is said to be **real analytic** if all transition maps are real analytic. Finally, if $n = 2m$ is even, so that $\mathbb{R}^n = \mathbb{C}^m$, then an atlas is called **complex analytic** if all its transition functions are complex analytic. ⋄

Example. The two-chart atlas for the circle S^1 defined by stereographic projections is real analytic, since $f(x) = \frac{1}{x}$ is analytic on $\mathbb{R} \setminus 0$. The same applies to there sphere S^n for any n. e.g. for S^2 the transition map $\mathbb{R}^2 \setminus 0 \to \mathbb{R}^2 \setminus 0$ is given by

$$f(x) = \left(\frac{x}{x^2 + y^2}, \frac{y}{x^2 + y^2} \right).$$

Using the complex coordinate $z = x + iy$, we get

$$f(z) = \frac{z}{|z|^2} = \frac{1}{\bar{z}},$$

so this atlas is not complex analytic. However, replacing one of the stereographic projections by its complex conjugate, we get $f(z) = \frac{1}{z}$ which is analytic. Thus, S^2 is a complex manifold (of dimension 1). △

Remark 1.1.7. It is known (although hard to prove) that S^n does not admit a complex analytic atlas for $n \neq 2, 6$. For $n = 6$, this is a famous conjecture. ◦

Exercise. Let $f_1, \ldots, f_m$ from $\mathbb{R}^n \to \mathbb{R}$ or $\mathbb{C}^n \to \mathbb{C}$ be C^k, real analytic or complex analytic. Let $X \subset \mathbb{R}^n$ be the set of points P such that $f_i(P) = 0$ for all i and $\mathrm{d}f_i(P)$ are linearly independent. Use the implicit function theorem to show that X is a topological manifold of dimension $n - m$ and equip it with a natural C^k, real analytic or complex analytic structure.

Definition 1.1.8. Two C^k, real analytic, or complex analytic atlases U_α, V_β are said to be **compatible** if the transition maps between U_α and V_β are of the same class (i.e. both C^k, both real analytic, or both complex analytic). ⋄

This is an equivalence relation.

Definition 1.1.9. A **C^k, real analytic, or complex analytic** structure on a topological manifold X is an equivalence class of atlases of the corresponding type. We call X equipped with such a structure a **C^k-manifold**, **real analytic manifold**, or **complex analytic manifold**. Complex analytic manifolds are also called **complex manifolds** and C^∞-manifolds are also called **smooth manifolds**. A **diffeomorphism** (or **isomorphism**) is a homeomorphism preserving the class. ⋄

Remark 1.1.10. This is really a *structure*, not a *property*. For example, consider $X = \mathbb{C}$ and $Y = D \subset \mathbb{C}$, the open unit disk, with the usual complex coordinate z. These are isomorphic as real analytic manifolds, but not as complex analytic manifolds: a complex isomorphism would be a holomorphic function $f : C \to D$, hence bounded, and hence constant by Liouville. Thus we have two different complex structures on $\mathbb{R}^2$ (no others by Riemann mapping theorem).

It's also true (but much harder to show) that $\mathbb{R}^4$ has uncountably many smooth structures and S^7 has 28. ◦

1.1.5 Regular functions

Let $P \in X$ and (U, φ) a local chart around P such that $\varphi(P) = 0$. We call such a chart a **coordinate chart** around P. In particular, we have **local coordinates** $x_1, \ldots, x_n : U \to \mathbb{R}$. Note that $x_i(P) = 0$ and $x_i(Q)$ determine Q if $Q \in U$.

Definition 1.1.11. A **regular function** on an open set $V \subset X$ in a C^k, real analytic, or complex analytic manifold X is a function $f : V \to \mathbb{R}$ (or $\mathbb{C}$ is the complex case) such that

$$f \circ \varphi_\alpha^{-1} : \varphi_\alpha(V \cap U_\alpha) \to \mathbb{R}, \mathbb{C}$$

is of the corresponding regularity class, for some (and then any) atlas $(U_\alpha, \varphi_\alpha)$. ⋄

Notation 1.1.12. The space (in fact, algebra) of regular functions on V will be denote by $O(V)$ or $\mathscr{O}(V)$.

Definition 1.1.13. Let V, U be neighborhoods of $P \in X$. We say that $f \in O(V)$ and $g \in O(U)$ are **equal near** P if there exists a neighborhood $W \subset U \cap V$ of P such that $f|_W = g|_W$. ⋄

The point is that we want to do "local analysis" so we do not need functions defined far away from a fixed point. Hence, we would like to work in an arbitrarily small neighborhood, and we think of functions on this arbitrarily small neighborhood as being germs, i.e. any two functions which agree near P are considered equal.

Definition 1.1.14. A **germ** of a regular function at P is a class of regular functions on neighborhoods of P which are equal near P. ◇

"germs are very very small. They're even smaller than the coronavirus."

The algebra of germs of regular functions at P is denoted by O_P, and in fact one has $O_P = \varinjlim O(U)$ where the direct limit is taken over neighborhoods of P.

Remark 1.1.15. Germs are not defined on any physical neighborhood of P, but capture the vague idea of working "near P." In particular, you can evaluate a germ at P but not at any other point. ○

1.1.6 Tangent spaces

From now on, we only consider smooth, real analytic and complex analytic manifolds. A **derivation at** P will mean a linear map

$$D : O_P \to \mathbb{R}, \mathbb{C}$$

satisfying the **Leibniz rule**

$$D(fg) = D(f)g(P) + f(P)D(g).$$

Now that for any such D, we have $D(1) = 0$.

Let $T_P X$ be the space of all such derivations.

Lemma 1.1.16. *Let $x_1, \dots, x_n$ be local coordinates at P. Then $T_P X$ has basis $D_1, \dots, D_n$, where*

$$D_i(f) := \frac{\partial f}{\partial x_i}(0).$$

Proof. We're working locally so may assume $X = \mathbb{R}^n$ or $\mathbb{C}^n$ and $P = 0$. Clearly, $D_1, \dots, D_n$ form a linearly independent set in $T_P X$. Need them to also span. Pick some $D \in T_P X$ and write $D(x_i) = a_i$. Consider $D_* = D - \sum_i a_i D_i$. Note that $D_*(x_i) = 0$ for all i (it also kills constants). We'll show that this implies $D_* = 0$. Given $f \in O_P$, we can write

$$f(x_1, \dots, x_n) = f(0) + \sum_{i=1}^{n} x_i h_i(x_1, \dots, x_n).$$

where

$$h_i(x_1, \dots, x_n) = \frac{f(x_1, \dots, x_i, 0, \dots, 0) - f(x_1, \dots, x_{i-1}, 0, \dots, 0)}{x_i}.$$

Once you believe this, we win by linearity + Liebniz.

The division in the definition of h_i may make you worried that it's not regular, but it is. In analytic case, use Taylor series. In smooth case, use finite Taylor approximation. Have to be a little careful, but it works out. ■

Definition 1.1.17. The space $T_P X$ is called the **tangent space at** P and its elements are called **tangent vectors** (at P). ◇

Observe that every tangent vector $v \in T_P X$ defines a derivation $\partial_v : O(U) \to \mathbb{R}, \mathbb{C}$ and the number ∂_v is called the **derivative of f in the direction of v**. For usual curves/surfaces in $\mathbb{R}^3$, this is exactly what you expect from calculus.

1.1.7 Regular maps

Definition 1.1.18. A continuous map $F : X \to Y$ between manifolds is **regular** if for any regular function h on an open set $U \subset Y$, the function $h \circ F$ is regular on $F^{-1}(U)$. i.e. F is expressed by regular functions in local coordinates. $\diamond$

Definition 1.1.19. Let $F : X \to Y$ be a regular map and $P \in X$. Then we can define the **differential** of F at P, $d_P F$, which is a linear map $T_P X \to T_{f(P)} Y$. Namely, for $f \in O_{F(P)}$ and $v \in T_P X$, the vector $d_P F \cdot v$ is defined by the formula

$$(d_P F \circ v)(f) := v(f \circ F).$$

Moreover, if $G : Y \to Z$ is another regular map, then we have the usual chain rule,

$$d(G \circ F)_P = dG_{F(P)} \circ dF_P.$$

$\diamond$

In particular, if $\gamma : (a, b) \to X$ is a regular **parametrized curve** then for $t \in (a, b)$, we can define the **velocity vector**

$$(\mathrm{d}\gamma(t))(1) = \gamma'(t) \in T_{\gamma(t)} X.$$

1.1.8 Submersions and immersions, submanifolds

Definition 1.1.20. A regular map of manifolds $F : X \to Y$ is a **submersion** if the derivative is surjective for all $P \in X$. $\diamond$

Proposition 1.1.21. *If F is a submersion then for any $Q \in Y$, $F^{-1}(Q)$ is a manifold of dimension* $\dim X - \dim Y$.

Proof. This is a local question, so reduced to earlier exercise. ∎

Definition 1.1.22. A regular map of manifolds $f : X \to Y$ is an **immersion** if the differential is injective for all $P \in X$. $\diamond$

Example. The inclusion $S^n \hookrightarrow \mathbb{R}^{n+1}$ is an immersion. The map $F : S^1 \to \mathbb{R}^2$ given by

$$x(t) = \frac{\cos\theta}{1 + \sin^2\theta}, y(t) = \frac{\sin\theta\cos\theta}{1 + \sin^2\theta}$$

traces out a ∞ and is an immersion, but not injective.

On the other hand, the map $F : \mathbb{R} \to \mathbb{R}^2$ given by $F(T) = (t^2, t^3)$ is injective but not an immersion. $\triangle$

Definition 1.1.23. An immersion $f : X \to Y$ is an **embedding** if the map $X \to f(X)$ is a homeomorphism. In this case, $f(X) \subset Y$ is called an **(embedded) submanifold**. $\diamond$

Example. $S^n \hookrightarrow \mathbb{R}^{n+1}$ is an embedding, but the lemniscate ∞ is not. The parametrization of the curve ρ by $\mathbb{R}$ is injective but not a homeomorphism. △

Definition 1.1.24. An embedding $F : X \to Y$ is a **closed embedding** if its image is closed. In this case $F(X)$ is a **closed (embedded) submanifold**. ⋄

I think we're running out of time, so skipping over some stuff.

Remark 1.1.25. A C^0 Lie group is a topological group which is a topological manifold. The Hilbert 5th problem was to show that any such group is actually a real analytic manifold. This was shown in the 1950s (in particular, analytic structure is unique), so regularity classes of Lie groups don't matter. Called **Gleason-Yamabe theorem**. ○

Because of this remark, we won't pay that much attention to regularity classes. We'll mainly just distinguish Real vs. Complex.

1.2 Lecture 2 (9/3)

1.2.1 Lie groups

Definition 1.2.1. A C^k, real or complex analytic **Lie group** is a manifold G of the same class, with a group structure such that the multiplication map $m : G \times G \to G$ is regular. ⋄

Thus, in a Lie group G for any $g \in G$ the left and right translation maps are diffeomorphisms.

Proposition 1.2.2. *In a Lie group G, the inversion map $\iota : G \to G$ is a diffeomorphism, and* $\mathrm{d}\iota_1 = -\mathrm{Id}$.

Proof. For the first statement, suffices to show ι is regular near 1; the rest follows by translation. Pick a coordinate chart near $1 \in G$ and write m in this chart in local coordinates. We know $m(x, 0) = x$ and $m(0, y) = y$ (since 0 corresponds to identity in this chart). Hence, the linear approximation of $m(x, y)$ at 0 is $x + y$. Thus, by the implicit function theorem, the equation $m(x, y) = 0$ is solved near 0 by a regular function $y = \iota(x)$ with $\mathrm{d}\iota(0) = -\mathrm{Id}$. ■

Recall 1.2.3. A C^0 Lie group is a topological group which is a topological manifold. The Hilbert 5th problem was to show that any such group is actually a real analytic manifold. This was shown in the 1950s (in particular, analytic structure is unique), so regularity classes of Lie groups don't matter. Called **Gleason-Yamabe theorem**. ⊙

Note also than any complex Lie group of dimension n is also a real Lie group of dimension $2n$. Also, the Cartesian product of real (complex) Lie groups is a real (complex) Lie group.

1.2.2 Homomorphisms

Definition 1.2.4. A **homomorphism of Lie groups** $f : G \to H$ is a group homomorphism which is also a regular map. An **isomorphism of Lie groups** is a homomorphism f which is a group isomorphism such that $f^{-1} : H \to G$ is regular. ⋄

We will see later that the last condition is in fact redundant.

Example. $(\mathbb{R}^n, +)$ is a real Lie group and $(\mathbb{C}^n, +)$ is a complex Lie group (both n-dimensional) △

Example. $(\mathbb{R}^\times, \times), (\mathbb{R}_{>0}, \times)$ are real Lie groups, and $(\mathbb{C}^\times, \times)$ is a complex Lie group (all 1-dimensional) $\triangle$

Example. $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ is a 1-dimensional real Lie group under multiplication of complex numbers. $\triangle$

Remark 1.2.5. Note that $\mathbb{R}^\times \cong \mathbb{R}_{>0} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{C}^\times \cong \mathbb{R}_{>0} \times S^1$ as real Lie groups (polar coordinates). Also, $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$ via $x \mapsto e^x$. $\circ$

Example. The group of $n \times n$ invertible matrices $\mathrm{GL}_n(\mathbb{R})$ is a real Lie group and $\mathrm{GL}_n \mathbb{C}$ is a complex Lie group. These are open sets in the corresponding spaces of all matrices and have dimension n^2. $\triangle$

Example. SU(2), the **special unitary group of size 2**, is a real Lie group. This is complex 2×2 matrices A such that

$$AA^\dagger = \mathbf{1} \text{ and } \det A = 1.$$

Hence writing

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix},$$

we get

$$a\overline{a} + b\overline{b} = 1, \;\; a\overline{c} + b\overline{d} = 0 \text{ and } c\overline{c} + d\overline{d} = 1.$$

The second equation implies that $(c, d) = \lambda(-\overline{b}, \overline{a})$, so

$$1 = \det A = ad - bc = \lambda(a\overline{a} + b\overline{b}) = \lambda.$$

Hence, SU(2) is identified with the set of $(a, b) \in \mathbb{C}^2$ such that $a\overline{a} + b\overline{b} = 1$. Writing $a = x + iy, b = z + it$, we have

$$\mathrm{SU}(2) \cong \left\{(x, y, z, t) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + t^2 = 1\right\}.$$

Thus SU(2) is a 3-dimensional real Lie group which, as a manifold, is the 3-dimensional sphere $S^3 \subset \mathbb{R}^4$. In fact, SU(2) can be though of as the unit quaternions.

In fact, it's known that S^0, S^1, S^3 are the only spheres which are Lie groups (think Hopf invariant one). $\triangle$

Example. Any countable group G with discrete topology is a (real or complex) Lie group of dimension 0. $\triangle$

1.2.3 The connected component of 1

Pavel recalls more topology stuff ((path-)connectedness, (path-)connected components, quotient topology, etc.)...

Exercise. Show that a manifold is connected iff it is path-connected.

Notation 1.2.6. Let G be a real or complex Lie group. We let G° (or G^0 or G^o since I'll be too lazy to type \circ) denote the connected component of $1 \in G$. Note that the connected component of any $g \in G$ is gG°.

Proposition 1.2.7.

(i) G° *is a normal subgroup of* G.

(ii) $\pi_0(G) = G/G^\circ$ *with the quotient topology is a discrete and countable group.*

Proof. **(i)** Let $g \in G$,$a \in G^o$, and $x : [0,1] \to G$ a path from 1 to a. Then, gxg^{-1} is a path connected 1 to gag^{-1}, so $gag^{-1} \in G^o$. We win (it's clearly a subgroup. To see this, multiply paths).

(ii) Since G is a manifold, for any $g \in G$, there is a neighborhood of g contained in $G_g = gG^\circ$ (e.g. since it has a connected neighborhood). This implies that any coset of G° in G is open (covered by connected opens around each point), so G/G° is discrete. Finally, G/G° is countable since G has a countable base. ∎

Thus, any Lie group is an extension of a discrete, countable group by a connected Lie group. This essentially reduced the study of Lie groups to the study of connected Lie groups. In fact, one can reduce further to simple connected Lie groups.

Pavel then spent quite a bit of time reviewing covering spaces...

At one point Pavel made an off-hand comment about approximating continuous paths by smooth paths. He said this basically comes done to continuous functions being approximated by polynomials.

1.2.4 Coverings of Lie groups

Let G be a connected (real or complex) Lie group and $\widetilde{G} = \widetilde{G}_1$ be its universal covering, consisting of homotopy classes of paths $x : [0,1] \to G$ with $x(0) = 1$. Then $\widetilde{G}$ is a group via $(x \cdot y)(t) = x(t)y(t)$, and also a manifold.

Proposition 1.2.8.

(i) $\widetilde{G}$ *is a simply connected Lie group, and the covering* $p : \widetilde{G} \to G$ *is a homomorphism of Lie groups.*

(ii) $\ker p$ *is a central subgroup of* $\widetilde{G}$*, naturally isomorphism to* $\pi_1(G) = \pi_1(G,1)$*. Thus,* $\widetilde{G}$ *is a central extension of* G *by* $\pi_1(G)$*. In particular,* $\pi_1(G)$ *is abelian.*

Proof. **(i)** We only need to show that multiplication $\widetilde{m} : \widetilde{G} \times \widetilde{G} \to \widetilde{G}$ is regular. This is a lifting of $m \circ (p,p) : \widetilde{G} \times \widetilde{G} \to G$ which is regular, so $\widetilde{m}$ is regular too.

(ii) Homework. ∎

Remark 1.2.9. The same argument shows that more generally, the fundamental gorup of any path connected topological group is abelian. ∘

Example. $z \mapsto z^n$ from $S^1 \to S^1$ △

Example. The map $x \mapsto \exp(ix)$ from $\mathbb{R} \to S^1$ △

Example. Consider the action of SU(2) on the trace zero Hermitian 2×2 matrices by conjugation. This preserves the inner product $(A,B) = \mathrm{Tr}(AB)$ and has determinant 1, so lands in SO(3). We'll see that this is a homomorphism $\mathrm{SU}(2) \to \mathrm{SO}(3)$ which is surjective with kernel ± 1.

We will see that it's a universal covering map (as $\mathrm{SU}(2) = S^3$ is simply connected), so $\pi_1(\mathrm{SO}(3)) = \mathbb{Z}/2\mathbb{Z}$ (in fact, we see that $\mathrm{SO}(3) \cong \mathbb{RP}^3$ as manifolds). This is demonstrated by the famous *Dirac belt trick*, which illustrates the notion of a spinor; namely, spinors are vectors in $\mathbb{C}^2$ acted upon by matrices from $\mathrm{SU}(2)$. Allegedly, this helps explain some stuff in quantum physics. △

1.2.5 Lie subgroups

Definition 1.2.10. A **closed Lie subgroup** of a (real or complex) Lie group G is a subgroup which is also an embedded submanifold. ⋄

Why are these called *closed* Lie subgroups?

Lemma 1.2.11. *A closed Lie subgroup of G is closed in G.*

Proof. Homework ■

Example. $\mathrm{SL}_n(K)$ is a closed Lie subgroup of $\mathrm{GL}_n(K)$ for $K = \mathbb{R}, \mathbb{C}$. Indeed, the equation $\det A = 1$ defines a smooth hypersurface in the space of matrices (use Jacobian condition). △

Example. Let $\varphi : \mathbb{R} \to S^1 \times S^1$ be the irrational torus $\varphi(x) = (e^{ix}, e^{ix\sqrt{2}})$. This is not a closed Lie subgroup e.g. since it's image isn't closed (the image is dense though). In particular, φ is an immersion, but its inverse $\varphi^{-1} : \varphi(\mathbb{R}) \to \mathbb{R}$ is not continuous. △

1.2.6 Generation of connected Lie groups by a neighborhood of 1

Proposition 1.2.12.

(i) *If G is a connected Lie group and U a neighborhood of $1 \in G$, then U generates G as a group.*

(ii) *If $f : G \to K$ is a homomorphism of Lie groups with K connected and $\mathrm{d}f_1 : T_1G \to T_1K$ is surjective, then f is surjective.*

Proof. **(i)** Let H be the subgroup of G generated by U. Then H is open in G since $H = \bigcup_{h \in H} hU$, so H is an embedded submanifold of G. However, this makes it a closed Lie subgroup, so H is nonempty clopen in the connected space G, but this means $H = G$.

(ii) Since $\mathrm{d}f_1$ is surjective, the implicit function theorem implies that $f(G)$ contains some neighborhood of $1 \in K$, so $f(G)$ generates K. ■

1.3 Lecture 3 (9/8)

1.3.1 Homogeneous spaces

Definition 1.3.1. Let $p : Y \to X$ be a regular map of manifolds. We say it is a **fibration** (or **fiber bundle**) if for every point $x \in X$, there is a neighborhood $U \ni x$ such there exists a manifold F, called the **fiber** at x, and a diffeomorphism $h : U \times F \to p^{-1}(U)$ s.t.

$$\begin{tikzcd} U \times F \arrow[rr, "h"] \arrow[dr, "\mathrm{pr}_1"'] & & p^{-1}(U) \arrow[dl, "p"] \\ & U & \end{tikzcd}$$

commutes. ◇

Question: Is every smooth topological fibration of manifolds automatically locally trivial?

Example (Coverings)**.** For covering maps, the fiber F is 0-dimensional. △

Theorem 1.3.2.

(i) *Let G be an n-dimensional Lie group with k-dimensional closed Lie subgroup $H \subset G$. Then, the* ***homogeneous space*** *G/H has a natural structure of an $(n-k)$-dimensional manifold, and the map $G \to G/H$ is a (locally trivial) fibration with fiber H.*

(ii) *If $H \triangleleft G$ is normal, then G/H is a Lie group.*

(iii) *There is a natural isomorphism*

$$T_1(G/H) \xrightarrow{\sim} T_1G/T_1H.$$

Proof. **(i)** Fix $\overline{g} \in G/H$ and $g \in p^{-1}(\overline{g})$, so $gH \subset G$ is an embedded submanifold. Pick a small transversal submanifold $U \subset G$ (i.e. $T_gU \oplus T_g(gH) = T_gG$) with image $\overline{U} = p(U) \subset G/H$. By the inverse function theorem, UH is an open subset of G (The map $U \times H \to G$ is a linear isomorphism at $(g, g) \in U \times H$), so $\overline{U}$ is open in G/H is quotient topology as $UH = p^{-1}(\overline{U})$. The homeomorphism $p|_U : U \xrightarrow{\sim} \overline{U}$ defines a local chart around $\overline{g}$ in G/H, giving it a manifold structure. Also, $U \times H \to UH$ is a diffeomorphism, so $p : G \to G/H$ is a fibration.

(ii) This follows from the construction in **(i)**

(iii) p is regular, so induces $T_gG \to T_{\overline{g}}G/H$ which is clearly surjective (e.g. since this is a fiber bundle). The kernel contains T_gH and so by dimension reasons, is equal to T_gH. Hence, $T_{\overline{g}}(G/H) \cong T_gG/T_gH$. ∎

Corollary 1.3.3. *If $H \subset G$ is a closed Lie subgroup, then*

(i) *If H is connected, the map $\pi_0(G) \to \pi_0(G/H)$ is a bijection.*

(ii) *If also G is connected, then the map $\pi_1(G) \to \pi_1(G/H)$ is surjective and its kernel equals the image of $\pi_1(H) \to \pi_1(G)$.*

Proof. Follows from theory of coverings (exercise), using that $G \to G/H$ is a fibration. (Look at the long exact sequence of a fibration) ∎

Remark 1.3.4. $\pi_1(H) \to \pi_1(G)$ is not injective in general. Consider $G = \mathrm{SU}(2) \cong S^3$, $H = S^1 = \left\{\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix} \in \mathrm{SU}(2) : |z| = 1\right\}$. On π_1's, this gives a map

$$\pi_1(H) = \mathbb{Z} \to 1 = \pi_1(G),$$

which is not injective. ○

1.3.2 Lie subgroups

We have talked about closed Lie subgroups, but non-closed ones come up to, so let's set up some language for those.

Example. We saw already the irrational torus winding $\mathbb{R} \to S^1 \times S^1$ winding by an irrational angle. e.g. $x \mapsto (e^{ix}, e^{is\sqrt{2}})$. △

Definition 1.3.5. An **Immersed submanifold** is the image of an injective immersion. ◇

Definition 1.3.6. A **Lie subgroup** of a Lie group G is a subgroup that is also an immersed submanifold. ◇

Example. Any countable subgroup $H \subset G$ is a Lie subgroup. e.g. $\mathbb{Q} \subset \mathbb{R}$ △

Non-example. A proper, uncountable $\mathbb{Q}$-vector subspace of $\mathbb{R}$ is not a Lie subgroup. ▽

Proposition 1.3.7. *Let $f : G \to K$ be a Lie group homomorphism. Then,* $\ker f$ *is a closed, normal Lie subgroup and* $\operatorname{im} f$ *is a (not-necessarily closed) Lie subgroup. Further, there is a Lie group isomorphism* $G/\ker f \xrightarrow{\sim} \operatorname{im} f$*.*

Proof. Later. ■

1.3.3 Actions and representations of Lie groups

Let X be a manifold, G a Lie group.

Definition 1.3.8. A 9set-theoretic) left action $a : G \times X \to X$ is called **regular** if a is a regular map of manifolds. ◇

Example. $\mathrm{GL}_n \mathbb{R}$ acts on $\mathbb{R}^n$, and $\mathrm{GL}_n \mathbb{C}$ acts on $\mathbb{C}^n$. △

Example. $\mathrm{SO}(3)$ acts on S^2. △

Definition 1.3.9. A **finite dimensional representation of a Lie group** G is an action of G on a finite dimensional vector space V by linear transformations, i.e. it is a Lie group homomorphism $G \to \mathrm{GL}(V)$. A **morphism of representations** (or **intertwining operator**) is a linear map $A : V \to W$ commuting with the G-action (i.e. $A(g \cdot v) = g \cdot A(v)$). ◇

Notation 1.3.10. The category of representations of G is denoted $\mathrm{Rep}G$.

You can with representations whatever you can do with vector spaces.

Example (dual representation). Given $\pi_V : G \to \mathrm{GL}(V)$, can define $\pi_{V^*} : G \to \mathrm{GL}(V^*)$ via $\pi_{V^*}(g) = \pi_V(g^{-1})^*$. △

Example (tensor product representation).

$$\pi_{V\otimes W}(g) = \pi_V(g) \otimes \pi_W(g)$$

△

1.3.4 Orbits and Stabilizers

Say $G \curvearrowright X$. Attached to any point $x \in X$ is its **orbit** $Gx \subset X$ as well as its **stabilizer**

$$G_x = \{g \in G : gx = x\} \subset G.$$

Example. $\mathrm{SO}(2) \curvearrowright \mathbb{R}^2$ via rotations or whatever. The orbits here are circles of fixed radii, so they look kinda like orbits of planets (hence the name). △

Proposition 1.3.11 (Orbit-stabilizer for Lie group actions). *The stabilize G_x is a closed Lie subgroup of G, and the natural map*

$$G/G_x \to X, g \mapsto gx$$

is an injective immersion of manifolds, whose image is the orbit Gx.

Proof. Later ■

Corollary 1.3.12. *The orbit Gx is an immersed submanifold of X, and*

$$T_x(Gx) = T_1G/T_1G_x.$$

Moreover, if Gx is an embedded submanifold, then the map

$$G/G_x \to Gx$$

is a diffeomorphism (which respects the G-action).

Remark 1.3.13. Gx is not always closed inside X. Consider $\mathbb{R}^\times$ acting on $\mathbb{R}$ by scaling. This has two orbits, $\{0\}$ and $\mathbb{R}^\times$. One of these is not closed. ○

As a consequence of the above corollary, if G acts on X transitively, then X is the only orbit, so $X = G/H$ is a homogeneous space where $H = G_x$ for any $x \in X$. In particular, the map $G \to X, g \mapsto gx$ is a fibration with fiber Gx.

Example. SO(3) acts transitively on S^2, and $G_x = \mathrm{SO}(2) = S^1$, so

$$S^2 = \mathrm{SO}(3)/\,\mathrm{SO}(2).$$

△

Example. SU(2) acts on $S^2 = \mathbb{CP}^1 = \mathbb{C} \cup \infty$. The stabilizer of $[1:0]$ is matrices of the form (these fix the line $\mathbb{C}(1,0)$. Since they are unitary, they also fix its complement, the line $\mathbb{C}(0,1)$. Hence, they are diagonal)

$$A = \begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}$$

so $G_x = S^1$. Hence, $S^2 = \mathrm{SU}(2)/S^1$. △

This shows that both $\mathrm{SO}(3) = \mathbb{RP}^3$ and $\mathrm{SU}(2) = S^3$ fiber over S^2 with fiber S^1. The fibration

$$S^1 \hookrightarrow S^3 \twoheadrightarrow S^2$$

is called the **Hopf fibration**. It's a fact that (any two?) fibers of this fibration are linked.

Example. Let F_n be the set of flags in $\mathbb{C}^n$ where a **flag** is a chain of subspaces

$$0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = \mathbb{C}^n$$

where $\dim V_i = i$. The group $\mathrm{GL}_n \mathbb{C}$ acts on $F_n(\mathbb{C})$ and does so transitively. What is $\mathrm{Stab}(0 \subset \mathbb{C}e_1 \subset \mathbb{C}e_1 \oplus \mathbb{C}e_2 \subset \dots)$? A little thought shows that this is $B_n(\mathbb{C})$, the group of upper triangular matrices. Hence,

$$G_n = \mathrm{GL}_n / B_n$$

working over $\mathbb{C}$ or $\mathbb{R}$. $\triangle$

1.3.5 Translations and Conjugation

We have left/right actions $L_g, R_g : G \to G$ given by

$$L_g(x) = gx \text{ and } R_g(x) = xg.$$

We can combine this to form an adjoint action

$$\mathrm{Ad}_g = L_g \circ R_{g^{-1}} = R_{g^{-1}} \circ L_g : G \to G \; x \mapsto gxg^{-1}$$

given by conjugation. Note that $\mathrm{Ad}_g(1) = 1$, so we get a differential

$$\mathrm{d}_1 \, \mathrm{Ad}_g : T_1 G \to T_1 G.$$

Notation 1.3.14. We'll set $\mathfrak{g} = T_1 G$ from now on.

We'll abuse notation by letting $\mathrm{Ad}_g : \mathfrak{g} \to \mathfrak{g}$ denote the differential as well. This is a representation of G on $\mathfrak{g}$, called the **adjoint representation**.

1.3.6 Crash course on vector bundles

"This will probably be the last crash course on geometry and topology, because if you have too many crash courses, then the course can crash" (paraphrase)

Let X be a real manifold, and $p : E \to X$ a (locally trivial) fibration.

Definition 1.3.15. We say that p is a **vector bundle** if every fiber $p^{-1}(x)$ is endowed with a structure of a K-vector space, and these are compatible with the fibre bundle structure. That is, the (projection-respecting) isomorphisms

$$U \times F = U \times K^n \to p^{-1}(U)$$

are fiberwise linear. $\diamond$

Assumption. Unless otherwise stated, assume complex bundles are holomorphic.

Next time, we'll finish this crash course, talk about classical groups, and then transition to Lie algebras. Also, homeworks due on Thursday from now on. This makes Tuesday office hours more useful.

1.4 Lecture 4 (9/10)

1.4.1 Vector Bundles Continued

Last time, we looked at vector bundles, which were fiber bundles with linear structure on fibers, varying continuously along the base. You have some total space E, a base space X, a (locally trivial) projection map $E \to X$, and $p^{-1}(x)$ is a vector space. In particular, there is an open cover U_α of X such that on each U_α, the bundle trivializes, i.e. $g_\alpha : E|_{U_\alpha} \xrightarrow{\sim} U_\alpha \times K^n$ via projection-preserving diffeomorphisms inducing linear maps on the fibers.

Note that given two trivializing opens U_α, U_β, we can compare their trivializations (on their overlap). This comparison gives the **clutching function**

$$h_{\alpha\beta} : U_\alpha \cap U_\beta \to \mathrm{GL}_n(K)$$

defined so that the map[2] $g_\alpha \circ g_\beta^{-1} : U_\beta \times K^n \dashrightarrow U_\alpha \times K^n$ is given by $(x, v) \mapsto (x, h_{\alpha\beta}(x)v)$. These functions will satisfy some consistency conditions.

Remember: $h_{\alpha\beta}$ goes from U_β to U_α in this class

- $h_{\alpha\beta} \circ h_{\beta\alpha} = \mathrm{Id}$
- Given 3 opens $U_\alpha, U_\beta, U_\gamma$, on the triple intersection, we have

$$h_{\alpha\beta} h_{\beta\gamma} = h_{\alpha\gamma}.$$

Moreover, given the above data, we can construct a corresponding vector bundle. Start with

$$\bigsqcup_\alpha (U_\alpha \times K^n),$$

and then glue according to the clutching functions. Formally, we quotient this disjoint union by the identifications

$$U_\beta \times K^n \ni (x, v) \sim (x, h_{\alpha\beta}(x)v) \in U_\alpha \times K^n$$

for all α, β, all $x \in U_\alpha \cap U_\beta$, and all $v \in K^n$. The consistence conditions make this relation symmetric and transitive, so it does indeed give a valid equivalence relation. Let $E = \bigsqcup (U_\alpha \times K^n)/\sim$ be the quotient by this relation. This is our desired vector bundle.

Remark 1.4.1. This discussion applies more generally to fiber bundles by replacing GL_n via the relevant automorphism group of the fiber. ∘

Example (Trivial bundle)**.** $p : X \times K^n \to X$ via $p(x, v) = x$ is a vector bundle. △

Example (**tangent bundle**)**.** Here, the fiber above a point will be its tangent space. This will be a vector bundle

$$p : TX \longrightarrow X$$

defined using gluing data. Start with an atlas of charts for X:

$$(U_\alpha, \varphi_\alpha : U_\alpha \to K^n)\,.$$

Recall that these give us transition maps $\theta_{\alpha\beta} = \varphi_\alpha \circ \varphi_\beta^{-1} : \varphi_\beta(U_\alpha \cap U_\beta) \to \varphi_\alpha(U_\alpha \cap U_\beta)$. Recall that the tangent space at a point in K^n is canonically identified with K^n itself, so the tangent space should

[2] This is really a map from $U_\alpha \cap U_\beta \times K^n \to U_\alpha \cap U_\beta \times K^n$. I didn't write this intersection to emphasize that we start with β-coordinates and go to α-coordinates. The arrow is dashed since the map is not defined everywhere (only on the overlap).

trivialize on charts. Furthermore, the clutching function is given by the derivative of the transition maps because this tells us exactly how tangent vectors change. That is, we set

$$h_{\alpha\beta}(x) = d_{\varphi_\beta(x)}\theta_{\alpha\beta} : K^n \xrightarrow{\sim} T_{\varphi_\beta(x)}K^n \to T_{\varphi_\alpha(x)}K^n \xleftarrow{\sim} K^n$$

for $x \in U_\alpha \cap U_\beta$. By construction, $p^{-1}(x) = T_xX$, so TX formalizes the idea of T_xX "varying smoothly" in x.

Exercise. Check that this satisfies consistency conditions, and does not depend on the atlas.

△

Definition 1.4.2. For a regular map $p : E \to X$, a **section** of p is a map $s : X \to E$ such that $p \circ s = \mathrm{id}_X$. ⋄

Example. If $p : X \times F \to X$ is a trivial fiber bundle, then a section is the same thing as a map $s : X \to F$. △

Notation 1.4.3. Let $\Gamma(U, E)$ be the vector space of sections of $E \to X$ over $U \overset{\text{text}}{\subset} E$.

Exercise. Show that a rank n vector bundle $E \xrightarrow{p} X$ is trivial (globally) if and only if there exists sections $s_1, \ldots, s_n \in \Gamma(X, E)$ which form a basis in every fiber, i.e. $s_1(x), \ldots, s_n(x) \in E_x := p^{-1}(x)$ is a basis for all x. A choice of such sections is called a **frame**.

1.4.2 Vector fields

Definition 1.4.4. A **vector field** on X is a section of TX. ⋄

In local coordinates, a vector field will look like

$$\vec{v} = \sum_i v_i(\vec{x}) \frac{\partial}{\partial x_i}$$

with v_i regular functions. If there is a change of coordinates $x_i \mapsto x_i'$, since we know the transition maps are given by the derivative of change of coordinates, we see that

$$\vec{v} = \sum_i v_i' \frac{\partial}{\partial x_i'} \quad \text{where} \quad v_i' = \sum_j \frac{\partial x_i'}{\partial x_j} v_j.$$

The matrix

$$\left(\frac{\partial x_i'}{\partial x_j}\right)_{i,j}$$

is called the **Jacobi matrix**.

Thus, we see that a vector field $\vec{v}$ defines a derivation of $\mathscr{O}(U)$, regular functions on $U \subset X$ open. The above formula (+ chain rule?) shows that the derivation does not depend on the choice of local coordinates. So, from a vector field $\vec{v}$, we get a derivation $D_{\vec{v}} : \mathscr{O}(U) \to \mathscr{O}(U)$ which is compatible with restriction, i.e.

$$\begin{array}{ccc} \mathscr{O}(U) & \xrightarrow{D_{\vec{v}}} & \mathscr{O}(U) \\ \downarrow & & \downarrow \\ \mathscr{O}(V) & \xrightarrow{D_{\vec{v}}} & \mathscr{O}(V) \end{array}$$

is commutative. Hence, $D_{\vec{v}}$ also acts on germs, it gives a map $\mathscr{O}_p \to \mathscr{O}_p$.

Note 2. I need to stop using $\mathscr{O}$ and just use O like Pavel does, or I'll probably confuse myself at some point.

Conversely, a collection of derivations compatible with these restriction maps gives a vector field (exercise).

Pavel just said the word "sheaf" (!), but not said he won't use sheaves in this course. He pointed out that the above shows that $D_{\vec{v}}$ is a derivation on the sheaf $\mathscr{O}$ of regular functions on X.

Definition 1.4.5. A manifold X is called **parallelizable** if TX is trivial. ⋄

Remark 1.4.6. X is parallelizable iff there exists vector fields $\vec{v}_1, \ldots, \vec{v}_n$ which form a basis in every fiber (i.e. iff there is a **frame**). ∘

Example. S^1 is parallelizable as is $S^1 \times S^1$ as is every Lie group. Fix an isomorphism $T_1 G \simeq K^n$ and then translate it to every point. △

Non-example. The sphere S^2 is not parallelizable. There are no nonvanishing vector fields on S^2 (**Hairy ball theorem** or **Hedgehog theorem**). ▽

1.4.3 Tensor fields and Differential Forms

Slogan. You can do with vector bundles whatever you can do with vector spaces.

Example. Given $E \to X$, get a dual bundle $E^* \to X$ by dualizing all fibers and all clutching functions. △

Example. Given vector bundles $E, F \to X$ get a tensor product $E \otimes F \to X$. △

Definition 1.4.7. The **tensor bundle of rank** (k, m) on a manifold X is

$$TX^{\otimes k} \otimes T^*X^{\otimes m}.$$

The bundle T^*X is also called the **cotangent bundle**. A **tensor field of rank** (k, m) is a section of $TX^{\otimes k} \otimes T^*X^{\otimes m}$. ⋄

Example. A vector field is a tensor field of rank $(1, 0)$. △

Definition 1.4.8. A **differential** m**-form** on X is a skew-symmetric tensor field of rank $(0, m)$, i.e. a section of $\bigwedge^m T^*M \subset T^*M^{\otimes m}$. ⋄

Example. A general 1-form (section of T^*X) locally looks like

$$\omega = \sum a_i \left(\frac{\partial}{\partial x_i}\right)^* = \sum a_i \mathrm{d}x_i$$

where $\mathrm{d}x_i$ is the dual basis element to $\partial/\partial x_i$, and $a_i = a_i(\vec{x})$ is a regular function. If you have a change of coordinates $x_i \to x_i'$, then

$$\omega = \sum_i a_i' \mathrm{d}x_i' \text{ where } a_i' = \sum_j \frac{\partial x_j}{\partial x_i'} a_j,$$

so the clutching function is the inverse Jacobi matrix. △

Example. For any $f \in \mathscr{O}(U)$, can define $\mathrm{d}f$, a 1-form on U, which locally looks like

$$\mathrm{d}f = \sum_i \frac{\partial f}{\partial x_i}\mathrm{d}x_i.$$

More generally, a general m-form will locally look like

$$\omega = \sum_{1 \le i_1 < i_2 < \cdots < i_m \le n} a_{i_1,\ldots,i_m}(\vec{x})\mathrm{d}x_{i_1} \wedge \cdots \wedge \mathrm{d}x_{i_m}.$$

△

1.4.4 Back to Lie groups

Left and right invariant tensor fields Let G be a Lie group, and say its acting on some manifold X. Then, G also acts on the tangent bundle TX as well as on all tensor bundles.

Definition 1.4.9. A tensor field T on G is **Left invariant** if $L_gT = T$ for all $g \in G$. It is **right invariant** if $R_gT = T$ for all $g \in G$. ⋄

Proposition 1.4.10. *For any $\tau\mathfrak{g}^{\otimes k} \otimes (\mathfrak{g}^*)^{\otimes m}$, there exists a unique left invariant tensor field τ_ℓ on G such that $\tau_\ell(1) = \tau$. Similarly, there exists a unique right invariant tensor field τ_r on G such that $\tau_r(1) = \tau$.*

Proof Idea. Translate. Set $\tau_\ell(g) = R_g\tau$ and $\tau_r(g) = L_g\tau$ or something like that. ■

Internet went out for a few minutes, so was temporaily kicked out of Zoom

Proposition 1.4.11 (Exercise)**.** *τ_ℓ is right invariant iff τ_r is left invariant iff $\tau \in \mathfrak{g}^{\otimes k} \otimes (\mathfrak{g}^*)^{\otimes m}$ is invariant under Ad_g.*

Corollary 1.4.12. *A Lie group is parallelizable, $TG \cong G \times \mathfrak{g}$.*

Proof. If $e_1, \ldots, e_n$ is a basis of $\mathfrak{g}$, then $L_ge_1, \ldots, L_ge_n$ is a frame. Also, $R_ge, \ldots, R_ge_n$ is a frame. ■

Example. S^1 and $S^3 \cong \mathrm{SU}(2)$ are parallelizable. △

Example. S^{2n} is not parallelizable, so cannot be a Lie group. △

Theorem 1.4.13. *S^n is parallelizable ($n \ge 1$) iff $n = 1, 3$ or 7.*

Corollary 1.4.14. *S^n is a not a Lie group if $n \notin \{0, 1, 3, 7\}$.*

There are other ways to arrive at the above corollary. The theorem preceding it is overkill.

Is S^7 a Lie group? No. We'll probably see this later. It is however, a "Lie group up to homotopy" (an H-space).

Remark 1.4.15. S^0 is a Lie group since it's unit real numbers, S^1 is a Lie group since its unit complex numbers, and S^3 is a Lie group since it's unit quaternions.

S^7 is the unit octonions, but the octonions are not associative, so S^7 is not a Lie group, merely an H-space. ○

1.4.5 Classical groups

These are Lie groups coming from Linear algebra.

Example.

$\mathrm{GL}_n(K)$ – **general linear group**

$\mathrm{SL}_n(K)$ – **special linear group**

$O_n(K)$ – **orthogonal group**. Matrices preserving quadratic form $x_1^2 + \cdots + x_n^2$ or bilinear form $x_1y_1 + \cdots + x_ny_n$.

$\mathrm{Sp}_{2n}(K)$ – **symplectic group**. Matrices preserving non-degenerate skew-form on K^{2n}, e.g. $x_1 \wedge x_{n+1} + \cdots + x_n \wedge x_{2n}$

$O(p, q)$ – **Pseudo-orthogonal group**. Matrices preserving the bilinear form of signature (p, q), e.g. $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$.

$U(p, q)$ – **Pseudo-unitary group**. Matrices preserving Hermitian form $|x_1|^2 + \cdots + |x_p|^2 - |x_{p+1}|^2 - \cdots - |x_n|^2$. In particular $U(n, 0) = U_n$ is the **unitary group**.

Get "special groups" by taking the determinant one subgroups.

$$\mathrm{SO}(p, q) \subset O(p, q), \quad \mathrm{SU}(p, q) \subset U(p, q), \quad \ldots$$

These are most classical groups. △

Proposition 1.4.16. *All the above are Lie groups.*

We will show this next time. We will use exp / log of matrices to show some neighborhood of the identity of these groups is homeomorphic to an open in Euclidean space. We stated earlier that every closed subgroup of GL_n is a Lie group, but did not prove this. This is harder to prove, so we'll do the exponential thing instead.

1.5 Lecture 5 (9/15)

Last time ended with classical groups, essentially Lie groups of matrices. See last time's notes or the text book for a list of these. I'm not retyping them all.

1.5.1 Classical groups, continued

We'll show today that these are Lie groups. Our main tool will be the matrix exponential. Let $\mathfrak{gl}_n(K)$ be the K-vector space of all $n \times n$ matrices. There is a map $\exp : \mathfrak{gl}_n(K) \to \mathrm{GL}_n(K)$ given by

$$\exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!}$$

and satisfying much of what you expect. For example, $\exp(-a) \cdot \exp(a) = 1$, so it does indeed land in invertible matrices. This map is a diffeomorphism in a small neighborhood of the identity with inverse

$$\log A = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(A - 1)^n}{n}.$$

While $\exp a$ converges for all matrices $a \in \mathfrak{gl}_n(K)$, $\log A$ defined above only converges when the spectral radius of A is < 1 (i.e. when all eigenvalues of A have absolute value < 1).

Proposition 1.5.1. *Here are some properties of* $\exp, \log$.

(1) *These are mutually inverse (when both defined)*

(2) *They are both conjugation invariant*

(3) $\mathrm{d}\exp_0 = \mathrm{id} : T_0\mathfrak{gl}_n(K) \to T_1 \mathrm{GL}_n(K)$ *so also* $\mathrm{d}\log_1 = \mathrm{id}$

(4) *If* $XY = YX$ *(and* X, Y *close to* 1*), then*

$$\log(XY) = \log X + \log Y.$$

(5) *If* $x \in \mathfrak{gl}_n(K)$*, then the map* $t \mapsto \exp(tx)$ *is a morphism of Lie groups* $K \to \mathrm{GL}_n(K)$ *(i.e.* $\exp(sx + tx) = \exp(sx)\exp(tx)$*).*

(6) $\det \exp(a) = \exp \operatorname{tr} a$ *and* $\log \det A = \operatorname{tr} \log A$.

We will use these properties to show that the classical groups are Lie groups. Well, the log map provides coordinate charts for these groups, as we will see.

Example ($\mathrm{SL}_n(K)$ is a Lie group)**.** We have a log map $\log : \mathrm{SL}_n(K) \to \mathfrak{sl}_n(K)$ defined in a neighborhood of the identity, where $\mathfrak{sl}_n(K) = \{a \in \mathfrak{gl}_n(K) : \operatorname{tr} a = 0\}$, i.e. "traceless matrices." This map is a bijection near the identity, so we get a local chart near identity. By translating this chart around, we get a manifold structure, and

$$\dim \mathrm{SL}_n(K) = \dim \mathfrak{sl}_n(K) = n^2 - 1.$$

△

Example ($O_n(K)$ is a Lie group)**.** Recall $O_n(K)$ is matrices A with $A^T = A^{-1}$. This translates to giving $(\log A)^T = -\log A$, so $\log A$ is skew-symmetric. Thus we have our logarithm map

$$\log : O_n(K) \to \mathfrak{o}_n(K)$$

defined near 1, and giving a bijection near 1 ($\mathfrak{o}_n(K)$ is **skew-symmetric matrices** $a^T = -a$). Thus, $O_n(K)$ is a Lie group with (a skew-symmetric matrix is determined by upper triangular part)

$$\dim O_n(K) = \dim \mathfrak{o}_n(K) = \frac{n(n-1)}{2}.$$

△

Example ($U(n)$ is a Lie group)**.** Recall $U(n)$ is (complex) matrices A with $\overline{A}^T = A^{-1}$. Hence, $\overline{\log A}^T = -\log A$, so $\log A$ is skey-Hermitian. Thus, we have our logarithm map

$$\log : U(n) \to \mathfrak{u}(n)$$

defined near 1, and giving a bijection near 1 ($\mathfrak{u}(n)$ is **skew-Hermitian** matrices $\overline{a}^T = -a$). Thus, $U(n)$ is a *real* Lie group with (a skew-Hermitian matrix is purely imaginary on the diagonal and every other entry determined by upper triangular part)

$$\dim U(n) = \dim \mathfrak{u}(n) = n + 2\frac{n(n-1)}{2} + n = n^2.$$

△

One can do the same thing for any other classical group. This gives

Proposition 1.5.2. *Classical groups are Lie groups. Moreover,* $\mathfrak{g} = T_1 G \subset \mathfrak{gl}_n(K)$. *More-moreover, if* $\mathfrak{u} \subset \mathfrak{gl}_n(K)$ *is a small enough neighborhood of* 0 *and* $U = \exp(\mathfrak{u})$, *then* $\exp$ *and* $\log$ *define mutually inverse diffeomorphisms* $\mathfrak{u} \cap \mathfrak{g} \xrightarrow{\sim} U \cap G$.

1.5.2 Quaternions

Definition 1.5.3. The algebra of **quaternions** has basis $1, i, j, k$ over $\mathbb{R}$ with multiplication determined by

$$i^2 = j^2 = k^2 = -1, \;\; ij = k = -ji, \;\; jk = i = -kj, \;\text{ and }\; ki = j = -ik.$$

◇

A general quaternion looks like $q = a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$, and we its **conjugate quaternion** to be $\overline{q} = a - bi - cj - dk$. One can check that

$$q\overline{q} = a^2 + b^2 + c^2 + d^2 = |q|^2 \in \mathbb{R}.$$

One can also check that the ring of quaternions is associative even if it is not commutative.

Notation 1.5.4. We use $\mathbb{H}$ to denote the quaternions.

Remark 1.5.5. $\mathbb{H}$ is a division algebra ("noncommutative field"). If $q \neq 0$, then it is invertible with inverse $q^{-1} = \overline{q}/|q|^2$. ○

Remark 1.5.6. The only division algebras over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$ and $\mathbb{H}$. ○

Since $\mathbb{H}$ is a division algebra, we can do linear algebra over it (turns out commutativity is not that important). In particular, every (left or right) module over $\mathbb{H}$ is free, and so has a basis. We call such a module a left/right **quaternionic vector space**. Any (right) quaternionic f.d. vector space is isomorphic to $\mathbb{H}^n$ for a unique n. Furthermore, $\mathbb{H}$ linear maps $\mathbb{H}^n \to \mathbb{H}^m$ are given by quaternionic matrices of size $m \times n$.

Remark 1.5.7. In a left vector space, matrices multiply on the right. In a right vector space, matrices multiply on the left. ○

Much of linear algebra carries over to these matrices. Gaussian elimination works the same way as over fields (e.g. an invertible square matrix is always a product of elementary matrices).

Proposition 1.5.8. $\overline{q_1 q_2} = \overline{q}_2 \overline{q}_1$.

Corollary 1.5.9. $|q_1 q_2| = |q_1|\,|q_2|$

Note that $\mathbb{C} \subset \mathbb{H}$ as the space of $\langle 1, i \rangle$, so $\mathbb{H}$ is a 2-dim complex vector space (using either left or right multiplication, giving 2 slightly different structures), but $\mathbb{H}$ is not a $\mathbb{C}$-algebra since $\mathbb{C}$ is not central. One can show that $Z(\mathbb{H}) = \mathbb{R}$.

Remark 1.5.10. To make a right $\mathbb{H}$-vector space V a $\mathbb{C}$-vector space, use right multiplication by $\mathbb{C}$. ◦

Proposition 1.5.11. *The group of unit quaternions* $\{q \in \mathbb{H} \mid |q| = 1\}$ *is isomorphic to* $\mathrm{SU}(2)$.

Proof. Realize $\mathbb{H}$ as a 2-dim $\mathbb{C}$ vector space (say $\mathbb{C}$ multiplying on the right) with basis $1, j$. Thus, a general quaternion can be written $q = z_1 + jz_2$ with $z_1, z_2 \in \mathbb{C}$. Hence, left multiplication by quaternions gives a $\mathbb{C}$-linear map $\mathbb{H} \to \mathbb{H}$, and so corresponds to some 2×2 matrix. In particular $q = z_1 + jz_2$ will correspond to the matrix

$$\begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix}.$$

This map identifies the unit quaternions with $\mathrm{SU}(2)$, the set

$$\left\{ \begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix} \middle| z_1, z_2 \in \mathbb{C}, |z_1|^2 + |z_2|^2 = 1 \right\}$$

■

Gives another way to see that $\mathrm{SU}(2) \cong S^3$.

Corollary 1.5.12. *The map*

$$q \longmapsto \left(\frac{q}{|q|}, |q| \right)$$

is an isomorphism of Lie groups $\mathbb{H}^\times \xrightarrow{\sim} \mathrm{SU}(2) \times \mathbb{R}_{>0}$.

This is an analogue of the trigonometric/polar form of a complex number $z = re^{i\theta}$. Here, we have phases in $S^3 = \mathrm{SU}(2)$ instead of in S^1.

We can use quaternions to construct even more classical groups.

Example. $\mathrm{GL}_n(\mathbb{H})$, invertible $n \times n$ matrices over $\mathbb{H}$, is an open set in $M_n(\mathbb{H})$ so is a real Lie group of dimension $4n^2$. △

We would like to define $\mathrm{SL}_n(\mathbb{H})$, but since $\mathbb{H}$ is non-commutative, we do not have a determinant map $\mathrm{GL}_n(\mathbb{H}) \to \mathrm{GL}_1(\mathbb{H}) = \mathbb{H}^\times$. However, $\mathbb{H}$ is a $\mathbb{C}$-vector space, so we can think of elements of $\mathrm{GL}_n(\mathbb{H})$ as acting a complex vector space, and so consider the map

$$\mathrm{GL}_n(\mathbb{H}) \hookrightarrow \mathrm{GL}_{2n}(\mathbb{C}) \xrightarrow{\det} \mathrm{GL}_1 \mathbb{C}.$$

Proposition 1.5.13. *For* $A \in M_n(\mathbb{H})$, $\det A \geq 0$ *(and* $> 0 \iff A$ *invertible) with above definition.*

Proof. Suffices to show that if A is invertible, then $\det A > 0$. We first do the case $n = 1$. For $q = z_1 + jz_2$, we have

$$\det q = \det \begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix} = |z_1|^2 + |z_2|^2 \geq 0.$$

For general n, use Gaussian elimination to reduce to case of elementary matrices. These are either diagonal with all but one entry equal to 1 (the determinant is then $|q|^2$ where q is the only entry not equal to one) or the identity matrix except with a single zero replace with q (the determinant is then 1 since the matrix is triangular with every diagonal entry equal to 1). ■

We define $\mathrm{SL}_n(\mathbb{H}) = \{A \in \mathrm{GL}_n(\mathbb{H}) : \det A = 1\}$.

Exercise. $\mathrm{GL}_n(\mathbb{H}) \cong \mathrm{SL}_n(\mathbb{H}) \times \mathbb{R}_{>0}$. Just write

$$A = \widehat{A} \cdot \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

with $\lambda = \sqrt[n]{\det A}$.

1.5.3 Groups preserving sesquilinear forms

Definition 1.5.14. Let V be a right quaternionic vector space. A **sesquilinear form** on V is a bi-additive function $(-,-) : V \times V \to \mathbb{H}$ such that

$$(\vec{x}\alpha, \vec{y}\beta) = \overline{\alpha}(\vec{x}, \vec{y})\beta$$

for $\vec{x}, \vec{y} \in V$ and $\alpha, \beta \in \mathbb{H}$. Note that the order of factors here is important. We call such a form **Hermitian** if moreover

$$(x, y) = \overline{(y, x)}$$

and is **skew-Hermitian** if

$$(x, y) = -\overline{(y, x)}.$$

◇

Remark 1.5.15. Over $\mathbb{C}$, Hermitian and skew-Hermitian are "equivalent" in that a Hermitian form multiplied by i gives a skew-Hermitian form and vice versa. ○

Proposition 1.5.16.

(1) *Every nondegenerate Hermitian form on $\mathbb{H}^n$ is isomorphic to*

$$(x, y) = \overline{x}_1 y_1 + \cdots + \overline{x}_p y_p - \overline{x}_{p+1} y_{p+1} - \cdots - \overline{x}_n y_n.$$

We say that it is a ***form of signature*** (p, q) *where $q = n - p$. The signature of a form is well-defined.*

(2) *Every nondegenerate skew-Hermitian form is isomorphic to*

$$(x, y) = \overline{x}_1 j y_n + \cdots + \overline{x}_n j y_n.$$

Proof. Exercise ■

Exercise. Show that a Hermitian form of signature (p, q) has the form

$$(x, y) = B_1(x, y) + jB_2(x, y)$$

where $B_1, B_2 : V \times V \to \mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ are complex forms with B_1 the usual nondegenerate Hermitian form of signature $(2p, 2q)$, and B_2 is a nondegenerate skew-symmetric form.

Exercise. A quaternionic nondegenerate skew-Hermitian form has the form

$$(x, y) = B_1(x, y) + jB_2(x, y)$$

where B_1 is a usual skew-Hermitian form and B_2 is a symmetric bilinear form. Furthermore, iB_1 is a Hermitian form of signature (n, n).

1.5.4 New classical groups

Example. Group of symmetric of a nondegenerate quaternionic Hermitian form of signature (p, q). By the exercises, this is the group

Remember: $\mathrm{Sp}_{2n}(\mathbb{C})$ preserves a skew-symmetric form on $\mathbb{C}^{2n}$

$$U(2p, 2q) \cap \mathrm{Sp}_{2n}(\mathbb{C}) =: \mathrm{Sp}(2p, 2q) = U(2p, 2q, \mathbb{H}),$$

the **quaternionic unitary group**. △

Example. Group of symmetries of a nondegenerate skew-Hermitian form. By the exercises, this is the group

$$U(n, n) \cap O_{2n}(\mathbb{C}) =: O^*(2n),$$

the **quaternionic orthogonal group**. △

Both of the previous examples give real Lie groups (use exponential map). One can also define $\mathrm{SO}^*(2n) \subset O^*(2n)$, an index 2 subgroup.

1.6 Lecture 6 (9/17)

1.6.1 Exponential map

The exponential map on matrices was useful for constructing local charts of matrix groups near the origin. Today, we will generalize this construction to any Lie group. Lie groups are better than general manifolds since the origin (and so any point) has a canonical local chart given by the exponential map we will construct.

Proposition 1.6.1. *Let G be a real Lie group with $\mathfrak{g} = T_1G$. Fix any $x \in \mathfrak{g}$. Then, there is a unique morphism of Lie groups $\gamma_x : \mathbb{R} \to G$ such that $\gamma'(0) = x$. The image of Γ_x is called the* ***1-parameter subgroup*** *defined by $x \neq 0$.*

Proof. Let $\gamma = \gamma_x$, so $\gamma(t)\gamma(s) = \gamma(t + s)$. Differentiating by s at $s = 0$, we see

$$(L_{\gamma(t)}x =)\gamma(t)x = \gamma(t)\gamma'(0) = \gamma'(t).$$

We also have the initial condition $\gamma(0) = 1$. By the existence and uniqueness theorem for solutions of ODEs (in $\mathbb{R}^n$), this ODE has a unique local/short-time solution $\gamma : (-\varepsilon, \varepsilon) \to G$ for some $\varepsilon > 0$. Note that if $|s| + |t| < \varepsilon$, then

$$\gamma_1(t) = \gamma(t+s) \text{ and } \gamma_2(t) = \gamma(s)\gamma(t)$$

both satisfy above ODE with initial condition $\gamma_1(0) = \gamma(s) = \gamma_2(0)$. Thus, $\gamma_1 = \gamma_2$ by uniqueness of solutions. Thus, $\gamma(t+s) = \gamma(s)\gamma(t)$ when $|s| + |t| < \varepsilon$. We now want to extend this to all of $\mathbb{R}$.

We will inductively show that γ extends to a path on $|t| < 2^n\varepsilon$ for all n, by induction on n. The base $(n = 0)$ is clear, so assume we have an extension to $|t| < 2^{n-1}\varepsilon$. For t with $|t| < 2^n\varepsilon$, set $\gamma(t) = \gamma\left(\frac{t}{2}\right)^2$. This agrees with the earlier definition of $\gamma(t)$ when $|t| < 2^{n-1}\varepsilon$. It also satisfies the desired differential equation as (use desired ODE holds for $t/2$ and the homomorphism property shows $\gamma(t/2)$ commutes with $\gamma(0) = x$)

$$\begin{aligned}
\gamma'(t) &= \frac{1}{2}\gamma'\left(\frac{t}{2}\right)\gamma\left(\frac{t}{2}\right) + \frac{1}{2}\gamma\left(\frac{t}{2}\right)\gamma'\left(\frac{t}{2}\right) \\
&= \frac{1}{2}\gamma\left(\frac{t}{2}\right)x\gamma\left(\frac{t}{2}\right) + \frac{1}{2}\gamma\left(\frac{t}{2}\right)^2 x \\
&= \gamma\left(\frac{t}{2}\right)^2 x \\
&= \gamma(t)x
\end{aligned}$$

Now, uniqueness of ODE again shows $\gamma(t+s) = \gamma(s)\gamma(t)$ when both sides defined. Thus, we win. ■

Definition 1.6.2. The **exponential map** $\exp : \mathfrak{g} \to G$ is defined by the formula $\exp(x) = \gamma_x(1)$. ◇

Remark 1.6.3. By definition, the 1-parameter subgroup associated to x is $\gamma_x(t) = \exp(tx)$. ○

In then follows that:

Proposition 1.6.4. *The flow defined by the right invariant vector field L_x (obtained by left translations of x) is given by $g \mapsto \exp(tx)g$, and the flow defined by R_x is given by $g \mapsto g\exp(tx)$.*

This is because

$$\left.\frac{\partial}{\partial t}\right|_{t=0} \exp(tx)g = xg = R_g(x) = L_x(g).$$

Example. Take $G = (K^n, +)$. Then, $\exp(x) = x$. The ODE is $\gamma'(t) = x$ so $\gamma(t) = tx$. △

Example. Take $G = \mathrm{GL}_n(K)$. Then, $\exp(x) = e^x$. The ODE here is

$$\gamma'(t) = \gamma(t)x = x\gamma(t)$$

where multiplication is not matrix multiplication. The initial condition is $\gamma(0) = 1$, so the solution is $\gamma_x(t) = e^{tx} = \sum_{n\geq 0} \frac{t^n x^n}{n!}$. △

Theorem 1.6.5.

(1) *$\exp : \mathfrak{g} \to G$ is a regular map, and a diffeomorphism from a neighborhood of $0 \in \mathfrak{g}$ to a neighborhood of $1 \in G$. In fact, the derivative $\mathrm{d}\exp_0 : \mathfrak{g} \to \mathfrak{g}$ is the identity map (in other symbols, $\exp'(0) = \mathrm{Id}$)*

(2) $\exp((s+t)x) = \exp(sx)\exp(tx)$.

(3) *If $\varphi : G \to K$ is a Lie group morphism, then*

$$\varphi(\exp(x)) = \exp(\varphi_*(x))$$

*where $\varphi_* = \mathrm{d}\varphi_1 : T_1G \to T_1K$, i.e. "*exp *commutes with morphisms."*

(4) *If $g \in G$ and $x \in \mathfrak{g}$, then*

$$g\exp(x)g^{-1} = \exp(\mathrm{Ad}_g\, x).$$

Proof. **(1)** We start with regularity. Solutions of ODEs depend regularly on their parameters if the ODE itself depends regularly on them. Also, $\gamma_0(t) = 1$ for all t, so $\exp(0) = 1$. Finally,

$$\exp'(0)x = \frac{\partial}{\partial t}|_{t=0}\exp(tx) = x \implies \exp'(0) = \mathrm{Id}\,.$$

(2) This is true since $\exp(tx) = \gamma_x(t)$.

(3) Both $\varphi(\exp(tx))$ and $\exp(\varphi_*(tx))$ satisfy the same ODE

$$\gamma'(t) = \gamma(t)\varphi_*(x),$$

and agree at $t = 0$, so we win.

(4) This is a special case of 3 since $a \mapsto gag^{-1}$ is a homomorphism $G \to G$. ■

Remark 1.6.6. If G is a complex Lie group, then **(1)** says that $\exp : \mathfrak{g} \to G$ is complex analytic (holomorphic). ○

Property **(1)** shows that $\exp : \mathfrak{g} \to G$ has an inverse $\log : U \to \mathfrak{g}$ defined on some neighborhood $U \subset G$ of the identity. It satisfies $\log(1) = 0$, and is called the **logarithm map**. When $G = \mathrm{GL}_n(K)$ (or one of its Lie subgroups), exp / log are exactly what you expect. This means that log defines a canonical chart near 1 on G.

Proposition 1.6.7. *Let G be a connected Lie group, and $\varphi : G \to K$ a morphism. Then, φ is completely determined by its differential $\varphi_* : T_1G \to T_1K$.*

Proof. For $x \in \mathfrak{g}$, we have $\varphi(\exp(x)) = \exp(\varphi_*(x))$ is determined by φ_*, so it suffices to show that $\operatorname{im}\exp$ generates G as a group. Well, its image contains an open neighborhood of 1 which necessarily generates G since G is connected, so we win. ■

1.6.2 Commutator

In general (for example for matrices), $\exp(x+y) \neq \exp(x)\exp(y)$. Let's measure the failure of this.

Let G be a Lie group. Consider the map $\mu : U \times U \to \mathfrak{g}$ given by

$$(x, y) \longmapsto \log(\exp(x)\exp(y))$$

where $U \subset \mathfrak{g}$ is some sufficiently small neighborhood of 0. If we had $\exp(x+y) = \exp(x)\exp(y)$, then the above would just be $x + y$. Hence, deviation of this map from $x + y$ measures failure of this identity (which will hold when G is abelian). Expand μ in a Taylor series:

$$\mu(x,y) = x + y + \frac{1}{2}\mu_2(x,y) + \dots \text{ where } \mu_2 = d^2\mu(0,0), \dots \text{ are higher order terms}$$

This is writing down the multiplication map of G in a canonical chart around the identity. We know $\mu_2(x,0) = 0 = \mu_2(0,y)$ so the quadratic terms give a bilinear map $\mu_2 : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ (it has no x^2 term or y^2 term, only xy and yx). Furthermore, we know that $\mu_2(x,-x) = 0$ since $\mu(x,-x) = \log(\exp(x)\exp(-x)) = 0$. This implies that μ_2 is skew-symmetric. This map is called the **commutator**.

Definition 1.6.8. We denote $[x,y] := \mu_2(x,y)$ with $x,y \in \mathfrak{g}$. $\diamond$

Thus, we have

$$\exp(x)\exp(y) = \exp(\mu(x,y)) = \exp\left(x + y + \frac{1}{2}[x,y] + \dots\right).$$

Example. Let $G = \mathrm{GL}_n(K)$. Then,

$$\exp(x)\exp(y) = \left(1 + x + x^2/x + \dots\right)\left(1 + y + y^2/2 + \dots\right) = 1 + (x+y) + \frac{1}{2}(x^2 + y^2 + 2xy) + \dots$$

Note that G is not commutative, so $(x+y)^2 = x^2 + y^2 + xy + yx$ is not $x^2 + 2xy + y^2$. We have

$$\exp(x)\exp(y) = 1 + (x+y) + \frac{(x+y)^2}{2} + \frac{xy - yx}{2} + \dots = \exp\left(x + y + \frac{xy - yx}{2} + \dots\right).$$

Thus,

$$[x,y] = xy - yx$$

in this case. $\triangle$

Corollary 1.6.9. *If $G \subset \mathrm{GL}_n(K)$ is a (not-necessarily closed) Lie subgroup, then $\mathfrak{g} \subset \mathfrak{gl}_n(K)$ is closed under $[x,y] = xy - yx$, and it coincides with the commutator of G.*

For $x \in \mathfrak{g}$, define a linear map $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}$ given by $\mathrm{ad}_x(y) = [x,y]$.

Proposition 1.6.10.

(1) *If G, K are Lie groups and $\varphi : G \to K$ a morphism, then $\varphi_* : T_1G \to T_1K$ preserves the commutator, i.e.*

$$\varphi_*([x,y]) = [\varphi_*(x), \varphi_*(y)].$$

(2) *The adjoint action preserves the commutator*

(3)

$$\exp(x)\exp(y)\exp(x)^{-1}\exp(y)^{-1} = \exp([x,y] + \dots)$$

(4) *If $X(t), Y(s)$ are parameterized curves in G such that $X(0) = 1 = Y(0)$ and $X'(0) = x$ and $Y'(0) = y$, then*

$$[x,y] = \lim_{s,t\to 0} \frac{\log(X(t)Y(s)X(t)^{-1}Y(s)^{-1})}{ts}.$$

In particular,

$$[x, y] = \lim_{s,t\to 0} \frac{\log(\exp(tx)\exp(sy)\exp(-tx)\exp(-sy))}{ts}.$$

Also,

$$[x, y] = \frac{\partial}{\partial t}\bigg|_{t=0} \operatorname{Ad}_{X(t)} y$$

and hence $\operatorname{ad} = \operatorname{Ad}_*$*, differential of* $\operatorname{Ad} : G \to \operatorname{GL}(\mathfrak{g})$ *at* 1.

(5) *If G is commutative, then $[x, y] = 0$ always.*

Proof. **(1)** Follows from φ commuting with exp.

(2) This is a special case of **(1)** with $\varphi = \operatorname{Ad}_g$.

(3) Recall that $\log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x, y] + \ldots$ and similarly $\log(\exp(y)\exp(x)) = x + y - \frac{1}{2}[x, y] + \ldots$. Thus,

$$\log(\exp(x)\exp(y)) = \log(\exp(y)\exp(x)) + [x, y] + \ldots.$$

Exponentiating, (In this case, exp of sum equals product of exp up to higher order terms)

$$\exp(x)\exp(y) = \exp([x, y] + \ldots)\exp(y)\exp(x).$$

Multiply on right by $\exp(x)^{-1}\exp(y)^{-1}$ to get the desired result.

(4) Let $x(t) = \log X(t)$ and $y(s) = \log Y(s)$, so $x'(0) = x$ and $y'(0) = y$. Then,

$$\log\left(X(t)Y(s)X(t)^{-1}Y(s)^{-1}\right) = \log\left(\exp(x(t))\exp(y(s))\exp(-x(t))\exp(-y(s))\right) = [x(t), y(s)] + \cdots = ts[x, y] + \ldots$$

which implies the statement. The point is $x(0) = 0$ and $x'(0) = x$ imply $x(t)$ looks like $tx + \ldots$ and similarly for $y(s)$. The last statement is obtained by letting $s \to 0$ in the second statement.

(5) This follows from 3 since $[x, y]$ is the leading term in the expansion of $\log\{\exp(x)\exp(y)\exp(x)^{-1}\exp(y)^{-1}\} = \log 1 = 0$. ∎

Next time we'll prove the Jacobi identity, and then finally define Lie algebras.

Remark 1.6.11. One can explicitly calculate these higher order terms, and they turn out to be commutators of commutators. e.g.

$$\log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x, y] + \frac{1}{12}[x, [x, y]] + \frac{1}{12}[y, [y, x]] + \ldots$$

or something like that. ○

Homework deadline moved to Monday, but also there is a new homework due on Thursday. Most, but not all, of the material for the new homework has been covered.

1.7 Lecture 7 (9/22)

* Missed first 15 minutes because of Zoom Shenanigans*

I think he's in the middle of proving the Jacobi identity

$$[x, [y, z]] + [[x, y], z] + [y, [x, z]] = 0$$

for Lie groups.

See section 6.2 of the notes

Proposition 1.7.1. *The Jacobi identity holds for any Lie group G.*

Proof. Let $\mathfrak{g} = T_1 G$, and recall that we have shown that

$$\mathrm{ad}x = \frac{\partial}{\partial t}\bigg|_{t=0} \mathrm{Ad}_{\exp(tx)} .$$

Furthermore, the Jacobi identity is equivalent to $\mathrm{ad}x$ being a derivation of the commutator:

$$\mathrm{ad}x([y,z]) = [\mathrm{ad}x(y), z] + [y, \mathrm{ad}x(z)].$$

To show this, let $g(t) = \exp(tx)$, so

$$\mathrm{Ad}_{g(t)}([y,z]) = [\mathrm{Ad}_{g(t)}\, y, \mathrm{Ad}_{g(t)}\, z].$$

Hence, the desired equality is obtained by differentiating this with respect to t (use the Liebniz rule) at $t = 0$. ■

Corollary 1.7.2. $\mathrm{ad}[x,y] = [\mathrm{ad}x, \mathrm{ad}y]$

Proof. This is equivalent to Jacobi ad $[\mathrm{ad}x, \mathrm{ad}y]\mathrm{ad}x\mathrm{ad}y - \mathrm{ad}y\mathrm{ad}x$ so applying both sides to z, we see this corollary says

$$[[x,y],z] = [x,[y,z]] - [y,[x,z]].$$

■

Proposition 1.7.3. *If $x \in \mathfrak{g}$, then* $\exp(\mathrm{ad}x) = \mathrm{Ad}_{\exp(x)} \in \mathrm{GL}(\mathfrak{g})$.

Proof. We'll show that

$$\gamma_1(t) := \exp(t \cdot \mathrm{ad}x) = \mathrm{Ad}_{\exp(tx)} =: \gamma_2(t)$$

by showing that these both satisfy the same ODE with initial conditions:

$$\gamma'(t) = \gamma(t) \cdot \mathrm{ad}x \;\text{ and }\; \gamma(0) = 1.$$

Hence, we get the prop by setting $t = 1$. ■

1.7.1 Lie algebras

Definition 1.7.4. A **Lie algebra** over any field k (not just $\mathbb{R}$ or $\mathbb{C}$) is a k-vector space $\mathfrak{g}$ equipped with a bilinear map $[-,-] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$, called **commutator** or **Lie bracket**, such that

- $[x,x] = 0$
- **Jacobi identity**

$$[[x,y],z] + [[y,z],x] + [[z,x],y] = 0.$$

If char $k \neq 2$, then the first condition is equivalent to $[x, y] = -[y, x]$ always. However, when char $k = 2$, $[x, x] = 0 \implies [x, y] = -[y, x]$ but the converse implication does not hold. $\diamond$

Example. Any subspace of $\mathfrak{gl}_n(K)$ closed under $[x, y] = xy - yx$ is a Lie algebra. $\triangle$

Example. If G is a Lie group, then $\mathfrak{g} = T_1 E$ is a Lie algebra and is called the **Lie algebra of the Lie group** G and sometimes denoted Lie G. $\triangle$

Definition 1.7.5. A **morphism of Lie algebras** is a linear map $\varphi : \mathfrak{g}_1 \to \mathfrak{g}_2$ such that $\varphi([x, y]) = [\varphi(x), \varphi(y)]$. $\diamond$

Example. The adjoint map ad : $\mathfrak{g} \to \mathrm{End}(\mathfrak{g})$ is a morphism of Lie algebras by one of the earlier corollaries. $\triangle$

Theorem 1.7.6. *If G is a K-Lie group, then $\mathfrak{g} = T_1 G$ is a Lie algebra over K, and moreover, for any Lie group morphism $\varphi : G \to H$, its differential at the identity $\varphi_* : \mathrm{Lie}\, G \to \mathrm{Lie}\, H$ is a morphism of Lie algebras. Thus, we have a map*

$$\mathrm{Hom}(G, K) \to \mathrm{Hom}(\mathrm{Lie}\, G, \mathrm{Lie}\, H)$$

which is injective when G is connected.

Remark 1.7.7. This map above is actually a functor from Lie groups to Lie algebras, and we're saying its restriction to the (full) subcategory of connected Lie groups is faithful. $\circ$

1.7.2 Lie subalgebras and ideals

Definition 1.7.8. A **Lie subalgebra** of a Lie algebra $\mathfrak{g}$ is a subspace $\mathfrak{h} \subset \mathfrak{g}$ which is closed under $[-, -]$. It is called a **Lie ideal** if moreover, $[\mathfrak{g}, \mathfrak{h}] \subset \mathfrak{h}$. $\diamond$

Proposition 1.7.9. *Let $H \subset G$ be a Lie subgroup. Then,*

(1) Lie $H \subset$ Lie G *is a Lie subalgebra.*

(2) If $H \triangleleft G$ is normal, then Lie H *is a Lie ideal in* Lie G

(3) If G, H are connected and Lie $H \subset$ Lie G *is a Lie ideal, then $H \subset G$ is a normal subgroup.*

Proof. **(1)** Let $\mathfrak{h} = \mathrm{Lie}\, H$ and $x, y \in \mathfrak{h}$ so $\exp(tx) \in H$ and $\exp(sy) \in H$. We've shown previously that

$$[x, y] = \lim_{t,s \to 0} \frac{\log(\exp(tx)\exp(sy)\exp(-tx)\exp(-sy))}{ts}.$$

This is in $\mathfrak{h}$ for every value of s, t so the limit is in there as well.

Remember: $\mathfrak{h} \subset \mathfrak{g}$ is closed always, even when $H \subset G$ isn't

(2) Suppose $H \triangleleft G$ is normal. Then, for any $g \in G$ and $h \in H$, we have $ghg^{-1} \in H$ by definition. Take $h = \exp(sy)$ for some $y \in \mathfrak{h}$. Then, $g \exp(sy) g^{-1} \in H$. Take derivative at $s = 0$:

$$\left.\frac{\partial}{\partial s}\right|_{s=0} (blah) = \mathrm{Ad}_g(y) \in \mathfrak{h}.$$

Taking $g = \exp(tx)$ for some $x \in \mathfrak{g}$, we get

$$\mathrm{Ad}_{\exp(yx)}(y) \in \mathfrak{h}.$$

Now take derivative at $t = 0$:

$$\frac{\partial}{\partial t}\bigg|_{t=0} (blah) = \underbrace{\mathrm{ad}x(y)}_{[x,y]} \in \mathfrak{h}.$$

(3) Suppose $\mathfrak{h} \subset \mathfrak{g}$ is a Lie ideal and that H, G are connected. Take $x \in \mathfrak{g}$ and $y \in \mathfrak{h}$. We will calculate

$$\exp(x)\exp(y)\exp(x)^{-1} = \mathrm{Ad}_{\exp(x)}\exp(y) = \exp\left(\mathrm{Ad}_{\exp(x)}\, y\right) = \exp(\exp(\mathrm{ad}x)y) = \exp\left(\sum_{n\geq 0}\frac{(\mathrm{ad}x)^n}{n!}y\right),$$

but the value being exponentiated is in $\mathfrak{h}$ since $\mathfrak{h}$ is a Lie ideal. Thus, $\exp(x)\exp(y)\exp(x)^{-1} \in H$. By connectedness of H, every element $h \in H$ is a product of those of the form $\exp(y)$, so

$$\exp(x)h\exp(x)^{-1} \in H \text{ for all } h \in H.$$

Since also G is connected, every element of g is a product of those of the form $\exp(x)$, so indeed $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. ■

Example (In response to closedness of H vs $\mathfrak{H}$ confusion)**.** Consider $G = S^1 \times S^1$ and $H \subset G$ an irrational torus winding, e.g. image of $\exp\left(t \cdot (1, \sqrt{2})\right)$. Then, $H \cong \mathbb{R} \subset S^1 \times S^1$ is a Lie subgroup. At the Lie algebra level, though, we just have some line in $\mathbb{R}^2$, so the Lie algebra doesn't easily see the difference between H and a copy of S^1 given by a rational slope line. △

Note 3. We will see later techniques for getting more information of our Lie groups out of our Lie algebras, but right now at least, figuring out when a map gives a closed embedding just from the Lie algebras seems hard.

Exercise. The Lie bracket on the Lie algebra of $G = (S^1)^n$ is trivial, so any subspace is a Lie subalgebra. Figure out when a subspace $\mathfrak{h} \subset \mathfrak{g}$ corresponds to a closed Lie subgroup.

Recall 1.7.10. A **vector field** on a manifold X is a compatible collection of derivations $v : \mathscr{O}(U) \to \mathscr{O}(U)$ for all open $U \subset X$. ⊙

Proposition 1.7.11. *If v, w are derivations of an algebra A, then $[v, w] = vw - wv$ is also a derivation of A (even though vw and wv separately are not).*

Proof. Exercise. ■

As a result, the space $\mathrm{Vect}(X)$ of vector fields on X is a Lie algebra under the operation $[v, w] = vw - wv$. This is called the **Lie bracket of vector fields** (it is usually infinite dimensional). What does this look like in local coordinates? If

$$v = \sum v_i \frac{\partial}{\partial x_i} \text{ and } w = \sum w_j \frac{\partial}{\partial x_j},$$

then

This kind of reminds me of Green's formula or whatever it's called from

$$[v,w] = vw - wv = \sum_i \left(\sum_j \left(v_j \frac{\partial w_i}{\partial x_j} - w_j \frac{\partial v_i}{\partial x_j} \right) \right) \frac{\partial}{\partial x_i}.$$

Remark 1.7.12. Say $U \subset \mathbb{R}^n$ open, $v, w \in \mathrm{Vect}(U)$ and $g_t, h_t : U \to \mathbb{R}^n$ smooth 1-parameter families of maps, defined for $t \in (-\varepsilon, \varepsilon)$, such that $g_0(x) = h_0(x) = x$. Also write

$$\left.\frac{\partial}{\partial t}\right|_{t=0} g_t(x) = v(x) \text{ and } \left.\frac{\partial}{\partial t}\right|_{t=0} h_t(x) = w(x).$$

Then (exercise), for any $x \in U$

$$[v,w](x) = \lim_{t,s\to 0} \frac{g_t h_s g_{-t} h_{-s}(x) - x}{ts}.$$

$\circ$

1.7.3 Back to Lie groups

Let G be a Lie group, and let $\mathrm{Vect}_L(G)$ be the space of left invariant vector fields. Similarly, let $\mathrm{Vect}_R(G)$ be right invariant vector fields. These are both Lie subalgebras of $\mathrm{Vect}(G)$.

We have constructed these before. Recall that for $x \in \mathfrak{g} = \mathrm{Lie}\, G$ we can get $R_x \in \mathrm{Vect}_L(G)$ and $L_x \in \mathrm{Vect}_R(G)$. The maps $x \mapsto L_x$ and $x \mapsto R_x$ are linear isomorphisms from $\mathfrak{g}$ to $\mathrm{Vect}_R(G)$ and $\mathrm{Vect}_L(G)$.

Proposition 1.7.13. *The maps $x \to -L_x$ and $x \mapsto R_x$ are isomorphisms of Lie algebras.*

Proof. We have $[R_x, R_y] = R_z$ for $x, y \in \mathfrak{g}$ and $z = [R_x, R_y](1) \in \mathfrak{g}$. We need to show $z = [x,y]$. Consider some $f \in \mathscr{O}(U)$ with U a neighborhood of 1 in G. Then,

$$\begin{aligned}
z(f) &= (R_x R_y f)(1) - (R_y R_x f)(1) \\
&= x\left((R_y f) - y(R_x f)\right) \\
&= x\left(\left.\frac{\partial}{\partial s}\right|_{s=0} f\left(g \exp(sy)\right) \right) - y\left(\left.\frac{\partial}{\partial t}\right|_{t=0} f\left(g\exp(tx)\right) \right) \\
&= \left.\frac{\partial}{\partial t}\right|_{t=0} \left.\frac{\partial}{\partial s}\right|_{s=0} f(\exp(tx)\exp(sy)) - \left.\frac{\partial}{\partial s}\right|_{s=0} \left.\frac{\partial}{\partial t}\right|_{t=0} f(\exp(sy)\exp(tx)) \\
&= \left.\frac{\partial^2}{\partial s \partial t}\right|_{t=s=0} \left(f(\exp(tx)\exp(sy)) - f(\exp(sy)\exp(tx)) \right).
\end{aligned}$$

Define $F(u) = f(\exp(u))$ for $u \in \mathfrak{g}$. Then, the above equals

$$\left.\frac{\partial^2}{\partial s \partial t}\right|_{t=s=0} \left(F(tx + sy + \frac{1}{2} ts[x,y] + \dots) - F(tx + sy - \frac{1}{2} ts[x,y] + \dots) \right) = [x,y](f).$$

When you expand this out, the linear terms cancel, but the quadratic terms don't; this is where the last equality comes from. Thus, $z = [x,y]$ so we win in the case of R_x. The case of L_x is similar. ∎

We can now prove some results that we claimed earlier but did not prove. Let G be a Lie group with $\mathfrak{g} = \mathrm{Lie}\, G$, and let X be a manifold with an action $a : G \times X \to X$ of G. For all $z \in \mathfrak{g}$ we have the vector field $a_*(z)$ on X given by

$$(a_*(z)f)(x) = \frac{\partial}{\partial t}\bigg|_{t=0} f(\exp(-tz)\cdot x).$$

(the minus is coming from the fact that G acts on the left, so it multiplies inside the function with an inverse) where $t \in \mathbb{R}$, $f \in \mathscr{O}(U)$, $U \subset X$ open, and $x \in U$.

Proposition 1.7.14. *a_* above is a linear map $\mathfrak{g} \to \mathrm{Vect}(X)$ and in fact a Lie algebra morphism, i.e.*

$$[a_*(z), a_*(w)] = a_*([z,w]).$$

Proof. Exercise. ■

Definition 1.7.15. An **action of a Lie algebra** $\mathfrak{g}$ on a manifold X is a Lie algebra morphism $\mathfrak{g} \to \mathrm{Vect}(X)$. ◇

Proposition 1.7.16. *An action of G on X gives rise to an action of $\mathfrak{g} = \mathrm{Lie}\, G$ on X.*

Question 1.7.17 (Audience)**.** *Do people also study the space of vector fields which are invariant on both the left and the right? Is this space usually non-trivial even if G is not commutative?*

Answer. Yes, and we actually talked about this when discussing tensor fields. One can talk about two sided invariant vector fields. Left invariants one are isomorphic to $\mathfrak{g}$, so two sided invariant ones are isomorphic to a subspace of $\mathfrak{g}$. In fact, they are $\mathfrak{g}^{\mathrm{Ad}(G)}$, vectors fixed by the adjoint action. For connected groups, this is the center of $\mathfrak{g}$. We'll talk more about this next time. ⋆

1.8 Lecture 8 (9/24)

Last time Given a Lie group G, manifold X, and action $a: G \times X \to X$, there is an action of the Lie algebra $\mathfrak{g} = \mathrm{Lie}\, G$ on X by vector fields, i.e. we have a homomorphism $a_*: \mathfrak{g} \to \mathrm{Vect}(X)$. In particular, for every $x \in X$, we have $a_{*x}: \mathfrak{g} \to T_xX$ given by $a_{*x}(z) = a_*(z)(x)$.

1.8.1 Orbit-Stabilizer Stuff We Didn't Prove Earlier

Theorem 1.8.1.

(1) The stabilizer G_x of x in G is a closed Lie subgroup of G with Lie algebra $\mathfrak{g}_x = \ker a_{*x}$

(2) The map $G/G_x \to X, g \mapsto gx$ is an immersion, so G_x is an immersed submanifold of X, and $T_x(Gx) \cong \mathrm{Im}(a_{*,x}) \subset T_xX$. Also, $\mathrm{Im}(a_{*,x}) \cong \mathfrak{g}/\mathfrak{g}_x$.

Proof. **(1)** It is clear that $G_x \subset G$ is closed, so it is a closed subgroup. We need to show that it is a Lie subgroup and compute its Lie algebra. Suffices to show that there exists a neighborhood $U \ni 1 \in G$ such that $U \cap G_x$ is a closed submanifold of U with $T_1(U \cap G_x) = \mathfrak{g}_x$. Note that $\mathfrak{g}_x \subset \mathfrak{g}$ is a Lie subalgebra since $[a_*(y), a_*(z)] = a_*([y,z])$ and since if v, w are vector fields vanishing at $x \in X$, then also $[v,w](x) = 0$. Furthermore, given $z \in \mathfrak{g}_x$, we claim that $\exp(tz) \in G_x$ for all $t \in \mathbb{R}$. Indeed, $\gamma(t) := \exp(tz)\cdot x \in G$ satisfies the differential equation

$$\gamma'(t) = a_{*,\gamma(t)}(z)$$

with initial condition $\gamma(0) = x$. At the same time, $\gamma_1(t) = x$ also satisfies this equation since $a_{*x}(z) = 0$. By uniqueness of solutions to ODEs, we get

$$\exp(tz) \cdot x = \gamma(t) = \gamma_1(t) = x$$

for all $t \in \mathbb{R}$. Thus, $\mathfrak{g}_x \subset \exp^{-1}(G_x)$. We want equality.

Choose a linear complement $\mathfrak{u}$ of $\mathfrak{g}_x$ in $\mathfrak{g}$, so $\mathfrak{g} = \mathfrak{u} \oplus \mathfrak{g}_x$ (and $\mathfrak{u} \cap \ker a_{*x} = 0$). The map $\mathfrak{u} \to G$, $u \mapsto \exp(u)x$ is injective for small u. This means that $\exp(u) \in G_x \iff u = 0$. On a small neighborhood U of $1 \in G$, any $g \in G$ can be written as $g = \exp(u)\exp(z)$ with $u \in \mathfrak{u}$ and $z \in \mathfrak{g}_x$ (comes from implicit function theorem). If $g \in G_x$ (so $gx = x$), we must have $u = 0$ (since $\exp(z)x = x$). Thus, $U \cap G_x = U \cap \exp(\mathfrak{g}_x)$ and so this gives our local chart near the identity. This proves **(1)**.

(2) We need to show $G/G_x \to X$ injective on tangent spaces, but $T_1(G/G_x) = \mathfrak{g}/\mathfrak{g}_x = \mathfrak{u}$ which does indeed map injectively into T_xX. ■

Corollary 1.8.2. *If $\varphi : G \to K$ is a morphism of Lie groups, and $\varphi_* : \operatorname{Lie} G \to \operatorname{Lie} K$ is the corresponding morphism of Lie algebras, then $H = \ker \varphi$ is a normal, closed Lie subgroup of G with Lie algebra $\mathfrak{h} = \ker \varphi_*$, and the induced map*

$$\overline{\varphi} : G/H \to K$$

is an immersion. Moreover, if $\overline{\varphi}(G/H) \subset K$ is a submanifold, then it is a closed Lie subgroup, and we have an isomorphism of Lie groups $G/H \cong \overline{\varphi}(G/H)$.

Proof. Apply theorem to $X = K$ with action $g \cdot x = \varphi(g)x$. ■

Corollary 1.8.3. *If V is a finite dimensional representation of G and $v \in V$, then G_v is a closed Lie subgroup of G with Lie algebra $\mathfrak{g}_v = \{z \in \mathfrak{g} : zv = 0\}$*

Proof. In this case, $a_* : \mathfrak{g} \to \operatorname{Vect}(V)$ is given by $a_{*v}(z) = zv$. ■

Example. Say A is a finite-dimensional (possibly non-associative) algebra, so it is a vector space with a "multiplication" map $\mu : A \otimes A \to A$. We get a group

$$G = \operatorname{Aut}(A) \subset \operatorname{GL}(A)$$

of automorphisms of A. Note that $\operatorname{GL}(A)$ acts on $V = \operatorname{Hom}_k(A \otimes A, A)$ (the space of multiplication maps), and $G = \operatorname{GL}(A)_\mu$, so G is a closed Lie subgroup with Lie algebra $\operatorname{Lie} G = \operatorname{Der} A \subset \operatorname{End}_K(A)$ where

$$\operatorname{Der} A = \{d \in \operatorname{End}_K(A) : d(ab) = d(a)b + ad(b) \text{ for all } a, b \in A\}$$

(above, $ab := \mu(a, b)$). △

1.8.2 Center of G and $\mathfrak{g}$

Definition 1.8.4. We let $Z(G)$ denote the **center** of G. This is

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}.$$

We also define the **Lie algebra center** of $\mathfrak{g}$ to be

$$\mathfrak{z} = \mathfrak{z}(\mathfrak{g}) = \{x \in \mathfrak{g} : [x, y] = 0 \text{ for all } y \in \mathfrak{g}\}.$$

$\diamond$

Proposition 1.8.5. *If G is connected, then Z is a closed Lie subgroup of G, and* $\operatorname{Lie} Z = \mathfrak{z}$.

Proof. Since G is connected, it is generated by the image of the exponential map, so

$$z \in Z \iff z \exp(u) = \exp(u) z$$

for all $u \in \mathfrak{g}$. This means $z \exp(-tu) z^{-1} \exp(tu) = 1$ which is the case iff $\operatorname{Ad}_z(u) = u$, so $Z = \ker \operatorname{Ad}$. Therefore, $Z \subset G$ is a closed Lie subgroup. Its Lie algebra is $\operatorname{Lie} Z = \ker(\operatorname{Ad}_*) = \ker \operatorname{ad} = \mathfrak{z}$ since $\operatorname{ad} x(y) = [x, y]$. ■

Example. Let $G = \mathrm{SL}_2(\mathbb{C})$. Then, $Z = \mathbb{Z}/2\mathbb{Z}$, so the center is not always connected, even when G is. In this case, $\mathfrak{z} = 0$ (which is good since Z is finite). △

Remark 1.8.6. If G is not connected, then Z is still a Lie subgroup, but now

$$\operatorname{Lie} Z = \mathfrak{z}^{G/G^\circ}$$

is the elements of the center of the Lie algebra fixed by the action of the components of G. ○

Definition 1.8.7. The quotient G/Z is also a Lie group, called the **adjoint group of** G. It is isomorphic to the image of $\operatorname{Ad} : G \to \mathrm{GL}(\mathfrak{g})$. $\diamond$

Example. The adjoint group of $\mathrm{SL}_2(\mathbb{C})$ is $\mathrm{SL}_2(\mathbb{C})/\pm 1 = \mathrm{PGL}_2(\mathbb{C})$. △

1.8.3 Fundamental Theorems of Lie Theory

Theorem 1.8.8. *For a Lie group G, there is a bijection between connected Lie subgroups $H \subset G$ and Lie subalgebras $\mathfrak{h} \subset \mathfrak{g} = \operatorname{Lie} G$ such that $\mathfrak{h} = \operatorname{Lie} H$.*

Theorem 1.8.9. *If G, K are Lie groups with G simply connected (in particular, G is connected), then the map*

$$\operatorname{Hom}(G, K) \to \operatorname{Hom}(\operatorname{Lie} G, \operatorname{Lie} K), \varphi \mapsto \varphi_*$$

is bijective.

Theorem 1.8.10. *Every finite dimensional Lie algebra is the Lie algebra of a Lie group (and therefore of a simply connected Lie group).*

We will not prove this last theorem this term, but will try to next term.

Corollary 1.8.11. *For $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, the assignment $G \to \operatorname{Lie} G$ gives an equivalence between the categories of simply connected K-Lie groups and K-Lie algebras.*

Remark 1.8.12. For more generality, one can study p-adic analytic Lie groups, algebraic groups, or formal groups. These are all related and have certain advantages/disadvantages compared to real and complex Lie groups. ○

1.8.4 Complexification and real forms

Given a real Lie algebra $\mathfrak{g}$, its **complexification** is $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C} = \mathfrak{g} \oplus i\mathfrak{g}$ which is now a complex Lie algebra.

Example. Take $\mathfrak{g}_1 = \mathfrak{u}(n)$ (skew-Hermitian $n \times n$ matrices) and $\mathfrak{g}_2 = \mathfrak{gl}_n(\mathbb{R})$. Then, $(\mathfrak{g}_1)_{\mathbb{C}} \cong (\mathfrak{g}_2)_{\mathbb{C}} = \mathfrak{gl}_n(\mathbb{C})$. I was distracted, but Pavel wrote something like $A = B + iC$ and $B = \frac{1}{2}(A + A^t)$ and $C = \frac{1}{2i}(A - A^t)$.

However, $\mathfrak{g}_1 \not\cong \mathfrak{g}_2$ as $\mathfrak{g}_2$ has nonzero elements x for which $\mathrm{ad} x$ is nilpotent, but $\mathfrak{g}_1$ does not. Indeed, any $A \in \mathfrak{g}_1$ is diagonalizable and so $\mathrm{ad} A$ is itself diagonal ($\mathrm{ad} A \cdot E_{ij} = (\lambda_i \lambda_j) E_{ij}$). △

Definition 1.8.13. We say that $\mathfrak{g}$ is a **real form** of $\mathfrak{g}_{\mathbb{C}}$. ◇

Can we do something similar for Lie groups?

Let $G \supset K$ be Lie groups such that G is complex and K is real. Assume that $\mathrm{Lie}\, G = \mathrm{Lie}\, E \otimes_{\mathbb{R}} \mathbb{C}$ and that G is connected. Then we say that K is a **real form** of G.

Example. $G = \mathrm{GL}_n(\mathbb{C})$. Then, $K_1 = \mathrm{GL}_n(\mathbb{R})$ and $K_2 = U(n)$ are real forms. Note that K_1 is not connected. $K_1^\circ = \mathrm{GL}_n(\mathbb{R})_+$ is another real form. △

What about complexification? This is tricky, but there's a sorta cheating solution using the third main theorem. Suppose K is a simply connected real Lie group. We can define its **complexification** to be the simply-connected complex Lie group associated to $\mathrm{Lie}\, K \otimes_{\mathbb{R}} \mathbb{C}$. Using the second theorem of Lie, we get a map $K \to G$, but it does not have to be injective; it's kernel will be a discrete central subgroup.

Example. Take $\overline{K} = \mathrm{SL}_2(\mathbb{R}) \cong D^2 \times S^1$ with maps to $\mathrm{SL}_2(\mathbb{C})$. The universal cover of $\overline{K}$ is $K = \widetilde{\mathrm{SL}_2}(\mathbb{R}) \cong D^2 \times \mathbb{R}$. The map $K \to \mathrm{SL}_2(\mathbb{C})$ has kernel $\mathbb{Z}$. △

1.8.5 Campbell-Baker-Hausdorff Formula

We had this map $\mu(x, y) = \log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x, y] + \dots$. We can write

$$\mu(x, y) = \sum_{n \geq 1} \frac{1}{n!} \mu_n(x, y)$$

with $\mu_1(x, y) = x + y$ and $\mu_2(x, y) = [x, y]$. One might wonder if we get any higher structure from μ_n with $n \geq 3$. We shouldn't expect so since the main theorems say that the Lie algebra structure already determines basically everything. Indeed,

Theorem 1.8.14. *All μ_n are $\mathbb{Q}$-Lie polynomials in x, y, independent of G (universal).*

Example. $\mu_3(x, y) = \frac{1}{2}\left([x, [x, y]] + [y, [y, x]]\right)$. △

1.9 Lecture 9 (9/29)

Last time we gave some fundamental theorems of Lie theory. Their proofs are based on the Frobenius theorem about distributions in differential geometry, so we should probably start by going over what this is.

1.9.1 Distributions

Let X be an n-dimensional manifold, and fix some $0 \leq k \leq n$.

Definition 1.9.1. A **k-dimensional distribution** on X is a rank k subbundle of TX, often denoted by D.

So in every tangent space T_xX, we get a k-dimensional subspace $D_x \subset T_xX$ which varies regularly with x. In other words, we have a neighborhood $X \supset U \ni x$ s.t. on U, D is spanned by k vector fields $v_1, \ldots, v_k$, i.e. for every $y \in U$, $D_y = \operatorname{span}\{v_1(y), \ldots, v_k(y)\}$. ⋄

Definition 1.9.2. A distribution D is **integrable** if every $x \in X$ has a neighborhood $U \subset X$ and local coordinates $x_1, \ldots, x_n$ on U such that D is defined by the equations

Question: Should this technically be $\frac{\partial}{\partial x_{k+i}} = 0$ instead?

$$\mathrm{d}x_{k+1} = \mathrm{d}x_{k+2} = \cdots = \mathrm{d}x_n = 0.$$

(i.e. we have joint level surfaces defined by $x_{k+1} = c_1, \ldots, x_n = c_{n-k}$ and the space D_y are the tangent spaces at y to this surface).

This is the case iff D_y is spanned at every $y \in U$ by $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_k}$. ⋄

Claim 1.9.3. *D is integrable $\iff$ every $x \in X$ is contained in an integral submanifold $S_x \subset X$ of dimension k such that for every $y \in S_x$, $T_yS_x = D_y$.*

To prove this, one typically chooses

$$S_x = \left\{ y \in X \mid \exists \gamma : [0,1] \to X, \gamma(0) = x, \gamma(1) = y, \gamma'(t) \in D_{\gamma(t)} \, \forall t \in [0,1] \right\}.$$

Note that the above is an equivalence class.

it is like the "integral component of x" or something

Remark 1.9.4. The usual concatenation of paths is not smooth, but you can reparameterize to make it smooth. ○

Remark 1.9.5. Note that S_x is an embedded submanifold. Given small $U \ni x$, $S \cap U$ splits into sheets/-connected components where each one is a level set. (Something like this). For this reason, an integrable distribution is also called a **foliation**, and the embedded submanifolds S_x are called **sheets**, so X is a disjoint union of sheets. ○

Example. When $k = 1$, a(n integrable) distribution D is a **direction field**. For every point, we get a line in the tangent bundle. By existence and uniqueness of ODEs, all 1-dimensional distributions are integrable. In this case, integrable submanifolds are called integral curves and are graphs of solutions to differential equation associated to the distribution. △

Example (Torus winding)**.** $X = S^1 \times S^1 = \mathbb{R}^2/\mathbb{Z}^2$. Consider the direction field given by parallel lines of slope $s \in \mathbb{R}$. If $s \in \mathbb{Q}$, then integral curves will be closed (and also closed subsets), so homeomorphic to S^1. If $s \notin \mathbb{Q}$, then we get an irrational torus winding, so integral curves are immersed submanifolds which are diffeomorphic to $\mathbb{R}$ (so not closed curves and not closed subsets). △

For $k \geq 2$, D is not always integrable. One has the following necessary condition: if v, w are two vector fields contained in D, then $[v, w]$ is also contained in D. This is because being contained in D is the same as being tangent to its sheets; if v, w are tangent to some submanifold $Y \subset X$, then so is $[v, w]$.[3]

Non-example (2-dim non-integrable distribution in $\mathbb{R}^3$)**.** Take $\vec{v} = \partial_x$ and $\vec{w} = x\partial_y + \partial_z$. These are linearly independent at every point, so they span a 2-dimensional distribution D. Note that

$$[\vec{v}, \vec{w}] = \partial_y \notin D_{x,y,z}$$

at any point $(x, y, z) \in \mathbb{R}^3$. Thus, D is not integrable. ▽

Theorem 1.9.6 (**Frobenius' Theorem**)**.** *A distribution D is integrable iff for all vector fields v, w contained in D, the commutator $[v, w]$ is also contained in D.*

Proof. Only need $\Longleftarrow$ direction. We argue by induction in $k = \operatorname{rank} D$. The base case $k = 0$ is trivial. Assume the claim for $k - 1$. The question is local, so we may assume $X = \mathbb{R}^n$. Suppose $v_1, \ldots, v_k \in \operatorname{Vect}(\mathbb{R}^n)$ is a basis of D. By local existence/uniqueness for ODE, $\exists U$ with local coordinates $x_1, \ldots, x_{n-1}, x_n = z$ s.t. $v_k = \partial_z$ ("we rectify this v_k"). We now write

$$v_i = \sum_j a_{ij}(\vec{x}, z)\frac{\partial}{\partial x_j} + d_i(\vec{x}, z)\frac{\partial}{\partial z}$$

for $i < k$ (here, $\vec{x} = (x_1, \ldots, x_{n-1})$. We only need these vector fields to can our distribution, so we can safely replace v_i by $v_i - d_i v_k$, so

$$v_i = \sum_{j=1}^{n-1} a_{ij}(\vec{x}, z)\frac{\partial}{\partial x_j},$$

i.e.

$$\begin{pmatrix} v_1 \\ \vdots \\ v_{k-1} \end{pmatrix} = A(\vec{x}, z) \begin{pmatrix} \frac{\partial}{\partial x_1} \\ \vdots \\ \frac{\partial}{\partial x_{n-1}} \end{pmatrix}$$

where $A = (a_{ij})$ is a $(k-1) \times (n-1)$ matrix. Then,

$$[v_k, v_i] = \left[\frac{\partial}{\partial z}, v_i\right] = \frac{\partial A}{\partial z} \begin{pmatrix} \frac{\partial}{\partial x_1} \\ \vdots \\ \frac{\partial}{\partial x_{n-1}} \end{pmatrix}.$$

On the other hand, by the assumption,

$$[v_k, v_i] = \sum_{m=1}^{n-1} b_{im}(\vec{x}, z) v_m = B(\vec{x}, z) \begin{pmatrix} v_1 \\ \vdots \\ v_{n-1} \end{pmatrix} = BA \begin{pmatrix} \frac{\partial}{\partial x_1} \\ \vdots \\ \frac{\partial}{\partial x_{n-1}} \end{pmatrix}.$$

[3]Indeed, locally Y is defined by $x_{k+1} = \cdots = x_n = 0$ so being tangent to Y means that $v = \sum_i a_i \frac{\partial}{\partial x_i}$ and $a_i = 0$ for $i > k$ when $x_{k+1} = \cdots = x + n = 0$. Recall that

$$[v, w] = \sum a_i \left(\frac{\partial}{\partial b_j} x_j - b_i \frac{\partial a_j}{\partial x_j}\right) \frac{\partial}{\partial x_i}$$

which also satisfies this condition.

This gives the differential equation

$$\frac{\partial A}{\partial z} = BA$$

with initial condition $A(\vec{x}, 0) = I_{k-1}$. This has a fundamental solution $A_0(\vec{x}, z)$, so $A = A_0 C$ where $C = C(x_1, \ldots, x_{n-1})$ is independent of z (and is a $(k-1) \times (n-1)$ matrix). If we set

$$w_i = \sum_{j=1}^{n-1} c_{ij}(\vec{x}) \frac{\partial}{\partial x_j},$$

then $\frac{\partial}{\partial z}, w_1, \ldots, w_{k-1}$ also span D but now these vector fields $w_1, \ldots, w_{k-1}$ have no dependence on z at all. Thus, there exists some neighborhood $U = (-\varepsilon, \varepsilon) \times U'$ so that $D = \mathbb{R} \times D'$ with k' a $(k-1)$-dimensional distribution on U'. This D' satisfies the necessary condition, so D' is integrable by the induction hypothesis. The product of two integrable distributions is integrable, so we win. ■

1.9.2 Application to fundamental theorems

Recall the first fundamental theorem.

Theorem 1.9.7. *Let G be a Lie group with Lie algebra $\mathfrak{g} = \operatorname{Lie} G$, and let $\mathfrak{h} \subset \mathfrak{g}$ be a Lie subalgebra. Then, there exists a unique connected Lie subgroup $H \subset G$ such that $\operatorname{Lie} H = \mathfrak{h}$.*

Proof. Uniqueness follows from the fact that the map $\operatorname{Hom}(H, G) \to \operatorname{Hom}(\mathfrak{h}, \mathfrak{g})$ is injective (since H connected).

Question: Why?

For existence, we will use the Frobenius theorem. We will define a $k := \dim \mathfrak{h}$-dimensional distribution on G by taking $\mathfrak{h} \subset T_1 G$ and spreading it around G by left translation. Hence, D is spanned by vector fields $L_{a_1}, \ldots, L_{a_k}$ where $a_1, \ldots, a_k$ is a basis of $\mathfrak{h}$. We want to show that D is integrable. Well,

$$[L_{a_i}, L_{a_j}] = \sum_k c_{ij}^k L_{a_k} \quad \text{where} \quad [a_i, a_j] = \sum_k c_{ij}^k a_k.$$

This implies that the commutator of any two vector fields tangent to this distribution will be tangent to this distribution, so Frobenius theorem now says that D is integrable.[4] Let H be the sheet of D going through $1 \in G$, an embedded submanifold with $T_1 H = \mathfrak{h}$. It remains to show that H is a subgroup of G. We claim that

$$H = \{\exp(b_1) \cdots \exp(b_m) \mid b_1, \ldots, b_m \in \mathfrak{h}\}$$

(exercise). ■

The second fundamental theorem was.

Theorem 1.9.8. *If G is simply connected, then the map $\operatorname{Hom}(G, K) \to \operatorname{Hom}(\operatorname{Lie} G, \operatorname{Lie} K)$ is bijective.*

Proof. We know this map is injective, so we only need surjectivity. Fix some $\psi : \operatorname{Lie} G \to \operatorname{Lie} K$. Consider $\theta = (\mathrm{id}, \psi) : \operatorname{Lie} G \to \operatorname{Lie}(G \times K) = \operatorname{Lie} G \oplus \operatorname{Lie} K$. This is the inclusion of a Lie subalgebra, so the previous fundamental theorem gives a connected Lie subgroup $H \subset G \times K$ such that $\operatorname{Lie} H = \operatorname{im} \theta$.

Remember: Graphs let you turn questions of maps into questions of spaces

[4] In general,

$$\left[\sum f_i L_{a_i}, \sum g_j L_{a_j}\right] = \sum f_i L_{a_i}(g_j) L_{a_j} - g_j L_{a_j}(f_i) L_{a_i} + f_i g_j [L_{a_i}, L_{a_j}]$$

We have projections $p_1 : H \to G$ and $p_2 : H \to K$. Note that $(p_1)_* = \mathrm{Id}$ so p_1 is a covering map, but G is simply connected, so p_1 is an isomorphism. Thus, $\varphi = p_2 \circ p_1^{-1} : G \to K$ has $\varphi_* = \psi$. ■

There was also a third fundamental theorem.

Theorem 1.9.9. *Every finite dimensional Lie algebra $\mathfrak{g}$ is the Lie algebra of a Lie group G.*

This one is harder, and so we won't give a complete proof. However, we remark that its deducible from a purely algebraic theorem.

Theorem 1.9.10 (Ado's theorem). *Any finite dimensional Lie algebra $\mathfrak{g}$ is isomorphic to a Lie subalgebra of $\mathfrak{gl}_n(K)$. This is true for any field K (even in positive characteristic).*

This is nontrivial. Note that we have seen homomorphisms $\mathfrak{g} \to \mathfrak{gl}_n(K)$, such as the adjoint representation, but the adjoint representation is usually not injective. Given Ado's theorem though, the third fundamental theorem follows from the second (and even shows that any finite dimensional Lie algebra is the Lie algebra of a connected Lie subgroup of $\mathrm{GL}_n(K)$).

Corollary 1.9.11 (of Ado's theorem)**.** *Any simply connected Lie group is a universal covering of a* ***linear Lie group****, i.e. a Lie subgroup of* $\mathrm{GL}_n(K)$.

1.10 Lecture 10 (10/1): Representations of Lie groups and Lie algebras

We've defined representations of Lie groups before. One can also represent Lie algebras.

Definition 1.10.1. A **representation of a Lie algebra** $\mathfrak{g}$ is a vector space V with a Lie algebra homomorphism $\rho : \mathfrak{g} \to \mathrm{End}(V)$, i.e.

$$\rho([x, y]) = [\rho(x), \rho(y)] = \rho(x)\rho(y) - \rho(y)\rho(x).$$

A **morphism of representations** (or **intertwining operator**) $A : V \to W$ is a linear map such that $A\rho_V(x) = \rho_W(x)A$ for $x \in \mathfrak{g}$. ◇

Remark 1.10.2. We usually consider Lie algebras (and representations of them) over $k = \mathbb{R}$ or $k = \mathbb{C}$ since we work with real and complex Lie groups. For a real Lie algebra $\mathfrak{g}$, we will use the phrase "complex representation of $\mathfrak{g}$" to mean a representation of $\mathfrak{g}_{\mathbb{C}}$. ○

What do the fundamental theorems of Lie theory tell us about representations?

Theorem 1.10.3. *Let G be a Lie group with Lie algebra $\mathfrak{g} = \mathrm{Lie}\, G$. Then,*

(1) *A finite dimensional rep $\rho : G \to \mathrm{GL}(V)$ of G gives rise to a Lie algebra representation $\rho_* : \mathfrak{g} \to \mathfrak{gl}(V)$, and any morphism of G-reps is also a morphism of $\mathfrak{g}$-reps.*

(2) *When G is connected, then conversely, an morphism of Lie algebra representations is also a morphism of Lie group representations.*

(3) *If G is simply connected, then the assignment $\rho \mapsto \rho_*$ is an equivalence between the corresponding categories of finite dimensional representations $\mathrm{Rep}G \xrightarrow{\sim} \mathrm{Rep}\mathfrak{g}$. In particular, any finite dimensional rep θ of $\mathfrak{g}$ can be "exponentiated" to a rep ρ of G s.t. $\rho_* = \theta$ (so for $x \in \mathfrak{g}$, $\rho(\exp(x)) = \exp(\theta(x))$).*

Example (Trivial rep). Let V be any vector space. Take $\rho(g) = \mathrm{Id}_V$ for any $g \in G$ and $\rho(x) = 0$ for any $x \in \mathfrak{g}$. △

Example (Adjoint rep). $\rho(g) = \mathrm{Ad}_g$ for $g \in G$ and $\rho(x) = \mathrm{ad} x$ for $x \in \mathfrak{g}$. △

We have standard notions in representation theory.

- A **subrepresentation** is a subspace $W \subset V$ invariant under the action of G or $\mathfrak{g}$.
- If $W \subset V$ is a subrep, we can form the **quotient representation** V/W
- There's the direct sum $V \oplus W$ with $\rho_{V \oplus W} = \rho_V \oplus \rho_W$
- And there's the tensor product. For groups $\rho_{V \otimes W}(g) = \rho_V(g) \otimes \rho_W(g)$. For Lie algebras, we want to think $g = \exp(tx)$ in the above and differentiate at $t = 1$; using Liebniz, this gives

$$\rho_{V \otimes W}(x) = \rho_V(x) \otimes 1_W + 1_V \otimes \rho_W(x).$$

- We also get symmetric and exterior powers of representations. These are quotients of $V^{\otimes n}$. In $\operatorname{char} k = 0$, we can view $S^n V$ and $\bigwedge^n V$ as the subspaces of symmetric, resp. skew-symmetric, tensors in $V^{\otimes n}$.
- And there's the dual representation $V^* = \mathrm{Hom}_k(V, k)$. For groups, we have $\rho_{V^*}(g) = \rho_V(g^{-1})^*$. Differentiating, for Lie algebras, we have $\rho_{V^*}(x) = -\rho_V(x)^*$.
- Given two reps V, W, then $\mathrm{Hom}_k(V, W)$ is also a representation where

$$g \circ A = \rho_W(g) A \rho_V(g)^{-1}$$

for Lie groups. For Lie algebras, we differentiate to get

$$x \circ A = \rho_W(x) A - A \rho_V(x).$$

- There's the notion of **invariants**. For V a rep of G, we set

$$V^G := \{v \in V : gv = v \,\forall g \in G\} \subset V.$$

Similarly,

$$V^{\mathfrak{g}} := \{v \in V : xv = 0 \,\forall x \in \mathfrak{g}\}.$$

Example. $\mathrm{Hom}_k(V, W)^G = \mathrm{Hom}_G(V, W)$ and $\mathrm{Hom}_k(V, W)^{\mathfrak{g}} = \mathrm{Hom}_{\mathfrak{g}}(V, W)$. △

- A representation $V \neq 0$ is **irreducible** if it has no nonzero, proper subrepresentations.
- We say V is **indecomposable** if $V \cong V_1 \oplus V_2 \implies V_1 = 0$ or $V_2 = 0$. Note that irreducible $\implies$ indecomposable. The converse is not true in general.

Example. $\rho : \mathbb{C} \to \mathrm{GL}_2(\mathbb{C})$ given by $\rho(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ is indecomposable but not irreducible (it is reducible). $W = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle \subset V$ is a subrepresentation, but it has no invariant complement. △

- Finally, we say V is **completely reducible** if $V = \bigoplus V_i$ with each V_i irreducible.

  Remark 1.10.4. Any finite dimensional representation is isomorphic to a direct sum of indecomposable representations. There's a nontrivial theorem which says that this decomposition is unique up to permutation (we won't prove this). ○

What are the main problems of representation theory?

- Classify all irreducible representations of G or $\mathfrak{g}$
- If V is a completely reducible representation, find its decomposition into irreps.
- For which G and $\mathfrak{g}$ is every representation completely reducible (this is the case e.g. for compact Lie groups. This will be proven in the spring)

Example. V is the vector representation of $\mathrm{GL}(V)$, i.e. $\rho : \mathrm{GL}(V) \to \mathrm{GL}(V)$ the identity map. Then, V is irreducible. Moreover, if $\operatorname{char} k = 0$, then $S^m V$ and $\bigwedge^m V$ are also irreducible (exercise). Note that

$$V \otimes V = \bigwedge^2 V \oplus S^2 V$$

is completely reducible. △

Our first statement in representation theory will be Schur's lemma.

Theorem 1.10.5 (Schur's lemma). *If V, W are finite dimensional irreducible representations of G or $\mathfrak{g}$ (over[5] $\mathbb{C}$), then*

$$\mathrm{Hom}_{\mathrm{Rep}}(V, W) = 0 \text{ if } V \ncong W$$

and

$$\mathrm{Hom}_{\mathrm{Rep}}(V, W) = \mathbb{C} \text{ if } V \cong W$$

(all homomorphisms are scalars).

Proof. Let $A : V \to W$ be a nonzero morphism. Then, $\operatorname{im} A \subset W$ is a nonzero subrep, so $\operatorname{im} A = W$. Similarly, $\ker A \subset V$ is a nonfull subrep, so $\ker A = 0$. Thus, $A : V \xrightarrow{\sim} W$ is an iso. This proves the first part of the statement.

Now consider some nonzero $A : V \to V$. Well, A has an eigenvalue λ (root of characteristic poly $\det(\lambda I - A)$). Look at $A - \lambda I : V \to V$. This is not an isomorphism, so it must be the zero map. ■

Corollary 1.10.6. *The center of $G, \mathfrak{g}$ acts on every irrep by a scalar. In particular, if G or $\mathfrak{g}$ is abelian, then every irrep is 1-dimensional.*

Example. Take $G = \mathbb{C}^\times = \mathbb{R}_{>0} \times S^1$, a real Lie group. The irreps of G are

$$\chi_{s,n}(z) = |z|^s \left(\frac{z}{|z|}\right)^n$$

for $s \in \mathbb{C}$ and $n \in \mathbb{Z}$ (exercise). △

[5] Theorem holds over any algebrically closed field

Corollary 1.10.7. *Let* $V = \bigoplus_i n_i V_i$ *and* $W = \bigoplus_i m_i V_i$ *be completely reducible representations. Then,*

$$\mathrm{Hom}_{\mathrm{Rep}}(V, W) = \bigoplus_{i,j} \mathrm{Hom}_{\mathrm{Rep}}(V_i, V_j)^{\oplus n_i m_j} = \bigoplus_i \mathrm{Hom}_{\mathrm{Rep}}(V_i, V_i)^{\oplus m_i n_i} \cong \bigoplus_i \mathrm{Mat}_{m_i \times n_i}(\mathbb{C}).$$

In particular, $\dim \mathrm{Hom} = \sum_i m_i n_i$.

1.10.1 Unitary representations

Definition 1.10.8. A finite dimensional complex representation of a group G is a **unitary representation** if it is equipped with a positive definite Hermitian inner product $(v, w) \mapsto B(v, w)$ which is invariant under G, i.e. $B(gv, gw) = B(v, w)$ always. ⋄

Proposition 1.10.9. *Any unitary representation of* G *is completely reducible.*

Proof. Let $W \subset V$ be a subrep. We will show it has an invariant complement. Let $W^\perp \subset V$ be the orthogonal complement of W in V under B. Then, $W^\perp$ is also a subrep since B is invariant under the action of G. Finally, $V = W \oplus W^\perp$ (i.e. $W \cap W^\perp = 0$ since B positive definite and $\dim V = \dim W + \dim W^\perp$ since B non-degenerate). Now induct. ■

Remark 1.10.10. It is important above that the form is positive definite. ∘

Example. The rep $\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$, $n \to \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ preserves a Hermitian form (of signature $(1, 1)$, but is not completely reducible. (Exercise) △

Proposition 1.10.11. *Any finite dimensional complex representation of a finite group* G *is unitary.*

Using a Haar measure, you can average against it to get the same conclusion for any compact G

Proof. Pick any pos def form $B(v, w)$ on V. Define

$$\widehat{B}(v, w) = \frac{1}{|G|} \sum_{g \in G} B(gv, gw).$$

Now, $\widehat{B}$ is positive definite and invariant, so we win. ■

Proposition 1.10.12. *If moreover* V *is irreducible (again a rep of a finite group), then this unitary structure is unique up to a positive factor.*

Or more generally, a compact group

Proof. Say $B_1, B_2 : V \times V \to V$ are two invariant, positive def. Hermitian forms. Then, there exists a linear map $A : V \to V$ such that $B_2(v, w) = B_1(Av, w)$. Since B_1, B_2 are invariant, A is a morphism of representations, but now Schur's lemma implies that $A = \lambda I$. Hence, $B_2 = \lambda B_1$. Since B_1, B_2 are positive, we must have $\lambda > 0$. ■

Remark 1.10.13. We are working with $\mathbb{C}$-reps above. There's another argument that works more generally, where you project to some subspace, and then average this projection map. In characteristic p, you want to make sure that $p \nmid |G|$ so that you can divide by the order. ∘

Remark 1.10.14. The theory of integration over Lie groups will be developed in the Spring. ∘

Corollary 1.10.15. *Every finite dimensional representation of a finite (or compact) group* G *over* $\mathbb{C}$ *is completely reducible.*

1.10.2 Representations of $\mathfrak{sl}(2,\mathbb{C})$

"This is really a cornerstone of representation theory. Basically everything you do in representation theory more or less boils down to this."

Recall 1.10.16.

$$\mathfrak{sl}_2(\mathbb{C}) = \{A \in \mathrm{Mat}_2(\mathbb{C}) : \mathrm{Tr}\, A = 0\}$$

It has the canonical basis

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \text{and } h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

with commutation relations

$$[h, e] = 2e, \quad [h, f] = -2f, \quad \text{and } [e, f] = h.$$

$\odot$

Note that $\mathfrak{sl}_2(\mathbb{C})$ has a standard action on $\mathbb{C}^2 = \mathbb{C}x \oplus \mathbb{C}y$. We therefore get an action on the space $S^*\mathbb{C}^2 = \mathbb{C}[x, y] =:$ of polynomials in these. One can show that they act by $e = x\partial_y$, $f = y\partial_x$, and $h = x\partial_x - y\partial_y$. Write $V = \bigoplus_{n=0}^{\infty} V_n$ where V_n is the space of homogenous polynomials of degree n. Note that V_n has basis $V_{pq} = x^p y^q$ with $p + q = n$. We have

$$hv_{p,q} = (p - q)v_{pq}, \quad ev_{pq} = qv_{p+1,q-1}, \quad \text{and } fv_{pq} = pv_{p-1,q+1}.$$

It's easy to see that V_0 is the trivial rep and V_1 is the standard rep.

Exercise. V_2 is the adjoint rep.

In general, $\dim V_n = n + 1$.

Theorem 1.10.17.

(1) *V_n is irreducible.*

(2) *If $V \neq 0$ a finite dimensional rep of $\mathfrak{sl}_2$, then $e, f|_V$ act by nilpotent operators (so $\ker e \neq 0$). Moreover, h acts on $\ker e$ diagonalizably with non-negative integer eigenvalues.*

(3) *Any f.d. irrep of $\mathfrak{sl}_2$ is isomorphic to V_n for some n*

(4) *Any f.d. rep V of $\mathfrak{sl}_2$ is completely reducible*

The same is true over any algebraically closed field of characteristic 0.

Proof. **(1)** Suppose $0 \neq W \subset V_n$ is a subrep, so $W = \langle v_{p,n-p} \mid p \in S \subset [0, n]\rangle$. We know $ev_{p,n-p} = (n - p)v_{p+1,n-p-1}$ and $fv_p = pv_{p-1,n-p+1}$ so $p \in S \implies \{p - 1, p + 1\} \subset S$. Since S is nonempty, this implies $S = [0, n]$, so $W = V_n$.

(2) Let V be a f.d. rep of $\mathfrak{sl}_2$. Write $V = \bigoplus_\lambda V(\lambda)$ where $V(\lambda)$ generalized eigenspace of h with eigenvalue λ. Now

$$[h, e] = 2e \implies he = e(h + 2) \text{ and } [h, f] = -2f \implies hf = f(h - 2).$$

Thus, $e : V(\lambda) \to V(\lambda+2)$ and $f : V(\lambda) \to V(\lambda-2)$, so these are both nilpotent (only finitely many eigenvalues). Hence, $U = \ker e \neq 0$. We claim that h preserves U. Well, for $v \in U$, we have

$$e(hv) = (h-2)ev = 0 \implies hv \in U.$$

It remains to show that it acts diagonalizably with eigenvalues being non-negative integers. ■

1.11 Lecture 11 (10/6)

1.11.1 Representation Theory of $\mathfrak{sl}_2$ continued

We were in the midst of proving the below theorem.

Theorem 1.11.1.

(1) *V_n is irreducible.*

(2) *If $V \neq 0$ a finite dimensional rep of $\mathfrak{sl}_2$, then $e, f|_V$ act by nilpotent operators (so $\ker e \neq 0$). Moreover, h acts on $U := \ker e$ diagonalizably with non-negative integer eigenvalues.*

(3) *Any f.d. irrep of $\mathfrak{sl}_2$ is isomorphic to V_n for some n*

(4) *Any f.d. rep V of $\mathfrak{sl}_2$ is completely reducible*

The same is true over any algebraically closed field of characteristic 0.

Proof. **(1)** Suppose $0 \neq W \subset V_n$ is a subrep, so $W = \langle v_{p,n-p} \mid p \in S \subset [0,n] \rangle$. We know $ev_{p,n-p} = (n-p)v_{p+1,n-p-1}$ and $fv_p = pv_{p-1,n-p+1}$ so $p \in S \implies \{p-1, p+1\} \subset S$. Since S is nonempty, this implies $S = [0,n]$, so $W = V_n$.

(2) Let V be a f.d. rep of $\mathfrak{sl}_2$. Write $V = \bigoplus_\lambda V(\lambda)$ where $V(\lambda)$ generalized eigenspace of h with eigenvalue λ. Now

$$[h,e] = 2e \implies he = e(h+2) \text{ and } [h,f] = -2f \implies hf = f(h-2).$$

Thus, $e : V(\lambda) \to V(\lambda+2)$ and $f : V(\lambda) \to V(\lambda-2)$, so these are both nilpotent (only finitely many eigenvalues). Hence, $U = \ker e \neq 0$. We claim that h preserves U. Well, for $v \in U$, we have

$$e(hv) = (h-2)ev = 0 \implies hv \in U.$$

It remains to show that it acts diagonalizably with eigenvalues being non-negative integers. Pick nonzero $v \in U$ (so $ev = 0$). Consider $v_m := e^m f^m v$. Note first that (use $ef = fe + h$ and $hf = fh - 2f$)

$$ef^m v = fef^{m-1}v + hfm - 1v = fef^{m-1}v + f^{m-1}(h - 2(m-1))v.$$

We can keep going (i.e. induct), and in the end we see that

$$ef^m v = f^{m-1}m(h-m+1)v.$$

Hence,

$$v_m = e^{m-1}ef^m v = e^{m-1}f^{m-1}m(h-m+1)v.$$

Since $m(h-m+1)v \in U$ ($hU \subset U$), we can repeat to get

$$v_m = e^{m-2}f^{m-2}m(m-1)(h-m+1)(h-m+2)v = \cdots = m!h(h-1)\dots(h-m+1)v.$$

From this, we see that there exists some m such that for every $u \in U$, $e^m f^m v = 0$ so $h(h-1)\dots(h-m+1) = 0$ on U, so h is diagonalizable with eigenvalues in $\{0, 1, \dots, m-1\}$.

(3) Let v be an irrep, and pick some nonzero $v \in U = \ker e$. Can assume $hv = \lambda v$, i.e. v is an eigenvector. Let $w_m = f^m v$. Note that w_m lives in the $(\lambda - 2m)$-eigenspace of h as

$$hw_m = hf^m v = f^m(h-2m)v = (\lambda - 2m)w_m.$$

We have a picture like

$$\cdots \xleftarrow{f} V(\lambda-4) \xleftarrow{f} V(\lambda-2) \xleftarrow{f} V(\lambda) \leftarrow \cdots.$$

We also have $ew_m = ef^m v = m(h-m+1)w_{m-1}$ and $fw_m = w_{m+1}$. From this, we see that if $w_m \neq 0$ and $\lambda \neq m$, then $w_{m+1} \neq 0$ since $ew_{m+1} = (m+1)(h-m)w_m \neq 0$. Also, the vectors w_m which are nonzero are linearly independent since that are h-eigenvectors with different eigenvalues. Thus, there are only finitely many m such that $w_m \neq 0$; more precisely, if $\lambda = n \in \mathbb{Z}_{\geq 0}$, then $v, fv, \dots, f^n v \neq 0$ but $f^{n+1}v = 0$, i.e. $w_0, \dots, w_n \neq 0$ and $w_i = 0$ for $i \geq n+1$. Now, our rep V_i is irred, so it is generated by $v = w_0$, so it is spanned by w_i for $i = 0, \dots, n$. Using the previous formulas for how e, f, h act on w_i, we see that $V \cong V_n$ via $w_m \mapsto n(n-1)\dots(n-m+1)x^m y^{n-m}$.

(4) Let V be a f.d. rep of $\mathfrak{sl}_2$. We may assume WLOG that V is indecomposable. We will need to use the **Casimir operator** (we'll later discuss where this comes from)

$$C = 2fe + \frac{h^2}{2} + h.$$

We claim that C commutes with the Lie algebra, i.e. $[C,e] = [C,f] = [C,h] = 0$ so $C : V \to V$ is a homomorphism. This is juat a direct computation, e.g.

$$[C,e] = [2fe + h^2/2 + h, e] = 2[f,e]e + \frac{h[h,e] + [h,e]h}{2} + [h,e] = -2he + he + eh + he - eh = 0.$$

This claim implies that C has only one eigenvalue on V. Indeed, we can write $V = \bigoplus_c V(c)$ where $V(c)$ is a generalized c-eigenspace of C, but these are all subreps (since C commutes with everything) and V is indecomposable, so $V = V(c)$ for some c.

Briefly consider $C|_{V_n}$. Pick some nonzero $v \in V_n$ so $ev = 0$, $hv = nv$ and $Cv = \left(\frac{n^2}{2} + n\right)v = \frac{n(n+2)}{2}v$. Hence,

Question: What is V_n?

Answer: It's the standard rep. $\mathfrak{sl}_2(\mathbb{C}) \curvearrowright \mathbb{C}[x,y]_n$

$$C(f^m v) = f^m Cv = \frac{n(n+2)}{2}f^m v.$$

We will prove that V is completely reducible by induction on its dimension. The base is $\dim V \leq 1$. Pick $W \subset V$ an irreducible subrepresentation. Then, $W \cong V_n$ for some n by **(3)**. This implies that $C|_W = \frac{n(n+2)}{2} \cdot \mathrm{Id}$. Consider V/W. This has smaller dimension, so $V/W = \bigoplus V_{n_i}$ is completely reducible. But C has only one eigenvalue on V/W which we know to be $n(n+2)/2$. This implies $n_i = n$ for all i, so $V/W \cong (V_n)^{\oplus(m-1)}$ is a multiple of V_n. Hence, $\dim V = m \dim V_n = m(n+1)$ and we have a short exact sequence

$$0 \longrightarrow V_n \longrightarrow V \longrightarrow V_n^{\oplus(m-1)} \longrightarrow 0.$$

In particular, the generalized eigenspace of h with eigenvalue n has dimension $\dim V_h(n) = m$. By **(2)**, h is diagonalizable on $V_h(n) \subset U$, so $hv = nv$ on $V(n)$. Pick a basis $u_1, \ldots, u_m$ of $V(n)$. We have a homomorphism $\varphi : V_n^{\oplus m} \to V$ given by $\varphi(f^{k_1}v, \ldots, f^{k_m}v) = f^{k_1}u_1 + \cdots + f^{k_m}u_m$. This map is injective since the vectors $\{f^i u_j\}$ are linearly independent. One can check

$$\sum_j c_j f^i u_j = 0 \implies \sum_j c_j u_j = 0.$$

By looking at dimensions, we see that φ is actually an isomorphism, so V is completely reducible, $V \cong V_n^{\oplus m}$ (in fact, $M = 1$ since V indecomposable). ■

Remark 1.11.2. Here's a sketch of an alternate proof for **(4)**. Representations of $\mathfrak{sl}_2$ are the same as representations of $\mathfrak{su}_2$, but $\mathrm{SU}(2)$ is compact, so its representations are all completely reducible. ○

Corollary 1.11.3 (**Jacobson-Morozov Lemma**). *Let V be a finite dimensional $\mathbb{C}$-vector space and $N : V \to V$ a nilpotent linear operator. Then, there exists a unique, up to isomorphism, representation of $\mathfrak{sl}_2$ on V such that $e|_V = N$.*

Proof. On V_n,

$$e = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ & & & & 0 \end{pmatrix} =: J_n$$

is a Jordan block of size n (basis w_m, $fw_m = w_{m+1}$, $fw_n = 0$). By Jordan Normal Form theorem, we have $N \sim \bigoplus_i J_{n_i}$. If $V = \bigoplus_i V_{n_i}$, then $e|_V = N$. Conversely, if $V = \bigoplus_i V_{n_i}$ (always true for some n_i + decomposition unique by looking at C-eigenspaces), then $e|_V = \bigoplus J_{n_i}$, so the n_i are completely determined; this gives uniqueness. ■

Definition 1.11.4. The **character of a rep V of $\mathfrak{sl}_2$** is

$$\chi_V(z) = \mathrm{Tr}_V(z^h),$$

where z^h makes sense since h is diagonalizable with $\mathbb{Z}$ eigenvalues. We have

$$\chi_V(z) = \sum z^m \dim \ker(h-m)|_V.$$

◇

Remark 1.11.5. We know $h|_{V\otimes W} = h|_V \otimes \mathrm{Id}_W + \mathrm{Id}_V \otimes h|_W$, so $z^h|_{V\otimes W} = z^h|_V \otimes z^h|_W$. Hence, we get

$$\chi_{V\otimes W}(z) = \chi_V(z)\chi_W(z) \text{ and } \chi_{V\oplus W}(z) = \chi_V(z) + \chi_W(z).$$

$\circ$

Example.

$$\chi_{V_n}(z) = z^n + z^{n-2} + z^{n-4} + \cdots + z^{-n} \text{``}=\text{''} \frac{z^{n+1} - z^{-n-1}}{z - z^{-1}}.$$

Thus (exercise),

$$\chi_{V_n}\chi_{V_m} = \sum_{i=0}^{\min(m,n)} \chi_{|m-n|+2i}.$$

$\triangle$

Example. $\chi_{V_2} = z^2 + 1 + z^{-2}$, so

$$\chi_{V_2}\chi_{V_1} = (z^2+1+z^{-2})(z+z^{-1}) = z^3+2z+2z^{-1}+z^{-3} = (z^3+z+z^{-1}+z^{-3})+(z+z^{-1}) = \chi_{V_3}+\chi_{V_1}.$$

Thus,

$$V_2 \otimes V_1 \simeq V_3 \oplus V_1.$$

$\triangle$

In general, we see that

$$V_n \otimes V_m \cong \bigoplus_{i=0}^{\min(m,n)} V_{|m-n|+2i}.$$

Proof. The characters

$$\chi_{V_m} = \frac{z^{m+1} - z^{-m-1}}{z - z^{-1}}$$

are linearly independent as polynomials. Hence, a f.d. rep of $\mathfrak{sl}_2$ is completely determined by its character. $\blacksquare$

This is called the **Clebsch-Gordan decomposition**.

Exercise. $V_n \cong V_n^\vee$. More precisely, V_n has a nondegenerate invariant inner product $(-,-) : V_n \times V_n \to \mathbb{C}$, where "invariant" means

$$(av, w) + (v, aw) = 0 \text{ for all } a \in \mathfrak{sl}_2 \text{ and } v, w \in V_n.$$

This inner product is symmetric for even n (= odd dimensions) and skew-symmetric for odd n (= even dimensions).

One can say more about reps of $\mathfrak{sl}_2$, but we won't.

1.11.2 The universal enveloping algebra

Suppose V is a (possibly infinite-dimensional) vector space over a field k.

Recall 1.11.6. We can define the **tensor algebra** $TV = \bigoplus_{i=0}^\infty V^{\otimes i}$ which is a graded (non-commutative) associative algebra with unit. For $a \in V^{\otimes i}$ and $b \in V^{\otimes j}$, their product is

$$a \cdot b := a \otimes b \in V^{\otimes(i+j)}.$$

The unit is $1 \in V^{\otimes 0} = k$.

If x_i is a basis of V, then TV is the free algebra $k\langle\{x_i\}\rangle$ with basis formed by words in the letters x_i, i.e. it is a polynomial algebra on the non-commuting indeterminings x_i. ⊙

Definition 1.11.7. Let $\mathfrak{g}$ be a Lie algebra over k with Lie bracet denoted by $[-,-] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ as usual. The **universal enveloping algebra** $U(\mathfrak{g})$ of $\mathfrak{g}$ is the quotient of $T\mathfrak{g}$ by the 2-sided ideal I generated by the elements

$$x \otimes y - y \otimes x - [x, y]$$

for $x, y \in \mathfrak{g}$. Note that the above elements are not homogeneous ($x \otimes y, y \otimes x$ are in degree 2, but $[x, y]$ is in degree 1). ⋄

So I guess $U(\mathfrak{g})$ doesn't have a natural grading

Recall 1.11.8. Recall that any associative algebra A is also a Lie algebra with operation $[a, b] = ab - ba$. ⊙

Proposition 1.11.9.

(1) *Let $J \subset T\mathfrak{g}$ be a two-sided ideal, and let $\rho : \mathfrak{g} \to T\mathfrak{g}/J$ be the natural linear map. Then, ρ is a homomorphism of Lie algebras iff $J \supset I$, i.e. ρ factors through $U(\mathfrak{g})$.*

Slogan. $U(\mathfrak{g})$ is the largest quotient of $T\mathfrak{g}$ for which ρ is a homomorphism of Lie algebras.

(2) *Let A be any associative k-algebra with unit. Then the map*

$$- \circ \rho : \mathrm{Hom}_{\mathrm{alg}}(U(\mathfrak{g}), A) \to \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g}, L(A))$$

is a bijection, where $L(A)$ is A with bracket $[a, b] = ab - ba$.

Slogan. The universal enveloping algebra is left adjoint to the forgetful functor.

Maybe not the best name for L, but whatever

Proof. Exercise. ■

Remark 1.11.10 (Universal property of $U(\mathfrak{g})$). Any Lie algebra map $\psi : \mathfrak{g} \to A$ can be extended to an associative algebra map $\varphi : U(\mathfrak{g}) \to A$ such that $\psi = \varphi \circ \rho$.

In particular, a Lie algebra representation of $\mathfrak{g}$ on V is the same thing as an associative algebra representation of $U(\mathfrak{g})$ on V. ○

Remark 1.11.11. If $C \in U(\mathfrak{g})$ is a central element, then $C : V \to V$ is a homomorphism of representations. For example, $C = 2fe + \frac{h^2}{2} + h \in U(\mathfrak{sl}_2)$, the Casimir operator. ○

Let $\{x_i\}$ of $\mathfrak{g}$ be a basis, and write

$$[x_i, x_j] = \sum_k c_{ij}^k x_k$$

with $c_{ij}^{\in} k$ called the **structure constants**. Then,

$$U(\mathfrak{g}) = \frac{k\langle\{x_i\}\rangle}{(x_i x_j - x_j x_i - \sum c_{ij}^k x_k)}.$$

Example. When $\mathfrak{g}$ is abelian ($[-,-] = 0$), we get $U(\mathfrak{g}) = S\mathfrak{g}$ is the symmetric algebra. In terms of the basis, this is the polynomial algebra $k[\{x_i\}]$. △

Example.

$$u(\mathfrak{sl}_2) = \frac{k\langle e, f, h\rangle}{(he - eh - 2e, hf - fh + 2f, ef - fe - h)}$$

△

"There will be no lecture on Tuesday because we are on Monday schedule."

I'm not sure what "Monday schedule" means

1.12 Lecture 12 (10/8)

Last time we defined the universal enveloping algebra

$$U(\mathfrak{g}) = T\mathfrak{g}/(xy - yx - [x, y])$$

for a Lie algebra $\mathfrak{g}$.

Proposition 1.12.1. *Let A be an associative algebra. Then,* $\mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g}, A) \cong \mathrm{Hom}_{\mathrm{alg}}(U(\mathfrak{g}), A)$*. In particular,* $\mathrm{Rep}\mathfrak{g} = \mathrm{Rep}U(\mathfrak{g})$*.*

What can we say about the center of $U(\mathfrak{g})$? Note that $\mathfrak{g}$ acts on $T\mathfrak{g}$ by derivations via the **adjoint action**

$$\mathrm{ad}z(x_1x_2\dots x_n) = [z, x_1]x_2\dots x_n + x_1[z, x_2]x_3\dots x_n + \cdots + x_1x_2\dots x_{n-1}[z, x_n].$$

Note that

$$\mathrm{ad}z(xy-yx-[x,y]) = [z,x]y+x[z,y]-[z,y]x-y[z,x]-[z,[x,y]] = ([z,x]y - y[z,x] - [[z,x],y])+(x[z,y] - [z,y]x - [x,[z,y]])$$

so $\mathrm{ad}z(I) \subset I$ where $I = (xy - yx - [x, y]) \subset T\mathfrak{g}$. Thus, the adjoint action descends to an action $\mathrm{ad}z : U(\mathfrak{g}) \to U(\mathfrak{g})$ of the enveloping algebra. For $a \in U(\mathfrak{g})$, this action is simply $\mathrm{ad}z(a) = za - az$. This is because $U(\mathfrak{g})$ is generated by $\mathfrak{g}$, and for $a \in \mathfrak{g}$, we do have

$$\mathrm{ad}z(a) = [z, a] = za - az$$

by definition of $U(\mathfrak{g})$. This gives the following.

Proposition 1.12.2. *The center of $U(\mathfrak{g})$ is* $U(\mathfrak{g})^{\mathrm{ad}\mathfrak{g}} = \{a \in U(\mathfrak{g}) : \mathrm{ad}z(a) = 0\}$*.*

Remark 1.12.3. There are three natural actions of $\mathfrak{g}$ on $U(\mathfrak{g})$, left, right, and adjoint. The left action is $\ell(x) \cdot a = xa$ and the right action is $r(x) \cdot a = -ax$, and so the adjoint action is the sum of these two. ◦

Remark 1.12.4. The grading on $T\mathfrak{g}$ does not descend to $U(\mathfrak{g})$ since I is not a homegeneous ideal (not generated by homogeneous elements). ◦

Instead of a grading, we get a filtration.

1.12.1 Digression into filtrations

Definition 1.12.5. A **filtered vector space** (really, $\mathbb{N}$**-filtered vector space**) is a vector space $V = \bigcup_{i\geq 0} F_iV$ with

$$0 \subset F_0V \subset F_1V \subset \cdots \subset V$$

an increasing sequence of subspaces. We say that $v \in V$ has **filtration degree** $\leq n$ if $v \in F_nV$. It has degree exactly n if $v \in F_nV \setminus F_{n-1}V$. ◇

Definition 1.12.6. A **filtered algebra** over a field k is an (associative) algebra A (with unit) along with a filtration $A = \bigcup_{i\geq 0} F_iA$ such that $1 \in F_0A$ and $F_iA \cdot F_jA \subset F_{i+j}A$. ◇

Example. If $B = \bigoplus_{i=0}^{\infty} B_i$ is a graded algebra (so $1 \in B_0$ and $B_iB_j \subset B_{i+j}$), then it is filtered with the natural filtration $F_iB = B_0 \oplus B_1 \oplus \cdots \oplus B_i$. △

Not all filtered algebra are graded though, so a filtration is a weaker structure than a grading. However, every filtered algebra has an associated graded algebra.

Definition 1.12.7. If V is filtered, then it as an **associated graded object** $\mathrm{gr}V = \bigoplus_{i=0}^{\infty} \mathrm{gr}_iV$ where $\mathrm{gr}_iV := F_iV/F_{i-1}V$. This is a functorial construction. ◇

In particular, if A is a filtered algebra, then $\mathrm{gr}A$ is a graded algebra.

Example. If A is generated by $\{x_i\}$ then it has a filtration defined by $\deg(x_i) = 1$, i.e.

$$F_nA = \mathrm{span}\left\{x_{i_1}\dots x_{i_r} : r \leq n\right\}.$$

It is clear that defines a valid filtration.

Exercise. $\mathrm{gr}A$ is generated by $\overline{x}_i$, the images of x_i in $\mathrm{gr}_1A = F_1A/F_0A$.

△

Exercise. If $\mathrm{gr}A$ is a domain, then so is A.

1.12.2 Back to Lie Theory

Note that $U(\mathfrak{g})$ is generated by $\mathfrak{g}$ (technically, it is generated by the image of the natural map $\rho : \mathfrak{g} \to U(\mathfrak{g})$ which a priori might not be injective). We put a filtration on $U(\mathfrak{g})$ by declaring $\deg(\mathfrak{g}) = 1$ (really, $\deg(\mathfrak{g}) \leq 1$ since $\deg 0 = 0$ but whatever). This means that $F_nU(\mathfrak{g})$ is the image of $\bigoplus_{i=0}^{n} \mathfrak{g}^{\otimes i} \subset T\mathfrak{g}$ in $U(\mathfrak{g})$. In other words, $F_nU(\mathfrak{g})$ is the image of $F_n(T\mathfrak{g})$.

This filtration has the special property that

$$[F_iU(\mathfrak{g}), F_jU(\mathfrak{g})] \subset F_{i+j-1}U(\mathfrak{g}).$$

This is because Liebniz gives us that

$$[x_1\dots x_i, y_1\dots y_j] = [x_1\dots x_i, y_1]y_2\dots y_j + y_1[x_1\dots x_i, y_2]\dots y)j + \dots$$

which we can decompose one more time to get

$$[x_1\dots x_i, y_1\dots y_j] = \underbrace{[x_1, y_1]}_{\mathfrak{g}}\underbrace{x_2\dots x_iy_2\dots y_j}_{\mathfrak{g}^{\otimes(i+j-2)}} + \dots$$

whose terms are all in $F_{i+j-1}U(\mathfrak{g})$.

Remark 1.12.8. We forgot to say what multiplication looks like in $\mathrm{gr}A$. Given $a \in \mathrm{gr}_i A = F_iA/F_{i-1}A$ and $b \in \mathrm{gr}_j A$, we can take lifts $\widetilde{a} \in F_iA$ and $\widetilde{b} \in F_jA$. Their product $\widetilde{a}\widetilde{b}$ lies in $F_{i+j}A$, so it maps to some element $ab := \overline{\widetilde{a}\widetilde{b}} \in \mathrm{gr}_{i+j}A = F_{i+j}A/F_{i+j-1}A$. This is easily checked to be well-defined. ○

We see that $\mathrm{gr}U(\mathfrak{g})$ is commutative, generated by a basis x_i of $\mathfrak{g}$. This is because $[x_i, x_j]$ lands in $F_{i+j-1}U(\mathfrak{g})$, so $[x_i, x_j] = 0$ in $\mathrm{gr}U(\mathfrak{g})$. Thus, we obtain the following proposition.

Proposition 1.12.9. *There is a natural map $\varphi : S\mathfrak{g} \to \mathrm{gr}U(\mathfrak{g})$ which is a surjective algebra homomorphism.*

Remark 1.12.10. Note that $S\mathfrak{g} = k[\{x_i\}]$ is just the polynomial algebra generated by a basis of $\mathfrak{g}$. ○

Here's the really surprising bit.

Theorem 1.12.11 (Poincaré-Birkhoff-Witt Theorem). *The map φ defined above is injective (i.e. is an isomorphism), so $\mathrm{gr}U(\mathfrak{g}) \cong S\mathfrak{g}$.*

Let's restate things in terms of a basis. Say $\{x_i\}$ is an ordered basis of $\mathfrak{g}$. An **ordered monomial** in this basis is $x_{i_1}^{n_1} \dots x_{i_r}^{n_r}$ where $i_1 < i_2 < \cdots < i_r$. The proposition (not the theorem) is equivalent to saying that the ordered monomials form a spanning set of $U(\mathfrak{g})$.

Proof of reformulation of the proposition. We need to show that any monomial in x_i is a linear combination of ordered monomials in $U(\mathfrak{g})$. We will induct on the degree. The base is trivial. Suppose this is known in degree $n-1$, and let $X = x_{j_1}x_{j_2}\dots x_{j_n}$ be a degree n monomial (we allow repetition in the j_i's). Suppose this is not ordered, so $j_k > j_{k+1}$ for some k. Then,

$$X = x_{j_1}\dots x_{j_{k+1}}x_{j_k}\dots x_{j_n} + x_{j_1}\dots x_{j_{k-1}}[x_{j_k}, x_{j_{k+1}}]x_{j_{k+2}}\dots x_{j_n}$$

where the right term has lower degree and the left term now has fewer inversions. We win by induction. ■

In this perspective, PBW theorem is saying that the ordered monomials are linearly independent, so they form a basis in $U(\mathfrak{g})$ (Checking this equivalence is an exercise).

Before proving PBW, let's look at some of its corollaries.

Corollary 1.12.12. *The natural map $\rho : \mathfrak{g} \to U(\mathfrak{g})$ is injective (since $\rho(x_i)$ are linearly independent).*

Remark 1.12.13. This setting makes sense if we are just given a "proto-Lie algebra", a vector space $\mathfrak{g}$ with bilinear map $[-,-] : \mathfrak{g} \otimes \mathfrak{g} \to \mathfrak{g}$. The map $\varphi : S\mathfrak{g} \to U(\mathfrak{g})$ is still a surjective algebra morphism and $\rho : \mathfrak{g} \to U(\mathfrak{g})$ still exists (with $\rho([x, y]) = xy - yx$), but $(x, y) \mapsto xy - yx$ satisfies the axioms of a Lie algebra ($[x, x] = 0$ and Jacobi). Thus, if ρ is injective, $\mathfrak{g}$ must be a Lie algebra! In other words, if $\mathfrak{g}$ is not a Lie algebra, then ρ is never injective (PBW fails). ○

The upshot of this remark is that we will need to use lie algebra axioms in the proof of PBW even though we have not needed them for anything yet. This makes PBW nontrivial.

We still have more PBW corollaries.

Corollary 1.12.14. *If $\mathfrak{g}_1, \mathfrak{g}_2 \subset \mathfrak{g}$ are Lie subalgebras and $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ as vector spaces, then the multiplication map $U(\mathfrak{g}_1) \otimes U(\mathfrak{g}_2) \xrightarrow{m} U(\mathfrak{g})$ is an isomorphism of filtered vector spaces.*

Proof. Look at $\mathrm{gr}(m) : \mathrm{gr}U(\mathfrak{g}_1) \otimes \mathrm{gr}U(\mathfrak{g}_2) \to \mathrm{gr}U(\mathfrak{g})$. Using PBW, this looks like $S\mathfrak{g}_1 \otimes S\mathfrak{g}_2 \to S\mathfrak{g}$ and is just the normal multiplication map, which is certainly an isomorphism. ■

Remark 1.12.15. This extends to arbitrarily many factors. If $\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_n$, then

$$U(\mathfrak{g}_1) \otimes \cdots \otimes U(\mathfrak{g}_n) \xrightarrow{\sim} U(\mathfrak{g}).$$

The same holds true for infinitely many summands. Say $\mathfrak{g} = \bigoplus_{i \in I} \mathfrak{g}_i$. Then,

$$m : \bigotimes_{i \in I} U(\mathfrak{g}_i) \xrightarrow{\sim} U(\mathfrak{g})$$

where $\bigotimes_{i \in I} U(\mathfrak{g}_i)$ is the span of $\bigotimes_{i \in I} u_i$ where $u_i = 1$ for almost all i. ○

Example. Say $\mathfrak{g} = \bigoplus_i kx_i$ with $\mathfrak{g}_i = kx_i$ a 1-dim Lie subalgra. Then, this corllary says

$$\bigotimes_{i \in I} k[x_i] \xrightarrow{\sim} U(\mathfrak{g})$$

which is equivalent to PBW itself. △

Just a couple more corollaries.

Corollary 1.12.16. *Assume* $\operatorname{char} k = 0$. *Define* $\sigma : S\mathfrak{g} \to U(\mathfrak{g})$, *a linear map (the* ***symmetrization****) defined by* ($y_i \in \mathfrak{g}$)

$$\sigma(y_1 y_2 \dots y_n) = \frac{1}{n!} \sum_{s \in S_n} y_{s(1)} \dots y_{s(n)} \in U(\mathfrak{g}).$$

This is not an algebra map, but it is linear and it preserves the adjoint action, so this is a morphism of representations. Now, σ *is an isomorphism (or* $\mathfrak{g}$*-reps).*

Proof. $\operatorname{gr}\sigma = \operatorname{id}$ is an isomorphism which implies that σ is an isomorphism. ■

Fact. If V, W are filtered space and $f : V \to W$ is a filtered linear map, then $\operatorname{gr} f : \operatorname{gr} V \to \operatorname{gr} W$ is an iso $\implies f : V \to W$ is an iso (exercise).

Corollary 1.12.17. *The map* σ *defines an isomorphism*

$$(S\mathfrak{g})^{\operatorname{ad}\mathfrak{g}} \xrightarrow{\sim} Z(U(\mathfrak{g})) = U(\mathfrak{g})^{\operatorname{ad}\mathfrak{g}}$$

of vector spaces.

For finite dimensional Lie algebras, there exists an isomorphism of algebras between these two objects, but it is not this map. This is another non-trivial theorem

Example. What is the center of $U(\mathfrak{sl}_2(\mathbb{C}))$? It is convient to replace $\mathfrak{sl}_2(\mathbb{C})$ with the isomorphic Lie algebra $\mathfrak{so}_3(\mathbb{C})$. This has basis i, j, k with $[i, j] = k$, $[j, k] = i$, and $[k, i] = j$. The adjoint action is the derivative of the rotation action of $\mathrm{SO}_e(\mathbb{R})$ on $\mathbb{R}^3$. Note that $S\mathfrak{g} = \mathbb{C}[x, y, z]$ with x, y, z the coordinates on $\mathbb{R}^3$. Thus, the center is polynomials invariant under rotation, i.e. $\operatorname{gr} Z = \mathbb{C}[x, y, z]^{\mathrm{rot}} = \mathbb{C}[r^2]$ where $r^2 = x^2 + y^2 + z^2$. This gives $Z = \mathbb{C}[i^2 + j^2 + k^2]$. We can write this in terms of e, f, h:

Remember: $\mathfrak{so}_3(\mathbb{R})$ is

$$i^2 + j^2 + k^2 = -4fe - h^2 - 2h = -2C,$$

so $Z = \mathbb{C}[C]$. △

No class on Tuesday, but there is class next Thursday. We have homework due in 2 weeks since we are a little bit behind.

1.13 Lecture 13 (10/15)

* 6 minutes late because of Zoom wahala*

We were trying to prove PBW.

Recall 1.13.1 (Poincaré-Birkhoff-Witt Theorem)**.** The map φ defined last time is injective (i.e. is an isomorphism), so $\mathrm{gr}U(\mathfrak{g}) \cong S\mathfrak{g}$. $\odot$

Our man tool in the proof will be the following lemma.

Lemma 1.13.2. *There exists a unique linear $\varphi : T\mathfrak{g} \to S\mathfrak{g}$ such that*

- *If X is an ordered monomial, then $\varphi(X) = X$*
- *$\varphi(I) = 0$, i.e. $\varphi(Y(ab - ba - [a, b])Z) = 0$ always.*

Remark 1.13.3. φ depends on the choice of $\{x_i\}$ $\circ$

Proof of PBW Given Lemma. Images of the ordered monomial under φ are usual monomials (commutative) in $S\mathfrak{g} = k[(x_i)]$, so they are linearly independent. This implies that the ordered monomials themselves are linearly independent. ■

Proof of Lemma. It is clear that φ is unique if it exists since it is defined on ordered monomials, and the second condition holds iff φ descends to a linear map $U(\mathfrak{g}) = T\mathfrak{g}/I \to S\mathfrak{g}$, but ordered monomials span $U(\mathfrak{g})$.

Hence, it remains to construct φ. We'll do so by defining it inductively on the spaces $F_nT\mathfrak{g} = k \oplus \mathfrak{g} \oplus \mathfrak{g}^{\otimes 2} \oplus \cdots \oplus \mathfrak{g}^{\otimes n}$. The base is clear. For the inductive step, we have

$$F_nT - \mathfrak{g} = F_{n-1}T\mathfrak{g} \oplus \mathfrak{g}^{\otimes n}$$

and we already have φ defined on $F_{n-1}T\mathfrak{g}$. Note that $\mathfrak{g}^{\otimes n}$ has basis $X = X_{i_1 \ldots i_n} x_{i_1} \ldots x_{i_n}$ with $i_1, \ldots, i_n \in I$. If ordered, we set $\varphi(X) = X$, so we need to extend it all monomials. Now, any monomial can be obtained from an ordered one by applying a permutation (i.e. a sequence of adjacent transpositions). Let X be an ordered monomial of degree n, choose some $s \in S_n$, and consider $s(X)$ (where $s(x_1 \ldots x_n) = x_{s(1)} \ldots x_{s(n)}$). To this end, fix a representation of s as a product of transpositions of neighbors, i.e. $s = s_{j_r} \ldots s_{j_1}$ where $s_j = (j, j+1)$ (for $1 \le j \le n-1$). Applying each adjacent transposition incurs a cost of the commutator, but this is fine because this lowers the degree to a place where φ is already defined. Adding up all the costs, we get

$$\varphi(s(X)) = X + \sum_{m=0}^{r-1} \varphi\left([-,-]_{j_{m+1}} s_{j_m} \ldots s_{j_1}(X)\right)$$

where

$$[-,-]_j(y_1 \ldots y_j y_{j+1} \ldots y_n) := y_1 \ldots [y_j, y_{j+1}] \ldots y_n.$$

We need to show that our definition of $s(X)$ is independent of the choice of decomposing s into adjacent transpositions. Call our choice D and let our "sum of costs" be

$$\Phi_D(s, X) := \sum_{m=0}^{r-1} \varphi\left([-,-]_{j_{m+1}} s_{j_m} \ldots s_{j_1}(X)\right).$$

We need to show that $\Phi_D(s,X)$ depends only on $s(X)$, but not individually on D or s. This is where we'll finally use the axioms of a Lie algebra.

Recall that

$$S_n = \left\langle s_j \,\middle|\, s_j^2 = 1, s_j s_k = s_k s_j \text{ for } j-k \geq 2, s_j s_{j+1} s_j = s_{j+1} s_j s_{j+1} \right\rangle$$

with s_j still the adjacent permutation $(j, j+1)$. With this presentation given, we see that any two representations D_1, D_2 of s as a product of adjacent transpositions can be identified by a sequence of applications of these relations.

Suppose first that D_1, D_2 are related by a relation of the first type, i.e. $D_1 : s = pq$ and $D_2 : s = ps_j s_j q$. In this case, $\Phi_{D_1} = \Phi_{D_2}$ follows from the relation that $[a,b]+[b,a]=0$.

Now consider a relation of the second type, i.e. $D_1 : s = ps_j s_k q$ (where $j < k-1$) and $D_2 : s = ps_k s_j q$. Note that $q(X) = YabZcdT$ with $a,b,c,d \in \mathfrak{g}$, a is position j (so b in position $j+1$) and c in position k. Then,[6]

$$\Phi_{D_1} - \Phi_{D_2} = \varphi(YabZ[c,d]T) + \varphi(Y[a,b]ZdcT) - \varphi(Y[a,b]ZcdT) - \varphi(YbaZ[c,d]T)$$

We can apply property 2 in degree $n-1$ to see that above equals

$$\Phi_{D_1} - \Phi_{D_2} = \varphi(Y[a,b]Z[c,d]T) + \varphi(Y[a,b]Z[d,c]T) = 0.$$

Finally, consider a relation of the third type, i.e. $D_1 : s = ps_j s_{j+1} s_j q$ and $D_2 : ps_{j+1} s_j s_{j+1} q$. Write

$$q(X) = YabcZ \text{ with } a,b,c \in \mathfrak{g} \text{ and } a \text{ in position } j.$$

Our two routes are

$$D_1 : YabcZ \to YbacZ \to YbcaZ \to YcbaZ$$

and

$$D_2 : YabcZ \to YacbZ \to YcabZ \to YcbaZ.$$

Hence,

$$\Phi_{D_1} - \Phi_{D_2} = \varphi(Y[a,b]cZ) + \varphi(Yb[a,c]Z) + \varphi(Y[b,c]aZ) - \varphi(Ya[b,c]Z) - \varphi(Y[a,c]bZ) - \varphi(Yc[a,b]Z).$$

Property 2 in degree $n-1$ and the Jacobi identity imply that the above expression is 0. In slightly more detail, combining the first and last terms gives a $\varphi(Y[[a,b],c]Z)$. When combining the other two terms, you get a $[[b,c],a]$ and a $[[c,a],b]$ also appearing, and then you use $[[a,b],c]+[[b,c],a]+[[c,a],b] = 0$ (Jacobi) to see that the entire expression is 0.

This shows that $\Phi_C(s,X)$ is independent of D, so we may call it $\varphi(s,X)$. We are not done yet; we need to show $\varphi(s,X)$ depends only on $s(X)$ and not on s: $\varphi(s,X) = \varphi(s',X)$ if $s(X) = s'(X)$. It is clear that $s(X) = s'(X) \iff s = s't$ where t is a product of s_j such that $i_j = i_{j+1}$. Therefore, it is enough to show that $\varphi(s,X) = \varphi(ss_j, X)$ for such j. However, this is clear from the relation $[a,a]=0$ (which

In characteristic 2, we haven't even used $[x,x]=0$ yet

[6] $YabZcdT \to YabZdsT \to YbaZdcT$ or $YabZcdT \to YbaZcdT \to YbaZdcT$. We're looking at the difference of costs between these two routes

appears in the incurred cost). Like, this is basically the identity

$$\varphi(YaaZ) = \varphi(YaaZ) + \varphi(Y[a,a]Z).$$

This finishes the defintion of φ. By construction it satisfies both conditions. The first one is clear. The second is essentially just the fact that

$$\varphi(s_j(X)) = \varphi(X) + \varphi([-,-]_j(X)).$$

■

Thus, we have proven PBW. On to the next topic.

1.13.1 Ideals and commutants

Definition 1.13.4. Let $\mathfrak{g}$ be a Lie algebra. Then, $\mathfrak{h} \subset \mathfrak{g}$ is an **ideal** if $[\mathfrak{g}, \mathfrak{h}] \subset \mathfrak{h}$. This implies that the quotient $\mathfrak{g}/\mathfrak{h}$ is also a Lie algebra. ⋄

Example (Exercise)**.** If $\varphi : \mathfrak{g}_1 \to \mathfrak{g}_2$ is a Lie algebra homomorphism, then $\ker\varphi \subset \mathfrak{g}_1$ is an ideal, and $\varphi : \mathfrak{g}_1/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$ is a Lie algebra isomorphism. △

Lemma 1.13.5. *If $I_2, I_2 \subset \mathfrak{g}$ are ideals, then so are $I_1 \cap I_2$, $[I_1, I_2]$, and $I_1 + I_2$.*

Proof. Exercise. ■

Definition 1.13.6. The **Commutant** (or **derived subalgebra**) of $\mathfrak{g}$ is $[\mathfrak{g}, \mathfrak{g}] = \operatorname{span}\{[x, y] : x, y \in \mathfrak{g}\}$. This is an ideal. ⋄

Lemma 1.13.7. *$\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$ is abelian and is in fact the maximal abelian quotient, i.e. if $I \subset \mathfrak{g}$ is any ideal s.t. $\mathfrak{g}/I$ is abelian, then $I \supset [\mathfrak{g}, \mathfrak{g}]$.*

Proof. Exercise ■

Example. If $\mathfrak{g} = \mathfrak{gl}_n(k)$, then $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{sl}_n(k)$. If $i \neq j$, then $E_{ij} = [E_{ii}, E_{ij}]$ and also $E_{ii} - E_{jj} = [E_{ij}, E_{ji}]$, so $\mathfrak{sl}_n(k) \subset [\mathfrak{gl}_n(k), \mathfrak{gl}_n(k)]$. At the same time, for any $x, y \in \mathfrak{gl}_n(k)$, we know $\operatorname{Tr}([x, y]) = 0$ so $[\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{sl}_n(k)$ as well. △

Exercise. Prove that if G is a connected Lie group with Lie algebra $\mathfrak{g}$, then the commutator subgroup $[G, G]$ is a closed Lie subgroup of G with Lie algebra $[\mathfrak{g}, \mathfrak{g}]$.

1.13.2 Solvable Lie algebras

Definition 1.13.8. Given a Lie algebra $\mathfrak{g}$, its **derived series** is the descending chain of ideals

$$\mathfrak{g} = D^0 \supset D^1 \supset D^2 \supset \dots$$

with $D^{i+1}(\mathfrak{g}) = [D^i(\mathfrak{g}), D^i(\mathfrak{g})]$ for $i \geq 0$. We say $\mathfrak{g}$ is **solvable** if $D^n(\mathfrak{g}) = 0$ for some n. ⋄

Example. Let $T_n(k)$ be the Lie algebra of upper triangular matrices. Then, $[T_n(k), T_n(k)]$ consists of *strictly* upper triangular matrices. With each success application of $[-,-]$, we push the diagonal further and further towards the top left, so this is solvable. △

Remark 1.13.9. We'll see later that every finite dimensional solvable Lie algebra is a subalgebra of upper triangular matrices. ○

Proposition 1.13.10. $\mathfrak{g}$ *is solvable iff there exists a sequence of ideals*

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \cdots \supset \mathfrak{g}_n = 0$$

such that $\mathfrak{g}_i/\mathfrak{g}_{i+1}$ *is abelian.*

Proof. $(\rightarrow)$ This holds simply because D^i/D^{i+1} is abelian.

$(\leftarrow)$ Necessarily $\mathfrak{g}_1 \supset D^1$ since $\mathfrak{g}/\mathfrak{g}_1$ is abelian. Furthermore, $\mathfrak{g}_2 \supset [\mathfrak{g}_1, \mathfrak{g}_1] \supset [D^1, D^1] = D^2$ and so on and so on. In particular, $0 = \mathfrak{g}_m \supset D^m \implies D^m = 0$ so $\mathfrak{g}$ is solvable. ■

Proposition 1.13.11. *Any Lie subalgebra of a solvable Lie algebra is solvable. Furthermore, if* $I \subset \mathfrak{g}$ *is an ideal with* $I, \mathfrak{g}/I$ *both solvable, then* $\mathfrak{g}$ *is solvable ("solvability is preserved under extension.")*

Proof. Exercise. ■

1.13.3 Nilpotent Lie algebras

Definition 1.13.12. Let $\mathfrak{g}$ be a Lie algebra. The **lower central series** of $\mathfrak{g}$ is the descending sequence of ideals $D_i(\mathfrak{g})$ with $D_0(\mathfrak{g}) = \mathfrak{g}$ and $D_{i+1}(\mathfrak{g}) = [\mathfrak{g}, D_i(\mathfrak{g})]$. We say $\mathfrak{g}$ is **nilpotent** if $D_n(\mathfrak{g}) = 0$ for some n. ◇

Example. Consider $T_n^+(k) = \left\{ \begin{pmatrix} 0 & & * \\ & \ddots & \\ & & 0 \end{pmatrix} \right\}$ strictly upper triangular $n \times n$ matrices. This is nilpotent. However, $T_n(k) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix} \right\}$ upper triangular $n \times n$ matrices is solvable but not nilpotent for $n \geq 2$, e.g. because $[E_{11}, E_{12}] = E_{12}$ so $E_{12} \in D_i(T_n(k))$ for all i. △

Proposition 1.13.13. $\mathfrak{g}$ *is nilpotent iff there's a sequence of ideals*

$$\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \cdots \supset \mathfrak{g}_m = 0$$

s.t. $[\mathfrak{g}, \mathfrak{g}_i] \subset \mathfrak{g}_{i+1}$.

Proof. $(\rightarrow)$ Just take $\mathfrak{g}_i = D_i(\mathfrak{g})$.

$(\leftarrow)$ $\mathfrak{g}_1 \supset D_1\mathfrak{g} \implies \mathfrak{g}_2 \supset [\mathfrak{g}, \mathfrak{g}_1] \supset [\mathfrak{g}, D_1(\mathfrak{g})] = D_2(\mathfrak{g})$ and so on. In particular, $0 = \mathfrak{g}_m \supset D_m(\mathfrak{g}) \implies D_m(\mathfrak{g}) = 0$. ■

Corollary 1.13.14. *Any nilpotent Lie algebra is solvable since* $[\mathfrak{g}, \mathfrak{g}_i] \subset \mathfrak{g}_{i+1} \implies [\mathfrak{g}_i, \mathfrak{g}_i] \subset \mathfrak{g}_{i+1} \implies \mathfrak{g}_i/\mathfrak{g}_{i+1}$ *is abelian.*

Proposition 1.13.15. *Any Lie subalgebra (or quotient) of a nilpotent Lie algebra is nilpotent.*

Proof. Exercise. ■

1.13.4 Lie Theorem

Theorem 1.13.16 (**Lie's Theorem**)**.** *Fix some algebraically closed field $k = \overline{k}$ of characteristic* 0*, and let $\mathfrak{g}$ be a solvable finite dimensional Lie algebra over k. Then any irreducible finite dimensional representation V of $\mathfrak{g}$ is necessarily one dimensional.*

We do not have time to prove this right now, but we will do so next lecture.

Remark 1.13.17. This is false in positive characteristic. Consider $\mathfrak{g} = \langle x, y \rangle$ with $[x, y] = y$, and let $V = k^{\oplus p} = \langle v_1, \dots, v_p \rangle$. The action is given by

$$xv_i = iv_i \text{ and } yv_i = v_{i+1}.$$

As an exercise, show that this is irreducible. ○

Here is another formulation of Lie, but we'll state it as a corollary.

Corollary 1.13.18. *Let V be a finite dimensional representation of $\mathfrak{g}$, a Lie algebra over $k = \overline{k}$ (when* $\operatorname{char} k = 0$*). Then, V has a basis in which all elements of $\mathfrak{g}$ act by upper triangular matrices. In other words, there exists a sequence of subrepresentations*

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

such that $\dim(V_{k+1}/V_k) = 1$.

Remark 1.13.19. If $\dim \mathfrak{g} = 1$ so $\mathfrak{g} = \langle x \rangle$ and a representation is just an operator $x : V \to V$, we recover the basis fact in linear algebra that there exists a basis in which x is upper triangular (e.g. Jordan normal form). ○

of Corollary. By induction on $\dim V$, Lie theorem gives some $v_0 \in V$ a common eigenvector of all elements of $\mathfrak{g}$. Let $V' = V/kv_0$, so $\dim V' = \dim V - 1$. The inductive hypothesis now gives a basis $v_1', \dots, v_n'$ of V' such that action of $\mathfrak{g}$ is upper triangular. Pick lifts $v_1, \dots, v_n \in V$ of $v_1', \dots, v_n' \in V/kv_0$. Then, $v_0, v_1, \dots, v_n$ is a basis of V in which the action of $\mathfrak{g}$ is upper triangular. ■

1.14 Lecture 14 (10/20)

Last time we stated Lie's theorem.

Recall 1.14.1 (Lie's Theorem)**.** Fix some algebraically closed field $k = \overline{k}$ of characteristic 0, and let $\mathfrak{g}$ be a solvable finite dimensional Lie algebra over k. Then any irreducible finite dimensional representation V of $\mathfrak{g}$ is necessarily one dimensional. ⊙

Proof. Let $V \neq 0$ be a f.d. representation of $\mathfrak{g}$. It suffices to show that V contains a common eigenvector for $\mathfrak{g}$. We will show that by induction on $\dim \mathfrak{g}$. The base case is trivial, so we just do the induction step. Since $\mathfrak{g}$ is solvable, $[\mathfrak{g}, \mathfrak{g}] \neq \mathfrak{g}$, so fix a subspace $\mathfrak{h} \subset \mathfrak{g}$ such that $\dim \mathfrak{g}/\mathfrak{h} = 1$. Then, $\mathfrak{h}$ is an ideal since $[\mathfrak{g}, \mathfrak{h}] \subset [\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{h}$. We know that $\mathfrak{h}$ is solvable as well, so inductive hypothesis tells us that there is some $\lambda : \mathfrak{h} \to k$ and some nonzero $v \in V$ such that $h \cdot v = \lambda(h)v$ for all $h \in \mathfrak{h}$. Now write $\mathfrak{g} = \mathfrak{h} \oplus kx$ (so $x \in \mathfrak{g} \setminus \mathfrak{h}$). Let $W = \langle v, xv, x^2v, \dots \rangle \subset V$ We claim that for all $a \in \mathfrak{h}$, $ax^nv \in \langle v, xv, x^2v, \dots, x^nv \rangle$, i.e it is a linear combination of the first $n+1$ vectors spanning W.

I guess $\mathfrak{h}$ is not just any codimension 1 subspace

We prove this by induction on this n. The case $n = 0$ is obvious. If $n > 0$, then we have

$$ax^nv = xax^{n-1}v + [a, x]x^{n-1}v,$$

but $[a, x] \in \mathfrak{h}$ ($\mathfrak{h}$ an ideal and $a \in \mathfrak{h}$), so $[a, x]x^{n-1}v \in \langle v, sv, \dots, x^{n-1}v \rangle$ by inductive hypothesis. Also, $ax^{n-1}v$ is in the same span for the same reason, so $ax^nv = xax^{n-1}v + [a, x]x^{n-1}v \in \langle v, sv, \dots, x^{n-1}v, x^nv \rangle$ as desired. In fact, we furthermore see that the coefficient of x^nv is just $\lambda(a)$, i.e.

$$ax^nv \in \lambda(a)x^nv + \langle v, xv, \dots, x^{n-1}v \rangle .$$

Now let r be the largest integer such that $v, xv, \dots, x^{r-1}v$ are linearly independent, so these gives a basis of W. How does a act on this basis? Well, it does so by an upper triangular matrix with diagonal entries $\lambda(a)$, i.e.

$$a|_W = \begin{pmatrix} \lambda(a) & & * \\ & \ddots & \\ * & & \lambda(a) \end{pmatrix}.$$

Also, W is a subspace, and we have that $\operatorname{tr} a|_W = r\lambda(a)$. Now suppose that $a \in [\mathfrak{g}, \mathfrak{g}]$. Then, $\operatorname{tr} a|_W = 0$, so $r\lambda(a) = 0$. Since we are in characteristic 0, this implies $\lambda(a) = 0$ as well. Now, we're almost done. By another induction in n, we get[7]

$$ax^nv = \lambda(a)x^nv.$$

Thus, $[\mathfrak{g}, \mathfrak{g}]$ acts by 0 on W, so W is a representation of $\mathfrak{g}/[\mathfrak{g}, \mathfrak{g}]$, but this quotient is abelian, so W certainly has a common eigenvector. ■

We saw a few corollaries last time, but here are some more. Still have $k = \overline{k}$ and $\operatorname{char} k = 0$.

Corollary 1.14.2. *A solvable finite dimensional Lie algebra $\mathfrak{g}$ admits a sequence of ideals*

$$\mathfrak{g} = I_n \supset I_{n-1} \supset \cdots \supset I_0 = 0$$

such that $\dim I_{j+1}/I_j = 1$. *We have a "complete flag of ideals."*

This is analogous to the fact that a solvable (finite) group G has normal subgroups

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_0 = 1$$

such that $H_{j-1}/H_j \cong \mathbb{Z}/p_j\mathbb{Z}$ for some p_j prime.

Proof. Consider the adjoint rep of $\mathfrak{g}$ on $\mathfrak{g}$. Then it has a basis $a_1, \dots, a_n$ on which the action of $\mathfrak{g}$ is by upper triangular matrices. Take $I_j = \langle a_1, \dots, a_j \rangle$. ■

[7] $ax^nv = xax^{n-1} + [a, x]x^{n-1}v = x\lambda(a)x^{n-1} + \lambda([a, x])x^{n-1}v = \lambda(a)x^n$ where we used $[a, x] \in [\mathfrak{g}, \mathfrak{g}]$ and inductive hypothesis in the second/third equalities (not respectively)

Corollary 1.14.3. $\mathfrak{g}$ *is solvable* $\iff$ $[\mathfrak{g},\mathfrak{g}]$ *is nilpotent.*

Proof. ($\leftarrow$) Say $[\mathfrak{g},\mathfrak{g}]$ is nilpotent, so it is solvable and $\mathfrak{g}/[\mathfrak{g},\mathfrak{g}]$ is also solvable (abelian even). This implies $\mathfrak{g}$ is solvable (this direction works in any characteristic).

($\rightarrow$) Now say $\mathfrak{g}$ is solvable. Then, $[\mathfrak{g},\mathfrak{g}]$ acts on $\mathfrak{g}$ by upper triangular matrices, which are moreover *strictly* upper triangular since $[x,x]=0$. Therefore, $[\mathfrak{g},\mathfrak{g}]$ acts on itself by strictly upper triangular matrices from which we can conclude that $[\mathfrak{g},\mathfrak{g}]$ is nilpotent (the matrices get even more strictly upper triangular as you commute them). ■

Example. Let $\mathfrak{g}=\langle x,y\,|[x,y]=y\rangle$ and $V=\langle v_1,\dots,v_p\rangle$ a vector space over a field k of characteristic $p>0$. Set $xv_j=jv_j$ and $yv_j=v_{j+1}$. Now form the **semi-direct product** $\widetilde{\mathfrak{g}}=\mathfrak{g}\ltimes V$ which is the vector space $\mathfrak{g}\oplus V$ with commutator

$$[(g_1,v_1),(g_2,v_2)]:=([g_1,g_2],g_1v_2-g_2v_1)\,.$$

This is a counterexample to both corollaries in positive characteristic. △

1.14.1 Engel's Theorem

Theorem 1.14.4. *Let $V\neq 0$ be a f.d. vector space over an arbitrary field k, and let $\mathfrak{g}\subset\mathfrak{gl}(V)$ be a Lie subalgebra consisting of nilpotent operators. Then, there exists a nonzero vector $n\in V$ such that $\mathfrak{g}v=0$.*

Proof. Induct on $\dim\mathfrak{g}$; the base case is trivial, so we may assume $\dim\mathfrak{g}>0$. We first seek an ideal $\mathfrak{h}\subset\mathfrak{g}$ of codimension 1. Take $\mathfrak{h}\subset\mathfrak{g}$ a maximal subalgebra (so $\mathfrak{h}\neq\mathfrak{g}$ and $\mathfrak{k}\supsetneq\mathfrak{h}\implies\mathfrak{k}=\mathfrak{g}$).

We claim that this $\mathfrak{h}$ is an ideal, and $\dim\mathfrak{g}/\mathfrak{h}=1$. For all $x\in\mathfrak{h}$, $\mathrm{ad}x:\mathfrak{g}/\mathfrak{h}\to\mathfrak{g}/\mathfrak{h}$ is nilpotent (since $\mathrm{ad}x:\mathfrak{g}\to\mathfrak{g}$ is nilpotent[8]). Now (by inductive assumption), there is some nonzero $\overline{a}\in\mathfrak{g}/\mathfrak{h}$ such that for all $x\in\mathfrak{h}$, $\mathrm{ad}x(\overline{a})=0$. Fix a preimage $a\in\mathfrak{g}$ of $\overline{a}$. This says that $[x,a]\in\mathfrak{h}$. Now let, $\mathfrak{h}'=\mathfrak{h}+ka$. This is a Lie subalgebra since $[\mathfrak{h},a]\subset\mathfrak{h}$, and also $\mathfrak{h}\subset\mathfrak{h}'$ is an ideal. Since $\mathfrak{h}$ was maximal, we must have $\mathfrak{h}'=\mathfrak{g}$, so $\mathfrak{h}\subset\mathfrak{g}$ is an ideal of codimension 1.

Now let $W=V^{\mathfrak{h}}$ be the $\mathfrak{h}$-invariants of V (i.e. $W=\{v\in V:\mathfrak{h}v=0\}$). By induction assumption $W\neq 0$ (since $\dim\mathfrak{h}<\dim\mathfrak{g}$). Recall that $\mathfrak{g}=\mathfrak{h}+ka$. For $w\in W$ and $x\in\mathfrak{h}$, we have

$$xaw=axw+\underbrace{[x,a]}_{\in\mathfrak{h}}w=0\implies aw\in W.$$

Thus, $W\subset V$ is a $\mathfrak{g}$-subrepresentation. Now fix $w\neq 0$ in W, and let r be the smallest integer such that $a^rw=0$ (exists because a acts nilpotently). Set $v:=a^{r-1}w\neq 0$. Then, $\mathfrak{h}v=0$ and $av=0$, so $\mathfrak{g}v=0$, and so we win. ■

Theorem 1.14.5 (Engel's Theorem). *A f.d. Lie algebra $\mathfrak{g}$ (still over an arbitrary field) is nilpotent iff for any $x\in\mathfrak{g}$, the operator $\mathrm{ad}x:\mathfrak{g}\to\mathfrak{g}$ is nilpotent.*

Proof. ($\rightarrow$) There exists n such that $[[x_1,x_2],\dots,x_n]=0$ for all $x_1,\dots,x_n\in\mathfrak{g}$ which implies $(\mathrm{ad}x)^{n-1}\mathfrak{g}=0$.

[8] $\mathrm{ad}x=\begin{pmatrix}\mathrm{ad}x|_{\mathfrak{h}} & *\\ 0 & \mathrm{ad}x|_{\mathfrak{g}/\mathfrak{h}}\end{pmatrix}$

(⟵) By theorem above, $\mathfrak{g}$ has a basis $a_1, \ldots, a_n$ in which $\mathrm{ad} x$ acts by strictly upper triangular matrices. Take $I_m = \langle a_1, \ldots, a_m \rangle$. Then, $[x, I_m] \subset I_{m-1}$ so $[x_1, [x_2, \ldots [x_n, x_{n+1}]]] = 0$ so $\mathfrak{g}$ is nilpotent. ■

1.14.2 Semisimple and simple Lie algebras, and also the radical

Proposition 1.14.6. *If $\mathfrak{g}$ is a f.d. Lie algebra, then $\mathfrak{g}$ has a unique maximal solvable ideal.*

Proof. Say $I_1, I_2 \subset \mathfrak{g}$ are solvable ideals. Then $I_1 + I_2 \subset \mathfrak{g}$ is also an ideal, and the nth isomorphism theorem says that

$n = 3?$

$$(I_1 + I_2)/I_1 = I_2/(I_1 \cap I_2) = \text{solvable}$$

so $I_1 + I_2$ is solvable (use I_1 solvable too). Thus, the sum of any finite set of solvable ideals is solvable. In fact, the sum of all solvable ideals is itself a solvable ideal (this sum is secretly finite since it has finite dimension). ■

Definition 1.14.7. The largest solvable ideal of $\mathfrak{g}$ is called the **radical** of $\mathfrak{g}$, and is denoted $\mathrm{rad}(\mathfrak{g})$. ◇

Definition 1.14.8. We say that $\mathfrak{g}$ is **semisimple** if $\mathrm{rad}(\mathfrak{g}) = 0$, i.e. if $\mathfrak{g}$ has no nonzero solvable ideals. ◇

Definition 1.14.9. $\mathfrak{g}$ is **simple** if it has no ideals other than 0 and $\mathfrak{g}$, and $\mathfrak{g}$ is not commutativie. ◇

This just excludes the abelian 1-dimensional Lie algebra

Remark 1.14.10. $\mathfrak{g}$ is simple $\iff$ its adjoint representation is irreducible and $\mathfrak{g}$ is not abelian. This is simply because a subrep of the adjoint rep is the same thing as an ideal. ○

Proposition 1.14.11. *Working with Lie algebras over some field k.*

(1) $\mathrm{rad}(\mathfrak{g} \oplus \mathfrak{h}) = \mathrm{rad}(\mathfrak{g}) \oplus \mathrm{rad}(\mathfrak{h})$. *In particular, semisimple Lie algebras are closed under direct sum.*

(2) A simple Lie algebra is semisimple. Hence, the direct sum of simple Lie algebras are semisimple, but not simple.

Proof. **(1)** Image of $\mathrm{rad}(\mathfrak{g} \oplus \mathfrak{h})$ in $\mathfrak{g}$ is a solvable ideal, so the image is contained in $\mathrm{rad}(\mathfrak{g})$ (and the same is true for $\mathfrak{h}$). Hence, $\mathrm{rad}(\mathfrak{g} \oplus \mathfrak{h}) \subset \mathrm{rad}(\mathfrak{g}) \oplus \mathrm{rad}(\mathfrak{h})$, but $\mathrm{rad}(\mathfrak{g}) \oplus \mathrm{rad}(\mathfrak{h})$ is solvable, so we get the opposite containment.

(2) The only nonzero ideal of $\mathfrak{g}$ is $\mathfrak{g}$, and $[\mathfrak{g}, \mathfrak{g}]$ is a nonzero ideal (since $\mathfrak{g}$ not commutative), so $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$. Hence, $\mathfrak{g}$ is not solvable, so $\mathrm{rad}\, \mathfrak{g} = 0$. ■

Remark 1.14.12. If $\mathfrak{g}$ is both solvable ($\mathrm{rad}\, \mathfrak{g} = \mathfrak{g}$) and semisimple ($\mathrm{rad}\, \mathfrak{g} = 0$), then $\mathfrak{g} = 0$. ○

Proposition 1.14.13. *The* ***semi-simplification*** $\mathfrak{g}_{ss} := \mathfrak{g}/\mathrm{rad}(\mathfrak{g})$ *is the largest semisimple quotient of $\mathfrak{g}$, i.e. if $I \subset \mathfrak{g}$ is an ideal such that $\mathfrak{g}/I$ is semisimple, then $I \supset \mathrm{rad}\, \mathfrak{g}$.*

Proof. Suppose $J \subset \mathfrak{g}/\mathrm{rad}\, \mathfrak{g}$ is a solvable ideal, and $\widetilde{J} \subset \mathfrak{g}$ is its preimage (so $\widetilde{J} \supset \mathrm{rad}\, \mathfrak{g}$). Then, $\widetilde{J}/\mathrm{rad}(\mathfrak{g}) = J$ is solvable as is $\mathrm{rad}(\mathfrak{g})$, so $\widetilde{J}$ is solvable, so $\widetilde{J} = \mathrm{rad}(\mathfrak{g})$, so $J = 0$. Hence, $\mathrm{rad}(\mathfrak{g}_{ss}) = 0$. The second part is left as an exercise. ■

Corollary 1.14.14. *We have a short exact sequence*

$$0 \longrightarrow \mathrm{rad}\, \mathfrak{g} \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}_{ss} \longrightarrow 0.$$

so every Lie algebra is the extension of a semisimple Lie algebra by a solvable Lie algebra.

Theorem 1.14.15 (Levi Decomposition Theorem). *In characteristic* 0 *(still don't need algebraically closed), the map* $\mathfrak{g} \to \mathfrak{g}_{ss}$ *splits (non-canonically), so* $\mathfrak{g} \cong \operatorname{rad}\mathfrak{g} \ltimes \mathfrak{g}_{ss}$.

Example. Consider $G =$ motions of $\mathbb{R}^3$ (in physics, **Galileo transformations**), so $G = \mathrm{SO}(3) \ltimes \mathbb{R}^3$ (rotations and translations). Then, $\mathfrak{g} = \operatorname{Lie} G = \mathfrak{so}(3) \ltimes \mathbb{R}^3$.

Claim 1.14.16. $\mathfrak{so}(3,k)$ *and* $\mathfrak{sl}(2,k)$ *are simple Lie algebras if* $\operatorname{char} k \neq 2$.

Then $\operatorname{rad}(\mathfrak{g}) = \mathbb{R}^3$ and $\mathfrak{g}_{ss} = \mathfrak{so}(3,\mathbb{R})$. △

1.15 Lecture 15 (10/22)

Last time we talked about the radical of a Lie algebra as well as (semi)simple Lie algebras.

Fix a field $k = \overline{k}$ of characteristic 0.

Proposition 1.15.1. *Let* $\mathfrak{g}$ *be a f.d. Lie algebra over* k *and* V *a f.d. irrep of* $\mathfrak{g}$. *Then,* $\operatorname{rad}(\mathfrak{g})$ *acts by scalars on* V, *so* $[\mathfrak{g}, \operatorname{rad}(\mathfrak{g})]$ *acts by zero.*

Since scalars are in the center

Proof. By Lie's theorem, there is a nonzero vector $v \in V$ along with some $\lambda \in \operatorname{rad}(\mathfrak{g})^\vee$ s.t. for any $a \in \operatorname{rad}(\mathfrak{g})$, $av = \lambda(a)v$. For any $x \in \mathfrak{g}$, set $\mathfrak{g}' = \operatorname{span}\{x, \operatorname{rad}(\mathfrak{g})\} \subset \mathfrak{g}$, a Lie subalgebra with the radical an ideal of codimension 1. By induction in n, as before,

$$ax^n v = \lambda(a)x^n v + \sum_{i=1}^{n} c_i x^{n-i} v$$

with $c_i \in k$.[9] Let $W = \operatorname{span}\{v, xv, x^2v, \dots\} \subset V$ also as before. We see that $W \subset V$ is a $\mathfrak{g}'$-subrep, and every $a \in \operatorname{rad}(\mathfrak{g})$ has a unique eigenvalue on W, which is $\lambda(a)$. Hence, $\lambda([x,a]) = 0$ since $\operatorname{tr}[x,a]|_W = \lambda([x,a]) \dim W = 0$ (and we're in characteristic 0). Hence,

Previous formula shows that $(a - \lambda(a))$ acts nilpotently since it decreases degree with each application

$$axv = xav + [a,x]v = xav + \lambda([a,x])v = xav = x\lambda(a)v = \lambda(a)xv.$$

So if $v \in V_\lambda$ (λ-eigenspace of $\operatorname{rad}(\mathfrak{g})$ in V), then $xv \in V_\lambda$ as well. Hence, $V_\lambda \subset V$ is a $\mathfrak{g}$-subrep. Since V is irreducible, this gives $V = V_\lambda$, so $\operatorname{rad}(\mathfrak{g})$ acts by scalars as claimed. ■

Definition 1.15.2. We say $\mathfrak{g}$ is **reductive** if $\operatorname{rad}(\mathfrak{g}) = \mathfrak{z}(\mathfrak{g})$, the center of $\mathfrak{g}$. This is equivalent to saying that $[\mathfrak{g}, \operatorname{rad}(\mathfrak{g})] = 0$ since we always have $\mathfrak{z}(\mathfrak{g}) \subset \operatorname{rad}(\mathfrak{g})$. ⋄

Remark 1.15.3. The Levi decomposition theorem implies that if $\mathfrak{g}$ is reductive, then $\mathfrak{g} = \mathfrak{g}_{ss} \oplus \mathfrak{z}(\mathfrak{g})$. (Usually get a semi-direct product with radical, but if the radical is the center then the action in the semi-direct product is trivial, so you just get a direct sum). ◦

Remark 1.15.4. Any abelian Lie algebra is reductive, any semisimple Lie algebra is reductive, and the direct sum of (finitely many) reductive Lie algebras is reductive. ◦

Looking at the two remarks above, one sees that Levi's theorem implies that any reductive Lie algebra is a direct sum of a semiseimple Lie algebra and an abelian Lie algebra. We will not use this, though, since we never proved Levi's theorem.

[9] $ax^n v = xax^{n-1}v + [a,x]x^{n-1}v$ and induct

1.15.1 Invariant inner products

Suppose that B is a bilinear form on a Lie algebra $\mathfrak{g}$.

Recall 1.15.5. B is $\mathfrak{g}$-invariant if

$$B([x,y],z)+B(y,[x,z])=0$$

which is the case iff

$$B([x,y],z)=B(x,[y,z]).$$

$\odot$

Example. If V is a finite dimensional representation of $\mathfrak{g}$, defined by $\rho:\mathfrak{g}\to\mathrm{End}(V)$, then

$$B_V(x,y)=\mathrm{tr}_V(\rho(x)\rho(y))$$

is a symmetric, $\mathfrak{g}$-invariant bilinear form. Symmetry and bilinearity are clear from niceties of trace. For invariance, observe that

$$\mathrm{tr}([x,y]z)=\mathrm{tr}(xyz-yxz)=\mathrm{tr}(xyz-xzy)=\mathrm{tr}(x[y,z]).$$

$\triangle$

This gives a large/useful class of invariant forms, but they can sometimes be degenerate or even 0. However, when they are aren't, they tell us stuff about our Lie algebra.

Proposition 1.15.6. *If B is a symmetric invariant bilinear form on $\mathfrak{g}$ and $I\subset\mathfrak{g}$ is an ideal, then*

$$I^{\perp}=\{a\in\mathfrak{g}:B(a,x)=0\,\forall x\in I\}\subset\mathfrak{g}$$

is also an ideal. In particular, $\ker B=\mathfrak{g}^{\perp}$ *is an ideal.*

Proof. Exercise. ∎

Remark 1.15.7. In general, $I\cap I^{\perp}$ can be nontrivial, and $I+I^{\perp}$ can be smaller than $\mathfrak{g}$. ∘

Proposition 1.15.8. *If B_V is non-degenerate for some representation $\rho:\mathfrak{g}\to\mathrm{End}(V)$ of $\mathfrak{g}$, then $\mathfrak{g}$ is reductive.*

Proof. Find a Jordan-Hölder series for V. Let

$$0=F^0V\subset F^1V\subset\cdots\subset F^nV=V$$

be a filtration of V by subreps with irreducible quotients, i.e. $V_i:=F^{i+1}V/F^iV$ is an irrep. Using a basis compatible with this filtration, elements of the Lie algebra will act via block upper-triangular matrices whose diagonal blocks correspond to $\mathfrak{g}$'s action on the V_i. Hence,

$$B_V(x,y)=\sum_{i=1}^{n}B_{V_i}(x,y).$$

So if $x \in [\mathfrak{g}, \mathrm{rad}(\mathfrak{g})]$, then it acts by 0 on each V_i, so $B_V(x,y) = 0$ for all $y \in \mathfrak{g}$ which means $x = 0$ by non-degeneracy. Hence, $[\mathfrak{g}, \mathrm{rad}(\mathfrak{g})] = 0$ so $\mathfrak{g}$ is reductive. ■

Example. $\mathfrak{g} = \mathfrak{gl}_n(k)$ and $V = k^n$ the usual representation. Then,

$$B_V(E_{ij}, E_{rs}) = \mathrm{tr}(E_{ij}E_{rs}) = \delta_{jr}\,\mathrm{tr}(E_{is}) = \delta_{jr}\delta is$$

so B_V is nondegenerate (dual basis of E_{ij} is E_{ji}). Thus, $\mathfrak{g}$ is reductive. If $\mathrm{char}\, k \nmid n$, then one can write (need $\mathrm{tr}(\mathrm{Id}) = n \neq 0 \in k$)

$$\mathfrak{gl}_n(k) = \mathfrak{sl}_n(k) \oplus k \cdot \mathrm{Id}$$

so $\mathfrak{sl}_n(K)$ is also reductive. In fact, $\mathfrak{sl}_n(k)$ is semisimple since $0 = \mathfrak{z}(\mathfrak{sl}_n(k)) = \mathrm{rad}(\mathfrak{sl}_n(k))$ (the center consists of traceless, scalar matrices).

In fact, not hard to check that $\mathfrak{sl}_n(k)$ is a simple Lie algebra in this case (for $n \geq 2$). This is an exercise (and gives another proof that $\mathfrak{sl}_n(k)$ is semisimple). △

Proposition 1.15.9. *All classical Lie algebras are reductive.*

Proof Sketch. Let V be a the standard matrix representation of $\mathfrak{g}$, and consider B_V. It's easy to see that it is nondegenerate (exercise). ■

Example. $\mathfrak{so}_n(K), \mathfrak{sp}_{2n}(K), \mathfrak{su}(p,q)$ all have trivial center and so are semisimple (need $n \geq 3$ in first case since $\mathfrak{so}_2(K)$ is abelian). This is an exercise.

In fact, these are all simple except for $\mathfrak{so}_4$. △

Which is maybe two copies of $\mathfrak{so}_3$

Example. The Lie algebra of upper triangular matrices of size $n \geq 2$ is not reductive. △

1.15.2 Killing form and Cartan Criteria

"We don't kill anybody here. This is the last name of a German mathematician who worked on this subject" (paraphrase)

All Lie algebras have an adjoint representation, so we can consider its associated bilinear form.

Definition 1.15.10. The **Killing form** of $\mathfrak{g}$ is the form

$$B_{\mathfrak{g}}(x,y) = \mathrm{tr}(\mathrm{ad}x \cdot \mathrm{ad}y).$$

We often denote it by $K_{\mathfrak{g}}(x,y)$ or by $K(x,y)$. ◇

Lemma 1.15.11. *If $I \subset \mathfrak{g}$ is an ideal, then $K_I = K_{\mathfrak{g}}|_I$.*

Proof. Write $\mathfrak{g} = I \oplus V$ and note that $\mathrm{ad}x(V) \subset I$, so $\mathrm{ad}x$ will be a block-upper triangular matrix with bottom-right block equal to 0. ■

Theorem 1.15.12 (**Cartan criterion of solvability**)**.** *A f.d. Lie algebra $\mathfrak{g}$ over k of characteristic* 0 *is solvable iff*

$$[\mathfrak{g}, \mathfrak{g}] \subset \ker K,$$

i.e. $K([\mathfrak{g}, \mathfrak{g}], \mathfrak{g}) = 0$.

Theorem 1.15.13 (**Cartan criterion of semisimplicity**). *A f.d. Lie algebra $\mathfrak{g}$ over k of characteristic 0 is semisimple iff K is nondegenerate.*

Remark 1.15.14. These may not always be so useful in practice, but they are important in theoretical considerations. ○

These theorem are not obvious, so we will have to work to prove them. We'll need Jordan decomposition from linear algebra.

Jordan Decomposition Let's do some linear algebra real quick.

Proposition 1.15.15 (**Jordan Decomposition**). *A square matrix $A \in \mathfrak{gl}_N(k)$ over k of characteristic 0 can be uniquely written as*

$$A = A_s + A_n \quad \text{with} \quad A_s, A_n \in \mathfrak{gl}_N(k)$$

so that A_s is ***semisimple*** *(diagonalizable over $\overline{k}$), A_n is nilpotent, and $A_sA_n = A_nA_s$.*[10] *Moreover, there is a polynomial $P \in k[x]$ such that $A_s = P(A)$.*

This is just putting the matrix in Jordan normal form and then taking A_s to be the diagonal, right? Yes. See a couple remarks down

Proof. By Chinese remainder theorem, there exists $P \in \overline{k}[x]$ s.t. for every eigenvalue λ of A, $P(x) \equiv \lambda \mod (x-\lambda)^N$. Note that this just means $P(x)-\lambda = (x-\lambda)^N Q_\lambda(x)$. Hence, $P(A)-\lambda = (A-\lambda)^N Q_\lambda(A) = 0$ on the generalized eigenspace $V(\lambda) \subset V$ of A. Thus, $A_s = P(A)|_{V(\lambda)} = \lambda \cdot \mathrm{Id}$ so A_s is semisimple. The different $A - A_s = A_n$ is nilpotent since it only has 0 eigenvalues. Finally, $A_sA_n = A_nA_s$ since A_s acts by a scalar on $V(\lambda)$. This gives the construction.

I got distracted while he was going over this, so I may have missed some of the things he said, but didn't write

Why is this unique? Suppose also that $A = A_s' + A_n'$. Then, A_s', A_n' commute with A and so with $A_s = P(A)$ and also with $A_n = A - A_s$. Now write

$$A_s + A_n = A_s' + A_n' \iff A_s - A_s' = A_n' - A_n$$

with the RHS nilpotent (sum of commuting nilpotent operators) and LHS semisimple (sum of commuting semisimple operators), so both sides are nilpotent and semisimple, i.e. both sides are 0. This gives uniqueness.

We are still not done yet. We need to show that $A_s, A_n \in \mathfrak{gl}_N(k)$, i.e. that they have entries in k. If $g \in \mathrm{Gal}(\overline{k}/k)$, then $g \cdot A_s = A_s$ and $g \cdot A_n = A_n$ by uniqueness, so A_s, A_n have entries in k. ■

Remark 1.15.16. We use characteristic 0 to get that $\overline{k}/k$ is Galois in previous proof. Hence, the same proof works over any perfect field. ○

Example. Consider $k = \mathbb{F}_p(t)$. One can construct a matrix[11] A such that $A^p = t$, so its eigenvalues are all equal to $t^{1/p}$. Hence, $A_s = t^{1/p}\,\mathrm{Id}$ so A_s does not have entries in k. △

Remark 1.15.17. If k is already algebraically closed, then there exists a basis in which A is upper triangular. In this case, A_s is diagonal part and A_n is off diagonal part. ○

[10] This gives uniqueness. Otherwise take a random nilpotent matrix and subtract it from A; the result is probably semisimple

[11] Take $p \times p$ matrix with 1's on the superdiagonal and a t in the bottom left, e.g.

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ t & 0 & 0 \end{pmatrix}$$

when $k = \mathbb{F}_3(t)$

Proof of Cartan's criteria First note that we may assume $k = \overline{k}$ is algebraically closed. This exactly preserves solvability.

I did not do the best job organizing these notes. Oh well

Proof of "Only if" direction of Theorem 1.15.12. ($\rightarrow$) If $\mathfrak{g}$ is solvable, then Lie's theorem gives a basis of $\mathfrak{g}$ in which $\mathrm{ad}x$ are upper triangular, strictly so if $x \in [\mathfrak{g},\mathfrak{g}]$. Thus, $[\mathfrak{g},\mathfrak{g}] \subset \ker K_{\mathfrak{g}}$ since the product of an upper triangular matrix and a strictly upper triangular matrix is a strictly upper triangular matrix (which then has trace 0). ∎

The other direction is more involved. We'll need to following lemma.

Lemma 1.15.18. *Let $\mathfrak{g} \subset \mathfrak{gl}(V)$ be a Lie subalgebra such that for all $x \in [\mathfrak{g},\mathfrak{g}]$ and $y \in \mathfrak{g}$, we have $\mathrm{tr}(xy) = 0$. Then, $\mathfrak{g}$ is solvable.*

Proof. Let $x \in [\mathfrak{g},\mathfrak{g}]$. We want to show that it is nilpotent, i.e. its eigenvalues are all 0. Let $\lambda_i \in k = \overline{k}$ be the eigenvalues of x. Let $E \subset k$ be the $\mathbb{Q}$-span of λ_i. Assume that $\lambda_m \notin \mathrm{span}\{\lambda_1, \dots, \lambda_{m-1}\}$ for some $m \geq 1$.

We're running out of time, so we'll just prove this next time... ∎

Taking the above lemma for granted, we can now prove the other direction.

Proof of "If" direction of Theorem 1.15.12. Replace $\mathfrak{g}$ with $\mathrm{ad}(\mathfrak{g}) = \mathfrak{g}/\mathfrak{z}(\mathfrak{g})$ and take $V = \mathfrak{g}$. The lemma then tells us that $\mathfrak{g}/\mathfrak{z}(\mathfrak{g})$ is solvable. Since $\mathfrak{z}(\mathfrak{g})$ is abelian, this then tells us that $\mathfrak{g}$ itself is solvable. ∎

What about semisimplicity? May no long assume $k = \overline{k}$, but this is fine since we know solvability criterion over any field (with $\mathrm{char}\, k = 0$).

Proof of Theorem 1.15.13. ($\rightarrow$) Say $\mathfrak{g}$ is semisimple, and let $I = \ker K_{\mathfrak{g}}$. We know that $K_I = K_{\mathfrak{g}}|_I = 0$, so Carton solvability criterion tells us that I is solvable. But I is also semisimple (since $\mathfrak{g}$ is), so $I = 0$ which makes $K_{\mathfrak{g}}$ nondegenerate.

($\leftarrow$) Now assume $K_{\mathfrak{g}}$ is non-degenerate. Then, $\mathfrak{g}$ is reductive by an earlier theorem. Furthermore $\mathfrak{z}(\mathfrak{g}) \subset \ker K_{\mathfrak{g}} = 0$, so $\mathfrak{g}$ is in fact semisimple. ∎

1.15.3 Consequences of Cartan's criteria

Fix k field of characteristic 0.

Corollary 1.15.19. *$\mathfrak{g}$ is semisimple $\iff$ $\mathfrak{g} \otimes_k \overline{k}$ is semisimple.*

Remark 1.15.20. This is *not* true with simple in place of semisimple. For example $\mathfrak{g}$ simple over $\mathbb{C}$ (like $\mathfrak{sl}_n(\mathbb{C})$) regarded as a real Lie algebra has $\mathfrak{g}_{\mathbb{C}} = \mathfrak{g} \oplus \mathfrak{g}$ which is semisimple but not simple. ○

1.16 Lecture 16 (10/27)

We had a lemma last time whose proof we didn't get to.

Lemma 1.16.1. *Let $\mathfrak{g} \subset \mathfrak{gl}(V)$ be a Lie subalgebra such that for all $x \in [\mathfrak{g},\mathfrak{g}]$ and $y \in \mathfrak{g}$, we have $\mathrm{tr}(xy) = 0$. Then, $\mathfrak{g}$ is solvable.*

Proof. Take $x \in [\mathfrak{g}, \mathfrak{g}]$, let λ_i be the distinct eigenvalues of x on V, for $i = 1, \ldots, m$. We want to show that $m = 1$ and $\lambda_1 = 0$, so x is nilpotent. It then follows that $[\mathfrak{g}, \mathfrak{g}]$ is nilpotent by Engel, so $\mathfrak{g}$ is solvable.

I really need to remember all these named theorems/lemmas we have

Let $E \subset k$ be the $\mathbb{Q}$-span of λ_i, and let $b : E \to \mathbb{Q}$ be a linear function. Then, there exists an interpolation polynomial Q such that

$$Q(\lambda_i - \lambda_j) = b(\lambda_i - \lambda_j) = b(\lambda_i) - b(\lambda_j)$$

for all i, j. By Jordan decomposition, we can write $x = x_s + x_n$. Note that $\mathrm{ad} x_s$ is diagonalizable on $\operatorname{End} V$ with eigenvalues $\lambda_i - \lambda_j$. This is because $V = \bigoplus V_{\lambda_i}$ and given $a : V_{\lambda_i} \to V_{\lambda_j}$, we have

$$[x_s, a] = x_s a - a x_s = (\lambda_j - \lambda_i) a.$$

Hence, $Q(\mathrm{ad} x_s)$ has eigenvalues $Q(\lambda_i - \lambda_j) = b(\lambda_i) - b(\lambda_j)$ on the same spaces. Thus, $Q(\mathrm{ad} x_s) = \mathrm{ad} b$ where $b : V \to V$ such that $b|_{V_{\lambda_i}} = b(\lambda_i)$, i.e. $Q(\mathrm{ad} x_s) \cdot a = ba - ab = [b, a]$. We also have $\mathrm{ad} x = \mathrm{ad} x_s + \mathrm{ad} x_n$ with $\mathrm{ad} x_s$ semisimple, $\mathrm{ad} x_n$ nilpotent, and the two of them commuting. Hence, this is the Jordan decomposition, so $\mathrm{ad} x_s = (\mathrm{ad} x)_s = P(\mathrm{ad} x)$ for some polynomial P s.t. $P(0) = 0$ since 0 is an eigenvalue of $\mathrm{ad} x$ (e.g. $\mathrm{ad} x . x = [x, x] = 0$). Note that $Q(0) = Q(\lambda_i - \lambda_i) = b(\lambda_i) - b(\lambda_i) = 0$ as well. Thus we get

Note that b may not lie in $\mathfrak{g}$, it's just some operator $V \to V$

$$\mathrm{ad} b = R(\mathrm{ad} x) \text{ where } R(t) = Q(P(t)) \text{ and } R(0) = 0.$$

We know $x \in [\mathfrak{g}, \mathfrak{g}]$, so let us write

$$x = \sum_i [y_i, z_i] \text{ with } y_i, z_i \in \mathfrak{g}.$$

Then,

$$\operatorname{Tr}(b \cdot x) = \sum_i \operatorname{Tr}(b[y_i, z_i]) = \sum_i \operatorname{Tr}([b, y_i] z_i) = \sum_i \operatorname{Tr}(R(\mathrm{ad} x)(y_i) \cdot z_i) = 0.$$

Since $R(0) = 0$, R has no constant term so $R(\alpha x)(y_i) \in [\mathfrak{g}, \mathfrak{g}]$ whence the last equality above. On the other hand, $V = \bigoplus_i V_{\lambda_i}$ is a direct sum of its generalized eigenspaces and b acts by a scalar on them, so

$$\operatorname{Tr}(bx) = \sum_i \operatorname{Tr}\left(bx|_{V_{\lambda_i}}\right) = \sum_i b(\lambda_i) \operatorname{Tr}\left(x|_{V_{\lambda_i}}\right) = \sum_i \dim V_{\lambda_i} b(\lambda_i) \lambda_i \in E$$

which we now know must be 0. The above is an element of our $\mathbb{Q}$-vector space E, so we can apply b to both sides to get

$$\sum_i \dim V_{\lambda_i} b(\lambda_i)^2 = 0.$$

Finally, this is a sum of non-negative numbers equalling 0, so we must have $b(\lambda_i) = 0$ for all i, so $b = 0$. Since b was an arbitrary linear functional $E \to \mathbb{Q}$, this implies that $E = 0$ which is only possible if $m = 1$ and $\lambda_1 = 0$ as claimed. We then win by Engel. ■

Remark 1.16.2. The book has a slightly different argument which works over $\mathbb{C}$, but the one above works over any field of characteristic 0. ∘

1.16.1 Properties of semi-simple Lie algebras

Unless otherwise state, assume throughout that char $k = 0$.

Recall 1.16.3. $\mathfrak{g}$ is semisimple (s.s.) iff $\mathfrak{g} \otimes_k \overline{k}$ is s.s. This is not the case for simple. $\odot$

Proposition 1.16.4. *Let $\mathfrak{g}$ be a semisimple Lie algebra with $I \subset \mathfrak{g}$ an ideal. Then there exists an ideal $J \subset \mathfrak{g}$ such that $\mathfrak{g} = I \oplus J$ as Lie algebras (in particular, $[I, J] = 0$).*

Proof. Let $I^\perp$ be the orthocomplement of I w.r.t. the Killing form of $\mathfrak{g}$. This is an ideal, and $I \cap I^\perp$ is an ideal with trivial Killing form. Thus, Cartan tells us that $I \cap I^\perp$ is solvable, so $I \cap I^\perp = 0$ since $\mathfrak{g}$ is semisimple (has no solvable subalgebras). Thus, $\mathfrak{g} = I \oplus I^\perp$ and $[I, I^\perp] \subset I \cap I^\perp = 0$, so this is a Lie algebra direct sum. ∎

We will in fact soon see that J above is unique, i.e. $J = I^\perp$ is the only choice.

Corollary 1.16.5. *$\mathfrak{g}$ is a semisimple if and only if $\mathfrak{g}$ is a direct sum of simple Lie algebras.*

Proof. Induct on $\dim \mathfrak{g}$ and apply proposition. ∎

Corollary 1.16.6. *If $\mathfrak{g}$ is semisimple, then $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$.*

Proof. This is true when $\mathfrak{g}$ is simple since it is non-abelian. In the general case,

$$\mathfrak{g} = \bigoplus_i \mathfrak{g}_i \implies [\mathfrak{g}, \mathfrak{g}] = \bigoplus_i [\mathfrak{g}_i, \mathfrak{g}_i] = \bigoplus_i \mathfrak{g}_i = \mathfrak{g}$$

where each $\mathfrak{g}_i$ simple. ∎

Corollary 1.16.7. *If $\mathfrak{g} = \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_k$ is a semisimple Lie algebra with $\mathfrak{g}_i$ simple, then all ideals in $\mathfrak{g}$ are of the form $I_s := \bigoplus_{i \in S} \mathfrak{g}_i$ where $S \subset \{1, \dots, k\}$.*

Proof. Induct on the number k of summands. Base is trivial. Let $I \subset \mathfrak{g}$ be an ideal, and suppose there exists an i such that ith projection $p_i : I \to \mathfrak{g}_i$ is zero. WLOG, may assume $i = k$, so $p_k : I \to \mathfrak{g}_k$ is zero. Then, $I \subset \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_{k-1}$, so we win by induction assumption. Otherwise, $p_i : I \to \mathfrak{g}_i$ is nonzero for all i. Then, $p_i(I) = \mathfrak{g}_i$ since it is a nonzero ideal in a simple Lie algebra, so $[\mathfrak{g}_i, I] = [\mathfrak{g}_i, \mathfrak{p}_i(I)] = \mathfrak{g}_i$ but this means $\mathfrak{g}_i \subset I$ for all i, so $\mathfrak{g} = \bigoplus_i \mathfrak{g}_i \subset I \implies I = \mathfrak{g}$. ∎

Corollary 1.16.8. *An ideal or quotient of a semisimple Lie algebra is itself semisimple.*

1.16.2 Derivations of a Lie algebra

Definition 1.16.9. Let $\mathfrak{g}$ be a Lie algebra. Then, $\operatorname{Der} \mathfrak{g}$ is the Lie algebra of **derivations** of $\mathfrak{g}$, i.e. linear maps $d : \mathfrak{g} \to \mathfrak{g}$ s.t.

$$d[x, y] = [dx, y] + [x, dy].$$

$\diamond$

We have a homomorphism $\operatorname{ad} : \mathfrak{g} \to \operatorname{Der} \mathfrak{g}$ where, as usual, $\operatorname{ad} x(y) = [x, y]$. The kernel of this map is $\ker(\operatorname{ad}) = \mathfrak{z}(\mathfrak{g})$, the center of $\mathfrak{g}$. Hence, if $\mathfrak{z}(\mathfrak{g}) = 0$, then $\operatorname{ad} : \mathfrak{g} \hookrightarrow \operatorname{Der}(\mathfrak{g})$, so $\mathfrak{g}$ is a Lie subalgebra of $\operatorname{Der}(\mathfrak{g})$. In fact, it is also an ideal. This is because

$$[d, \operatorname{ad} x](y) = d[x, y] - [x, dy] = [dx, y] = \operatorname{ad}(dx).y \implies [d, \operatorname{ad} x] = \operatorname{ad}(dx).$$

Proposition 1.16.10. *If $\mathfrak{g}$ is semisimple, then $\mathfrak{g} = \mathrm{Der}(\mathfrak{g})$, i.e.*

Remember: $\mathfrak{z}(\mathfrak{g}) = 0$ if $\mathfrak{g}$ is semisimple

$$\text{“}\textit{all derivations are inner}\text{”}.$$

Proof. Consider invariant symmetric bilinear form on $\mathrm{Der}(\mathfrak{g})$ given by

$$K(a, b) = \mathrm{tr}_{\mathfrak{g}}(a \cdot b).$$

This is an extension of the Killing form on $\mathfrak{g}$. Hence, $K|_{\mathfrak{g}}$ is non-degenerate by Cartan's criterion. Let $I = \mathfrak{g}^{\perp} \subset \mathrm{Der}(\mathfrak{g})$ under K. This is an ideal such that $I \cap \mathfrak{g} = 0$. Thus, we get a direct sum decomposition $\mathrm{Der}(\mathfrak{g}) = \mathfrak{g} \oplus I$ as Lie algebras. So for any $d \in I$ and $x \in \mathfrak{g}$, we have

$$[d, \mathrm{ad}x] = \mathrm{ad}(dx) = 0 \implies dx = 0 \implies d = 0 \implies I = 0$$

with first implication since $\mathfrak{z}(\mathfrak{g}) = 0$. Thus, $\mathrm{Der}\,\mathfrak{g} = \mathfrak{g}$. ■

1.16.3 Complete reducibility of representations

Our main goal is the following theorem.

Theorem 1.16.11. *If $\mathfrak{g}$ is semisimple over k of characteristic 0, then any finite dimensional representation of $\mathfrak{g}$ is completely reducible, i.e. a direct sum of irreps.*

There are many different proofs with the first due to Hermann Weyl. He noticed that if you have a complex semisimple Lie algebra, then it is the complexification of the Lie algebra of a compact Lie group, and complete irreducibility of representations of compact Lie groups is easy. We may discuss this proof next semester.

Today, we discuss a purely algebraic proof which is based on the theory of extensions of representations.

Let $\mathfrak{g}$ be a Lie algebra, and let W, U be (possibly infinite dimensional) representations of $\mathfrak{g}$.

Definition 1.16.12. An **extension** of W by U is a representation V sitting in a short exact sequence

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0.$$

In other words, we have a 2-step filtration of V by subreps s.t. $F_0V = U$ and $F_1U = V$ with graded piece $F_1V/F_0V = W$. A **trivial extension** if one of the form

$$0 \longrightarrow U \longrightarrow U \oplus W \longrightarrow W \longrightarrow 0.$$

◇

Remark 1.16.13. An extension is trivial if it is split. ○

The complete reducibility theorem is equivalent to saying that any short exact sequence

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

splits, i.e. any extension of W by U is trivial.

If we end up saying the word Ext in this class, I'm gonna be so

This leads to the question: how do we classify extensions?

Well, a priori, an extension is not split as a sequence of representations, but it is as a sequence of vector spaces. Given

$$0 \longrightarrow U \xrightarrow{j} V \xrightarrow{p} W \longrightarrow 0,$$

let $i : W \to V$ be a linear (potentially non-equivariant) splitting. We still have $\widetilde{i} : U \oplus W \longrightarrow V$ given by $\widetilde{i}(u,w)u + i(w)$ which is a linear isomophism, but probably not a map of representations. We can still use it to transfer the action of $\mathfrak{g}$ from V to $V \oplus W$. We get

$$x(u,w) = (xu + a(x)w, xw)$$

where $a : \mathfrak{g} \to \mathrm{Hom}_k(W,U)$. What is the condition for a to give rise to a representation?

$$[x,y](u,w) = ([x,y]u + a([x,y])w, [x,y]w) \text{ and } xy(u,w) - yx(u,w) = ([x,y]u + ([x,a(y)] + [a(x),y])\, w, [x,y]w)$$

so the condition is

$$a([x,y]) = [x,a(y)] + [a(x),y] = [x,a(y)] - [y,a(x)].$$

This is a special case of a more general situation. When E is a representation of $\mathfrak{g}$ and $a : \mathfrak{g} \to E$ is a linear map, we call a a **1-cocycle of $\mathfrak{g}$ with coefficients in** E if

$$a([x,y]) = x \circ a(y) - y \circ a(x).$$

We denote the space of such cocycles by $Z^1(\mathfrak{g}, E)$.[12]

I was wrong. We're not thinking in terms of Ext, but in terms of Lie algebra cohomology. These will agree, but its a difference in perspectives

In our setting, we are looking at $a \in Z^1(\mathfrak{g}, \mathrm{Hom}_k(W,U))$. When do $a, b \in Z^1$ define isomorphic extensions? When does a define a trivial extension? we have $a \in Z^1$ giving rise to

$$0 \longrightarrow U \longrightarrow V_a \longrightarrow W \longrightarrow 0.$$

When $V_a \cong V_b$ as extensions, we have $f : V_a \to V_b$ a homomorphism of representations s.t. $\mathrm{gr}(f) : \mathrm{gr}(V_a) \to \mathrm{gr}(V_b)$ is the identity (note $\mathrm{gr}(V_a) = V \oplus W$ using natural filtration), so $f(u,w) = (u + Aw, w)$ with $A : W \to U$ a linear map. Note that

$$xf(u,w) = x(u+Aw,w) = (xu+xAw+b(x)w, xw) \text{ and } fx(u,w) = f(xu+a(x)w, xw) = (xu+a(x)w+Axw, xw)$$

so f is a homomorphism exactly when

$$xA + b(x) = Ax + a(x) \iff [x,A] = a(x) - b(x).$$

In particular, taking $b = 0$, we see that V_a is trivial iff

$$a(x) = [x,A] \text{ for some } A : W \to U.$$

Again, this is a special case of a more general setting. For E a representation of $\mathfrak{g}$ and $v \in E$, the

[12]Extensions split as vector spaces in bijection with $\mathrm{H}^1(\mathfrak{g}, \mathrm{Hom}(W,U))$. This was (basically) a Taylor problem

1-coboundary of $v \in E$ is the linear map

$$a : \begin{array}{ccc} \mathfrak{g} & \longrightarrow & E \\ x & \longmapsto & xv \end{array}.$$

Any 1-coboundary is a 1-cocycle, and the space of 1-coboundaries is denoted $B^1(\mathfrak{g}, E) \subset Z^1(\mathfrak{g}, E)$.

We have shown that $V_a \cong V_b$ as extensions iff $a - b \in B^1(\mathfrak{g}, \mathrm{Hom}_k(W, V))$. Thus, we've shown that extensions are bijection with

$$\mathrm{Ext}^1(W, V) := \frac{Z^1(\mathfrak{g}, \mathrm{Hom}_k(W, U))}{B^1(\mathfrak{g}, \mathrm{Hom}_k(W, U)}.$$

I'm so shocked.

In general,

$$\mathrm{H}^1(\mathfrak{g}, E) = \frac{Z^1(\mathfrak{g}, E)}{B^1(\mathfrak{g}, E)}$$

is the **first cohomology of $\mathfrak{g}$ with coefficients in** E (one can define higher cohomology groups).

Proposition 1.16.14. *Extensions of W by U, up to isom of extensions, are classified by*

$$\mathrm{Ext}^1(W, U) \simeq \mathrm{H}^1(\mathfrak{g}, \mathrm{Hom}_k(W, U)).$$

Thus, the theorem we will prove next time is

Theorem 1.16.15. *If $\mathfrak{g}$ is semisimple and V is a f.d. representation of $\mathfrak{g}$, then $\mathrm{H}^1(\mathfrak{g}, V) = 0$. In particular,* $\mathrm{Ext}^1(W, U) = 0$.

This directly implies complete reducibility.

1.17 Lecture 17 (10/29)

1.17.1 Complete reducibility of representations, Continued

Our goal is to prove

Theorem 1.17.1. *If $\mathfrak{g}$ semisimple over a field of characteristic 0 with a f.d. rep V, then* $\mathrm{H}^1(\mathfrak{g}, V) = 0$. *In particular,*

$$\mathrm{Ext}^1(W, U) = \mathrm{Hom}^1(\mathfrak{g}, \mathrm{Hom}_k(W, U)) = 0$$

is trivial.

In general, when talking about semisimple Lie algebras, we always assume characteristic 0 unless otherwise stated

This immediately implies the complete reducibility of representations of semisimple Lie algebras.

Given an extension

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

of W by U, we get a class $[V] \in \mathrm{Ext}^1(W, U) = \mathrm{Hom}^1(\mathfrak{g}, \mathrm{Hom}_k(W, U))$. Furthermore, $[V] = 0 \iff V \cong U \oplus W$ as extensions.

Lemma 1.17.2. *Let E be a representation of $\mathfrak{g}$, and let $C \in U(\mathfrak{g})$ be central so that*

$$C|_k = 0 \text{ and } C|_E = \lambda \cdot \mathrm{Id}\ (\lambda \neq 0),$$

then $\mathrm{H}^1(\mathfrak{g}, E) = 0$ *(*$= \mathrm{Ext}^1(k, E)$*).*

Note: a representation can always be split into generalized Eigenspaces

Proof. Need to show any extension

$$0 \longrightarrow E \longrightarrow V \longrightarrow k \longrightarrow 0$$

of k by E splits. We claim $\exists! v \in V$ such that $p(v) = 1$ and $Cv = 0$. Indeed, pick any $w \in V$ s.t. $p(w) = 1$; then $Cw \in E$ since p is equivariant. Now set $v = w - \lambda^{-1}Cw$, so $Cv = Cw - \lambda^{-1}C^2w = Cx - \lambda^{-1}\lambda Cw = 0$ (C acts on $Cw \in E$ by λ). This gives existence of v. For uniqueness, with v' has the same property, then

$$v - v' \in E \implies 0 = C(v - v') = \lambda(v - v') \implies v = v'.$$

Now consider the space $kv \subset V$, a complement of E invariant under $\mathfrak{g}$. Indeed, given $x \in \mathfrak{g}$, one has

$$C(xv) = xCv = 0 \implies xv \in kv$$

with the implication coming from uniqueness of v. Thus, $V = E \oplus k \cdot v$ and we win. ∎

Lemma 1.17.3. *Let $\mathfrak{g}$ be semisimple in char 0 and V a nontrivial finite dimensional irrep of $\mathfrak{g}$. Then, there exists a central element $C \in U(\mathfrak{g})$ such that $C|_k = 0$ and $C|_V = \lambda \operatorname{Id}$ with $\lambda \neq 0$.*

Proof. Consider the invariant symmetric bilinear form

$$B_V(x, y) = \operatorname{tr}_v(xy)$$

on $\mathfrak{g}$. We claim that $B_V \neq 0$. Indeed, let $\bar{\mathfrak{g}} \subset \mathfrak{gl}(V)$ be the image of $\mathfrak{g}$ (so $\bar{\mathfrak{g}}$ is semisimple). We have $[\bar{\mathfrak{g}}, \bar{\mathfrak{g}}] = \bar{\mathfrak{g}}$ and B_V is an invariant form on $\bar{\mathfrak{g}}$. By Lemma 1.16.1, if $B_V = 0$, we would have $\bar{\mathfrak{g}}$ solvable which would then mean $\bar{\mathfrak{g}} = 0$, which would then mean that V is trivial. However, V is not trivial.

Now let $I = \ker B_V$, so $I \subset \mathfrak{g}$ is an ideal, and we can write $\mathfrak{g} = I \oplus \mathfrak{g}'$ for some semisimple $\mathfrak{g}'$ with B_V nondegenerate (since complement of I). Let x_i be a basis of $\mathfrak{g}'$ with dual basis $x^i \in \mathfrak{g}'$ under B_V. Let $C = \sum_i x_i x^i = m(\Omega)$ with

$$\Omega = \sum_i x_i \otimes x^i \in \mathfrak{g}' \otimes \mathfrak{g}'$$

independent of the choice of basis.[13] Since B_V is invariant, Ω is too, so for all $y \in \mathfrak{g}$, we have

$$\sum \left([y, x_i] \otimes x^i + x_i \otimes [y, x^i] \right) = 0.$$

This implies that C is central since

$$[y, \sum x_i x^i] = \sum [y, x_i] x^i + x_i [y, x^i] = 0.$$

Now, we clearly have $C|_k = 0$ since all x_i act by 0 on the trivial representation. We want to show $C|_V = \lambda \operatorname{Id}$. Note that

$$\operatorname{Tr}|_V C = \dim V \cdot \lambda = \sum_i \operatorname{Tr}|_V (x_i x^i) = \sum_i B_V(x_i, x^i) = \dim \mathfrak{g}'$$

[13] It's the identity element of $\mathfrak{g}' \otimes \mathfrak{g}' \simeq \mathfrak{g}' \otimes (\mathfrak{g}')^\vee = \operatorname{Hom}_k(\mathfrak{g}, \mathfrak{g})$

so $\lambda = \dim \mathfrak{g}' / \dim V \neq 0$. ■

The two lemmas above imply that $\mathrm{H}^1(\mathfrak{g}, V) = 0$ for all irred f.g. representations V (when $\mathfrak{g}$ semisimple). They do so directly for $V \neq k$. When $V = k$, $\mathrm{H}^1(\mathfrak{g}, k) = \mathfrak{g}/[\mathfrak{g}, \mathfrak{g}] = 0$. To finish the proof of Theorem 1.17.1, we use the following.

Claim 1.17.4. *If $0 \to U \to V \to W \to 0$ is a short exact sequence and $\mathrm{H}^1(\mathfrak{g}, U) = 0 = \mathrm{H}^1(\mathfrak{g}, W)$, then $\mathrm{H}^1(\mathfrak{g}, V) = 0$.*

Proof. Indeed, we have maps

$$\mathrm{H}^1(\mathfrak{g}, U) \xrightarrow{\gamma} \mathrm{H}^1(\mathfrak{g}, V) \xrightarrow{p} \mathrm{H}^1(\mathfrak{g}, W)$$

(if it helps, think of these as cocycles/coboundaries). We claim this sequence is exact (it's clear the composition is 0 so only need $\ker p \subset \operatorname{im} \gamma$). Now suppose we have $\alpha \in \mathrm{H}^1(\mathfrak{g}, V)$ with $p(\alpha) = 0$. Then, $\alpha = [\widetilde{\alpha}]$ for some cocycle $\widetilde{\alpha} \in Z^1(\mathfrak{g}, V)$ and the projection $p(\widetilde{\alpha})$ is a coboundary:

$$p(\widetilde{\alpha})(x) = xw$$

for some $w \in W$. Pick $\widetilde{w} \in V$ projecting to w. Let

$$\widetilde{\alpha}'(x) = \widetilde{\alpha}(x) - x\widetilde{w}$$

so $p(\widetilde{\alpha}') = 0 \implies \widetilde{\alpha}' : \mathfrak{g} \to U$ and is of course a cocycle. Thus, $\alpha = \gamma(\widetilde{\alpha}')$, so $\ker p = \operatorname{im} \gamma$.

Exactness of this sequence gives the claim. ■

With that, we have proven Theorem 1.16.11 (every f.d. rep has a filtration by subreps with irreducible quotients. Induct).

Corollary 1.17.5 (of Theorem 1.16.11)**.** *Any reductive Lie algebra $\mathfrak{g}$ (over a field of characteristic 0) is a direct sum of a semisimple Lie algebra with an abelian Lie algebra (in a unique way).*

Proof. Let $\mathfrak{g}' = \mathfrak{g}/\mathfrak{z}(\mathfrak{g}) = \mathfrak{g}/\operatorname{rad}(\mathfrak{g})$, so we have

$$0 \longrightarrow \mathfrak{z}(\mathfrak{g}) \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}' \longrightarrow 0.$$

This is actually a sequence of representations of $\mathfrak{g}'$ which is semisimple, so this extension splits. This gives $\mathfrak{g} = \mathfrak{z}(\mathfrak{g}) \oplus \mathfrak{g}'$ as $\mathfrak{g}'$-modules (under adjoint action) so as ideals. Thus, we have existence.

Uniqueness is easy (exercise). ■

Remark 1.17.6. We proved this fact earlier as a consequence of Levi decomposition, but we never proved Levi decomposition. ○

Example. $\mathfrak{gl}_n(k) = k \oplus \mathfrak{sl}_n(k)$ when $\operatorname{char} k = 0$. △

1.17.2 Semisimple elements

Let $\mathfrak{g}$ be any f.d. Lie algebra over $k = \overline{k}$ (no assumption on characteristic), and consider some $x \in \mathfrak{g}$. We have $\mathrm{ad}x : \mathfrak{g} \to \mathfrak{g}$, so we can write

$$\mathfrak{g} = \bigoplus_{\lambda \in k} \mathfrak{g}_\lambda$$

with $\mathfrak{g}_\lambda = \ker(\mathrm{ad}x - \lambda)^N$ for $N \gg 0$ is the generalized λ-eigenspace of $\mathrm{ad}x$ (can take $N = \dim \mathfrak{g}$).

Lemma 1.17.7. *This defines a grading, i.e.*

$$[\mathfrak{g}_\lambda, \mathfrak{g}_\mu] \subset \mathfrak{g}_{\lambda+\mu}$$

Proof. Fix $y \in \mathfrak{g}_\lambda$ and $z \in \mathfrak{g}_\mu$. Then,

$$\begin{aligned}
(\mathrm{ad}x - \lambda - \mu)^N([y,z]) &= \sum_{k+r+s=N} (-1)^{+s} \frac{N!}{k!r!s!} \lambda^r \mu^s (\mathrm{ad}x)^k([y,z]) \\
&= \sum_{k+r+s=N} \sum_{p+q=k} (-1)^{r+s} \frac{N!}{k!r!s!} \frac{k!}{p!q!} \lambda^r \mu^s \left[(\mathrm{ad}x)^p(y), (\mathrm{ad}x)^q(z)\right] \\
&= \sum_{p+q+r+s=N} (-1)^{r+s} \frac{N!}{p!q!r!s!} \lambda^r \mu^s \left[(\mathrm{ad}x)^p(y), (\mathrm{ad}x)^q(z)\right] \\
&= \sum_{k+\ell=N} \sum_{p+r=k} \sum_{q+s=\ell} (-1)^{r+s} \frac{N!}{k!\ell!} \left[(\mathrm{ad}x - \lambda)^k(y), (\mathrm{ad}x - \mu)^\ell(z)\right]
\end{aligned}$$

with second equality coming from Liebniz. Thus, if $N \geq 2\dim \mathfrak{g}$, this expression is 0, so we win. ■

Definition 1.17.8. An element $x \in \mathfrak{g}$ is **semisimple** if the operator $\mathrm{ad}x : \mathfrak{g} \to \mathfrak{g}$ is semisimple, and x is called **nilpotent** if $\mathrm{ad}x$ is a nilpotent operator. ◇

Remark 1.17.9. If x is both semisimple and nilpotent, then $\mathrm{ad}x = 0$, so x is central. This is an iff. Hence, if $\mathfrak{g}$ is semisimple (trivial center), then an element with is both semisimple and nilpotent must be 0. ○

Proposition 1.17.10 (Jordan decomposition for semisimple Lie algebras). *Let $\mathfrak{g}$ be a semisimple Lie algebra, and fix $x \in \mathfrak{g}$. Then, x has a unique decomposition*

$$x = x_s + x_n$$

where $x_s \in \mathfrak{g}$ is semisimple, $x_n \in \mathfrak{g}$ is nilpotent, and $[x_s, x_n] = 0$. Moreover, if $y \in \mathfrak{g}$ s.t. $[x,y] = 0$, then also $[x_s, y] = 0 = [x_n, y]$.

Proof. Consider $\mathfrak{g} \hookrightarrow \mathfrak{gl}(\mathfrak{g})$ by adjoint representation, so work the Jordan decomposition $x = x_s + x_n$ of x as a linear operator on $\mathfrak{g}$. For $y \in \mathfrak{g}_\lambda$, we have $x_s(y) = \lambda y$. We know $[\mathfrak{g}_\lambda, \mathfrak{g}_\mu] \subset \mathfrak{g}_{\lambda+\mu}$ so $x_s : \mathfrak{g} \to \mathfrak{g}$ is a derivation as

$$x_s([y,z]) = [x_s(y), z] + [y, x_s(z)]$$

when $y \in \mathfrak{g}_\lambda$ and $z \in \mathfrak{g}_\mu$ (note that all elements of $\mathfrak{g}$ spanned by such things). We know that all derivations of $\mathfrak{g}$ are inner (Proposition 1.16.10), so $x_s \in \mathfrak{g}$ which then implies that $x_n \in \mathfrak{g}$. These commute as operators on $\mathfrak{g}$, and therefore do so as elements of $\mathfrak{g}$ too (i.e. $[x_s, x_n] = 0$). Finally, if $y \in \mathfrak{g}$ and $[x,y] = 0$, then they also commute as operators so $\mathrm{ad}y$ preserves the generalized eigenspaces $\mathfrak{g}_\lambda$ of $\mathrm{ad}x$ which implies that $[y, x_s] = 0$.

Uniqueness is proved the same way as before. If $x = x_s' + x_n'$ is another decomposition, then $x_s - x_s' = x_n' - x_n$ with the LHS semisimple and the RHS nilpotent (the terms on either side commute with each other by above), so both sides are 0 (use $\mathfrak{g}$ semisimple). ■

Corollary 1.17.11. *Any nonzero semisimple Lie algebra $\mathfrak{g}$ contains nonzero semisimple elements.*

Proof. Otherwise, for any $x \in \mathfrak{g}$, we have $x = x_s + x_n = x_n$ ($x_s = 0$), so Engel tells us that $\mathfrak{g}$ is nilpotent and hence $\mathfrak{g} = 0$. ∎

Remark 1.17.12. If $\mathfrak{g} = \mathfrak{sl}_n(k)$, the definitions of semisimple/nilpotent elements are the same as usual, and this proposition is the usual Jordan decomposition. ∘

1.17.3 Toral subalgebras

Fix a semisimple Lie algebra over $k = \overline{k}$ of characteristic 0.

Definition 1.17.13. An abelian subalgebra $\mathfrak{h} \subset \mathfrak{g}$ is called a **toral subalgebra** if it consists of semisimple elements. ◇

Proposition 1.17.14. *Let $\mathfrak{g}$ be a semisimple Lie algebra with toral subalgebra $\mathfrak{h} \subset \mathfrak{g}$, and let $B : \mathfrak{g} \times \mathfrak{g} \to k$ be a non-degenerate invariant symmetric bilinear form (e.g. $B = K$ the Killing form). Then,*

(i) $\mathfrak{g} = \bigoplus_{\alpha \in \mathfrak{h}^*} \mathfrak{g}_\alpha$ *where*

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} \mid \forall h \in \mathfrak{h} : [h, x] = \alpha(h)x\}.$$

In particular, $\mathfrak{g}_0 \supset \mathfrak{h}$.

Question: Are these α's "roots" of whatever they're called?

(ii) $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subset \mathfrak{g}_{\alpha+\beta}$

(iii) *If $\alpha + \beta \neq 0$, then $\mathfrak{g}_\alpha, \mathfrak{g}_\beta$ are orthogonal under B*

(iv) *B restricts to a nondegenerate pairing*

$$\mathfrak{g}_\alpha \times \mathfrak{g}_{-\alpha} \longrightarrow k.$$

Proof. **(i)** The eigenspace decomposes for action of $\mathfrak{h}$ on $\mathfrak{g}$. Commuting operators have simultaneous eigenspaces or something.

(ii) This is a consequence of the lemma about generalized eigenspaces (in fact, the proof is simpler here since there are ordinary eigenspaces)

(iii,iv) follow as B is non-degenerate and invariant.

$$\alpha(h)B(x, y) = B([h, x], y) = -B(x, [h, y]) = -\beta(x)B(x, y)$$

so if $\alpha(h) + \beta(h) \neq 0$ we get that $B(x, y) = 0$. Also B non-degenerate means every nonzero vector must have nonzero pairing with some vector, but the above shows that other vector must have opposite weight. ∎

Corollary 1.17.15.

(i) *$\mathfrak{g}_0$ is reductive.*

(ii) *If $x \in \mathfrak{g}_0$, then $x_s, x_n \in \mathfrak{g}_0$.*

Proof. **(i)** Cartan's criterion tells us that

$$\begin{array}{ccc} \mathfrak{g}_0 \times \mathfrak{g}_0 & \longrightarrow & k \\ (x,y) & \longmapsto & \mathrm{tr}_{\mathfrak{g}}(xy) \end{array}$$

is nondegenerate since $\mathfrak{g}$ is semisimple (and then use **(iv)** of above proposition). Therefore, $\mathfrak{g}_0$ is reductive since $\mathfrak{g}$ is a $\mathfrak{g}_0$-rep such that $(x,y) \mapsto \mathrm{tr}_{\mathfrak{g}}(xy)$ is nondegenerate.

(ii) Since $x \in \mathfrak{g}_0$, for any $h \in \mathfrak{h}$, we have $[h,x] = 0$. Thus, $[h,x_s] = 0[h,x_n]$ which by definition says that $x_s, x_n \in \mathfrak{g}_0$. ∎

1.17.4 Cartan subalgebras

Definition 1.17.16. A **Cartan subalgebra** in a semisimple $\mathfrak{g}$ is a toral subalgebra $\mathfrak{h} \subset \mathfrak{g}$ such that $\mathfrak{g}_0 = \mathfrak{h}$ (i.e. $\mathfrak{h}$ is its own centralizer). ◇

Question: Is this gonna be associated to a maximal torus?

Class at MIT on Tuesday (election day).

1.18 Lecture 18 (11/3)

Last time we discussed toral Lie subalgebras. We're working with semisimple Lie algebras, so assume $\mathrm{char}\, k = 0$.

Recall 1.18.1. Let $\mathfrak{g}$ be a semisimple Lie algebra with $\mathfrak{h} \subset \mathfrak{g}$ an abelian subalgebra. It is called *toral* if it consists of semisimple elements. In this case, we get a decomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{0 \neq \alpha \in \mathfrak{h}^*} \mathfrak{g}_\alpha$$

where

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} : [h,x] = \alpha(h)x \,\forall h \in \mathfrak{h}\}$$

We showed that $\mathfrak{g}_0$ (the centralizer of $\mathfrak{h}$) is reductive. We also showed that for B non-degenrate, invariant, bilinear form, we have $\mathfrak{g}_\alpha \perp \mathfrak{g}_\beta$ if $\alpha + \beta \neq 0$ and $B : \mathfrak{g}_\alpha \times \mathfrak{g}_{-\alpha} \to k$ is a nondegenerate pairing. ⊙

Recall 1.18.2. A toral subalgebra $\mathfrak{h} \subset \mathfrak{g}$ is a Cartan subalgebra if $\mathfrak{g}_0 = \mathfrak{h}$. This implies that it is a maximal toral subalgebra. ⊙

Theorem 1.18.3. *Any maximal toral subalgebra $\mathfrak{h} \subset \mathfrak{g}$ is a Cartan subalgebra. In particular, Cartan subalgebras exist.*

Proof. Choose $x \in \mathfrak{g}_0$ and write $x = x_s + x_n$. Then, $[h,x] = 0$ for all $h \in \mathfrak{h}$ which implies that $[h,x_s] = 0$ so $x_s \in \mathfrak{h}$ by maximality of $\mathfrak{h}$. Hence, $\mathrm{ad}x|_{\mathfrak{g}_0} = \mathrm{ad}x_n|_{\mathfrak{g}_0}$ so $\mathrm{ad}x|_{\mathfrak{g}_0}$ is nilpotent. By Engel's theorem, $\mathfrak{g}_0$ is nilpotent. But we also know that it is reductive, so $\mathfrak{g}_0$ must be abelian. We now claim

Claim 1.18.4. *For any $x \in \mathfrak{g}_0$ such that $\mathrm{ad}x|_{\mathfrak{g}}$ is nilpotent, one has $x = 0$.*

Indeed, take any $y \in \mathfrak{g}_0$, so $\mathrm{ad}x.\mathrm{ad}y|_{\mathfrak{g}}$ is nilpotent (since these commute (as $\mathfrak{g}_0$ is abelian) and $\mathrm{ad}x$ is nilpotent). Thus, the Killing form $K(x,y) = \mathrm{tr}_{\mathfrak{g}}(\mathrm{ad}x.\mathrm{ad}y) = 0$ for all $y \in \mathfrak{g}_0$. But $K|_{\mathfrak{g}_0}$ is nondegenerate[14],

[14] $\mathfrak{g}$ semisimple so Cartan's criterion gives $K^{\mathfrak{g}}$ nondegenerate, but then the first recall implies that $K^{\mathfrak{g}_0}$ is also nondegenerate ($\alpha = 0 = -\alpha$)

so $x = 0$.

So for all $x \in \mathfrak{g}_0$, we have $x_n \in \mathfrak{g}_0$ and $\mathrm{ad}x_n|_{\mathfrak{g}}$ nilpotent, so $x_n = 0 \implies x = x_s \in \mathfrak{h}$, so $\mathfrak{g}_0 = \mathfrak{h}$. ■

We will later show that any two Cartan subgroups are conjugate by an inner automorphism of $\mathfrak{g}$; in particular, they all have the same dimensional, called the **rank of $\mathfrak{g}$**.

Example. $\mathfrak{g} = \mathfrak{sl}_n(k)$ and $\mathfrak{h} =$ traceless, diagonal matrices $\subset \mathfrak{g}$ is a Cartan subalgebra. $\mathfrak{h}$ clearly consists of semisimple elements and also any matrix commuting with all diagonal matrices (even just all traceless diagonal matrices) must itself be diagonal. △

1.18.1 Root decomposition

Let $\mathfrak{h} \subset \mathfrak{g}$ be a Cartan subalgebra, so they have a **root decomposition**

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{0 \neq \alpha \in \mathfrak{h}^*} \mathfrak{g}_\alpha.$$

Note that $\mathfrak{g}_\alpha \neq 0$ only for a finite set $R \subset \mathfrak{h}^*$. We call R the **root system** of $\mathfrak{g}$, and elements $\alpha \in R$ are called **roots**. Note that $\alpha \in R \implies -\alpha \in R$ since the paring between $\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}$ is non-degenerate so they have the same dimension.

Proposition 1.18.5. *Let $\mathfrak{g}_1, \ldots, \mathfrak{g}_n$ be simple Lie algebras, and let $\mathfrak{g} = \bigoplus \mathfrak{g}_i$.*

(i) *If $\mathfrak{h}_i \subset \mathfrak{g}_i$ are Cartan subalgebras, then so it $\mathfrak{h} = \bigoplus_i \mathfrak{g}_i \subset \mathfrak{g}$.*

(ii) *Any Cartan subalgebra of $\mathfrak{g}$ is of this form.*

Proof. **(i)** is clear because it is clearly a maximal toral subalgebra (its centralizer is itself).

(ii) Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$. Let $\mathfrak{h}_i$ be the projection of $\mathfrak{h}$ to $\mathfrak{g}_i$. Then, $\mathfrak{h}_i$ is Cartan since it consists of semisimple elements, and if it were not maximal, then $\mathfrak{h}$ would not be maximal. Hence, $\bigoplus \mathfrak{h}_i \supset \mathfrak{h}$ is also Cartan, but maximality of $\mathfrak{h}$ means this must be an equality. ■

Example. Let $\mathfrak{g} = \mathfrak{sl}_n(k)$ and $\mathfrak{h} =$ diagonal matrices of trace 0. Then,

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{i \neq j} kE_{ij}$$

where E_{ij} is the elementary matrix with a 1 in slot ij and 0's elsewhere. For $x = \mathrm{diag}(x_1, \ldots, x_n) \in \mathfrak{h}$, we get $[x, E_{ij}] = (x_i - x_j)E_{ij}$. Hence, letting e_i be the standard basis of k^n, the roots are $R = \{e_i - e_j \mid i \neq j\}$ so there are $n(n-1)$ roots. △

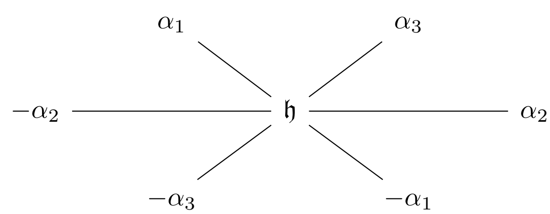
Example. When $n = 1$, $\mathfrak{g} = 0$ and $R = \emptyset$.

When $n = 2$, $\mathfrak{g} = \mathfrak{sl}_2(k)$ and $R = \{\pm\alpha\}$ with $\alpha \begin{pmatrix} t & 0 \\ 0 & -t \end{pmatrix} = 2t$. Hence, $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$ but $\mathfrak{h} = \langle h \rangle$, $\mathfrak{g}_\alpha = \langle e \rangle$ and $\mathfrak{g}_{-\alpha} = \langle f \rangle$, so the usual generators e, f, h are exactly the ones coming from the root decomposition. △

Example. $\mathfrak{g} = \mathfrak{sl}_3(k)$ has roots

$$R = \{\pm(1, -1, 0), \pm(1, 0, -1), \pm(0, 1, -1)\}$$

We can try to draw these in the plane. Let $\alpha_1 = (1, -1, 0)$ and $\alpha_2 = (0, 1, -1)$.



They form a Hexagon. These is a good picture to keep in mind when talking about semisimple Lie algebras. △

Let $\mathfrak{g}$ be a semisimple Lie algebra with Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$ and nondegenerate, invariant, symmetric form $(-,-)$ (e.g. the Killing form). Since this is non-degenerate, it gives rise to $A : \mathfrak{h} \xrightarrow{\sim} \mathfrak{h}^*$ with $A(h) = (h, -)$. We will let $A^{-1}(\alpha) = H_\alpha \in \mathfrak{h}$ denote the image of α under the inverse map $A^{-1} : \mathfrak{h}^* \to \mathfrak{h}$. This gives us a form on $\mathfrak{h}^*$ via

$$(\alpha, \beta) = \alpha(H_\beta) = (H_\alpha, H_\beta).$$

Lemma 1.18.6. *For any $e \in \mathfrak{g}_\alpha$ and $f \in \mathfrak{g}_{-\alpha}$, we have*

$$[e, f] = (e, f)H_\alpha \in \mathfrak{g}_0 = \mathfrak{h}.$$

Proof. By non-degeneracy of $(-,-)$, it suffices to show that both sides have the same inner product with any element of $\mathfrak{h}$. Choose $h \in \mathfrak{h}$ and observe that

$$([e, f], h) = (e, [f, h]) = \alpha(h)(e, f) = (H_\alpha, h)(e, f) = ((e, f)H_\alpha, h)$$

where the first equality is invariance of $(-,-)$. This completes the proof. ■

Lemma 1.18.7.

(i) *If $\alpha \in R$, then $(\alpha, \alpha) \neq 0$.*

(ii) *If $e \in \mathfrak{g}_\alpha$ and $f \in \mathfrak{g}_{-\alpha}$ s.t. $(e, f) = \frac{2}{(\alpha,\alpha)}$ then for $h_\alpha = \frac{2H_\alpha}{(\alpha,\alpha)}$, we have that h_α, e, f satisfy relations of $\mathfrak{sl}_2$ (i.e. we get a copy of $\mathfrak{sl}_2$ attached to each root).*

(iii) *h_α is independent of the choice of $(-,-)$*

Proof. **(i)** Pick $e \in \mathfrak{g}_\alpha$ and $f \in \mathfrak{g}_{-\alpha}$ s.t. $(e, f) \neq 0$ (these exist since $(-,-) : \mathfrak{g}_\alpha \times \mathfrak{g}_{-\alpha} \to k$ is non-deg). Let $h = [e, f] = (e, f)H_\alpha$. Consider the Lie algebra $\mathfrak{a} = \langle e, f, h\rangle$. Then,

$$[h, e] = \alpha(h)e = (e, f)\alpha(H_\alpha)e = (e, f)(\alpha, \alpha)e$$

and

$$[h, f] = -\alpha(h)f = -(e, f)(\alpha, \alpha)f.$$

If $(\alpha, \alpha) = 0$, then $[h, e] = [h, f] = 0$ and $[e, f] = h$; this is the Heisenberg Lie algebra which is nilpotent (so solvable). Lie's theorem implies that there exists a basis of $\mathfrak{g}$ in which h, e, f act by upper triangular matrices. ad$h$ will act by a strictly upper triangular matrix which means that h is nilpotent, but also $h \in \mathfrak{h}$, so h is semisimple and hence $h = 0$, a contradiction (as $(e, f) \neq 0$ and $h = (e, f)H_\alpha$). Thus, $(\alpha, \alpha) \neq 0$ which proves **(i)**.

(ii) Since $(\alpha, \alpha) \neq 0$, we can pick e, f so that $(e, f) = 2/(\alpha, \alpha)$. One easily gets that

$$[h, e] = 2e,\ \ [h, f] = -2f,\ \text{ and }\ [e, f] = h \text{ where } h = \frac{2H_\alpha}{(\alpha, \alpha)}.$$

(iii) Enough to prove this for simple Lie algebras. In this case, the form is unique up to scaling, and scaling it by λ sends $H_\alpha \rightsquigarrow \lambda H_\alpha$, so the ratio remains unchanged. ∎

Notation 1.18.8. The Lie algebra spanned by e, f, h_α obtained in **(ii)** of the above lemma is denoted $\mathfrak{sl}_2(k)_\alpha$ and called the **root $\mathfrak{sl}_2$ subalgebra**. Right now, it seems like it depends on choices, but we'll soon show $\dim \mathfrak{g}_\alpha \leq 1$, so there are no choices.

Proposition 1.18.9. *Let $\mathfrak{a}_\alpha = kH_\alpha \oplus \bigoplus_{m \in \mathbb{Z}\setminus 0} \mathfrak{g}_{m\alpha}$. Then, $\mathfrak{a} \subset \mathfrak{g}$ is a Lie subalgebra.*[15]

Proof. Only need to show that $[\mathfrak{g}_{m\alpha}, \mathfrak{g}_{-m\alpha}] \subset kH_\alpha$. But we know that for all $x \in \mathfrak{g}_{m\alpha}$ and $y \in \mathfrak{g}_{-m\alpha}$,

$$[x, y] = (x, y)H_{m\alpha} = m(x, y)H_\alpha$$

so we win. ∎

In particular, $\mathfrak{a}_\alpha$ is a representation of $\mathfrak{sl}_2(k)_\alpha \subset \mathfrak{a}_\alpha$. Now we're in business, because we know the representation theorem of $\mathfrak{sl}_2$. What are the weights/eigenspaces of $h = h_\alpha$? For $x \in \mathfrak{g}_{m\alpha}$, we have

$$[h_\alpha, x] = m\alpha(h_\alpha)x = m\alpha\left(\frac{2H_\alpha}{(\alpha, \alpha)}\right)x = 2mx$$

and also $[h_\alpha, h_\alpha] = 0$. Hence, the eigenvalues are all even integers and the 0-eigenspace is 1-dimensional. From this, it is easy to see that $\mathfrak{a}_\alpha \simeq V_{2r}$ for some $r \in \mathbb{Z}_{>0}$ is the irrep with highest weight $2r$. This implies the following proposition.

Proposition 1.18.10.

(i) *$\mathfrak{g}_\alpha$ is 1-dimensional for every root α.*

(ii) *If α is a root, then $\mathfrak{g}_{2\alpha} = \mathfrak{g}_{3\alpha} = \cdots = 0$, a nontrivial positive integral multiple of a root is not a root.*

Proof. We showed **(i)** by showing that $\mathfrak{a}_\alpha$ is an irrep of $\mathfrak{sl}_2(k)_\alpha$. Hence, we know that $\mathfrak{g}_\alpha = \langle e \rangle$ since it is 1-dimensional. Hence, $\mathfrak{g}_\alpha \to \mathfrak{a}_{2\alpha}$ is the zero map. Thus, $\mathfrak{g}_{2\alpha} = 0$ and e is a highest weight eigenvector. This means that $\mathfrak{a}_\alpha = V_2$ so $\mathfrak{a}_\alpha = \mathfrak{sl}_2(k)_\alpha$. ∎

Theorem 1.18.11. *Let $\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$ be a root decomposition of a semisimple Lie algebra, and let $(-, -)$ be a nondeg, invariant, symmetric form on $\mathfrak{g}$. Then,*

(i) *$\alpha \in R$ span $\mathfrak{h}^*$, and the h_α span $\mathfrak{h}$.*

(ii) *For all roots α, β, $a_{\alpha\beta} = 2(\alpha, \beta)/(\alpha, \alpha)$ is an integer*

[15]This will turn out to be $\mathfrak{sl}_2(k)_\alpha$, but we don't know that yet.

(iii) *For all $\alpha \in R$, define the* ***reflection operator***

$$s_\alpha(\lambda) = \lambda - \lambda(h_\alpha)\alpha = \lambda - \frac{2(\lambda,\alpha)}{(\alpha,\alpha)}\alpha$$

(so $s_\alpha^2 = 1$). If $\beta \in R$, then $s_\alpha(\beta) \in R$, so $s_\alpha(R) = R$.

(iv) *For roots $\alpha, \beta \neq \pm\alpha$, the space $V_{\alpha,\beta} = \bigoplus_{m\in\mathbb{Z}} \mathfrak{g}_{\beta+m\alpha}$ is an irrep of $\mathfrak{sl}_2(k)_\alpha$.*

Proof. **(i)** Let $h \in \mathfrak{h}$ be such that $\alpha(h) = 0$ for all $\alpha \in R$. Then, $\mathrm{ad}h = 0$ (acts by 0 on $\mathfrak{h}$ and by $0 = \alpha(h)$ on $\mathfrak{g}_\alpha$) so $h = 0$ since $\mathfrak{g}$ semisimple. This means the α span $\mathfrak{h}^*$.

(ii) Note that $[h_\alpha, e_\beta] = \beta(h_\alpha)e_\beta = \beta\left(\frac{2H_\alpha}{(\alpha,\alpha)}\right)$ so $2(\alpha,\beta)/(\alpha,\alpha)$ is an eigenvalue of h under a f.d. rep of $\mathfrak{sl}_2(\mathfrak{h})_\beta$ which must then be an integer.

(iii) $s_\alpha^2(\beta) = s_\alpha(\beta - \beta(h_\alpha)\alpha) = \beta - \beta(h_\alpha)\alpha - (\beta - \beta(h_\alpha)\alpha)(h_\alpha)\alpha = \beta - 2\beta(h_\alpha)\alpha + \beta(h_\alpha)\alpha(h_\alpha)\alpha = \beta$. Let $\beta \in R$ and $x \in \mathfrak{g}_\beta$ nonzero. Then,

$$[h_\alpha, x] = \frac{2(\alpha,\beta)}{(\alpha,\alpha)}x = \beta(h_\alpha)x.$$

We now want to shift eigenspaces by applying f (to lower eigenvalue) or e (to raise eigenvalue). If $\beta(h_\alpha) \geq 0$, then $y = (\mathrm{ad}f)^{\beta(h_\alpha)}x \neq 0 \in \mathfrak{g}_{s_\alpha(\beta)}$ so $s_\alpha(\beta) \in R$. If $\beta(h_\alpha) \leq 0$, then $y = (\mathrm{ad}e)^{-\beta(h_\alpha)}x \neq 0 \in \mathfrak{g}_{s_\alpha(\beta)}$, so $s_\alpha(\beta) \in R$.

(iv) $V_{\alpha,\beta} \subset \mathfrak{g}$ is a subspace. It is clearly a subep since $\{\beta + m\alpha\}$ is invariant under shifting by $\pm\alpha$. The eigenvalues of h_α are

$$2\frac{(\alpha,\beta)}{(\alpha,\alpha)} + 2m$$

which are all even. Since its eigenspaces are also all 1-dim, we conclude by rep theory of $\mathfrak{sl}_2$ that $V_{\alpha,\beta}$ is irreducible. ■

1.19 Lecture 19 (11/5)

Last time we talked about root decompositions. For $\mathfrak{h} \subset \mathfrak{g}$ a Cartan subalgebra, we have $\mathfrak{g} = \mathfrak{h} \bigoplus_{\alpha\in R} \mathfrak{g}_\alpha$ for a root system $R \subset \mathfrak{h}^*$. We saw that each $\mathfrak{g}_\alpha$ is 1-dimensional, as well as various out properties of these.

Attached to each root is an $\mathfrak{sl}_2$-subalgebra

$$\mathfrak{sl}_2(k)_\alpha = \langle e_\alpha, f_\alpha, h_\alpha\rangle \quad \text{with} \quad h_\alpha \in \mathfrak{h}.$$

Proposition 1.19.1. *Let $\mathfrak{h}_\mathbb{R}$ be the $\mathbb{R}$ span of the $h_\alpha \in \mathfrak{h}$, $\alpha \in R$. Then, $\mathfrak{h} = \mathfrak{h}_\mathbb{R} \oplus i\mathfrak{h}_\mathbb{R}$ and the restriction of the Killing form to $\mathfrak{h}_\mathbb{R}$ is positive definite (this is when $\mathfrak{g}/\mathbb{C}$).*

Proof. We have seen that the eigenvalues of $\mathrm{ad}h_\alpha$ are integers (in particular, real numbers), so for any $\mathbb{R}$-linear combination $h = \sum c_\alpha h_\alpha \in \mathfrak{h}_\mathbb{R}$, the eigenvalues of $\mathrm{ad}h$ are also real. Thus, $\mathfrak{h}_\mathbb{R} \cap i\mathfrak{h}_\mathbb{R} = 0$. Also, $\mathfrak{h}_\mathbb{R} + i\mathfrak{h}_\mathbb{R} = \mathfrak{h}_\mathbb{R} \oplus i\mathfrak{h}_\mathbb{R} = \mathfrak{h}$ since we know that the h_α span $\mathfrak{h}$ over $\mathbb{C}$ (See Theorem 1.18.11 **(i)**).

If λ_i are the eigenvalues of $\mathrm{ad}h$, then $K(h,h) = \sum \lambda_i^2 \geq 0$ with equality only if all λ_i are 0, so $K|_{\mathfrak{h}_\mathbb{R}}$ is positive definite. ■

1.19.1 Regular elements

Example. Let $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{C})$, and let $x \in \mathfrak{g}$ be a diagonal matrix with distinct eigenvalues. Then the centralizer $\mathfrak{h} = C(X) \subset \mathfrak{g}$ is simply the set of all diagonal matrices inside $\mathfrak{g}$, which is a Cartan subalgebra. Thus $C(x)$ is a Cartan subalgebra whenever x has distinct eigenvalues (so is furthermore diagonalizable); note that these form a dense subset of matrices.[16]. $\triangle$

We want to generalize this to any semisimple LA: if x is "generic" then $C(x)$ is a Cartan subalgebra.

Definition 1.19.2. The **nullity** of x, denote $n(x)$, is the multiplicity of the 0 eigenvalue of $\mathrm{ad}x$, i.e. the dimension of the generalized 0-eigenspace of $\mathrm{ad}x$. The **rank** of $\mathfrak{g}$ is the minimal value of $n(x)$ for $x \in \mathfrak{g}$. In particular, this will be equal to the dimension of any Cartan subalgebra of $\mathfrak{g}$. An element $x \in \mathfrak{g}$ is called **regular** if $n(x) = \operatorname{rank} \mathfrak{g}$. $\diamond$

Example. $\mathfrak{g} = \mathfrak{sl}_n(\mathbb{C})$, x is regular $\iff$ it is diagonalizable with distinct eigenvalues (Exercise). Hence, $\operatorname{rank} \mathfrak{sl}_n(\mathbb{C}) = n - 1$. $\triangle$

Lemma 1.19.3. *The set $\mathfrak{g}^{\text{reg}}$ of regular elements is connected, dense and open.*

This is what we mean by "generic." It will be useful to have the following auxiliary lemma.

Lemma 1.19.4. *Let $P(z_1, \ldots, z_n)$ be a complex polynomial, and let $U \subset \mathbb{C}^n$ be its nonzero set (i.e. $(z_1, \ldots, z_n)$ s.t. $P(z_1, \ldots, z_n) \neq 0$). We assume $U \neq \emptyset$. Then, U is path-connected, open and dense in $\mathbb{C}^n$.*

Proof. It is clear that U is open since $U = P^{-1}(\mathbb{C} \setminus \{0\})$. To see that U is dense, note that its complement is the hypersurface $\{\vec{z} : P(\vec{z}) = 0\}$ which does not contain any ball. Finally, to see that U is connected, fix any $x, y \in U$. Consider the line $z_t = (1-t)x + ty$. Note that $P((1-t)x + ty) \in \mathbb{C}[t]$ is a nonzero, one variable polynomial, so it has finitely many roots $t_1, \ldots, t_m$. Hence,

$$x, y \in L \setminus \{t_1, \ldots, t_m\} \subset U,$$

but $L \setminus \{t_1, \ldots, t_m\}$ is connected (since $L \cong \mathbb{C}$), so U is path-connected. ■

Proof of Lemma 1.19.3. Consider the characteristic polynomial of $\mathrm{ad}x$. Note that $\mathrm{ad}x$ always has 0 as an eigenvalue (since $\mathrm{ad}x.x = 0$), so its char poly is of the form ($\operatorname{rank} \mathfrak{g}$ is the minimum possible nullity)

$$P_x(t) = t^{\operatorname{rank}(\mathfrak{g})} \left(t^m + a_{m-1}(x)t^{m-1} + \cdots + a_0(x)\right)$$

where $m = \dim \mathfrak{g} - \operatorname{rank} \mathfrak{g}$. These $a_i(x)$ are polynomial functions of x, so

$$\mathfrak{g}^{\text{reg}} = \{x \in \mathfrak{g} : a_0(x) \neq 0\}$$

is dense, open, and path-connected by the previous lemma. ■

Proposition 1.19.5. *Let $\mathfrak{g}$ be a complex semisimple Lie algebra with Cartan algebra $\mathfrak{h} \subset \mathfrak{g}$. Then,*

[16] These are matrices where characteristic poly has distinct roots, so ones where the discriminant of the characteristic poly is nonzero. This is generically the case

(i) $\dim \mathfrak{h} = \operatorname{rank} \mathfrak{g}$*;*

(ii) *Setting* $\mathfrak{h}^{\text{reg}} = \mathfrak{h} \cap \mathfrak{g}^{\text{reg}}$*, we get*

$$\mathfrak{h}^{\text{reg}} = \{h \in \mathfrak{h} : \alpha(h) \neq 0 \, \forall \alpha \in R\} =: V.$$

Proof. Let G be a connected $\mathbb{C}$-Lie group with Lie algebra $\mathfrak{g}$ (e.g. $\operatorname{Aut}(\mathfrak{g})^\circ$ since $\mathfrak{g}$ semisimple). Consider the regular map

$$\begin{array}{rccc} \varphi : & G \times V & \longrightarrow & \mathfrak{g} \\ & (g, x) & \longmapsto & \operatorname{Ad} g \cdot x \end{array}.$$

We want to show that this is a submersion, so let us compute its derivative at $(1, x) \in G \times V$. First note that

$$T_{(1,x)}(G \times V) = T_1 G \oplus T_x V = \mathfrak{g} \oplus \mathfrak{h}$$

so we want to compute $\varphi_* : \mathfrak{g} \oplus \mathfrak{h} \to \mathfrak{g}$. We compute

$$\varphi_*(0, h) = \left.\frac{\partial}{\partial t}\right|_{t=0} \varphi(1, x + th) = \left.\frac{\partial}{\partial t}\right|_{t=0} (x + th) = h$$

and

$$\varphi_*(y, 0) = \left.\frac{\partial}{\partial t}\right|_{t=0} \operatorname{Ad} e^{ty} \cdot x = [y, x],$$

so $\varphi_*(y, h) = [y, x] + h$. What is $\ker \varphi_*$? It is

$$\ker \varphi_* = \{(y, h) : [y, x] = -h\} \cong \{y \in \mathfrak{g} : [y, x] \in \mathfrak{h}\}.$$

If $[y, x] \in \mathfrak{h}$, then (for $z \in \mathfrak{h}$)

$$K([y, x], z) = K(y, [x, z]) = 0 \implies [y, x] = 0$$

(since $K|_{\mathfrak{h}}$ is non-degenerate), so $\ker \varphi_* \cong C(x)$. Since $x \in V$, we have $C(x) = \mathfrak{h}$, so φ_* is surjective by dimension counting. Hence, φ is a submersion at the point $(1, x)$, so the image U of $\varphi : G \times V \to \mathfrak{g}$ contains a neighborhood of x. By using the adjoint action, this implies that U is open. Since $\mathfrak{g}^{\text{reg}}$ is open and dense, we see that $U \cap \mathfrak{g}^{\text{reg}}$ is open and nonempty. But for $u = \varphi(g, x) \in U \cap \mathfrak{g}^{\text{reg}}$, $n(u) = n(x) = \dim C(x) = \dim \mathfrak{h}$ from which we conclude that $\dim \mathfrak{h} = \operatorname{rank} \mathfrak{g}$. This proves **(i)**.

(ii) Consider any $x \in \mathfrak{h}$. Using the root decomposition, it is easy to see that

$$n(x) = \dim \mathfrak{h} + \# \{\alpha \in R : \alpha(x) = 0\}$$

which immediately implies $\mathfrak{h}^{\text{reg}} = V$. ■

1.19.2 Conjugacy of Cartan subalgebras

Below, $\mathfrak{g}$ is a complex semisimple Lie algebra.

Theorem 1.19.6. *Let* $x \in \mathfrak{g}$ *be a regular semisimple element (e.g.* $x \in \mathfrak{h}^{\text{reg}}$*). Then,*

(i) *the centralizer* $\mathfrak{h}_x = C(x)$ *is a Cartan subalgebra.*

(ii) *any Cartan subalgebra is of this form.*

Proof. Consider the eigenspace decomposition[17] of $\mathfrak{g}$ with respect to the adjoint action $\mathrm{ad}x$:

$$\mathfrak{g} = \bigoplus_\lambda \mathfrak{g}_\lambda.$$

Note that $\mathbb{C}x$ is a (one-dimensional) toral subalgebra, so $\mathfrak{g}_0 = C(x)$ is a reductive Lie group with $\dim \mathfrak{g}_0 = \operatorname{rank} \mathfrak{g}$.

We claim that $\mathfrak{g}_0$ is also nilpotent. To this end, we will show that for $y \in \mathfrak{g}_0$, the operator $\mathrm{ad}y|_{\mathfrak{g}_0}$ is nilpotent (this suffices by Engel's theorem). Consider $\mathrm{ad}(x+ty) = \mathrm{ad}x + t\mathrm{ad}y$ ($x, y \in \mathfrak{g}_0 \implies x+ty \in \mathfrak{g}_0$). This preserves $\mathfrak{g}_0$, so we can consider its actions on both $\mathfrak{g}_0$ and $\mathfrak{g}/\mathfrak{g}_0$. On $\mathfrak{g}/\mathfrak{g}_0$, $\mathrm{ad}x$ is invertible ($\ker \mathrm{ad}x = C(x) = \mathfrak{g}_0$), so for small t, $\mathrm{ad}(x+ty)$ is also invertible. Hence, the multiplicity of 0 as an eigenvalue of $\mathrm{ad}(x+ty)$ is at most $\operatorname{rank}\mathfrak{g} = \dim \mathfrak{g}_0$ (it is $\operatorname{rank}\mathfrak{g} - \#$nonzero eigenvalues of $\mathrm{ad}(x+ty)|_{\mathfrak{g}_0}$) Thus, all eigenvalues of $\mathrm{ad}(x+ty)|_{\mathfrak{g}_0}$ on $\mathfrak{g}_0$ must be 0, but x acts trivially on $\mathfrak{g}_0$, so $\mathrm{ad}(x+ty)|_{\mathfrak{g}_0} = \mathrm{ad}y|_{\mathfrak{g}_0}$ is nilpotent. This proves the claim that $\mathfrak{g}_0$ is nilpotent.

Compare this proof with that of Theorem 1.18.3

Thus, $\mathfrak{g}_0$ is both reductive and nilpotent; hence, abelian. Now we want to show that every element $y \in \mathfrak{g}_0$ is semisimple (i.e. $y_n = 0$). For this, consider the operator $\mathrm{ad}y_n \cdot \mathrm{ad}z$ where $z \in \mathfrak{g}_0$. This is nilpotent (product of nilpotent with an operator that commutes with it), so $K_\mathfrak{g}(y_n, z) = \mathrm{tr}_\mathfrak{g}(\mathrm{ad}y_n \cdot \mathrm{ad}z) = 0$. Since the Killing form is non-degenerate on $\mathfrak{g}_0$, this implies that $y_n = 0$ as desired. Thus, $\mathfrak{g}_0$ is a toral subalgebra. It is also maximal since any element y commuting with $\mathfrak{g}_0$ necessarily commutes with x, and so lies in $\mathfrak{g}_0$. Thus, $\mathfrak{g}_0$ is Cartan. This proves **(i)**.

Let $\mathfrak{h} \subset \mathfrak{g}$ be a Cartan subalgebra. It contains a regular element x which is necessarily semisimple. One easily sees that $\mathfrak{h} = C(x)$ so **(ii)** holds as well. ■

Warning 1.19.7. Usually in the literature, *regular* means that the usual (not generalized) eigenspace of x has minimal dimension. Does not have to be semisimple, e.g.

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \mathfrak{sl}_3$$

is regular in this sense. What we call *regular* is usually called *regular semisimple*. •

Corollary 1.19.8.

(1) *Any regular element* $x \in \mathfrak{g}$ *is semisimple.*

(2) *Such* x *is contained in a unique Cartan subalgebra, namely* $\mathfrak{h}_x$.

Proof. If x is regular, then so is x_s (multiplicity of 0 as an eigenvalue of $\mathrm{ad}x$ and $\mathrm{ad}x_s$ are the same). But $x \in C(x_s)$, a Cartan subalgebra, so x is semisimple. Furthermore, any Cartan subalgebra $\mathfrak{h}$ containing x contains $C(x)$ (by maximality of $\mathfrak{h}$) and so is $C(x)$ by maximality (of $C(x)$). ■

[17] x semisimple so don't need generalized eigenspaces

Theorem 1.19.9. *Any two Cartan subalgebras are conjugate, i.e. for $\mathfrak{h}_1, \mathfrak{h}_2 \subset \mathfrak{g}$ Cartan subalgebras, there exists some $g \in G$ (connected Lie group with $\operatorname{Lie} G = \mathfrak{g}$) such that $\operatorname{Ad} g(\mathfrak{h}_1) = \mathfrak{h}_2$. In particular, the theory of root systems of G is the independent of the choice of Cartan subalgebra.*

Proof. We showed that every regular $x \in \mathfrak{g}$ is semisimple and contained in a unique Cartan $\mathfrak{h}_x$. We now introduce an equivalence relation on $\mathfrak{g}^{\text{reg}}$. We say $x \sim y$ if $\mathfrak{h}_x$ conjugate to $\mathfrak{h}_y$. If $x, y \in \mathfrak{h}$, a Cartan subalgebra, are regular, then $\mathfrak{h}_x = \mathfrak{h}_y = \mathfrak{h}$ and $x \sim y$. Moreover, $\operatorname{Ad} g.x \sim y$ for any $g \in G$. So for all y regular, $\operatorname{Ad} g.x \sim y$ for all $x \in \mathfrak{h}_y^{\text{reg}}$ and $g \in G$. Recall the map $\varphi : G \times \mathfrak{h}_y^{\text{reg}} \to \mathfrak{h}$ sending $(g, x) \mapsto \operatorname{Ad} g.x$. Let $U_y = \operatorname{Im} \varphi$. This is precisely the equivalence class of y. We saw previously that it is open, so all equivalence classes are open in $\mathfrak{g}^{\text{reg}}$. They are also disjoint (since they're equivalence classes). As $\mathfrak{g}^{\text{reg}}$ is connected, this means that there is only one equivalence class. Thus, for any $x, y \in \mathfrak{g}$, $\mathfrak{h}_x$ is conjugate to $\mathfrak{h}_y$. Finally, every Cartan subalgebra is of the form $\mathfrak{h}_x$, so we win. ■

Remark 1.19.10. The same result and proof works over any algebraically closed field of characteristic 0. Instead of the usual topology on $\mathbb{C}^n$, one should use the Zariski topology on $\overline{k}^n$. ○

New homework due next week. Holiday on Wednesday apparently.

1.20 Lecture 20 (11/10)

We talked last time about root decompositions for semisimple Lie algebra $\mathfrak{g}$, which is defined once we fix a Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$. You then get

$$\mathfrak{g} = \mathfrak{h} \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha$$

for $R \subset \mathfrak{h}^* = E$ some finite set of roots (and $\dim \mathfrak{a}_\alpha = 1$ when $\alpha \in R$).

Example. When $\mathfrak{g} = \mathfrak{sl}_n$, we saw that $R = \{e_i - e_j\} \subset \mathbb{R}^{n-1} = \{x \in \mathbb{R}^n : \sum x_i = 0\}$. △

Example. Consider $\mathfrak{g} = \mathfrak{sp}_{2n}$. Let $J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$, so

$$\mathfrak{sp}_{2n} = \left\{ A \in \mathfrak{gl}_{2n} : AJ + JA^t = 0 \right\}.$$

Writing $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as a block matrix, this says

$$\begin{pmatrix} -b & a \\ -d & c \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a^t & c^t \\ b^t & d^t \end{pmatrix} = -\begin{pmatrix} b^t & d^t \\ -a^t & -c^t \end{pmatrix}.$$

Thus, $b = b^t$ and $c = c^t$ are symmetric, and $a = -d^t$. Thus,

$$A = \begin{pmatrix} a & b \\ c & -a^t \end{pmatrix}$$

with b, c symmetric. Let $\mathfrak{h} \subset \mathfrak{g}$ be the subspace of diagonal matrices, so

$$A = \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix} \quad \text{where} \quad a = \operatorname{diag}(x_1, \ldots, x_n).$$

These form a maximal commutative subalgebra consisting of semisimple elements, so $\mathfrak{h}$ is a Cartan subalgebra. What's the root decomposition? Write

$$\mathfrak{g} = \mathfrak{g}_a \oplus \mathfrak{g}_b \oplus \mathfrak{g}_c$$

where

$$\mathfrak{g}_a = \left\{ \begin{pmatrix} a & 0 \\ 0 & -a^T \end{pmatrix} \right\} = \mathfrak{gl}_n \supset \mathfrak{h},$$

$$\mathfrak{g}_b = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b = b^t \right\},$$

and

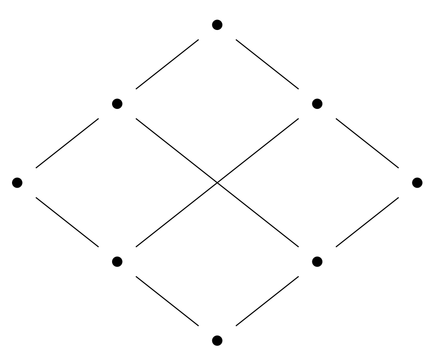
$$\mathfrak{g}_c = \left\{ \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} : c = c^t \right\}.$$

Note that $\mathfrak{g}_a = \mathfrak{h} \oplus_{\alpha \in R_a} \mathfrak{g}_\alpha$ where $\mathfrak{h} \cong k^n$, and $R_a = \{e_i - e_j : i \neq j\}$ are the roots of $\mathfrak{gl}_n$. One can check that the root sytem for b is $R_b = \{e_i + e_j : \forall i, j\}$ (consider Lie bracket with $b = E_{ii}$ and $b = E_{ij} + E_{ji}$ or something like that). Symmetrically, $R_c = \{-e_i - e_j : \forall i, j\}$. Thus, the roots are $e_i - e_j$ for $i \neq j$ and $e_i + e_j$ for any i, j. △

Question: Why don't we have $-e_i - e_j$ for all i, j as well?

Example. Say $\mathfrak{g} = \mathfrak{sp}_4$ so $n = 2$ in the previous example. The root system looks like

I think I should have just drawn arrows for the vectors (i.e. from orgin to •) instead



so we have a square, and the roots are its verticles as well as the midpoints of its edges. This is called a **root system of type** C_n. For $\mathfrak{sl}_n$, we has a **root system of type** A_{n-1}. △

Example. $\mathfrak{g} = \mathfrak{o}(2n)$ so take $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (used quadratic form $Q = x_1 x_{n+1} + \cdots + x_n x_{2n}$) and now $\mathfrak{g} = \{A : AJ + JA^t = 0\}$. Thus, we can always write

Remember: All quadratic forms (of the same rank) over $\mathbb{C}$ are equivalent

$$A = \begin{pmatrix} a & b \\ c & -a^t \end{pmatrix}$$

as before, but now with b, c skew-symmetric (e.g. $b^t = -b$). One gets the same answer but no roots $2e_i$, so only have $e_i - e_j$ and $e_i + e_j$ for $i \neq j$. This gives a **root system of type** D_n. △

Example. $\mathfrak{g} = \mathfrak{o}(2n+1)$. We'll use the quadratic form $Q = x_0^2 + x_1 x_{n+1} + \cdots + x_n x_{2n}$, so $\mathfrak{g}$ is the Lie algebra of matrices annihilating this form Q. Write

$$J = \begin{pmatrix} I_1 & 0 & 0 \\ 0 & 0 & I_n \\ 0 & I_n & 0 \end{pmatrix},$$

so $\mathfrak{g} = \{A \in \mathfrak{gl}(2n+1) : AJ + JA^t = 0\}$. Writing

$$A = \begin{pmatrix} p & u & v \\ w & a & b \\ z & c & d \end{pmatrix},$$

we get that $p = 0$, $v = -u$, $z = -w$, and a, b, c, d as before. so we can write

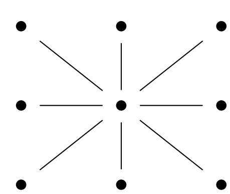
$$A = \begin{pmatrix} 0 & u & -u \\ w & a & b \\ -w & c & -a^t \end{pmatrix}$$

with b, c skew-symmetric. The Cartan subalgebra is now

$$\mathfrak{g} = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & -a \end{pmatrix} \right\} \text{ with } a = \operatorname{diag}(x_1, \dots, x_n).$$

What about the roots? For the a part, get roots $e_i - e_j$ $(i \neq j)$; for the the b part, get roots $e_i + e_j$ $(i \neq j)$; for the c part, get roots $-e_i - e_j$ $(i \neq j)$; for the u part, get roots $-e_i$; and for the w part, get roots $+e_i$. This gives the **root system of type** B_n. $\triangle$

Example. Take $\mathfrak{g} = \mathfrak{o}(5)$ so $n = 2$ in the previous example. Get



which is again a square with vertices and midpoints of the edges being the roots. In fact, this is the same root system (up to rotation/dilation), so $B_2 \cong C_2$. Is it true that $\mathfrak{sp}_4 \cong \mathfrak{o}_5$? Yes, $\mathfrak{sp}_4$ has 4-dim tautological representation V; consider $\bigwedge^2 V = k \oplus E$ where $E = \bigwedge^2_0 V$ is 5-dim. The map $\mathfrak{sp}_4 \to \mathfrak{gl}(E)$ factors through $\mathfrak{o}_5(E)$ since $\bigwedge^2 V$ has an inner product

$$\bigwedge^2 V \otimes \bigwedge^2 V \longrightarrow \bigwedge^4 V \cong k$$

which is symmetric. Its an exercise that $\mathfrak{sp}_4 \to \mathfrak{o}_5$ given by this is an isomorphism (hint: $\mathfrak{sp}_4$ is simple). $\triangle$

1.20.1 Abstract root systems

Let $E \cong \mathbb{R}^n$ be a **Euclidean space**, i.e. real vector space with positive inner product.

Definition 1.20.1. A **root system** $R \subset E \setminus 0$ is a *finite* subset of nonzero vectors s.t.

(R1) R spans E

(R2) For all $\alpha, \beta \in R$, the number

$$n_{\alpha\beta} := \frac{2(\alpha, \beta)}{(\alpha, \alpha)}$$

is an integer.

(R3) If $\beta \in R$, then

$$s_\alpha(\beta) := \beta - \frac{2(\alpha, \beta)}{(\alpha, \alpha)}\alpha = \beta - n_{\alpha\beta}\alpha$$

is also a root (i.e. in R).

The number $r = \dim E$ is called the **rank** of the root system. ⋄

Remark 1.20.2. Applying R3 for $\beta = \alpha$ shows that

$$\alpha \in R \implies s_\alpha(\alpha) = -\alpha \in R$$

so R is centrally symmetric. ○

Remark 1.20.3. s_α is really the reflection with respect to the hyperplane $H = \{x \in E : (\alpha, x) = 0\}$. In particular, $s_\alpha^2 = \mathrm{Id}$. ○

Remark 1.20.4. We can "take slices." If $R \subset E$ is a root system, and $F \subset E$ is a subspace, then $R' = R \cap F$ inside $E' = \operatorname{span}\{R'\} \subset F$ is also a root system. ○

Definition 1.20.5. A root system $R \subset E$ is **reduced** if whenever $\alpha, \beta \in R$ are collinear, we have $\alpha = \pm\beta$. ⋄

Exercise. $\{1, 2, -1, -2\} \subset \mathbb{R}$ is a nonreduced root system.

Definition 1.20.6. Given $\alpha \in R$, $\alpha^\vee \in E^\vee$ is defined by the formula

$$\alpha^\vee(x) = \frac{2(\alpha, x)}{(\alpha, \alpha)}$$

and called a **coroot**. ⋄

Remark 1.20.7. $\alpha^\vee(\alpha) = 2$, $n_{\alpha\beta} = \alpha^\vee(\beta)$, and $s_\alpha(\beta) = \beta - \alpha^\vee(\beta)\alpha$. ○

Theorem 1.20.8 (Proven earlier)**.** *If $\mathfrak{g}$ is a semisimple Lie algebra with Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$, then the corresponding $R \subset \mathfrak{h}^*$ is a reduced root system. Moreover, the coroots are $\alpha^\vee = h_\alpha$.*

We will eventually show that every reduced root system in fact gives rise to a semisimple Lie algebra.

Example. $\mathfrak{g} = \mathfrak{sl}_n$ with $R = \{e_i - e_j\}$. Note that $(e_i - e_j, e_i - e_j) = 2$, so

Question: What is this inner product again?

Answer: It's just the normal dot product

$$\begin{aligned} s_{e_i - e_j}(x) &= x - (x, e_i - e_j)(e_i - e_j) = x - (x_i - x_j)(e_i - e_j) \\ &= x - \operatorname{diag}(0, \ldots, 0, \underbrace{x_i - x_j}_{i\text{th spot}}, 0, \ldots, 0, \underbrace{x_j - x_i}_{j\text{th spot}}, 0, \ldots, 0) \\ &= \operatorname{diag}(x_1, \ldots, \underbrace{x_j}_{i\text{th spot}}, \ldots, \underbrace{x_i}_{j\text{th spot}}, \ldots, x_n) \end{aligned}$$

which says that $s_{e_i - e_j} = (ij)$ just acts by transposing the ith and jth coordinates. △

Definition 1.20.9. Suppose $R_1 \subset E_1$ and $R_2 \subset E_2$ are root systems. An **isomorphism** $\varphi : R_1 \to R_2$ is a linear isomorphism $\varphi : E_1 \to E_2$ such that $\varphi(R_1) = R_2$, and $n_{\alpha,\beta} = n_{\varphi(\alpha),\varphi(\beta)}$ for any $\alpha, \beta \in R$. In particular, it *does not* have to preserve the inner product (e.g. it may rescale it). ⋄

Definition 1.20.10. The **Weyl group** W of R is the group of automorphisms of E generated by s_α. ⋄

Proposition 1.20.11. *W is a finite subgroup of $O(E)$ (and any element of W maps R to itself).*

Proof. The parenthetical follows from R3. Every s_α is an orthogonal reflection, so we also immediately get that $W \subset O(E)$. We need to show that W is finite. Well, the roots span E (by R1), so an element of W is determined by its action on R, so $W \hookrightarrow \operatorname{Aut}(R)$ and hence is finite. ■

Example. Root system of type A_{n-1}. We say $s_{e_i - e_j} = (ij)$. We have all transpositions, so $W = S_n$ is the symmetric group on n elements. △

Remark 1.20.12. $\operatorname{Aut}(R)$ may be bigger than W. e.g. for A_{n-1} with $n \geq 3$, we have $x \mapsto -x$ not in S_n (if it were in S_n, it'd be a central element). Note that $x = (x_1, x_2) = (a, -a)$ so negating is the same as changing these two pieces. ∘

1.20.2 Root systems of rank 2

Say α, β a pair of **independent roots** (i.e. $\beta \neq \pm\alpha$). Let $E' = \operatorname{span}\{\alpha, \beta\}$ and $R' = R \cap E'$, so $R' \subset E'$ is a root system of rank 2.

Theorem 1.20.13. *Let R be a reduced root system with $\alpha, \beta \in R$ independent. Assume WLOG $|\alpha| \geq |\beta|$, and let φ be the angle between α, β. Then, we have one of the following possibilities*

Remember: If α is longer than β, then $n_{\alpha\beta}$ is the smaller one.

- ***(1)*** *$\varphi = \frac{\pi}{2}$ ($= 90°$) and $n_{\alpha\beta} = n_{\beta\alpha} = 0$, i.e. α, β are orthogonal.*
- ***(2a)*** *$\varphi = \frac{2\pi}{3}$ ($= 120°$), $n_{\alpha\beta} = n_{\beta\alpha} = -1$, and $|\alpha|^2 = |\beta|^2$.*
- ***(2b)*** *$\varphi = \frac{\pi}{3}$ ($= 60°$), $n_{\alpha\beta} = n_{\beta\alpha} = 1$, and $|\alpha|^2 = |\beta|^2$.*
- ***(3a)*** *$\varphi = \frac{3\pi}{4}$ ($= 135°$), $n_{\alpha\beta} = -1$, $n_{\beta\alpha} = -2$, and $|\alpha|^2 = 2|\beta|^2$.*
- ***(3b)*** *$\varphi = \frac{\pi}{4}$ ($= 45°$), $n_{\alpha\beta} = 1$, $n_{\beta\alpha} = 2$, and $|\alpha|^2 = 2|\beta|^2$.*
- ***(4a)*** *$\varphi = \frac{5\pi}{6}$ ($= 150°$), $n_{\alpha\beta} = -1$, $n_{\beta\alpha} = -3$, and $|\alpha|^2 = 3|\beta|^2$.*
- ***(4b)*** *$\varphi = \frac{\pi}{6}$ ($= 30°$), $n_{\alpha\beta} = 1$, $n_{\beta\alpha} = 3$, and $|\alpha|^2 = 3|\beta|^2$.*

Proof. We know $(\alpha, \beta) = |\alpha|\,|\beta| \cos\varphi$. Thus,

$$2\frac{|\beta|}{|\alpha|}\cos\varphi = n_{\alpha\beta} \in \mathbb{Z}.$$

In particular,

$$4\cos^2\varphi = n_{\alpha\beta} n_{\beta\alpha} \in \mathbb{Z}.$$

Hence, $4\cos^2\varphi \in \{0,1,2,3\}$. Now, it's just casework. $4\cos^2\varphi = n \in \{0,1,2,3\}$ corresponds to (some subcase of) case $(n+1)$. Use that $n_{\alpha\beta}/n_{\beta\alpha} = |\alpha|^2 / |\beta|^2$ when $n_{\beta\alpha} \neq 0$. ■

In fact, all the above possibilities are realized. **(1)** is root system $A_1 \times A_1$. **(2a)**,**(2b)** are realized in A_2. **(3a)**,**(3b)** are realized in B_2. Finally, **(4a)**,**(4b)** are realized by taking the root system of type A_2 (the hexagon) and then extending it by adding the sum of adjacent vectors: This gives the **root system**

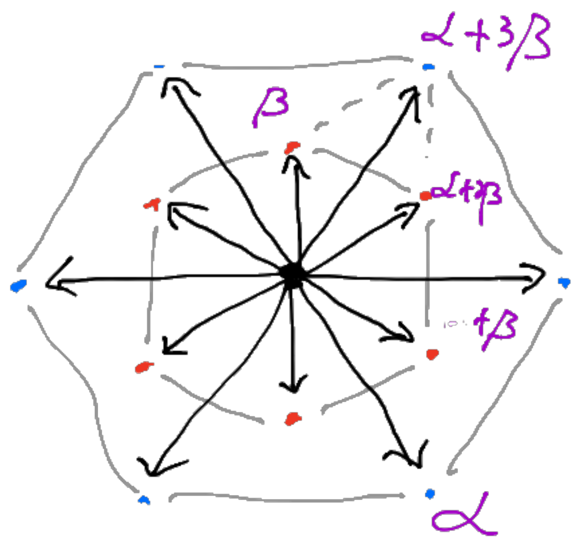


Figure 1: The G_2 root system

of type G_2.

Theorem 1.20.14. *Any reduced root system of rank 2 is one of the above, i.e. it is $A_1 \times A_1$, A_2, B_2, or G_2.*

Remark 1.20.15. A_2 is a hexagon, B_2 is a square (vertices + midpoints), and G_2 is this double hexagon thing I haven't actually drawn. ∘

Proof. Pick $\alpha, \beta \in R$ with $|\alpha| \geq |\beta|$ and angle $\varphi(\alpha, \beta)$ maximal possible; in particular, $\varphi \geq \frac{\pi}{2}$ (otherwise change sign of α). Thus, $\varphi = \pi/2, 2\pi/3, 3\pi/4, 5\pi/6$. Now, it's just case work. These give $A_1 \times A_1, A_2, B_2, G_2$, respectively.

Let's look at the $\pi/2$ case. Then, we have

$$\begin{tikzcd} & \beta \arrow[d, dash] & \\ -\alpha \arrow[r, dash] & {} & \alpha \arrow[l, dash] \\ & -\beta \arrow[u, dash] & \end{tikzcd}$$

but there can be no other roots, because they'd give an angle larger thatn $90°$. Thus, this is everything which is precisely $A_1 \times A_1$. ■

Corollary 1.20.16. *If $\alpha, \beta \in R$ are independent and $(\alpha, \beta) < 0$ (i.e. their angle is obtuse), then $\alpha + \beta$ is a root.*

Proof. By inspection of $A_1 \times A_1, A_2, B_2, G_2$. ■

1.20.3 Positive and simple roots

We first talk about polarizations. Fix $t \in E^*$ with $t(\alpha) \neq 0$ for all $\alpha \in R$. Then, $R = R_+ \sqcup R_-$ where $R_+ = \{\alpha : t(\alpha) > 0\}$ and $R_- = -R_+ = \{\alpha : t(\alpha) < 0\}$. Imagine picking a half-plane and then just separating the roots by which side of the plane they fall in. This decomposition (or maybe the choice of t?) is called a **polarization**. The set R_+ consists of **positive roots** while R_- is the **negative roots**.

Example. A_{n-1} so $R = \{e_i - e_j\}$. Take $t = (t_1, \ldots, t_n)$ so $t(\alpha) \neq 0 \iff t_i \neq t_j$ (distinct coord). Say $t_1 > t_2 > \cdots > t_n$. Then, $e_i - e_j \in R_+ \iff i < j$, so there are $n!$ polarizations (labeled by S_n). Furthermore $W = S_n$ acts transitively on the set of all polarizations; we will see this is the case in general. △

1.21 Lecture 21 (11/12)

Last time we talked about polarizations of root systems $R \subset E$. We choose $t \in E$ s.t. $(t, \alpha) \neq 0$ for all $\alpha \in R$, and then set

$$R_+ = \{\alpha \in R : (t, \alpha) > 0\} \text{ and } R_- = \{\alpha \in R : (t, \alpha) < 0\},$$

so $R = R_+ \sqcup R_-$ and $R_+ = -R_-$.

1.21.1 Simple roots

Given some polarization, a root $\alpha \in R_+$ is **simple** if it is not the sum of two other positive roots.

Lemma 1.21.1. *Every positive root is a sum of simple roots.*

Proof. If $\alpha \in R_+$ is not simple, then $\alpha = \beta + \gamma$ with $\beta, \gamma \in R_+$. Note that $(t, \alpha) = (t, \beta) + (t, \gamma) \implies (t, \beta), (t, \gamma) < (t, \alpha)$. Now induct. There are only finitely many steps since there are only finitely bounded non-negative integers (recall, $(t, R_+) \subset \mathbb{Z}_{>0}$). ■

Lemma 1.21.2. *For every two simple $\alpha, \beta \in R_+$, we have $(\alpha, \beta) \leq 0$.*

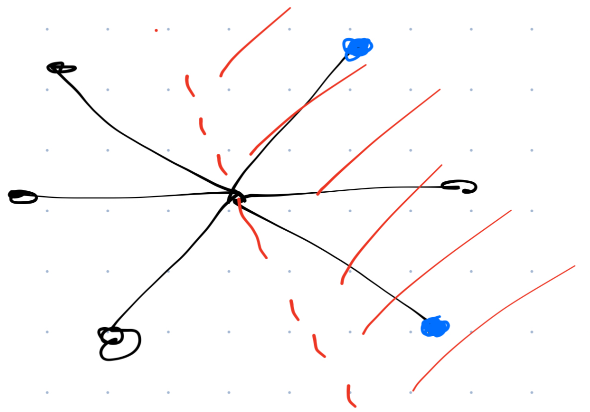


Figure 2: An example of (blue) simple roots for a polarization of A_2.

Proof. Contrapositve. Suppose $(\alpha, \beta) > 0$ for $\alpha, \beta \in R_+$. Then, $(-\alpha, \beta) < 0$, so $\gamma := \beta - \alpha$ is a root by Corollary 1.20.16. If $\gamma \in R_+$, then $\beta = \gamma + \alpha$ is a sum of two positive roots, so β would not be simple. If $\gamma \in R_-$, then $\alpha = \beta + (-\gamma)$ is a sum of two positive roots, so α would not be simple. One of these is the case. ■

Theorem 1.21.3. *The set $\Pi \subset R_+$ of simple roots is a basis of E. In particular, $|\Pi| = \sigma := \operatorname{rank}(E, R)$.*

We use the following lemma from linear algebra.

Lemma 1.21.4. *Let v_i be a collection of vectors in a Euclidean space s.t.*

This is giving me Bourbaki flashbacks.

- $(v_i, v_j) \leq 0$ *for all* $i \neq j$
- $(t, v_i) > 0$ *for some* $t \in E$.

Then the v_i are linearly independent.

Proof. Write $\sum_{i \in I} c_i v_i = \sum_{j \in J} c_j v_j$ with $c_i, c_j > 0$ and $I \cap J = \emptyset$ (and we're suppose $I \cup J \neq \emptyset$). Evaluate t on this relation to get $\sum c_i(t, v_i) = \sum c_j(t, v_j) > 0$ (so both I, j are nonempty). Square the LHS to get

$$0 < \left| \sum_{i \in I} c_i v_i \right|^2 = \left(\sum_{i \in I} c_i v_i, \sum_{j \in J} c_j v_j \right) \leq 0,$$

a contradiction. ■

Proof of Theorem 1.21.3. By this lemma, the simple roots are linearly independent. They are also spanning since the roots span E but ever positive root is a sum of simple roots. ■

Example. Recall A_{n-1} has roots $e_i - e_j$. For $t = (t_1, \ldots, t_n)$ with $t_1 > t_2 > \cdots > t_n$, the positive roots are $e_i - e_j$ for $i < j$. The simple roots are $\alpha_i := e_i - e_{i+1}$ for $i = 1, \ldots, n-1$. Note that $e_i - e_j = \alpha_i + \alpha_{i+1} + \cdots + \alpha_{j-1}$. △

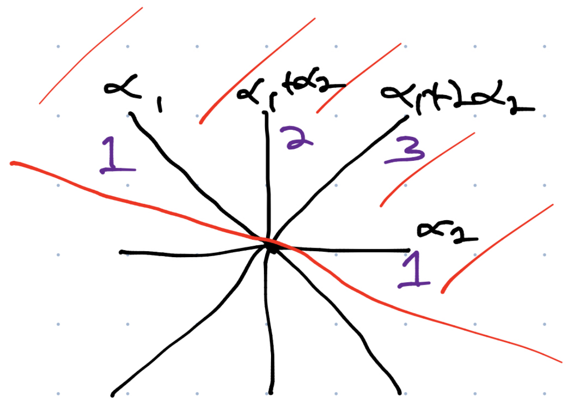


Figure 3: A picture of a polarized B_2 with heights of positive roots labelled in purple

Corollary 1.21.5. *Any root α can be uniquely written as an integral combination of simple roots, i.e.*

$$\alpha = \sum_{i=1}^{r} n_i \alpha_i \text{ with } n_i \in \mathbb{Z}$$

and α_i simple. Futhermore, $n_i > 0$ if $\alpha \in R_+$ and $n_i < 0$ if $\alpha \in R_-$.

Definition 1.21.6. The **height** of $\alpha \in R_+$ is $h(\alpha) = \sum n_i$, the number of simple roots needed to write α. ◇

Example. In the example given in figure 2, there are two simple roots (of height 1) and one positive root of height 2. △

Example. In G_2, there are two simple roots, and one positive root of each height $h \in \{2, 3, 4, 5\}$. I'm not drawing this. △

1.21.2 Dual root system

Let $R \subset E$ be a root system. For $\alpha \in R$, we defined the coroot $\alpha^\vee \in E^*$ s.t.

$$(\alpha^\vee, x) = \frac{2(\alpha, x)}{(\alpha, \alpha)}.$$

Exercise. $R^\vee = \{\alpha^\vee : \alpha \in R\} \subset E^*$ is also a root system, called the **dual root system**. Furthermore, $(R^\vee)^\vee = R$, and polarizations of R are in bijection with polarizations of $R^\vee$ (since we have an iso $E \xrightarrow{\sim} E^*$ given by the form on E). In fact, $R_+^\vee = \{\alpha^\vee : \alpha \in R_+\}$ and similarly for the simple roots: $\Pi^\vee = \{\alpha_i^\vee : \alpha_i \in \Pi\}$.

Example. $R = B_n$ so consists of vectors

$$e_i - e_j, e_i + e_j, e_i, -e_i - e_j, -e_i.$$

In this case, we have $E = \mathbb{R}^n$ and we're identifying it with E^* via the usual inner product. Then,

$$R^\vee : e_i - e_j, e_i + e_j, -e_i - e_j, 2e_i, -2e_i$$

since $e_i^\vee = 2e_i/(e_i, e_i) = 2e_i$. Hence, $R^\vee = C_n$. △

Exercise. A_{n-1}, D_n and G_2 are self-dual. For G_2, the roots and coroots do not coincide on the nose, but the systems are abstractly isomorphic.

1.21.3 Root and Weight lattices

We should probably start with recalling what a lattice is.

Recall 1.21.7. A **lattice** in a real vector space E is the subgroup ($\mathbb{Z}$-module) generate by a basis of E. ⊙

As a $\mathbb{Z}$-module, any lattice is isomorphic to $\mathbb{Z}^n$.

Definition 1.21.8. If $L \subset E$ is a lattice, then the **dual lattice** $L^* \subset E^*$ is defined as

$$L^* = \{f \in E^* : f(L) \subset \mathbb{Z}\}.$$

If L is generated by $e_i \in E$, then Q^* is generated by the dual basis. ⋄

Let's return to thinking about root systems. For any polarized root system $R \subset E$, we have a canonical lattice Q generated by the simple roots. In fact, Q is independent of the polarization since it is simple the span of *all* the roots; we call Q the **root lattice**. There is also the **coroot lattice** $Q^\vee \subset E^*$ which is just the root lattice for the dual root system (spanned by the coroots). The dual lattice $P^\vee := Q^* \subset E^*$ is called the **coweight lattice**

$$P^\vee = \{\lambda \in E^* : (\lambda, \alpha) \in \mathbb{Z} \forall \alpha \in R\}.$$

Finally, the **weight lattice** is

$$P = (Q^\vee)^* = \{\lambda \in E : (\lambda, \alpha^\vee) \in \mathbb{Z} \forall \alpha \in R\} \subset E.$$

Hence, the weight lattice of $R^\vee$ is the coweight lattice of R.

Now, we know that $\alpha, \beta \in R \implies (\alpha, \beta^\vee) \in \mathbb{Z}$, so $Q \subset P$ and $Q^\vee \subset P^\vee$ ((co)root lattice contained in (co)weight lattice).

Example. A_1 which one two roots $\pm\alpha$. We have $(\alpha, \alpha^\vee) = 2$, so $P = \left\langle \frac{1}{2}\alpha \right\rangle$. Hence, $P/Q = \mathbb{Z}/2\mathbb{Z}$. △

Example. $R = A_{n-1}$. Hence, $R \subset E = \{x \in \mathbb{R}^n : \sum x_i = 0\} \cong E^*$ with identification to the dual coming from the standard inner product. Then, $R^\vee = R$, $Q^\vee = Q$, and $P^\vee = P$. We know

$$Q = \{x \in E : x_i \in \mathbb{Z}\}$$

since the roots are $e_i - e_j$. Now,

$$P = \left\{\lambda \in \mathbb{R}^n : \sum \lambda_i = 0 \text{ and } \lambda_i - \lambda_j \in \mathbb{Z} \forall i, j\right\}.$$

This does not mean that $\lambda_i \in \mathbb{Z}$, only that they all have the same fractional part. We have a homomorphism $\varphi : P \to \mathbb{R}/\mathbb{Z}$ sending λ to its common fractional part. Furthermore, $\sum \lambda_i = 0$ tells us that in face φ lands in $\mathbb{Z}/n\mathbb{Z} \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{R}/\mathbb{Z}$. The kernel of φ is exactly Q, so we have $P/Q \hookrightarrow \mathbb{Z}/n\mathbb{Z}$. In fact, this is easily seen to be surjective, so

$$\varphi : P/Q \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}.$$

△

Remark 1.21.9. Note that P/Q will always be some finite abelian group. It turns out that for G_2 it is trivial. For D_n, it will have order 4, but will be $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ depending on the parity of n. ○

1.21.4 Fundamental (co)weights

The **fundamental weights** are $\omega_i \in E$ defined by

$$(\omega_i, \alpha_j^\vee) = \delta_{ij}$$

and **fundamental coweights** $\omega_i^\vee \in E^*$ s.t.

$$(\omega_i^\vee, \alpha_j) = \delta_{ij}.$$

Hence, these give dual bases to $\alpha_i, \alpha_i^\vee$. Note that P is generated by ω_i and $P^\vee$ is generated by $\omega_i^\vee$.

Example. Pavel drew the root lattice for A_2 along with the fundamental weights, but this is beyond my quick artistic skills. The root lattice is a hexagonal lattice consisting of a bunch of triangles, and the weight lattice contains the centers of all of these triangles. Looking at it shows that $[P : Q] = 3$, so $P/Q \cong \mathbb{Z}/3\mathbb{Z}$. △

1.21.5 Weyl chambers

How different are the different systems of simple roots? Suppose $\Pi, \Pi' \subset R$ are two systems of simple roots. Are they equivalent in some sense?

Recall the polarization is determined by some $t \in E$ such that $(t, \alpha) \neq 0$ for all $\alpha \in R$. In fact, it only depends on the signs of (t, α). As long as we vary t in a way that does not affect these signs, the polarization won't change either.

Definition 1.21.10. A **Weyl chamber** is a connected component of $E \setminus \bigcup_{\alpha \in R} L_\alpha$ where

$$L_\alpha = \{x \in E : (\alpha, x) = 0\}.$$

Moving t withing a Weyl chamber will not change the polarization. ◇

Remark 1.21.11. A Weyl chamber is defined by a system of strict linear homogeneous inequalities $I(\alpha, x) = 0$ for $\alpha \in R$. For each L_α, you get a sign saying which side of the line the chamber lies on. Not every choice of signs will give a non-empty set, but if it is non-empty, then it is a Weyl chamber. ○

Lemma 1.21.12 ("Obvious").

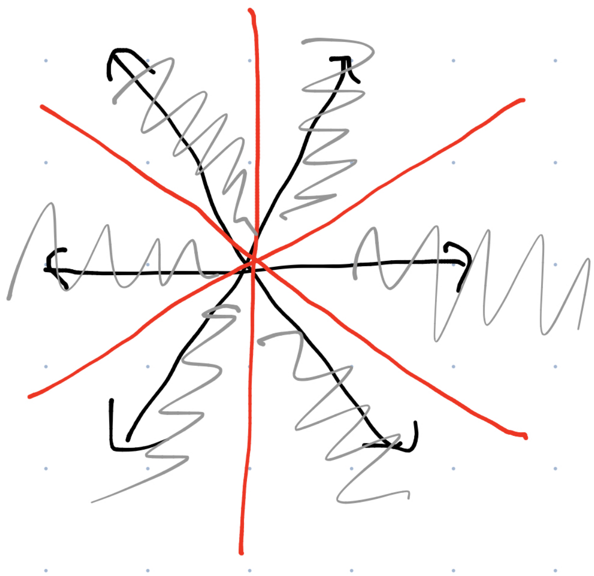


Figure 4: The 6 Weyl chambers for A_2. Each chamber has 2 faces, and each face is a ray (not a whole line).

(1) *For any Weyl chamber C, its closure $\overline{C}$ is a convex cone.*

(2) *The boundary $\partial\overline{C}$ of C' closure is a union of codimension 1 faces F_i which are convex cones inside root hyperplanes define inside hypeplane by a system of non-strict homogeneous linear inequalities. ("so it's clear" – Pavel, 2020)*

Question: What is this saying?

Definition 1.21.13. The root hyperplanes containing F_i are called the walls of C. $\diamond$

It's clear that a Weyl chamber gives rise to a polarization. We can also go back. Given a polarization of R, we can attach to it the **positive Weyl chamber** C_+ defined by $(x, \alpha_i) > 0$ for all $\alpha_i \in \Pi$. We can describe this in terms of fundamental weights. Writing $x = \sum_{i=1}^r x_i\omega_i$, we have $(x, \alpha_j) = x_j$, so

$$C_+ = \left\{ \sum_i x_i\omega_i : x_i > 0 \right\} \cong \mathbb{R}^r_{>0}.$$

Hence the walls are $L_{\alpha_i} = \{x_i = 0\}$.

Lemma 1.21.14. *These assignments are mutually inverse bijections between Weyl chambers and polarizations of R.*

Proof. Exercise. ∎

It is clear that the Weyl group (generated by the reflections s_α, $\alpha \in R$) acts on the set of Weyl chambers, e.g. because these chambers are determined by root hyperplanes and the Weyl group permutes the roots so permutes the hyperplanes.

Theorem 1.21.15. *The Weyl group acts transitively on the set of Weyl chambers.*

Proof. Say Weyl chambers C, C' are **adjacent** if they have a common face. If that face $F \subset L_\alpha$, then $s_\alpha(C) = C'$ (and $s_\alpha(C') = C$) since s_α is just reflection across that line. Now, if you have any Weyl chambers C, C', pick some $t \in C$ and $t' \in C'$. Connect them with a line segment. This well give a sequence

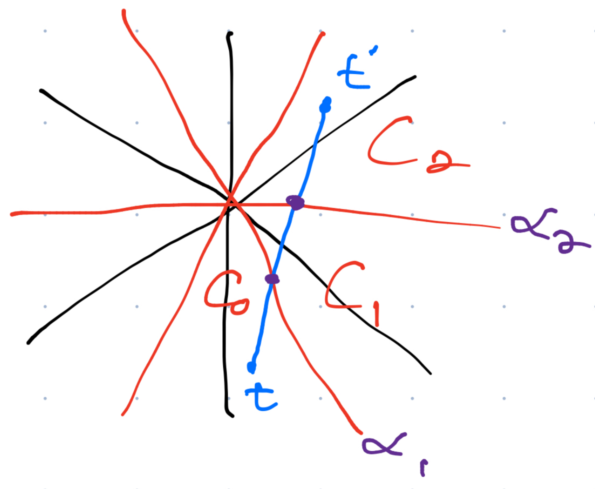


Figure 5: Artist's rendition of the proof that the Weyl group acts transitively on chambers

of Weyl chambers $C = C_0, C_1, \ldots, C_m = C'$ s.t. C_i, C_{i+1} are adjacent (if you pick t, t' generically). Thus, C, C' are in the same W-orbit, so we win. ■

Corollary 1.21.16. *Every Weyl chamber is* $\cong \mathbb{R}^r_{>0}$ *and has exactly* r *walls.*

Proof. C_+ looks like this. Any C can be mapped to C_+ by an element of the Weyl group. ■

Corollary 1.21.17. *Any two polarizations are relate by an action of* $w \in W$*. Hence if* Π, Π' *are two systems of simple roots, then* $\exists w \in W$ *s.t.* $w(\Pi) = \Pi'$*.*

1.21.6 Simple reflections

Suppose we have a polarization of R, say $\Pi = \{\alpha_1, \ldots, \alpha_r\}$. The **simple reflections** are $s_{\alpha_i} =: s_i$ for $i = 1, \ldots, r$.

Proposition 1.21.18. *For all Weyl chambers* C*, there exists* $i_1, \ldots, i_m$ *s.t.*

$$C = s_{i_1} \ldots s_{i_m}(C_+).$$

Proof. Next time. ■

Corollary 1.21.19.

(i) s_i *generate* W

(ii) $W(\Pi) = R$*.*

Proof. For any $\alpha \in R$, L_α is a wall for some chamber C, so $L_\alpha = s_{i_1} \ldots s_{i_m}(L_{\alpha_j})$ which implies that s_α is conjugate of s_j by $s_{i_1} \ldots s_{i_m}$. **(ii)** follows from **(i)**. ■

In particular, Π determines R (Take $S = \langle s_{\alpha_i} : \alpha_i \in \Pi \rangle$ and then $R = W(\Pi)$).

Homework due tonight. New homework coming out (due on Thursday). Lecture at MIT on Tuesday; it's the last lecture at MIT.

1.22 Lecture 22 (11/17)

We talked about combinatorics of root systems last time. We will continue with this today.

1.22.1 Simple reflections

Let $R \subset E$ be a reduced root system, and let $t \in E$ be a polarization, so we have a set $\Pi = \{\alpha_1, \ldots, \alpha_r\} \subset R$ be the set of simple roots (note $r = \dim E$).

Definition 1.22.1. A **simple reflection** is $s_{\alpha_i} = s_i \in W$. $\diamond$

We will see that these generate W and one can even write down some relations for them.

Lemma 1.22.2. *For every Weyl Chamber C, there exists $i_1, \ldots, i_n$ s.t. $s_{i_1} \ldots s_{i_m}(C_+) = C$.*

Proof. Pick $t \in C$ and $t_+ \in C_+$ generically, and draw a line segment connecting t and t_+. Let m be the number of root hyperplanes ($h_\alpha = \{x \in E : \alpha(x) = 0\}$) intersected by this segment. We induct on m. The base case ($m = 0$, so $C = C_+$) is trivial, so assume $m > 0$. Let C' be the chamber entered from C along this segment. To get from C' to C_+, we only need cross $m-1$ hyperplanes, so by inductive hypothesis, $C' = s_{i_1} \ldots s_{i_{m-1}}(C_+)$. Now C, C' are adjacent, so they are separated by a wall L_α. Letting $u = s_{i_1} \ldots s_{i_{m-1}}$, we have $u^{-1}(C') = C_+$ so $u^{-1}L_\alpha = L_{\alpha_i}$ for some i (as $u^{-1}L_\alpha$ is a wall adjacent to C_+). Thus, reflection across L_α is $s_\alpha = u s_i u^{-1}$ (change coordinates so L_α becomes L_i, reflect across L_i, and then change coordinates back to normal). This implies that $C = s_\alpha(C') = u s_i u^{-1}(C') = u s_i u^{-1} u(C_+) = u s_i(C_+) = s_{i_1} \ldots s_{i_{m-1}} s_i(C_+)$ which completes the induction. $\blacksquare$

Note that we build $s_1 \ldots s_{i_m}$ by appending elements to the right because of this conjugation trick

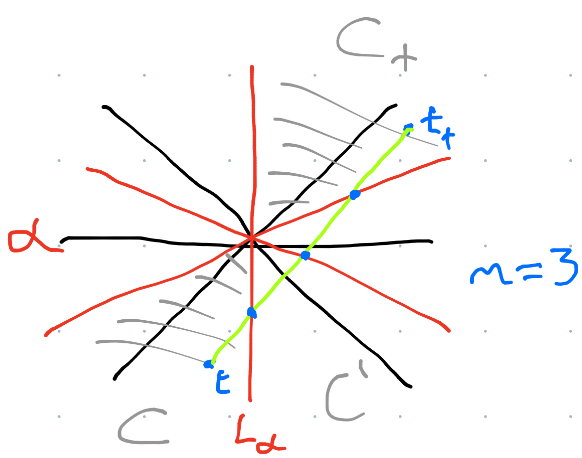


Figure 6: A drawing of this proof

Corollary 1.22.3. *(i) Simple reflections generate W, and (ii) $W(\Pi) = R$.*

Proof. **(i)** For all α, L_α is a wall of some chamber $C = u(C_+)$ which implies $s_\alpha = us_iu^{-1}$ for some i where $u = s_{i_1} \dots s_{i_{m-1}}$. Thus, s_α is a product of simple reflections. Hence, W is generated by the s_i. Now, **(ii)** follows from **(i)**. ■

Here's (Figure 7) a potentially better picture/example of the previous proof than Figure 6.

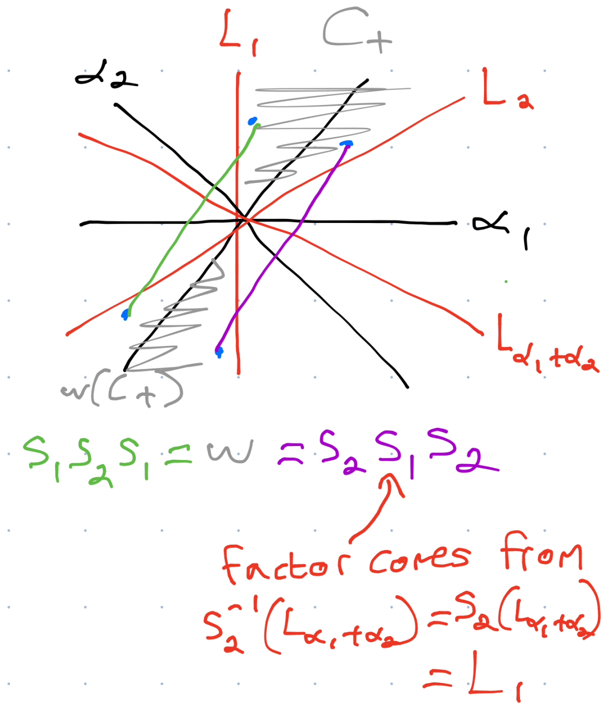


Figure 7: An example of carrying out the process in the proof of Lemma 1.22.2

In particular, the root system R be reconstructed from Π as $W = \langle s_i = s_{\alpha_i} \rangle$ and $R = W(\Pi)$.

Example. A_{n-1}. Then $s_i = s_{e_i - e_{i+1}} = (i, i+1)$ is a transposition of neighbors. Thus, we recover the statement that the symmetric group S_n is generated by transpositions of neighbors. △

1.22.2 Length of elements in the Weyl group

Say a wall L_α **separates** C, C' if they lie on two different sides of L_α.

Definition 1.22.4. The **length** of an element $w \in W$ of the Weyl group is the number of walls separating the chambers C_+ and $w(C_+)$. This is denoted by $\ell(w)$. ⋄

Remark 1.22.5. Choose $t \in C_+$ defining the polarization. Then,

$$\begin{aligned}
\ell(w) &= \#\left\{(\alpha, t) > 0 \ \text{ but } \ (\alpha, wt) < 0\right\} \\
&= \#\left\{\alpha \in R : (\alpha, t) > 0 \ \text{ and } \ (w^{-1}\alpha, t) < 0\right\} \\
&= \#\left\{\alpha \in R : \alpha \in R_+ \ \text{ and } \ w^{-1}\alpha \in R_-\right\}
\end{aligned}$$

$$= \#(R_+ \cap wR_-).$$

Also note that $\ell(w) = \ell(w^{-1})$. We conclude that

$$\ell(w) = \# \{\alpha \in R_+ : w(\alpha) \in R_-\}.$$

$\circ$

Example. $\ell(1) = 0$.

Also, $\ell(s_i) = 1$ since C_+ and $s_i(C_+)$ are adjacent ($s_i(C_+)$ is just reflecting it about one of its walls). This means s_i maps only one positive root to a negative root, namely α_i since $s_i(\alpha_i) = -\alpha_i$. Thus, s_i permutes $R_+ \setminus \{\alpha_i\}$. $\triangle$

Corollary 1.22.6. *Define*

$$\rho = \frac{1}{2} \sum_{\alpha \in R_+} \alpha \in E.$$

Then, its coordinates $(\rho, \alpha_i^\vee) = 1$ *for all* i*, i.e.* $\rho = \sum_i \omega_i$ *is the sum of the fundamental weights.*

Remember: Fundamental weights are dual basis to coroots, so $(\omega_i, \alpha_j^\vee) = \delta_{ij}$

Proof. Write $\rho = \frac{1}{2}\alpha_i + \frac{1}{2} \sum_{\substack{\alpha \in R_+ \\ \alpha \neq \alpha_i}} \alpha$. Then, $s_i(\rho) = -\frac{1}{2} + \frac{1}{2} \sum_{\substack{\alpha \in R_+ \\ \alpha \neq \alpha_i}} \alpha = \rho - \alpha_i$. Hence,

$$\rho - (\rho, \alpha_i^\vee)\alpha_i = s_i \rho = \rho - \alpha_i \implies (\rho, \alpha_i^\vee) = 1.$$

$\blacksquare$

Example. In A_{n-1}, write $\rho = (\rho_1, \dots, \rho_n)$. Then, $\alpha_i^\vee = e_i - e_{i+1} \implies \rho_i - \rho_{i+1} = 1$. The coordinates should sum to 0, so

Question: why?

Answer: The Euclidean vector space for A_{n-1} is $E = \{\lambda \in \mathbb{R}^n : \sum \lambda_i$

$$\rho = \left(\frac{n-1}{2}, \frac{n-3}{2}, \dots, -\frac{n-1}{2} \right).$$

$\triangle$

Theorem 1.22.7. *Let $w = s_{i_1} \dots s_{i_\ell}$ be a representation of $w \in W$ as a product of simple reflections, with minimal length (such a product is called a* ***reduced decomposition****). Then, $\ell(w) = \ell$.*

Proof. Connect C_+ and $w(C_+)$ by a chain of Weyl chambers: $C_k = s_{i_1} \dots s_{i_k}(C_+)$. So $C_0 = C_+$, $C_\ell = w(C_+)$, and C_k, C_{k+1} are adjacent. We can pick a generic point $t_k \in C_k$ and connect these via line segments to get a "zigzag" path from C_+ to $w(C_+)$ intersecting ℓ walls. Hence, $\ell \geq \ell(w)$.

We have not yet used that this decomposition is reduced. Consider instead a straight path from $t \in C_+$ to $w(t) \in w(C_+)$ (t chosen generically as usual); it intersects exactly $\ell(w)$ walls. Furthermore, this gives a corresponding decomposition of w of length $\ell(w)$, so minimality tells us that $\ell \leq \ell(w)$ too. $\blacksquare$

Corollary 1.22.8. *The Weyl group acts simply transitively on Weyl chambers. Hence, #Weyl chambers = #polarizations = $\#W$.*

Proof. We have shown already that it acts transitively. We only need show that $w(C_+) = C_+ \implies w = 1$. For such w, we know $\ell(w) = 0$, so there must be a decomposition of w into a product of 0 simple reflections, so $w = 1$. $\blacksquare$

This tells us that $\overline{C}_+$ is a fundamental domain for the action of W on E. Moreover, on the homework, we'll show that $\overline{C}_+ = E/W$ as topological spaces, so any W-orbit contains a unique element of $\overline{C}_+$.

Corollary 1.22.9. *Let $C_- = -C_+$ be the negative Weyl chamber. Then $\exists! w_0 \in W$ such that $w_0(C_+) = C_-$ and $\ell(w_0) = |R_+|$. Furthermore, for any $w \in W$ with $w \neq w_0$, $\ell(w) < \ell(w_0)$. Finally, $w_0^2 = 1$.*

Proof. Exercise (hint: uses $\ell(w) = \#\{\alpha \in R_+ : w(\alpha) \in R_-\}$) ■

Example. For A_{n-1} with $W = S_n$, w_0 is the permutation reversing the order, i.e. $w_0(k) = (n+1) - k$ for $k \in \{1, 2, \ldots, n\}$. △

Definition 1.22.10. The element $w_0 \in W$ is called the **longest element of** W. ◇

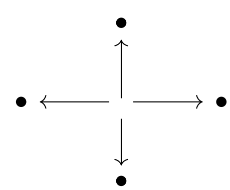
Remark 1.22.11. Keep in mind that all this length stuff depends on a choice of polarization. ○

1.22.3 Dynkin diagrams and Cartan matrices

We have seen that to classify root systems, we need to classify sets Π of simple roots.

Construction 1.22.12. Given roots systems $R_1 \subset E_1$ and $R_2 \subset E_2$, their **direct product root system** if $R_1 \sqcup R_2 \subset E_1 \oplus E_2$.

Example. $A_1 \times A_1$ has roots the four standard unit vectors.



Note that $R_1 \perp R_2$. △

Definition 1.22.13. A root system R is **irreducible** if it cannot be written as a nontrivial direct product. ◇

What happens to simple roots in direct sums. Given $t = (t_1, t_2) \in E_1 \oplus E_2$, the component t_i polarizes E_i, and one gets $\Pi = \Pi_1 \sqcup \Pi_2$. Note that $\Pi_1 = \Pi \cap R_1$ and $\Pi_2 = \Pi \cap R_2$.

Lemma 1.22.14. *Let R be a root system with $\Pi = \Pi_1 \sqcup \Pi_2$ and $\Pi_1 \perp \Pi_2$. Then, $R = R_1 \sqcup R_2$ is reducible with $R_1 = \langle \Pi_1 \rangle$ and $R_2 = \langle \Pi_2 \rangle$.*

Proof. For $\alpha \in \Pi_1$ and $\beta \in \Pi_2$, we're given $(\alpha, \beta) = 0$, so $s_\alpha(\beta) = \beta$ and $s_\beta(\alpha) = \alpha$. This implies that they commute: $s_\alpha s_\beta = s_\beta s_\alpha$. Thus, taking $W_1 = \langle s_\alpha : \alpha \in \Pi_1 \rangle$ and $W_2 = \langle s_\beta : \beta \in \Pi_2 \rangle$, these two commute and $W = W_1 \times W_2$. Since W_1 acts trivially on Π_2 and W_2 acts trivially on Π_1, we also have

$$R = W(\Pi) = W_1(\Pi_1) \sqcup W_2(\Pi_2) = R_1 \sqcup R_2.$$

■

Corollary 1.22.15. *Any root system has a unique decomposition into a direct product of irreducible root systems.*

Proof. To produce it, write $\Pi = \bigsqcup_i \Pi_i$ with Π_i mutually orthogonal with a maximal number of factors. Visually, consider the graph whose vertices are simple roots with edges between any two which are not orthogonal; the Π_i's are just connected components of this graph. ■

Thus, we see we only need to classify irreducible root systems. For this, we need to classify irreducible sets Π of simple roots. How should we encode a Π?

Since these live in a Euclidean space they correspond to some **Gram matrix** (α_i, α_j). However, this depends e.g. on the scaling of the inner product, so it's not the best choice. Instead, we prefer the **Cartan matrix** $A = (a_{ij})$ with $a_{ij} = (\alpha_i^\vee, \alpha_j)$. This now has integer coordinates and only depends on the ordering of the (simple) roots.

Proposition 1.22.16. *(1)* $a_{ii} = 2$

(2) $a_{ij} \in \mathbb{Z}_{\leq 0}$

(3) $a_{ij}a_{ji} = 4\cos^2\varphi \in \{0, 1, 2, 3\}$ *with* φ *the angle between* α_i, α_j.

(4) Let $d_i = |\alpha_i|^2$. *Then,* $d_i a_{ij} d_j a_{ji}$, *so the matrix* $\widehat{\alpha}_{ij} = d_i a_{ij}$ *is symmetric and positive definitive.*

We will see that these are exactly the properties a matrix needs to come from a root system.

Example. Look at A_{n-1}. We have $\alpha_i = e_i - e_{i+1}$ with $i = 1, \ldots, n-1$. Also, $\alpha_i^\vee = \alpha_i$. The Cartan matrix A here is tridiagonal with 2's on the main diagonal and -1's on the off-diagonal above and below it.

$$\begin{pmatrix} 2 & -1 & & \\ -1 & 2 & \ddots & \\ & \ddots & \ddots & -1 \\ & & -1 & 2 \end{pmatrix}$$

△

Example. Look at B_n. Fix $t = (t_1, \ldots, t_n)$ with $t_1 > t_2 > \cdots > t_n > 0$. The simple, positive roots are $\alpha_i = e_i - e_{i+1}$, $i = 1, \ldots, n-1$ and $\alpha_n = e_n$. We have $\alpha_i^\vee = \alpha_i$ except $\alpha_n^\vee = 2\alpha_n$. This is tridiagonal again. It has 2's on the main diagonal as always. Above the main diagonal is all -1's except the last (bottommost) entry is $-1 = (\alpha_{n-1}^\vee, \alpha_n) = (e_{n-1} - e_n, e_n)$. Below the main diagonal is all -1's except the last is $-2 = (\alpha_n^\vee, \alpha_{n-1}) = (2e_n, e_{n-1} - e_n)$.

$$\left(\begin{array}{cccc|c} 2 & -1 & & & \\ -1 & 2 & \ddots & & \\ & \ddots & \ddots & -1 & \\ & & -1 & 2 & -1 \\ \hline & & & -2 & 2 \end{array}\right)$$

△

Example. For C_n, the matrix you get is the transpose of the one for B_n.

$$\left(\begin{array}{cccc|c} 2 & -1 & & & \\ -1 & 2 & \ddots & & \\ & \ddots & \ddots & -1 & \\ & & -1 & 2 & -2 \\ \hline & & & -1 & 2 \end{array}\right)$$

△

Example. For D_n, the simple roots can be taken to be $\alpha_i = e_i - e_{i+1}$ for $i = 1, \ldots, n-1$ and $\alpha_n = e_{n-1} + e_n$. This matrix is no longer tridiagonal. It looks like

$$\left(\begin{array}{cccc|c} 2 & -1 & & & \\ -1 & 2 & \ddots & & \\ & \ddots & \ddots & -1 & -1 \\ & & -1 & 2 & 0 \\ \hline & & -1 & 0 & 2 \end{array}\right)$$

△

Example. For G_2, the matrix is

$$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}.$$

△

1.23 Lecture 23 (11/19): Dynkin diagrams

Let R be a reduced root system with simple roots $\Pi = \{\alpha_1, \ldots, \alpha_r\} \subset R$. To this, we attach the Cartan matrix

$$A = (a_{ij}) \text{ where } a_{ij} = \langle \alpha_i^\vee, \alpha_j \rangle \in \mathbb{Z}.$$

The satisfies

(1) $a_{ii} = 2$

(2) $a_{ij} \leq 0$ if $i \neq j$

(3) $a_{ij}a_{ji} = 4\cos^2\varphi$ where $\varphi = \text{angle}(\alpha_i, \alpha_j)$

(4) Let $d_i = |\alpha_i|^2$. Then $d_i a_{ij} = d_j a_{ji}$, so DA is symmetric and positive definitive where $D = \text{diag}(d_1, \ldots, d_r)$.

Any matrix satisfying the above is called a **Cartan matrix**.

Fact. R is irreducible $\iff$ the Cartan matrix is indecomposable (up to permutation).

1.23.1 Dynkin diagrams

We still have $R \subset E$ our reduced root system with simple roots $\Pi = \{\alpha_1, \dots, \alpha_r\} \subset R$. To this, we also attach a **Dynkin diagram**. This is a graph with

- vertices labelled by $1, \dots, r$
- Vertices i, j are connected iff $a_{ij} \neq 0$ iff $a_{ji} \neq 0$. The number of edges depends on $a_{ij}a_{ji} \in \{0, 1, 2, 3\}$.
  - if $a_{ji}a_{ij} = 1$, then there is one edge $i \leftrightarrow j$
  - if $a_{ij}a_{ji} = 2$, then there are two edges $i \rightrightarrows j$ pointing towards the shorter root (so $d_i > d_j$ the way I drew it)
  - if $a_{ij}a_{ji} = 3$, then there are thee edges pointing towards the shorter root.

Example. A_{n-1} with simple roots $\alpha_i = e_i - e_{i+1}$ for $i = 1, \dots, n-1$. This just gives a path of length $n-2$ (so $n-1$ vertices in total). $\triangle$

Figure 8: The Dynkin Diagram A_{n-1}

Example. B_n with simple roots $\alpha_1 = e_1 - e_2, \dots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_n$. This is a path of length $n-2$ followed by a double arrow from vertex $n-1$ to vertex n (since $|e_n|^2 < |\alpha_{n-1}|^2$) $\triangle$

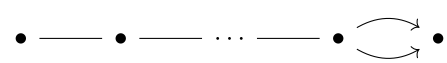


Figure 9: The Dynkin Diagram B_n

Example. The diagram for C_n will be the same as B_n but with the (last) arrow reversed. The roots here are the same as for B_n except now $\alpha_n = 2e_n$ instead of e_n. $\triangle$

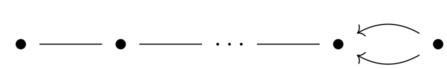


Figure 10: The Dynkin Diagram C_n

Fact. In general, the Dynkin diagram of the dual root system is the original diagram with the arrows reversed.

Example. D_n with simple roots $\alpha_1 = e_1 - e_2, \dots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_{n-1} + e_n$. This is a path of length $n-3$ (so consisting of $n-2$ vertices usually labelled $\{1, \dots, n-2\}$) but then $n-2$ has two additional edges, connected to $n-1$ and n. $\triangle$

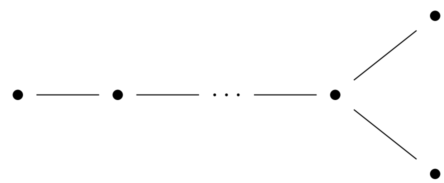


Figure 11: The Dynkin Diagram D_n

Remark 1.23.1. Looking at the diagrams shows that $D_2 = A_1 \times A_1$, corresponding to $\mathfrak{o}(4) = \mathfrak{sl}(2) \oplus \mathfrak{sl}(2)$. Also, $D_3 = A_3$, corresponding to $\mathfrak{o}(6) = \mathfrak{sl}(4)$. We also see that $B_2 = C_2$ (by flip), corresponding to $\mathfrak{o}(5) = \mathfrak{sp}(4)$. ○

Example. G_2, with Cartan matrix $\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ corresponds to two vertices with a triple edge between them. △

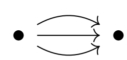


Figure 12: The Dynkin Diagram G_2

Proposition 1.23.2. *The Dynkin diagram (equivalently, the Cartan matrix) completely determines the root system.*

Proof. We may assume that the Dynkin diagram is connected (i.e. the system is irreducible). Then it determines

- the angle between α_i, α_j. $a_{ij}a_{ji} = 4\cos^2\varphi$ so it determines the angle up to replacing with $\pi - \varphi$ (i.e. it determines complementary pairs). However, we know the angle must be right or obtuse, so it determines the angle.

  By Lemma 1.21.2

- the ratio of lengths if roots are not orthogonal

Hence, if we fix the norm (length) of one of the roots, then we get (α_i, α_j) for all i, j. ■

1.23.2 Classification of Dynkin diagrams

Theorem 1.23.3.

(1) *The connected Dynkin diagrams are A_n, B_n, C_n, D_n, G_2 (seen in the previous section) along with the exceptional diagrams*

There's nothing I *enjoy* more than trying to figure out how to get latex to position figures the way I want

Note that the subscript of each diagram refers to the rank of the corresponding root system (equivalently, the number of vertices of the diagram).

(2) *Every Cartan matrix is a Cartan matrix of some (unique) root system.*

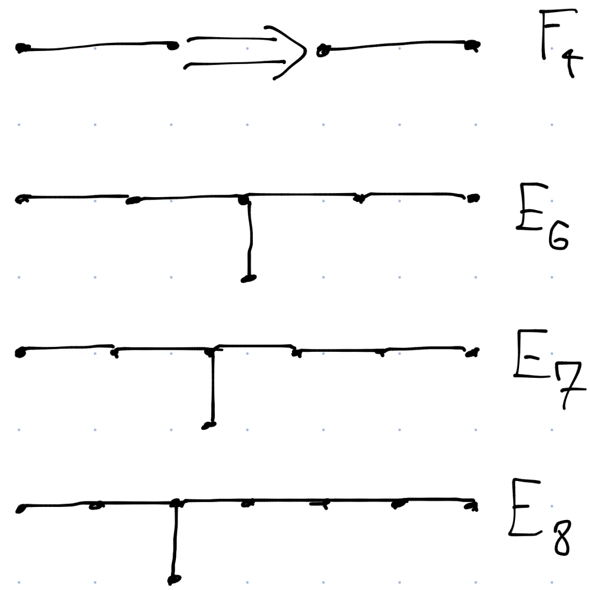


Figure 13: Exceptional Dynkin diagrams

Proof of part 1 of Theorem 1.23.3. The construction of F_4, E_6, E_7, E_8.

(F_4) Let $F_4 \subset \mathbb{R}^4$ be the union of B_4 and the vectors $\left(\pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}\right) = \frac{1}{2}\sum_{i=1}^4 (\pm e_i)$ for all choices of signs. Recall that B_4 had roots $\pm e_i \pm e_j$ for $1 \le i \ne j \le 4$. and $\pm e_i$ for $1 \le i \le 4$. Hence, B_4 has $4\binom{4}{2} + 2(4) = 32$ roots. We've just added 16 more, so altogether F_4 has 48 roots.

Exercise. Show this is an irreducible root system.

Pick a polarization $t = (t_1, t_2, t_3, t_4)$ such that $t_1 \gg t_2 \gg t_3 \gg t_4 > 0$ (e.g. $t_i = N^i$ for $N \gg 1$) where $\gg$ informally means "much bigger." Clearly e_4 is a simple root (it has positive inner product t_4 and also minimizes the inner product of t with any positive root). We now look at roots involving t_3, t_4. The simple root here will be $e_3 - e_4$ since it has the smallest positive inner product with t (after through away e_4). The next one is $e_2 - e_3$ and then finally we have $\frac{1}{2}(e_1 - e_2 - e_3 - e_4)$. We call these

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \left(\frac{1}{2}(e_1 - e_2 - e_3 - e_4), e_4, e_3 - e_4, e_2 - e_3\right).$$

Then,

$$\begin{aligned}
\alpha_1^\vee &= 2\alpha_1 = e_1 - e_2 - e_3 - e_4 \\
\alpha_2^\vee &= 2\alpha_2 = 2e_4 \\
\alpha_3^\vee &= \alpha_3 \\
\alpha_4^\vee &= \alpha_4
\end{aligned}$$

Finally, we draw the diagram

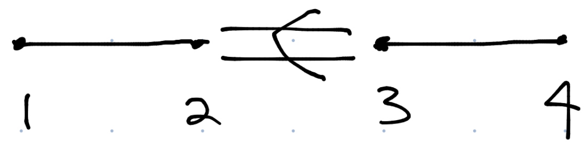


Figure 14: A Dynkin diagram of type F_4

(E_8) Here, $E_8 \subset \mathbb{R}^8$ is the union of D_8 and the vectors

$$\frac{1}{2}\sum_{i=1}^{8}(\pm e_i)$$

with an *even* number of minuses. The roots are $\pm e_i \pm e_j$ with $1 \le i \ne j \le 8$ (112 of them) and $\frac{1}{2}\sum_{i=1}^{8} \pm e_i$ (128 of them (7 choices of sign)). Thus, we have 240 roots in total.

Exercise. Show this is a reduced, irreducible root system.

Note that all roots in this case have the same length $|\alpha|^2 = 2$. We need to find the simple roots. As before, choose a polarization with

$$t_1 \gg t_2 \gg \cdots \gg t_8 > 0.$$

The first simple root will be $e_7 - e_8$, followed by $e_7 + e_8$. We next have $e_6 - e_7$ and then $e_5 - e_6$, then $e_4 - e_5$, then $e_3 - e_4$, then $e_2 - e_3$. Finally, we have $\frac{1}{2}(e_1 - e_2 - e_3 - \cdots - e_7 + e_8)$. We label these

$$(\alpha_1, \alpha_2, \ldots, \alpha_8) = \left(\frac{1}{2}(e_1 - e_2 - \cdots - e_7 + e_8), e_7 + e_8, e_7 - e_8, e_6 - e_7, e_5 - e_6, e_4 - e_5, e_3 - e_4, e_2 - e_3\right)$$

We obtain the diagram pictured in Figure 15.

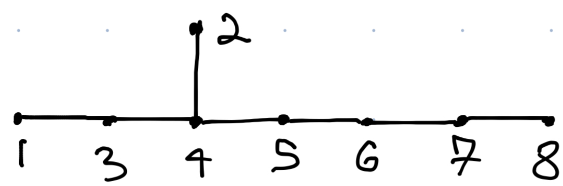


Figure 15: A Dynkin diagram of type E_8

(E_7) Note that E_7 is a subdiagram of E_8 obtained by throwing away the 8th vertex. Hence, we can describe it as the subsystem of E_8 generated by $\alpha_1, \ldots, \alpha_7$. Note that these all satisfy the equation $x_1 + x_2 = 0$. Hence, $E_7 = E_8 \cap \{x \in \mathbb{R}^8 : x_1 + x_2 = 0\}$. The roots are $\pm e_i \pm e_j$ for $3 \le i \ne j \le 8$ (60 of these), $\pm(e_1 - e_2)$ (2 of these), and $\frac{1}{2}\sum_{i=1}^{8}(\pm e_i)$ with evenly many $-$'s and sign of e_1 opposite to sign of e_2 (64 of these). Hence, 126 roots in total.

(E_6) Like before, this is a subsystem of E_7 (and of E_8) generated by $\alpha_1, \ldots, \alpha_6$ (cut $7, 8$ from the E_8 diagram). These roots have the equations $x_1 + x_2 = 0$ and $x_2 + x_3 = 0$ (but not for α_7, α_8) so $E_6 = E_8 \cap \{x \in \mathbb{R}^8 : x_1 + x_2 = 0 = x_2 + x_3\}$. What are the roots? Our vectors are of the form $(a, -a, a, b, c, \ldots)$. We have roots $\pm e_i \pm e_j$ with $4 \le i \ne j \le 8$ (40 of these) and $\frac{1}{2}\left(\sum_{i=1}^{8}(\pm e_i)\right)$ with evenly many $-$'s and the signs of e_1, e_3 both opposite to that of e_2 (32 of these). Hence, 72 roots in total. ■

For the next part of the classification proof, we need to show that there are no other connected Dynkin diagrams. We first list some graphs which are not Dynkin diagrams, but in some sense, are minimally not Dynkin diagrams. These are the **affine Dynkin diagrams** found in Figures 17 and 16.

Fun fact: (Some of) the untwisted affine Dynkin diagrams are used to classify possible degenerations in families of elliptic curves.

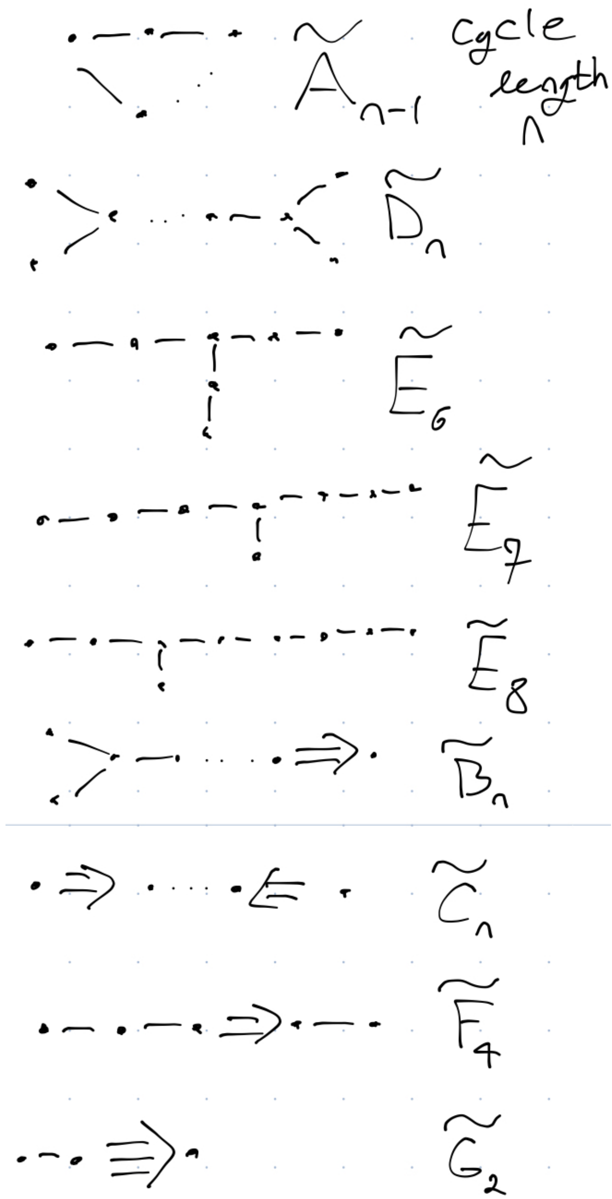


Figure 16: The untwisted affine Dynkin diagrams

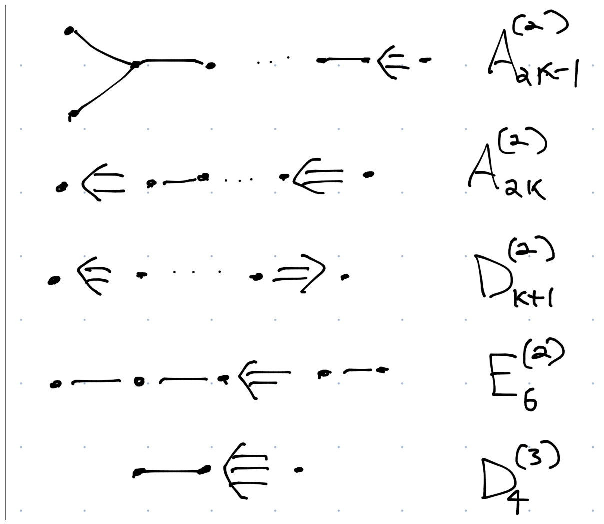


Figure 17: The twisted affine Dynkin diagrams

These are not Dynkin diagrams since their associated Cartan matrices A are degenerate ($\exists v \neq 0$ s.t. $Av = 0$). One can write down such a v by looking at the diagrams. e.g. for simple edges you want $v = (v_i)$ s.t. $2v_i = \sum_j v_j$ where j ranges over neighbors of i.

Secretly, these correspond to diagrams attached to certain infinite dimensional Lie algebras, but we won't talk about that in this class

Example. $\widetilde{E}_8$. You can take v given in red below in Figure 18. △

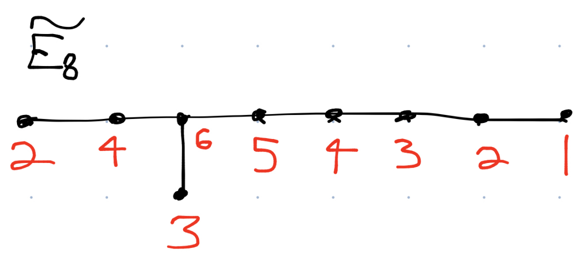


Figure 18: An element in the kernel of the Cartan matrix of $\widetilde{E}_8$

Since none of the affine Dynkin diagrams are Dynkin, we conclude that none of them can be contained inside any Dynkin diagram (principal submatrices of pos. def. matrices are pos. def). Now, it is a purely combinatorial fact that the only diagrams not containing any of these as a subdiagram are the ones on our list. Let G be a diagram not containing any affine Dynkin diagram.

- First note that G has no cycles since $\widetilde{A}_{n-1}$ is forbidden. This gives no cycles with simple edges ($Av = 0$, $v = (1, 1, \ldots, 1)$). If have multiple edges, even worse as $(DAv, v) < 0$.
- There are no vertices with ≥ 4 edges coming out (no $\widetilde{D}_4$ subdiagram). All vertices have degree ≤ 3 (and at least 1).
- If there is a 3-valent vertex, then it is unique (since $\widetilde{D}_n$ is forbidden).
- If G has a triple edge, then $G = G_2$ (since $\widetilde{G}^2$ and $D_4^{(3)}$ are forbidden).

- If there is a trivalent vertex, then there is no double edge. Since no $\widetilde{E}_6, \widetilde{E}_7, \widetilde{E}_8$, we must have (reason about lengths of legs[18]) D_n, E_6, E_7 or E_8.
- All that remains are chain-like diagrams. These can have at most one double edge. So we have A_n, B_n, C_n, or double edge in the middle. If it's in the middle, then it must be F_4.

Remark 1.23.4. These affine dynkin diagrams have Cartan matrices which are negative semi-definite. ∘

1.24 Lecture 24 (12/1)

23 minutes[19] late because covid testing

Notes taken after class from recording and whatnot.

Fix an algebraically closed field k of characteristic 0. We want to show that any reduced root system gives rise to a unique semisimple Lie algebra over k. It'll suffice to biject irreducible (reduced) root systems and simple Lie algebras.

Let $\mathfrak{g}$ be a f.d. simple Lie algebra over k with Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$ and root system $R \subset \mathfrak{h}^*$ (which is then reduced and irreducible). Fix a polarization of R with simple roots $\Pi = \{\alpha_1, \ldots, \alpha_r\}$, and let $A = (a_{ij})$ be the Cartan matrix of R. We have a decomposition $\mathfrak{g} = \mathfrak{n}_+ \oplus \mathfrak{h} \oplus \mathfrak{n}_-$ with $\mathfrak{n}_\pm := \bigoplus_{\alpha \in R_\pm} \mathfrak{g}_\alpha$. Fix elements $e_i \in \mathfrak{g}_{\alpha_i}$, $f_i \in \mathfrak{g}_{-\alpha_i}$ so that $e_i, f_i, h_i = [e_i, f_i]$ form an $\mathfrak{sl}_2$-triple.

Theorem 1.24.1 (Serre relations).

(1) *e_i, f_i, h_i generate $\mathfrak{g}$.*

(2) *They satisfy the following relations*

$$\begin{aligned} [h_i, h_j] &= 0 \\ [h_i, e_j] &= a_{ij} e_j \\ [h_i, f_j] &= -a_{ij} f_j \\ [e_i, f_j] &= \delta_{ij} \cdot h_i \end{aligned}$$

+ the Serre relations

$$\begin{aligned} (\mathrm{ad} e_i)^{1-a_{ij}} e_j &= 0 && \text{for } i \neq j \\ (\mathrm{ad} f_i)^{1-a_{ij}} f_j &= 0 && \text{for } i \neq j \end{aligned}$$

Proof. **(1)** We know that the h_i are a basis of $\mathfrak{h}$ since they correspond to simple (co)roots, so it suffices to show that e_i generates $\mathfrak{n}_+$ and the f_i generate $\mathfrak{n}_-$. We will only write out the proof of the first of these; the second is the same with the opposite polarization. Let $\mathfrak{n}'_+$ be the Lie subalgebra generated by e_i. Suppose that $\mathfrak{n}'_+ \neq \mathfrak{n}_+$, so $\mathfrak{n}'_+ = \bigoplus_{\alpha \in R'_+} \mathfrak{g}_\alpha$ for some $R'_+ \subsetneq R_+$. Pick $\alpha \in R_+ \setminus R'_+$ of smallest height.[20]

[18] $\widetilde{E}_6$ forbidden means one leg of length 1. $\widetilde{E}_7$ forbidden means one leg of length 2. $\widetilde{E}_8$ forbidden bounds length of last remaining leg

[19] I guess technically 18 minutes late because of the whole start 5 past the hour thing

[20] Recall that $\alpha = \sum k_i \alpha_i \implies \mathrm{ht}(\alpha) = \sum k_i$

This is not a simple root (since $\mathfrak{g}_i$ spanned by e_i), so consider $\mathfrak{g}_{\alpha-\alpha_i} \subset \mathfrak{n}'_+$ as $\operatorname{ht}(\alpha-\alpha_i) = \operatorname{ht}(\alpha) - 1$. At the same time,

$$[e_i, \mathfrak{g}_{\alpha-\alpha_i}] \subset \mathfrak{g}_\alpha = 0.$$

Now take $x \in \mathfrak{g}_{-\alpha}$ and $y \in \mathfrak{g}_{\alpha-\alpha_i}$. Then,

$$([x, e_i], y) = (x, [e_i, y]) = 0$$

which implies $[x, e_i] = 0$ (by non-degeneracy?) for all i. Recall that $[h_i, x] = -(\alpha, \alpha_i^\vee)x$; x is a highest weight vector for $(\mathfrak{sl}_2)_i$ of weight $-(\alpha, \alpha_i^\vee)$ so $(\alpha, \alpha_i^\vee) \leq 0$ which implies $(\alpha, \alpha_i) \leq 0$ for all i. This implies $(\alpha, \alpha) \leq 0$ which is a contradiction since our inner product is positive definite. Thus, $\mathfrak{n}'_+ = \mathfrak{n}_+$ after all.

(2) We really only need to prove (one of) the Serre relations. We will prove

$$(\operatorname{ad} e_i)^{1-a_{ij}} e_j = 0.$$

Regard $\mathfrak{g}$ as an $(\mathfrak{sl}_2)_i$-module. Consider the submodule M_{ij} generated by f_j (keep in mind $i \neq j$). Note that $e_i \cdot f_j = [e_i, f_j] = 0$ and $h_i \cdot f_j = [h_i, f_i] = -a_{ij} f_j$, so f_j is a highest weight vector for $(\mathfrak{sl}_2)_i$ with highest weight $-a_{ij}$. So $M_{ij} \cong V_{-a_{ij}}$, but if $v \in V_n$ highest weight, then $f^{n+1} v = 0$. Thus, $f_i^{-a_{ij}+1} \cdot f_j = 0$ which exactly gives the Serre relation. ■

This is not exactly what we want. We've started with a (simple) Lie algebra and just written down some relations. We know want to claim that these relations completely determine the system; that we could just start with the root system and require these relations to reconstruct the Lie algebra. We need to make this rigorous before we can prove it.

1.24.1 Free Lie algebras

Let $x_1, \ldots, x_m$ be some letters (formal symbols), and let k be a field. The **free Lie algebra** $FL_m(k)$ is freely generated by $x_1, \ldots, x_m$, i.e. it is spanned by all possible iterated commutators of $x_1, \ldots, x_m$ modulo the axioms

More generally, a (commutative) ring

- $[x, x] = 0$ ($\implies [x_i, x_j] = -[x_j, x_i]$)
- $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$.

Note that $FL_m(k)$ is a graded Lie algebra:

$$FL_m = \bigoplus_{n \geq 1} FL_m[n]$$

whose degree n part $FL_m[n]$ consists of elements containing exactly n letters.

Remark 1.24.2. FL_m will be infinite dimensional as soon as $m \geq 2$. ○

Example. What does FL_2 look like? Say x, y are our generators. △

Example. What about FL_3? $\dim FL_3[3] = 8$. △

degree d	$FL_2[d]$
1	x, y
2	$[x, y]$
3	$[x, [x, y]], [y, [x, y]]$

Table 1: Homogeneous parts of free Lie algebra FL_2

degree d	$FL_2[d]$
1	x, y, z
2	$[x, y], [y, z], [x, z]$
3	$[x, [x, y]], [y, [x, y]], [y, [y, z]], [z, [y, z]], [z, [z, x]], [x, [z, x]], [[x, y], z], [[y, z], x]$

Table 2: Homogeneous parts of free Lie algebra FL_3

Univseral Property 1. *The free Lie algebra satisfies*

$$\mathrm{Hom}(FL_m(k), \mathfrak{g}) \cong \mathfrak{g}^m$$

for any Lie algebra $\mathfrak{g}$, i.e. is it left adjoint to the forgetful functor. That is, $\varphi : FL_m(k) \to \mathfrak{g}$ is determined by $\varphi(x_i)$ for $i = 1, \ldots, m$ and these can be chosen arbitrarily.

Remark 1.24.3. What is its universal enveloping algebra? We have

$$\mathrm{Hom}(U(FL_m(k)), A) = \mathrm{Hom}_{\mathrm{Lie}}(FL_m(k), A) = A^m$$

for any associative algebra A. Hence, $U(Fl_m(k))$ is the **free associative algebra** $k\langle x_1, \ldots, x_m\rangle$ (i.e. non-commutative polynomial algebra) whose basis consists of words $x_{i_1} \ldots x_{i_k}$. ○

In particular, PBW theorem then implies that $FL_m(k) \subset k\langle x_1, \ldots, x_m\rangle$; one can determine its image, but we do not have time to do so.

1.24.2 Serre presentation of a simple Lie algebra

Let R be a reduced, irreducible root system.

Definition 1.24.4. $\mathfrak{g}(R)$ is the Lie algebra generated by e_i, f_i, h_i for $i = 1, \ldots, r = \operatorname{rank} R$ with defining relations given by Theorem 1.24.1, i.e. $\mathfrak{g}(R) = \mathrm{FL}_{3r}/I$ where I is the ideal generated by $(LHS - RHS)$ of the relations. ◇

Theorem 1.24.5 (Serre)**.**

(1) *Let $\mathfrak{n}_+ \subset \mathfrak{g}(R)$ generated only by e_i. This has Serre relations*

$$(\mathrm{ad} e_i)^{1-a_{ij}} e_j = 0 \text{ for } i \neq j$$

as defining relations. Similarly for $\mathfrak{n}_-$ generated by the f_i.

(2) *$\mathfrak{g}(R)$ is a sum of finite dimensional $(\mathfrak{sl}_2)_i$-modules.*

(3) *$\mathfrak{g}(R)$ is itself finite dimensional.*

(4) $\mathfrak{g}(R)$ *is simple with root system* R.

Remark 1.24.6. We can do this whole this with a reducible root system R instead, and the only thing that changes is now $\mathfrak{g}(R)$ is semisimple. ∘

Proof. The relations imply that $\mathfrak{g}(R_1 \sqcup R_2) = \mathfrak{g}(R_1) \oplus \mathfrak{g}(R_2)$ (any generator coming from R_1 will commute with any generator coming from R_2). Hence, despite making the above remark, it really does suffice to just do the irreducible root system case.

(1) Consider the (in general, ∞-dim) Lie algebra $\widetilde{\mathfrak{g}(R)} = \langle e_i, f_i, h_i \rangle$ with defining relations (all but Serre)

$$
\begin{aligned}
[h_i, h_j] &= 0 \\
[h_i, e_j] &= a_{ij} e_j \\
[h_i, f_j] &= -a_{ij} f_j \\
[e_i, f_j] &= \delta_{ij} \cdot h_i
\end{aligned}
$$

Note that these are already enough to have the decomposition

$$\widetilde{\mathfrak{g}(R)} = \widetilde{\mathfrak{n}}_+ \oplus \mathfrak{h}' \oplus \widetilde{\mathfrak{n}}_-$$

where

$$\widetilde{\mathfrak{n}}_+ = \langle e_i \rangle, \ \ \widetilde{\mathfrak{n}}_- = \langle f_i \rangle, \ \text{ and } \ \mathfrak{h}' = \operatorname{span}\{h_i\}.$$

This is because every iterated commutator of e_i, f_i, h_i in $\widetilde{\mathfrak{g}(R)}$ can be simplified to contain only e_i, only f_i, or only one h_i. At this point, it is not clear that the h_i are linearly independent, that $\widetilde{\mathfrak{n}}_+$ is free, or even that $\widetilde{\mathfrak{g}(R)} \neq 0$.

Lemma 1.24.7. $\widetilde{\mathfrak{n}}_+$ *is free Lie algebra in* e_i*, and* $\widetilde{\mathfrak{n}}_-$ *is free on generators* f_i.

Proof. As usual, we only prove that $\widetilde{\mathfrak{n}}_+$ case and note that the $-$ case is the $+$ case for the opposite polarization. Let R be the vector space with basis h_i. Consider $\mathfrak{a} = \mathrm{FL}_r \rtimes \mathfrak{h}'$ where FL_r has generators $f_1', \dots, f_r'$. This only has the semi-direct product relations

$$[h_i', f_j'] = -a_{ij} f_j' \ \text{ and } \ [h_i', h_j'] = 0.$$

Take the universal enveloping algebra

$$U = U(\mathfrak{a}) = U(\mathrm{FL}_r) \rtimes k[h_1', \dots, h_r'] = k\langle f_1', \dots, f_r' \rangle \otimes k[h', \dots, h_r'].$$

The key idea now is to define a representation of $\widetilde{\mathfrak{g}(R)}$ on U, building from the condition that $e_i \cdot 1 = 0$. For $w \in k\langle f_1', \dots, f_r' \rangle$ some word of weight $-\alpha$ and $P \in k[h_1', \dots, h_r']$ some polynomial, we'll want

$$h_i(w \otimes P) = \text{“}h_i(w \otimes P) \cdot 1\text{”} = w \otimes (h_i' - \alpha(h_i'))P$$

and (here we add a letter to w)

$$f_i(w \otimes P) = (f_i' w) \otimes P,$$

and

$$e_i(w \otimes P) = \text{“}e_i'(w \otimes P) \cdot 1''.$$

To see what this should be, consider

$$e_i(f_{j_1}' \dots f_{j_s}' \otimes P) = \sum_{k : j_k = 1} f_{j_1}' \dots \widehat{f_{j_k}} \dots f_{j_s}' \otimes (h_i' - (\alpha_{j_{k+1}} + \dots + \alpha_{j_s})(h_i'))P.$$

These are the rules of our action.

Exercise. Check that this defines a representation of $\mathfrak{g}(R)$ on U (i.e. the relations of $\mathfrak{g}(R)$ are satisfied).

Thus, we get a linear map $\varphi : \widetilde{\mathfrak{g}(R)} \to U$ via $x \mapsto x \cdot 1$. It restricts to a map $\varphi|_{\widetilde{\mathfrak{n}}_+} : \widetilde{\mathfrak{n}}_+ \to \mathrm{FL}_r \subset U$ since the f-action is simply appending it to the word. We see that $\varphi|_{\widetilde{\mathfrak{n}}_+}$ is an isomorphism, so $\widetilde{\mathfrak{n}}_+$ is free. ■

We now want to show that $\mathfrak{n}_+$ is free on the e_i subject only to the Serre relation. Let $S_{ij}^+ = (\mathrm{ad} e_i)^{1-a_{ij}} e_j \in \widetilde{\mathfrak{n}}_+$ and $S_{ij}^- = (\mathrm{ad} f_i)^{1-a_{ij}} f_j \in \widetilde{\mathfrak{n}}_-$.

Lemma 1.24.8.

$$[f_k, S_{ij}^+] = 0 \ \textit{ and } \ [e_k, S_{ij}^-] = 0 \ \textit{ for all } k.$$

Proof. The proof uses the rep theory of $\mathfrak{sl}_2$, and is left as an exercise. ■

Let $I^+ \subset \widetilde{\mathfrak{n}}_+$ be the ideal generated by S_{ij}^+ (for all $i \neq j$) and let I_- be the ideal in $\widetilde{\mathfrak{n}}_-$ generated by S_{ij}^- (for all $i \neq j$). Then, $I_+ \oplus I_-$ is the ideal of Serre relations in $\widetilde{\mathfrak{g}(R)}$. Hence,

$$\mathfrak{g}(R) = \frac{\widetilde{\mathfrak{g}(R)}}{I_+ \oplus I_-} = \mathfrak{h} \oplus \widetilde{\mathfrak{n}}_+/I_+ \oplus \widetilde{\mathfrak{n}}_-/I_-.$$

This completes the proof of **(1)**. In particular, we see that $e_i \neq 0$, $f_i \neq 0$, and the h_i are linearly independent. This is because

$$\left[\sum c_i h_i, e_j\right] = \sum c_i a_{ij} e_j = 0 \implies \sum c_i a_{ij} = 0 \implies c_i = 0$$

since the Cartan matrix is invertible (negative definite).

(2) We now want to show that $\mathfrak{g}(R)$ is a sum of d.d. $\mathfrak{sl}_2(i)$ representations. As $(\mathfrak{sl}_2)_i$-modules, we have $V_{-a_{ij}}$ generated by the f_j's (e.g. $e_i \cdot f_j = [e_i, f_j] = f_i^{1-a_{ij}} \cdot f_j = 0$). Similarly, the e_j generate a copy of $V_{-a_{ij}}$. Finally, the h_k generate V_0 or V_2 or $V_0 \oplus V_2$. If x generate X and y generate Y, then $[x, y]$ generates a representation which is a quotient of $X \otimes Y$; thus, any element of $\mathfrak{g}(R)$ generates a f.d. representation of $(\mathfrak{sl}_2)_i$ which gives part 2. ■

Question: Why?

Next time we will prove parts **(3)** and **(4)**. This will give that classification of simple Lie algebras is given by Dynkin diagrams, and then we will end the class with some more representation theory.

1.25 Lecture 25 (12/3)

1.25.1 Finishing Proof of Theorem of Serre

t We were in the middle of proving a theorem of Serre about the Lie algebra determined by a reduced root system R. We restate it for convenience. We have so far proven parts **(1)** and **(2)**.

Theorem 1.25.1 (Serre)**.**

(1) *Let $\mathfrak{n}_+ \subset \mathfrak{g}(R)$ generated only by e_i. This has Serre relations*

$$(\mathrm{ad} e_i)^{1-a_{ij}} e_j = 0 \ \textit{for} \ i \neq j$$

as defining relations. Similarly for $\mathfrak{n}_-$ generated by the f_i.

(2) *$\mathfrak{g}(R)$ is a sum of finite dimensional $(\mathfrak{sl}_2)_i$-modules.*

(3) *$\mathfrak{g}(R)$ is itself finite dimensional.*

(4) *$\mathfrak{g}(R)$ is semisimple with root system R.*

Recall that we had reduced to the case where R is moreover irreducible (so $\mathfrak{g}(R)$ will be simple in **(4)**). Before proving **(3)**, we take a digression into representations...

Let V be a (not necessarily fin dim) representation of $\mathfrak{g}(R)$. Choose Cartan $\mathfrak{h} \subset \mathfrak{g}(R)$ so that $\mathfrak{g}(R) = \mathfrak{n}_+ \oplus \mathfrak{h} \oplus \mathfrak{n}_-$.

Definition 1.25.2. We say that V **has weight decomposition** if $V = \bigoplus_{\lambda \in \mathfrak{h}^*} V[\lambda]$ where $V[\lambda]$ is the so called **weight subspace of weight** λ

$$V[\lambda] = \{v \in V : h \cdot v = \lambda(h)v \ \text{ for all } \ h \in \mathfrak{h}\}.$$

If $v \in V[\lambda]$ we say v is a **vector of weight** λ. ◇

Clearly, one always has

$$V \supset V' := \bigoplus_{\lambda \in \mathfrak{h}^*} V[\lambda],$$

and V has weight decomposition $\iff V = V' \iff \mathfrak{h}$ acts semisimply on V.

Non-example. $\mathfrak{sl}_2 \curvearrowright V = U(\mathfrak{sl}_2)$ via left multiplication, but $V' = 0$. ▽

Recall 1.25.3. Every finite-dim rep of $\mathfrak{sl}_2$ has a weight decomposition. ⊙

Lemma 1.25.4. *Let V be a representation of $\mathfrak{g}(R)$ with weight decomposition into finite dimensional weight subspaces $V[\lambda]$, such that $V|_{(\mathfrak{sl}_2)_i}$ is **locally finite dimensional** (i.e. is a sum of finite dimensional $(\mathfrak{sl}_2)_i$-modules, i.e. every vector $v \in V$ generates a f.d. $(\mathfrak{sl}_2)_i$-module). Then, for all weights $\lambda \in \mathfrak{h}$ with $V[\lambda] \neq 0$, we have $\lambda \in P = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_r$, the weight lattice, and* $\dim V[\lambda] = \dim V[w\lambda]$ *for all $w \in W$.*

Proof. Choose (nonzero) $v \in V[\lambda]$, and let $\langle v \rangle_i$ be the $(\mathfrak{sl}_2)_i$-submodule generated by v, so $\langle v \rangle_i$ is finite dimensional. By rep theory of $\mathfrak{sl}_2$, this implies that h_i has integer eigenvalues on $\langle v \rangle_i$. In particular,

$h_i v = \lambda(h_i)v \implies (\lambda, \alpha_i^\vee) = \lambda(h_i) \in \mathbb{Z}$. This holds for all i, so this exactly says that $\lambda \in P$ (P the weight lattice).

To show $\dim V[\lambda] = \dim V[w\lambda]$, it suffice to address to the case of $w = s_i$, a simple reflection. Furthermore, it is enough to show that $\dim V[\lambda] \leq \dim V[s_i\lambda]$ by symmetry ($s_i^{-1} = s_i$). Assume first that $(\lambda, \alpha_i^\vee) \geq 0$. Then consider the operator $f_i^m : V[\lambda] \to V[\lambda - m\alpha_i] = V[s_i\lambda]$ ($m := (\lambda, \alpha_i^\vee)$). We claim this operator is injective. Suppose $v \in V[\lambda]$ is nonzero. Then, $v \in \langle v \rangle_i [m]$, the space of weight m of the $(\mathfrak{sl}_2)_i$-rep $\langle v \rangle_i$. By rep theory of $\mathfrak{sl}_2$, we have $f_i^m v \neq 0$ since $f_i^m : \langle v \rangle_i [m] \xrightarrow{\sim} \langle v \rangle_i [-m]$. Thus, $\dim V[\lambda] \leq \dim V[s_i\lambda]$ as desired.

It remains to consider the the second case, where $-m := (\lambda, \alpha_i^\vee) \leq 0$. In this case, run the same argument instead with the operator $e_i^m : V[\lambda] \to V[s_i\lambda]$. This finishes the proof. ■

Now we return to proving Theorem 1.25.1.

*Proof of Theorem 1.25.1**(3)**.* We wish to show that $\dim \mathfrak{g}(R) < \infty$. Consider $\mathfrak{g}(R)$ as a module over itself by the adjoint action. We have a decomposition

Question: What is Q? Is it the root lattice?

$$\mathfrak{g}(R) = \mathfrak{h} \oplus \bigoplus_{\alpha \in Q} \mathfrak{g}_\alpha$$

where $\mathfrak{h} = \mathfrak{g}(R)[0]$ and $\mathfrak{g}_\alpha = \mathfrak{g}(R)[\alpha]$. We know from **(2)** that $\mathfrak{g}(R)$ is a sum of f.d. $(\mathfrak{sl}_2)_i$-modules for all i. The previous lemma then tells us that $\dim \mathfrak{g}_\alpha$ is a W-invariant. At the same time, $\mathfrak{g}(R) = \mathfrak{h} \oplus \mathfrak{n}_+ \oplus \mathfrak{n}_-$ where $\mathfrak{n}_\pm = \bigoplus_{\alpha \in Q_\pm \setminus 0} \mathfrak{g}_\alpha$. We claim that $\mathfrak{g}_\alpha \neq 0$ (for $\alpha \neq 0$) implies that $\alpha \in R$. Since R is finite and each of these spaces are finite-dimensional, this will imply that $g(R)$ is finite-dimensional as claimed.

We induct on the height $\operatorname{ht}(\alpha) = \sum k_i$ where $\alpha = \sum k_i \alpha_i$ ($\alpha \in Q_+ \setminus 0$. Run a similar argument for $\alpha \in Q_- \setminus 0$). The base is trivial since height 1 roots are simple roots of R. We now do the induction step. Let $k_i = (\alpha, \omega_i^\vee) \geq 0$ for all i. If there is only one i for which $k_i > 0$ (there must be at least one), then $\alpha = m\alpha_i$. However, if $m \geq 2$, then $\mathfrak{g}_{m\alpha_i} = 0$ as this is $\mathfrak{n}_{+,m\alpha_i}$, but $\mathfrak{n}_+$ is generated by e_i. So we have at least two i such that $k_i > 0$. Fix an i with $(\alpha, \alpha_i^\vee) > 0$ (exists since $(\alpha, \alpha) > 0$). By lemma just proven, this forces $\mathfrak{g}_{s_i\alpha} \neq 0$, but $s_i\alpha = \alpha - (\alpha, \alpha_i^\vee)\alpha_i \notin Q_-$ (we've removed one positive coefficient, but we started with ≥ 2 of them). Hence, $s_i\alpha \in Q_+ \setminus 0$ and $\operatorname{ht}(s_i\alpha) = \operatorname{ht}(\alpha) - (\alpha, \alpha_i^\vee) < \operatorname{ht}(\alpha)$. Thus, by induction assumption, we know $s_i\alpha \in R$, so $\alpha = s_i(s_i\alpha) \in s_i(R) = R$. This completes the proof. ■

This only leaves part **(4)**. We need to show that $\mathfrak{g}(R)$ is a simple Lie algebra (recall R an irreducible root system).

*Proof of Theorem 1.25.1**(4)**.* Let $I \subset \mathfrak{g}(R)$ be a nonzero ideal. Then,

$$I = (\mathfrak{g} \cap I) \oplus \bigoplus_{\alpha \in R} (\mathfrak{g}_\alpha \cap I).$$

If $\mathfrak{g} \cap I = 0$, then there must be some α such that $\mathfrak{g}_\alpha \subset I$ (since $\dim \mathfrak{g}_\alpha = 1$ as there's some $w \in W$ s.t. $\alpha = w\alpha_i$ which implies $\dim \mathfrak{g}_\alpha = \dim \mathfrak{g}_{\alpha_i} = 1$). If $\mathfrak{g} \cap R \neq 0$, then $\exists h \neq 0$ in this intersection, so there's some i s.t. $\alpha_i(h) \neq 0$ so

$$[h, e_i] = \alpha_i(h)e_i \implies e_i = \frac{1}{\alpha_i(h)}[h, e_i] \in I \implies \mathfrak{g}_{\alpha_i} \subset I.$$

Since the weights of I are also W-invariant (by lemma from before), in any case we see that $\exists i$ s.t. $\mathfrak{g}_{\alpha_i} \in I$, i.e. $e_i \in I$ for some i. Now, let J be the set of indices $i \in [1, r]$ (i.e. vertices of the Dynkin diagram) such that $e_i \in I$. Fix some $i \in J$, and choose $j \in [1, r]$ such that $a_{ij} \neq 0$ (i.e. i, j are connected by some kind of edge). Then, $h_i = [e_i, f_i] \in I$ as is $f_i = [f_i, h_i]/2$. Hence,

$$[h_i, e_j] = a_{ij} e_j \implies e_j = \frac{1}{a_{ij}}[h_i, e_j] \in I \implies j \in J.$$

Thus J must be a (nonempty) union of connected components of the Dynkin diagram. Since R is irreducible, its Dynkin diagram is connected, so we conclude $J = [1, r]$, i.e. $I = \mathfrak{g}(R)$. Thus, $\mathfrak{g}(R)$ is a simple Lie algebra, and we know that its root system is R itself (we saw in the proof of **(3)** that $\mathfrak{g}_\alpha \neq 0 \implies \alpha \in R$). ■

Corollary 1.25.5. *Isomorphism classes of finite dimensional simple Lie algebras $\mathfrak{g}/k$ (when $k = \overline{k}$ and $\operatorname{char} k = 0$) corresponding bijectively to Dynkin diagrams A_n ($n \geq 1$), B_n ($n \geq 2$), C_n ($n \geq 3$), D_n ($n \geq 4$), E_6, E_7, E_8, F_4, and G_2.*

$B_1 = A_1$

$C_1 = A_1, C_2 = B_2$

$D_1 = A_1, D_2 = B_2, D_3 = A_3$

Wow, we actually proved this.

The remainder of the course will be spent on representation theory.

1.25.2 Representation theory of semisimple Lie algebras $/\mathbb{C}$

Recall 1.25.6. Any finite dimensional representation of $\mathfrak{g}$ is completely reducible. Thus, to understand finite dimensional representations, it'll suffice to classify the irreducible ones. ⊙

Fix a Cartan subalgebra $\mathfrak{h} \subset \mathfrak{g}$, and let V be a (possibly infinite-dimensional) $\mathfrak{g}$-rep with weight decomposition, i.e.

$$V = \bigoplus_{\lambda \in \mathfrak{h}^*} V[\lambda].$$

Exercise. $\mathfrak{g}_\alpha \cdot V[\lambda] \subset V[\lambda + \alpha]$

Notation 1.25.7. Let

$$P(V) = \{\lambda \in \mathfrak{h}^* : V[\lambda] \neq 0\},$$

the set of all weights of $\mathfrak{g} \curvearrowright V$. We say $\lambda \in \mathfrak{h}^*$ is a **weight** of V if $V[\lambda] \neq 0$.

Proposition 1.25.8. *Any f.d. representation of $\mathfrak{g}$ has weight decomposition and moreover $P(V) \subset P$ ("all the weights lie in the weight lattice").*

Proof. $V|_{(\mathfrak{sl}_2)_i}$ is a f.d. rep of $\mathfrak{sl}_2$, and so h_i acts semisimply on V. ■

Definition 1.25.9. A vector $v \in V[\lambda]$ is called a **highest weight vector** of weight λ if $e_i v = 0$ for all i, i.e. $\mathfrak{n}_+ v = 0$ (note also that $h \cdot v = \lambda(h) v$ for $h \in \mathfrak{h}$). ◇

Definition 1.25.10. V is a **highest weight representation of highest weight** λ if it is generated by a nonzero highest weight vector $v \in V[\lambda]$. ◇

Proposition 1.25.11. *Any f.d. rep $V \neq 0$ of $\mathfrak{g}$ contains a nonzero highest weight vector of some weight $\lambda \in P$. Hence every irreducible f.d. representation V of $\mathfrak{g}$ is a highest weight representation.*

Proof. The set $P(V)$ of weights is finite (since V f.d.), so pick $\lambda \in P(V)$ maximizing $(\lambda, \rho^\vee)$, where $\rho^\vee = \sum \omega_i^\vee = \sum_{\alpha \in R_+} \alpha^\vee$ as usual. Then,

$$(\lambda + \alpha_i, \rho^\vee) = (\lambda, \rho^\vee) + 1 > (\lambda, \rho^\vee) \implies \lambda + \alpha_i \notin P(V).$$

At the same time, $e_i : V[\lambda] \to V[\lambda + \alpha_i] = 0$, so any nonzero $v \in V[\lambda]$ is a highest weight vector of weight λ.

An irreducible representation is generated by any nonzero vector, so the second part follows immediately. ■

1.25.3 Verma modules

Verma modules are certain ∞-dimensional modules which are useful for studying finite dimensional modules. They are the "largest" highest weight modules with highest weight λ. They are generated by a single highest weight vector v_λ with *defining relations*

$$hv_\lambda = \lambda(h)v_\lambda \text{ and } e_i v_\lambda = 0 \forall i.$$

More formally...

Definition 1.25.12. Let $I_\lambda \subset U(\mathfrak{g})$ be the (left) ideal generated by the elements $h - \lambda(h) \cdot 1$ for $h \in \mathfrak{h}$ and e_i for $i \in [1, r]$. Then,

$$M_\lambda := U(\mathfrak{g})/I_\lambda$$

is the **Verma module** with highest weight λ. In the above presentation, $v_\lambda = 1 \in U(\mathfrak{g})$. ◇

Proposition 1.25.13. *The map*

$$\varphi : U(\mathfrak{n}_-) \to M_\lambda$$

given by $\varphi(x) = xv_\lambda$ is an isomorphism of $U(\mathfrak{n}_-)$-modules (so M_λ is free of rank 1 over $U(\mathfrak{n}_-)$).

Proof. Recall PBW tells us that

$$\mathfrak{g} = \mathfrak{n}_- \oplus (\mathfrak{h} \oplus \mathfrak{n}_+) \implies U(\mathfrak{n}_-) \otimes U(\mathfrak{h} \oplus \mathfrak{n}_+) \xrightarrow{\sim} U(\mathfrak{g})$$

(linearly, not as algebras). The ideal $I_\lambda \subset U(\mathfrak{g})$ corresponds to $U(\mathfrak{n}_-) \otimes K_\lambda \subset U(\mathfrak{n}_-) \otimes U(\mathfrak{h} \oplus \mathfrak{n}_+)$ where $K_\lambda = \ker \chi_\lambda$ for $\chi_\lambda : U(\mathfrak{h} \oplus \mathfrak{n}_+) \to \mathbb{C}$ is given by $\chi_\lambda(h) = \lambda(h)$ (for $h \in \mathfrak{h}$) and $\chi_\lambda(e_i) = 0$ (showing this is an exercise). Thus, the PBW isomorphism identifies

$$U(\mathfrak{n}_-) = U(\mathfrak{n}_-) \otimes \mathbb{C} = U(\mathfrak{n}_-) \otimes \frac{U(\mathfrak{h} \oplus \mathfrak{n}_+)}{K_\lambda} \xrightarrow{\sim} U(\mathfrak{g})/I_\lambda = M_\lambda$$

and this composition is precisely $x \mapsto xv_\lambda$ (exercise). ■

Corollary 1.25.14. *M_λ has a weight decomposition into finite dimensional weight spaces, and its set of weights is $P(M_\lambda) = \lambda - Q_+$. Moreover, $\dim M_\lambda[\lambda] = 1$.*

Proof. Have PBW basis of $U(\mathfrak{n}_-) : \prod_{\alpha \in R_+} f_\alpha^{n_\alpha}$ gives a basis of $M_\lambda : \prod_{\alpha \in R_+} f_\alpha^{n_\alpha} \cdot v_\lambda$ which has weight $\lambda - \sum_{\alpha \in R_+} n_\alpha \cdot \alpha$. Thus, the weights are all in $\lambda - Q_+$ and $M_\lambda[\lambda] = \langle v_\lambda \rangle$ is one dimensional. Finally,

$\dim M_\lambda[\lambda-\beta] < \infty$ for $\beta \in Q_+$. In particular, its dimension is equal to the **Kostant partition function**, the number of ways to write β as $\sum_{\alpha\in R_+} n_\alpha \alpha$ with $n_\alpha \in \mathbb{Z}_{\geq 0}$. ■

Theorem 1.25.15 (**Universal Property of Verma Modules**).

(1) If V is a $\mathfrak{g}$-module an $v \in V$ a highest weight vector with weight λ. Then there exists a unique homomorphism $\eta : M_\lambda \to V$ such that $\eta(v_\lambda) = v$. In particular, if V is generated by v (so it is a highest weight representation), then η is surjective, so V is a quotient of M_λ.

(2) Every highest weight representation (with highest weight λ) has a weight decomposition into finite dimensional weight spaces with weights $\subset \lambda - Q_+$.

Proof. **(1)** Uniqueness is simply because v_λ generates M_λ. To construct η, start with $\widetilde{\eta} : U(\mathfrak{g}) \to V, x \mapsto xv$. By construction, $\widetilde{\eta}|_{I_\lambda} = 0$, so $\widetilde{\eta}$ descends to a map $\eta : M_\lambda \to V$. The rest of **(1)** is easy.

(2) This follows from **(1)** + the previous corollary. ■

Corollary 1.25.16. *Every highest weight representation has exactly one highest weight vector up to scaling (and so has a unique highest weight).*

Proof. Suppose v, w are two highest weight vectors each generating V, of weights λ, μ. If $\lambda = \mu$, then we win since $\dim V[\lambda] \leq \dim M_\lambda[\lambda] = 1$.

If $\lambda \neq \mu$, then WLOG $\lambda - \mu \notin Q_+$. Hence, $\mu \notin \lambda - Q_+$ so $M_\lambda[\mu] = 0 \implies V[\mu] = 0$ so $V = 0$. ■

Last class on Tuesday.

1.26 Lecture 26 (12/8): Last Class

3 minutes late

Note 4. My nose has been running an ungodly amount since I woke up today, so I was periodically distracted by having to deal with that, and these notes suffered a little. I hope this was a one-off thing, but if you don't see me writing more notes after today, it's almost certainly because I caught the vid and died.

Proposition 1.26.1. *For all $\lambda \in \mathfrak{h}^*$, the Verma module M_λ has a unique irreducible quotient L_λ, which is also a quotient of every nonzero highest weight representation with highest weight λ.*

Proof. Let $Y \subsetneq M_\lambda$ be a proper submodule, and let $v_\lambda \in M_\lambda$ be a generator. Then, $v_\lambda \notin Y$ (and Y has a weight decomposition), so Y's weights $P(Y) \subset (\lambda - Q_t) \setminus \{\lambda\}$ do not include λ. Let J_λ be the sum of all proper submodules of M_λ. Then, $P(j_\lambda) \subset (\lambda - Q_+) \setminus \{\lambda\}$, so $J_\lambda \neq M_\lambda$. We call J_λ the *maximal proper submodule* of M_λ. Thus, the quotient $L_\lambda := M_\lambda / J_\lambda$ is irreducible with highest weight λ. Furthermore, if V is any nonzero quotient of M_λ, then we have $\xi : M_\lambda \twoheadrightarrow V$ with kernel $K = \ker \xi \subsetneq M_\lambda$, so $K \subset J_\lambda$. Thus, $M_\lambda \twoheadrightarrow L_\lambda$ descends to a map $V \twoheadrightarrow L_\lambda$, finishing the proof (note that if V is irred then this is an iso). ■

Remark 1.26.2. The representations with highest weight λ form a poset (under surjection) with maximal element M_λ and minimal element L_λ. ○

Example. $\mathfrak{g} = \mathfrak{sl}_2$ so $\mathfrak{h}^* = \mathbb{C}$, $Q = 2\mathbb{Z}$ (root lattice), and $\alpha = 2$ is the only root. Have $f : V[\lambda] \to V[\lambda-2]$ and $e : V[\lambda] \to V[\lambda+2]$. One can show

$$ef^n v_\lambda = n(\lambda - n + 1) f^{n-1} v_\lambda,$$

so $f^n v_\lambda$ is a highest weight vector $(n > 0) \iff \lambda = n - 1 \in \mathbb{Z}_{\geq 0}$. Hence, M_λ is irreducible iff $\lambda \notin \mathbb{Z}_{\geq 0}$ (in this case, $M_\lambda = L_\lambda$). If $\lambda = m \in \mathbb{Z}_{\geq 0}$, then $f^{m+1} v_\lambda$ is a highest weight vector of weight $\lambda - 2(m+1) = m - 2(m+1) = -m-2$. In this case, one gets $J_\lambda = M_{-\lambda-2}$ and $L_\lambda = M_\lambda / M_{-\lambda-2}$ which is f.d. of dimension $\lambda + 1$. △

Corollary 1.26.3. *Irreducible highest weight representations of $\mathfrak{g}$ are classified by their highest weight $\lambda \in \mathfrak{h}^*$ via the assignment $\lambda \mapsto L_\lambda$.*

Example. $L_0 = \mathbb{C}$ is the trivial rep. △

Question 1.26.4. *For which λ is L_λ finite dimensional?*

Answering this will give us a classification of finite dimensional representations.

They are finite dimensional for some subset $P_F \subset P$ (eigenvalues of h_i are in $\mathbb{Z}$). Let

$$P_+ = P \cap \overline{C}_+ = \left\{\lambda \in P : (\lambda, \alpha_i^\vee) \geq 0 \,\forall i\right\},$$

be the set of **dominant integral weights**.

Lemma 1.26.5. $P_F \subset P_+$.

Proof. $v_\lambda \in L_\lambda$ is a highest weight vector for each $(\mathfrak{sl}_2)_i$ of highest weight $\lambda(h_i) = (\lambda, \alpha_i^\vee)$. If it generates a f.d. representation, then we have $(\lambda, \alpha_i^\vee) \geq 0$ by rep theory of $\mathfrak{sl}_2$. ■

We will show that the converse holds as well.

Lemma 1.26.6. *If $\lambda \in P_+$, then in L_λ we have $f_i^{\lambda(h_i)+1} v_\lambda = 0$.*

Proof. First consider the restriction of the representation to $(\mathfrak{sl}_2)_i$. Got districated... but one can show $e_i f_i^{\lambda(h_i)+1} v_\lambda = 0$, and for $j \neq i$,

$$e_j f_i^{\lambda(h_i)+1} v_\lambda = f_i^{\lambda(h_i)+1} e_j v_\lambda = 0.$$

Hence, $f_i^{\lambda(h_i)+1} v_\lambda$ is a highest weight vector of weight $\lambda - \lambda(h_i)\alpha_i$, so it generates a proper submodule of L_λ, but L_λ irreducible so $f_i^{\lambda(h_i)+1} = 0$ as claimed. ■

Theorem 1.26.7. *For any $\lambda \in P_+$, L_λ is finite dimensional, i.e. $P_F = P_+$.*

Proof. We know $f_i^{\lambda(h_i)+1} v_\lambda = 0$, so v_λ generates a f.d. $(\mathfrak{sl}_2)_i$-module (namely $V_{\lambda(h_i)}$). Also, any $x \in \mathfrak{g}$ generates a f.d. $(\mathfrak{sl}_2)_i$-module, so for any $x_1^i, \ldots, x_n^i \in \mathfrak{g}$, one has

$$\sum_{i=1}^{n} x_1^i \ldots x_n^i v_\lambda$$

generates a f.d. $(\mathfrak{sl}_2)_i$-module (it is a quotient of $\mathfrak{g}^{\otimes n} \otimes V_{\lambda(h_i)}$ which is f.d.). Hence, any vector $v \in L_\lambda$ generates a f.d. $(\mathfrak{sl}_2)_i$-module. By Lemma 1.25.4, this means that for all μ, $\dim L_\lambda[\mu] = \dim L_\lambda[w\mu]$ for all $w \in W$. Now take $\mu \in P(L_\lambda) \cap P_+$. Then $\mu = \lambda - \beta$, $\beta \in Q_+$, so

$$(\mu, \rho^\vee) = (\lambda, \rho^\vee) - (\beta, \rho^\vee) \leq (\lambda, \rho^\vee)$$

where recall $\rho^\vee = \sum \omega_i^\vee$ (sum of fundamental coweights) and where we've used $(\beta, \rho^\vee) = \sum (\beta, \omega_i^\vee) \geq 0$. But $\mu = \sum m_i \omega_i$ with $m_i \in \mathbb{Z}_{\geq 0}$, so

$$(\mu, \rho^\vee) = \sum m_i(\omega_i \rho^\vee) \text{ and } (\omega_i, \rho^\vee) = \frac{1}{2} \sum_{\alpha \in R_+} (\omega_i, \alpha^\vee) \geq \frac{1}{2}.$$

Thus, $\sum m_i \leq 2(\lambda, \rho^\vee)$, but there are only finitely many collections $\{m_i\}$ of nonnegative integers satisfying this. Hence, $P(L_\lambda) \cap P_+$ is finite, but $WP_+ = P$, so $W(P(L_\lambda) \cap P_+) = P(L_\lambda)$ ($P(L_\lambda)$ is W-invariant). Thus, $P(_\lambda)$ is finite, so L_λ is finite dimensional. ■

Corollary 1.26.8. *Finite dimensional irreducible representations of $\mathfrak{g}$ are classified by $\lambda \in P_+$ via $\lambda \mapsto L_\lambda$. Also, for all $\mu \in P$ and $w \in W$,*

$$\dim L_\lambda[\mu] = \dim L_\lambda[w\mu].$$

I left for one minute and now he's drawn the A_2 root system and I'm confused about what's going on... Something about drawing the 'weight diagram' of an $\mathfrak{sl}_3$-rep. It looks like a hexagon unless λ lies on a root hyperplane; then it looks like a triangle. Something like this.

1.26.1 Last topic: Weyl character formula

Let G be a group, and let V be a f.d. representation of G. Then it has attached a character $\chi_V(g) = \mathrm{Tr}_V(g)$.

Let $\mathfrak{g}$ be a semisimple Lie algebra with corresponding simply connected complex Lie group G. Let V be a f.d. holomorphic representation of G (so also a representation of $\mathfrak{g}$). How do we compute $\chi_V(g)$? Let $\mathfrak{h} \subset \mathfrak{g}$ be Cartan, so $h \in \mathfrak{h} \implies e^h \in G$. Hence,

$$\chi_V(e^h) = \sum_\mu \dim V[\mu] \cdot e^\mu(h) \text{ when } V = \bigoplus_{\mu \in P} V[\mu]$$

as $e^h|_{V[\mu]} = e^{\mu(h)}$. This alone determines the entire character. It determines e^x for any semisimple element $x \in \mathfrak{g}$, and semisimple elements are dense, open in $\mathfrak{g}$, so elements e^x (with x semisimple) cover a dense open set in a neighborhood of 1 in G (so cover a generating set for $G^\circ = G$).

Question: Why?

More generally, for any representation of $\mathfrak{g}$ with weight decomposition

$$V = \bigoplus_\mu V[\mu], \quad \dim V[\mu] < \infty,$$

we can define the **formal character**

$$\chi_V = \sum_\mu \dim V[\mu] e^\mu$$

as some formal expression. Here, e^μ another notation for $\nu \in \mathfrak{h}^*$; this notation is inspired by the previous example (where we take a literal exponential) and by the relation $e^\mu \cdot e^\nu = e^{\mu+\nu}$.

Definition 1.26.9. A representation V of $\mathfrak{g}$ lies in the category $\mathscr{O}$ if $V = \bigoplus_{\mu \in \mathfrak{h}^*} V[\mu]$ with $\dim V[\mu] < \infty$ (i.e. V has a weight decomp) and

$$P(V) \subset \bigcup_{i=1}^{N} (\lambda^i - Q_+)$$

for some N depending on V. ◇

Example. Any highest weight representation belongs to $\mathscr{O}$. Further, $\mathscr{O}$ supports direct sums and tensor products. Even furthermore, $X \subset Y$ and $Y \in \mathscr{O} \implies X \in \mathscr{O}$ and $Y/X \in \mathscr{O}$. △

Let R denote the ring of formal series

$$a = \sum_{\mu \in \mathfrak{h}^*} a_\mu e^\mu \text{ with } a_\mu \in \mathbb{Z}$$

such that its support

$$P(a) = \{\mu : a_\mu \neq 0\}$$

is contained in a set of the form

$$(\lambda^1 - Q_+) \cup \cdots \cup (\lambda^N - Q_+).$$

Exercise. Show that R is a ring under usual multiplication of series.

Remark 1.26.10. If $V \in \mathscr{O}$, then $\chi_V \in R$ and

$$\chi_{V \otimes W} = \chi_V \chi_W \qquad \text{(exercise)}.$$

Further, if you have a short exact sequence

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

in $\mathscr{O}$, then $\chi_Y = \chi_X + \chi_Z$. More generally, one gets that the alternating sum of characters vanishes, e.g.

$$0 \to X \to Y \to Z \to T \to 0 \in \mathscr{O} \implies \chi_X - \chi_Y + \chi_Z - \chi_T = 0.$$

○

Example. $V = M_\lambda$ and $\mathfrak{g} = \mathfrak{sl}_2$. Recall

$$M_\lambda \simeq \mathbb{C}[f] \cdot v_\lambda,$$

so all weight spaces are one-dimensional. Something something

$$\sum \mathbb{C}[f][m] x^m = \frac{1}{1 - x^{-2}},$$

and we see that

Question: What is α?

$$\chi_{M_\lambda} = \frac{e^\lambda}{1-e^{-\alpha}}.$$

More generally,

$$M_\lambda = U(\mathfrak{n}_-)v_\lambda \simeq U(\mathfrak{n}_-) = \bigotimes_{\alpha\in R_+} \mathbb{C}[e_{-\alpha}]$$

and

$$\chi_{M_\lambda} = e^\lambda \prod_{\alpha\in R_+} \frac{1}{1-e^{-\alpha}} = \frac{e^\lambda}{\prod_{\alpha\in R_+}(1-e^{-\alpha})}.$$

We can rewrite this, using $\rho = \frac{1}{2}\sum_{\alpha\in R_+}\alpha$. One gets

$$\prod_{\alpha\in R_+}(1-e^{-\alpha}) = e^{-\rho}\prod_{\alpha\in R_+}(e^{\alpha/2}-e^{-\alpha/2}),$$

so

$$\chi_{M_\lambda} = \frac{e^{\lambda+\rho}}{\prod_{\alpha\in R_+}(e^{\alpha/2}-e^{-\alpha/2})}.$$

Above,

$$\Delta := \prod_{\alpha\in R_+}(e^{\alpha/2}-e^{-\alpha/2})$$

is called the **Weyl denominator**. △

Why the rewrite above? Recall the **sign character** $\varepsilon : W \to \mathbb{Z}/2\mathbb{Z}$ given by

$$\varepsilon(w) = \det w|_{\mathfrak{h}} = (-1)^{\ell(w)}.$$

Example. Type A_{n-1}, $W = S_n$, and this is the usual sign of a permutation. △

Definition 1.26.11. An element of $\mathbb{Z}[\mathfrak{h}^*]$ is W**-antiinvariant** if for any $w \in W$,

$$w(f) = (-1)^{\ell(w)} f = \varepsilon(w) f.$$

◇

Lemma 1.26.12. *Δ is W-antiinvariant.*

Proof. Recall s_i permutes $R_+ \setminus \{\alpha_i\}$ and that $s_i(\alpha_i) = -\alpha_i$. Thus,

$$s_i\left(\prod_{\alpha\in R_+}\left(e^{\alpha/2}-e^{-\alpha/2}\right)\right) = -\prod_{\alpha\in R_+}\left(e^{\alpha/2}-e^{-\alpha/2}\right)$$

since most factors are permuted, but one is negated (summands switched). ■

Corollary 1.26.13 (Weyl denominator formula).

$$\Delta = \sum_{w\in W}(-1)^{\ell(w)} e^{w\rho} \in \mathbb{Z}[P].$$

Proof. The RHS is W-antiinvariant by construction. Since $s_i\Delta = -\Delta$ is a Laurent polynomial, we must have Δ divisible by $e^{\alpha_i/2} - e^{-\alpha_i/2}$. Hence, it is divisible by $e^{\alpha/2} - e^{-\alpha/2}$ for all α, so

$$f = \frac{\sum_{w\in W}(-1)^{\ell(w)}e^{w\rho}}{\Delta} \in \mathbb{Z}[P]^W.$$

We also know that its support (the set of occurring weights) satisfies

$$P(f) \subset -Q_+$$

since the weights of the both the numerator and the denominator lie in $\rho - Q_+$. Thus, $P(f) \subset \{0\}$ so any element of P can be mapped by an element of W to a dominant element. Thus, f is constant. Looking at the leading coefficient, we in fact have $f = 1$. ■

Exercise. For type A_{n-1}, this is the Vandermonde determinant.

Theorem 1.26.14 (Weyl Character Formula).

$$\chi_{L_\lambda} = \frac{\sum_{w\in W}(-1)^{\ell(w)}e^{w(\lambda+\rho)}}{\prod_{\alpha\in R_+}(e^{\alpha/2} - e^{-\alpha/2})}$$

Example. $\lambda = 0$ gives $L_\lambda = \mathbb{C}$ and $\chi_{L_\lambda} = 1$, so we recover the Weyl denominator formula. △

Not enough time for the whole proof (find it in the notes), so we'll just give the ideas...

We know $\Delta\chi_\lambda$ is W-antiinvariant (χ_λ is W-invariant), so we can write

$$\Delta\chi_\lambda = \sum_{\mu\in P} C_\mu e^\mu \text{ where } C_{w\mu} = (-1)^{\ell(w)}C_\mu.$$

We also know $C_\mu = 0$ unless $\mu \in \lambda + \rho - Q_+$ and $C_{\lambda+\rho} = 1$. Hence, it suffices to show that

$$\lambda + \rho \neq \mu \in P_+ \cap (\lambda + \rho - Q_+) \implies C_\mu = 0.$$

Use rep theory; have $0 \to J_\lambda \to M_\lambda \to L_\lambda \to 0$, so $\chi_\lambda = \chi_{M_\lambda} - \chi_{J_\lambda}$. Thus,

$$\Delta\chi_\lambda = e^{\lambda+\rho} - \Delta\chi_{J_\lambda}.$$

We also have

$$0 \to K \to M_\mu \to J_\lambda \to C \to 0 \implies \chi_{J_\lambda} = \chi_{M_\mu} - \chi_K + \chi_C.$$

Hence,

$$\Delta\chi_\lambda = e^{\lambda+\rho} - e^{\mu+\rho} + \Delta\chi_K - \Delta\chi_C.$$

Continue...

$$K' \to M_{\gamma'} \to K \to C' \text{ and } K'' \to M_{\gamma''} \to C \to C'$$

giving more exponentials and more things you can resolve. In the limit, you get

$$\Delta\chi_\lambda = e^{\lambda+\rho} - e^{\mu+\rho} + \cdots.$$

Then consider the Casimir C and check that $C|_{M_\lambda, L_\lambda} = (\lambda, \lambda + 2\rho)$ so it has the same eigenvalues on all these other spaces we've constructed along the way. Thus, if $\gamma + \rho$ occurs in our sum of exponentials, then $(\gamma, \gamma + 2\rho) = (\lambda, \lambda + 2\rho)$. Make a combinatorial argument saying this can't happen in $\gamma + \rho \in (\lambda + \rho - Q_+) \cap P_+$ unelss $\nu = \lambda$, and then you're done. See notes for details.

2 18.785 (Number Theory I)

This class overlaps with 273X on Wednesdays, and I do not plan on attending/watching many of the lectures in the beginning weeks, so these notes will be (very) incomplete.

Instructor: Wei Zhang There is a Dropbox with live-written notes during class as well as some texed notes.

2.1 Lecture 1 (9/2)

Missed the first half

I think most of the lecture was spent showing that $\mathscr{O}_K$ is a free $\mathbb{Z}$-algebra of rank $[K:\mathbb{Q}]$ when K is a number field. Also contained the following (apparently open) question.

Open Question 2.1.1. *Fix some positive $X > 0$. Is the set of number fields $K/\mathbb{Q}$ satisfying $\left|\Delta_{K/\mathbb{Q}}^{1/n}\right| < X$ finite? Here, $\Delta_{K/\mathbb{Q}}$ is the discriminant and $n = [K:\mathbb{Q}]$ is the degree of the number field.*

2.2 Lecture 6 (9/23)

Setup 2.2.1.

$$\begin{array}{ccc} & B & L \\ & \Big| & \Big| \\ 0 \neq \mathfrak{p} & A & K \end{array}$$

A Dedekind with $K = \operatorname{Frac} A$ and L/K a finite extension of fields. $\mathfrak{p} \subset A$ is a nonzero prime, and we factor
$$\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}.$$

Definition 2.2.2. We say $\mathfrak{q}_i/\mathfrak{p}$ is **unramified** if $e_i = 1$ and $B/\mathfrak{q}_i$ is separable over $K = A/\mathfrak{p}$. ◇

Lemma 2.2.3 (and Definition)**.** *Let K be a field of positive characteristic p. Then, TFAE*

- *every finite extension of K is separable.*
- *The pth power map $\operatorname{Frob} : K \to K, x \mapsto x^p$ is an isomorphism (i.e. $K = K^p$).*

*If either holds, we call K a **perfect field** (we also call K perfect if $\operatorname{char} K = 0$).*

Example. Any characteristic 0 field, finite field, or algebraically closed field is perfect. △

Non-example. $\mathbb{F}_q(t)$ is not perfect since $t^{1/p} \notin \mathbb{F}_q(t)$. ▽

Recall 2.2.4. We defined $\operatorname{Disc}(B/A) \subset A$ as an ideal. When B is A-free, it is generated by the discriminant of the bilinear trace form $(a,b) \mapsto \operatorname{tr}(ab)$. ⊙

Theorem 2.2.5. *$\mathfrak{p}$ is ramified (i.e. $e_i > 1$ or residue field inseparable) $\iff$ $\mathfrak{p} \mid \operatorname{disc}(B/A)$.*

Proof Sketch. Can localize to assume that B is a free A-module, so write $B = \bigoplus_{i=1}^n Ax_i$. Then, $(\det(x_ix_j)) = \operatorname{Disc}(B/A)$ and $B/\mathfrak{p}B \simeq \bigoplus_{i=1}^n k\overline{x_i}$ where $k = A/\mathfrak{p}A$. This is a finite-dimensional k-algebra and one has $\operatorname{Disc}(B/A) \equiv \operatorname{Disc}(\overline{B}/k)$. At the same time,

I really messed up these notes, but I'm not fixing it.

$$\overline{B} \cong B/\prod \mathfrak{q}_i^{e_i} = \bigoplus_{i=1}^{g} B/\mathfrak{q}_i^{e_i}$$

so everything boils down to facts about f.d. k-algebras. Note that $\mathfrak{p}$ is unramified iff all $e_i = 1$ and all $B/\mathfrak{q}_i$ separable over k iff $\overline{B}$ is a finite product of separable field extensions.

Thus, it suffices to prove the following.

Lemma 2.2.6. *Let R be a finite dimensional k-algebra. Then,*

$$\operatorname{Disc}(R/k) \neq 0 \iff \text{“}R \text{ separable over } k\text{”}$$

(i.e. R is a finite product of separable fields extensions).

Nice to interpret this using differentials. Let $A \to B$ be a ring map. One can define the B-module $\Omega_{B/A}$ of differentials. Directly,

$$\Omega_{B/A} = B\left\langle \mathrm{d}x : x \in B \,|\, \mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y, \mathrm{d}(ax) = a\mathrm{d}x, \mathrm{d}(xy) = x\mathrm{d}y + y\mathrm{d}x \right\rangle$$

(where $x, y \in B$ and $a \in A$). This comes equipped with a natural A-linear derivation $\mathrm{d} : B \to \Omega_{B/A}, x \mapsto \mathrm{d}x$. The pair $(\Omega_{B/A}, \mathrm{d})$ is universal in a sense we won't make precise right now because we've kind of gone on a tangent.

In above lemma, our condition will hold also $\iff$ $\Omega_{R/k} = 0$. Let's quickly prove that separable implies the differential being trivial.

Example. $A = k$ and $B = k' = k[x]/(f(x))$ are both fields. We see that $\Omega_{k'/k}$ is generated (over k') by $\mathrm{d}x$ and satisfies the relation $\mathrm{d}f(x) = 0$, i.e. $f'(x)\mathrm{d}x = 0$ (this is the only relation). Hence, $\Omega_{k'/k} = B/(f'(x)) = k[x]/(f(x), f'(x))$ so $\Omega_{k'/k} = 0 \iff k'/k$ is separable (i.e. $f'(x) \neq 0$ in B). △

Example. If $B = \prod k_i$ and $A = k$, then one can easily show that $\Omega_{B/k} = \prod \Omega_{k_i/k}$. Therefore, $\Omega_{B/A} = 0 \iff k_i/k$ separable for all i (B is a separable k-algebra). △

Example. Suppose $k' = k[x]/(f(x))$ is a field. The discriminant is defined in terms of the trace pairing

$$\begin{array}{rccc} \operatorname{Tr} : & k' \times k' & \longrightarrow & k \\ & (x, y) & \longmapsto & \operatorname{Tr}(xy) \end{array}$$

Note that k' has a k-basis $1, x, x^2, \ldots, x^{n-1}$. We claim

$$\operatorname{Disc}(k'/k) \neq 0 \iff f'(x) \neq 0 \iff k'/k \text{ separable.}$$

More on this in a bit. △

Fact. Let R be a finite dimensional k-algebra. Then, TFAE

- $R = \prod_{i=1}^{d} k_i$ with k_i/k field.
- R is reduced (i.e. has no nilpotents)

Allegedly, all the examples/facts in the aside combine to (basically) finish the proof of this lemma, which then clearly finishes the proof of the claim. ■

Let's reformulate a little. We have the same setup as before. A better formulation is the following.

Theorem 2.2.7. *Assume A is a dvr with unique nonzero prime $\mathfrak{p}$. Then, $\mathfrak{p}$ is unramified $\iff$ $\Omega_{B/A} = 0$.*

Definition 2.2.8. B is **étale** over A if B is flat over A and $\Omega_{B/A} = 0$. $\diamond$

Fact. Over a Dedekind domain, flat $\iff$ torsion free. Hence, étale = unramified over a Dedekind domain.

Example. Suppose $B = A[x]/(f(x))$ is a field. The discriminant is defined in terms of the trace pairing

$$\begin{array}{rccc} \mathrm{Tr}: & B \times B & \longrightarrow & A \\ & (x, y) & \longmapsto & \mathrm{Tr}(xy) \end{array}$$

It's not too hard to show that

$$L \ni \mathrm{Tr}\left(\frac{x^i}{f'(x)}\right) = \begin{cases} 0 & \text{if } 0 \le i \le n-2 \\ 1 & \text{otherwise.} \end{cases}.$$

This tells us that the codifferent

$$D_{B/A}^{-1} = \{b \in L : \mathrm{Tr}(bB) \subset A\}$$

has a basis as an A-module given by $\alpha^i/f'(\alpha)$ for $i = 0, \dots, n-1$. Thus, as a fractional ideal, $D_{B/A}^{-1} = (1/f'(x))$, so $D_{B/A} = (f'(x)) \subset B$. What's the conclusion? Well, under this (big) assumption that B is monogenic, we have

$$\Omega_{B/A} \simeq B/(f'(x)) \simeq B/D_{B/A}.$$

$\triangle$

How are the different and discriminant related? We have a norm map $\mathrm{N} : \mathrm{Id}(B) \to \mathrm{Id}(A)$ from invertible ideals of B to those of A given, on primes, by $\mathrm{N}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$ where this f is the inertia degree.

Example. Suppose $\mathfrak{q} = (\beta)$ is principal. Then, $\mathrm{N}\,\beta = \prod_{\sigma \in \mathrm{Gal}} \sigma(\beta)$, so $(\mathrm{N}\,\beta) = \prod \sigma(\mathfrak{q})$ as ideals in B. Hence,

$$(\mathrm{N}\,\beta) = \prod_{\sigma \in \mathrm{Gal}} \sigma(\mathfrak{q}) = \left(\prod_{\mathfrak{q}_i | \mathfrak{p}} \mathfrak{q}_i^e\right)^f = (\mathfrak{p}B)^f.$$

This is why we define $\mathrm{N}\,\mathfrak{q} = \mathfrak{p}^f$. It makes the following diagram commutative

$$\begin{tikzcd} L^\times \arrow[r] \arrow[d, "\mathrm{N}"'] & \mathrm{Id}(B) \arrow[d, "\mathrm{N}"] \\ K^\times \arrow[r] & \mathrm{Id}(A) \end{tikzcd}$$

$\triangle$

Claim 2.2.9.

$$\mathrm{N}(D_{B/A}) = \mathrm{Disc}(B/A) \subset A.$$

Can reduce to the base $B = A[\alpha]$ is monogenic since this is always the case when B, A are dvrs and both L/K and $(B/\mathfrak{q})/(A/\mathfrak{p})$ are separable.

Remark 2.2.10 (From Ravi's notes). It seems that, in general, the different of B/A is the annihilator $D_{B/A} = \mathrm{Ann}(\Omega_{B/A})$ of the module of differentials, and then the discriminant is attained from the different via push-forward. $\circ$

2.3 Lecture 10 (10/7)

Today we'll talk about the arithmetic Riemann-Roch for algebraic integers.

Recall 2.3.1. In the past few lectures, proved two foundational results on the the structure of $\mathscr{O}_K$ for $K/\mathbb{Q}$ a number field. The first was the finiteness of the class group $\#\,\mathrm{Cl}_K < \infty$. The second was **Dirichlet's Unit Theorem** $\mathrm{rank}_{\mathbb{Z}}\,\mathscr{O}_K^\times = r_1 + r_2 - 1$ where r_1 is the number of real embeddings $K \hookrightarrow \mathbb{R}$ and r_2 is the number of (conjugate pairs of) complex embeddings $K \hookrightarrow \mathbb{C}$. $\odot$

We want to look at these results in analogy with geometry.

2.3.1 The Geometric Situation

Consider a compact Riemann surface X, e.g. $X = \mathbb{P}^1_{\mathbb{C}}$. Let K be the field of meromorphic functions on X (i.e. $f : X \dashrightarrow \mathbb{C}$). For example, when $X = \mathbb{P}^1$, $K \simeq \mathbb{C}(t)$ is the field of rational functions over $\mathbb{C}$.

Definition 2.3.2. The **group of divisors** $\mathrm{Div}(X)$ on X is the free abelian group $\mathrm{Div}(X) = \bigoplus_{x \in X} \mathbb{Z}x$, i.e. a **divisor** on X is a finite formal sum of points on x, $D = \sum_{x \in X} m_x \cdot x$. The **degree of a divisor** $\deg : \mathrm{Div}(X) \to \mathbb{Z}$ is the map $\deg(\sum m_x x) = \sum m_x$. $\diamond$

Remark 2.3.3. Given a nonzero rational function $f \in K = K(X)$, one can associate to it the **principal divisor**

$$\mathrm{div}(f) = \sum_x \mathrm{ord}_x(f) x.$$

This gives a group map $\mathrm{div} : K^\times \to \mathrm{Div}(X)$. $\circ$

Given D, one can consider a line bundle $\mathscr{O}(D) = \mathscr{L}$ and so D has some associated cohomology groups. One can define this explicitly without reference to sheaf cohomology if they want. We set

$$\mathrm{H}^0(X, \mathscr{O}(D)) = \left\{f \in K(X)^\times : \mathrm{div}(f) \geq -D\right\} \cup \{0\} = \{f \in K(X) : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

where $D = \sum_x m_x x \geq 0$ iff $m_x \geq 0$ for all x (such a divisor is called an **effective divisor**).

Definition 2.3.4. The **Picard group** is $\mathrm{Pic}(X) := \mathrm{Div}(X)/\left\langle \mathrm{div}(f) : f \in K^\times\right\rangle$. This is an analogue of the class group. $\diamond$

Fact. $\deg \mathrm{div}\, f = 0$.

Hence we define $\mathrm{Pic}^0(X)$ via its position in the short exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0.$$

Exercise. $\mathrm{Pic}^0(\mathbb{P}^1) = 0$.

Lemma 2.3.5. *If $D \in \mathrm{Div}^0(X)$ (i.e. D has degree 0) with $\mathrm{H}^0(X, \mathscr{O}(D)) \neq 0$, then D is principal, i.e. $[D] = 0 \in \mathrm{Pic}(X)$.*

The most important thing is Riemann-Roch. For a line bundle $\mathscr{L}$, its Euler characteristic is

$$\chi(\mathscr{L}) = \dim \mathrm{H}^0(\mathscr{L}) - \dim \mathrm{H}^1(\mathscr{L})$$

where we haven't defined higher cohomology groups here, but don't worry about that.

Theorem 2.3.6 (**Riemann-Roch**). *$\chi(\mathscr{O}(D)) = \deg D + \chi(\mathscr{O})$. Setting $g := \dim \mathrm{H}^1(\mathscr{O})$, this says*

$$\chi(\mathscr{O}(D)) = \deg D + 1 - g.$$

*This g is called the **genus** (it agrees with the topologically defined genus of a surface).*

Corollary 2.3.7. *If $\deg D > -\chi(\mathscr{O}) = g - 1$, then $\mathrm{H}^0(\mathscr{O}(D)) \neq 0$.*

Remark 2.3.8. Need strict $>$ above. For example, consider $\mathscr{O}(-1)$ on $\mathbb{P}^1$. Here, $\deg D = -1 = 0-1 = g-1$, but $\mathrm{H}^0(\mathscr{O}(-1)) = 0$. Also, $\mathrm{H}^1(\mathscr{O}(-1)) = \mathrm{H}^0(\mathscr{O}(-2+1)) = 0$. ○

Remark 2.3.9. If $\mathrm{H}^0(\mathscr{O}(D)) \neq 0$, then D is equivalent to an effective divisor. ○

Corollary 2.3.10 (of Riemann-Roch). *If $\deg D \geq g$, then D is equivalent to an effective divisor, i.e.*

$$X^d \twoheadrightarrow \mathrm{Pic}^d(X) = \{\textit{degree } d \textit{ divisor classes}\}$$

(when $d \geq g$).

2.3.2 The Arithmetic Situation

We will give an arithmetic version of Riemann-Roch which will unify finiteness of class group and Dirichlet's unit theorem.

Recall 2.3.11. For $\mathfrak{a} \subset K$ a fractional ideal in a number field K, there exists some $x \in \mathfrak{a}^{-1}$ such that $\mathrm{Nm}(x\mathfrak{a}) \leq C_K$ with C_K the Minkowski constant, i.e. any fractional ideal has a representative in Cl_K with norm bounded by Minkowski constant. ⊙

How should we interpret cohomology in the number field case?

Thinking about the definition in the geometric case, we want field elements with vanishing order at each point bounded below. In the number field case, we need to also take into account the archimedean places.

Naively, one may think we should consider $\mathrm{Div}\, \mathscr{O}_K = \bigoplus_{\mathfrak{p}} \mathbb{Z}\mathfrak{p}$, the group of fractional ideals (along with the subgroup of principal divisors/fractional ideals). However, $\mathscr{O}_K$ is not a compact/complete/proper curve, so this would not give a proper analogy to the geometric case (where X was assumed compact).

Hence, we consider the **compactified divisors**

$$\widehat{\mathrm{Div}}(\mathscr{O}_K) = \left\{ \left(D, (\lambda_\sigma)_{\sigma \mid \infty} \right) : D \in \mathrm{Div}, \lambda_\sigma \in \mathbb{R} \right\}$$

where $\sigma \mid \infty$ means we range over infinite places (i.e. embeddings $K \hookrightarrow \mathbb{C}$ up to equivalence of conjugate pairs). Hence,

$$\widehat{\mathrm{Div}}(\mathscr{O}_K) \simeq \mathrm{Div}(\mathscr{O}_K) \times \mathbb{R}^{r_1+r_2}.$$

The **compactified principal divisors** are

$$\widehat{\mathrm{Pr}}(\mathscr{O}_K) = \left\{ \widehat{\mathrm{div}}(f) = (\mathrm{div}\, f, \varepsilon_\sigma \log |f|_\sigma) \right\}$$

where

$$\varepsilon_\sigma = \begin{cases} 1 & \text{if } \sigma \text{ real} \\ 2 & \text{otherwise.} \end{cases}.$$

One then gets the **compactified Picard group**

$$\widehat{\mathrm{Pic}}(\mathscr{O}_K) = \frac{\widehat{\mathrm{Div}}(\mathscr{O}_K)}{\widehat{\mathrm{Pr}}(\mathscr{O}_K)}.$$

This is the true analogue of the Picard group for a compact Riemann surface.

We can even define a degree map, although now it is real-valued. We set the **degree of a compactified divisor** to be

$$\deg \widehat{D} = \deg\left(D, (\lambda_\sigma)\right) = \log \mathrm{Nm}\, D + \sum_{\sigma \mid \infty} \lambda_\sigma.$$

If you write $D = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \mathfrak{p}$, then the left summand is

$$\log \mathrm{Nm}\, D = \sum_{\mathfrak{p}} m_{\mathfrak{p}} \log \mathrm{Nm}\, \mathfrak{p}.$$

We define $\widehat{\mathrm{Pic}}^0(\mathscr{O}_K)$ via the exact sequence

$$0 \longrightarrow \widehat{\mathrm{Pic}}^0(\mathscr{O}_K) \longrightarrow \widehat{\mathrm{Pic}}(\mathscr{O}_K) \xrightarrow{\deg} \mathbb{R} \longrightarrow 0$$

and similarly define $\widehat{\mathrm{Div}}^0$. Note that we also have another exact sequence

$$0 \longrightarrow \frac{\mathbb{R}^{r_1+r_2}}{\log \mathscr{O}_K^\times} \longrightarrow \widehat{\mathrm{Pic}}(\mathscr{O}_K) \longrightarrow \mathrm{Cl}_K \longrightarrow 0$$

(this requires a proof, but is not too hard).

By taking the degree zero part everywhere, we just as well see that we have an exact sequence

$$0 \longrightarrow \frac{\mathbb{R}^{r_1+r_2-1}}{\log \mathscr{O}_K^\times} \longrightarrow \widehat{\mathrm{Pic}}^0(\mathscr{O}_K) \longrightarrow \mathrm{Cl}_K \longrightarrow 0.$$

Theorem 2.3.12. *$\widehat{\mathrm{Pic}}(\mathscr{O}_K)^0$ is compact. This combines both finiteness of the class group and Dirichlet's unit theorem.*

Remark 2.3.13. What's the topology above? The kernel $\frac{\mathbb{R}^{r_1+r_2-1}}{\log \mathscr{O}_K^\times}$ has a natural topology ($\log \mathscr{O}_K^\times$ is a lattice in $\mathbb{R}^{r_1+r_2-1}$) and Cl_K is given the discrete topology. We require both of these maps to the continuous. ○

Remark 2.3.14. In the geometric case, secretely $\mathrm{Pic}^0(X) \simeq \mathbb{C}^g/\mathbb{Z}^{2g}$ is also a compact Riemann Surface ○

Let's define cohomology. Consider $\widehat{D}$. We set

$$\mathrm{H}^0(\mathscr{O}(\widehat{D})) := \left\{f \in K^\times : \widehat{\mathrm{div}}(f) \geq -\widehat{D}\right\} \cup \{0\}.$$

Note that we say $\widehat{D} = \sum_{\mathfrak{p}} m_{\mathfrak{p}} + (\lambda_\sigma)_\sigma \geq 0$ iff

$$m_{\mathfrak{p}} \geq 0\, \forall \mathfrak{p} \text{ and } \lambda_\sigma \geq 0\, \forall \sigma.$$

We can alternatively write this as

There might be missing/misplaced negative signs somewhere in these notes. If everything is done correctly, one should have $\widehat{\deg}\widehat{\mathrm{div}} f = 0$

$$\mathrm{H}^0(\mathscr{O}(\widehat{D})) = \left\{0 \neq f \in D^{-1} : |f|_\sigma \leq e^{\varepsilon_\sigma^{-1}\lambda_\sigma}\right\} \cup \{0\}$$

where $D \subset K$ is a fractional ideal (and $\widehat{D} = (D, (\lambda_\sigma)_\sigma))$. Note that we have $D \hookrightarrow K \otimes \mathbb{R} = \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C}$ and $\mathrm{H}^0(\mathscr{O}(\widehat{D}))$ is basically lattice points (elements of D^{-1}) living in some bounded region (and so finite).

Lemma 2.3.15. *If* $\deg \widehat{D} = 0$ *and* $\mathrm{H}^0(\mathscr{O}(\widehat{D})) \neq 0$, *then* $\widehat{D} \equiv (\mathscr{O}_K, \lambda_\sigma = 0) \in \widehat{\mathrm{Pic}}(\mathscr{O}_K)$.

Theorem 2.3.16 (arithmetic Riemann-Roch). *If* $\deg \widehat{D} \geq -\chi(\widehat{D}) \implies \mathrm{H}^0(\widehat{D}) \neq 0$.

This is secretly a reformulation of Minkowski's lemma. We define

$$\chi(\mathscr{O}_K) := -\log\left(\frac{2}{\pi}\right)^{r_2} |\Delta_K|^{1/2}.$$

This Riemann-Roch let's one prove compactness of $\widehat{\mathrm{Pic}}^0$.

2.4 Lecture 11 (10/13)

Didn't pay attention for first 5 minutes

2.4.1 Arithmetic Riemann-Roch

Last time talked about analogy between never fields and Riemann surfaces. A key definition is the "space of global sections"

$$\mathrm{H}^0(\widehat{D}) = \left\{x \in K^\times : \widehat{\mathrm{div}}(x) \geq -\widehat{D}\right\}$$

Riemann surfaces	Number fields
D	$\widehat{D} = (\mathfrak{a}, (\lambda_\sigma)_{\sigma\mid\infty})$, a nonzero fractional ideal and a bunch of real numbers
$\mathrm{div}\, f$	$\widehat{\mathrm{div}\, f}$
$\mathrm{Pic}(\mathscr{O}_K)$	$\widehat{\mathrm{Pic}(\mathscr{O}_K)}$
$\deg \in \mathbb{Z}$	$\widehat{\deg} \in \mathbb{R}$
$\deg \mathrm{div}(f) = 0$	$\widehat{\deg}\widehat{\mathrm{div}}(f) = 0$

Table 3: An analogy between Riemann surfaces and number fields

We'll drop the hat and just understand that D is a compactified divisor. When $D = (\mathfrak{a}, (\lambda_\sigma)) \in \widehat{\mathrm{Div}}(\mathscr{O}_K)$, we have

I really should have watched the previous lecture before coming to this one

$$\mathrm{H}^0(D) = \left\{ x \in \mathfrak{a}^{-1} : |x|_\sigma \le e^{\frac{\lambda_\sigma}{\varepsilon_\sigma}} \right\}.$$

Recall that $\deg D = \log \mathrm{Nm}\,\mathfrak{a} + \sum_{\sigma|\infty} \lambda_\sigma \in \mathbb{R}$. Here are some facts

- $\deg D < 0 \implies \mathrm{H}^0(D) = 0$
- Say $\deg D = 0$. Then, $\mathrm{H}^0(D) \neq 0 \iff D$ trivial, i.e. $D = (\mathscr{O}_K, (0)_{\sigma|\infty})$. When D trivial, we see that

  $$\mathrm{H}^0((\mathscr{O}_K, \lambda_\sigma = 0)) = \{x \in \mathscr{O}_K : |x|_\sigma \le 1\, \forall \sigma\} = \mu_K$$

  is the set of roots of unity in $\mathscr{O}_K$.
- Define the **Euler-Poincaré characteristic**

  $$\chi(\mathscr{O}_K) = -\log \left(\frac{2}{\pi}\right)^{r_2} |\Delta_K|^{1/2}.$$

  This looks strange, but the point is that we get an **arithmetic Riemann-Roch** result.

  $$\deg D \ge -\chi(\mathscr{O}_K) \implies \mathrm{H}^0(D) \neq 0.$$

  The above comes from Minkowski.

  Identify $K \otimes \mathbb{R} \xrightarrow{\sim} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, so $\mathscr{O}_K$ is a lattice. It's volume is

  $$\mathrm{vol}(\mathscr{O}_K) = 2^{-r_2} |\Delta_K|^{1/2}.$$

  Now consider the convex domain $\Omega = \{(x_\sigma) : |x_\sigma| \le 1\} \cong [-1,1]^{r_1} \times D(0,1)^{r_2}$. We see that

  $$\mathrm{vol}(\Omega) = 2^{r_1} \times \pi^{r_2}.$$

  The constant in the above implication is then

  $$\frac{2^{r_1+2r_2}\,\mathrm{vol}(\mathscr{O}_K)}{\mathrm{vol}(\Omega)} = \left(\frac{2}{\pi}\right)^{r_2} |\Delta_K|^{1/2}.$$

TODO: Remember the statement of Minkowski's lemma

Remark 2.4.1. Note that $\mathrm{H}^0(D)$ does not have a natural group structure. ○

We have a fundamental exact sequence

$$0 \longrightarrow \widehat{\mathrm{Pic}}^0\,\mathscr{O}_K \longrightarrow \widehat{\mathrm{Pic}}\mathscr{O}_K \xrightarrow{\deg} \mathbb{R} \longrightarrow 0.$$

Note that we can ignore the archimedean part of our divisors to get a sequence

$$0 \longrightarrow \frac{\mathbb{R}^{r_1+r_2-1}}{\log \mathscr{O}_K^\times} \longrightarrow \widehat{\mathrm{Pic}}^0\,\mathscr{O}_K \longrightarrow \mathrm{Cl}_K \longrightarrow 0.$$

The big theorem is now

Theorem 2.4.2. $\widehat{\operatorname{Pic}}^0 \mathscr{O}_K$ *is compact.*

This includes both finiteness of the class group and Dirichlet's theorem on the rank of units. See Szipiro's paper for a proof.

An easier result is

Theorem 2.4.3. $\pi_1(\mathbb{Z}) = 0$*, i.e.* $|\Delta_K| > 1$ *unless* $K = \mathbb{Q}$*.*

Proof. Suppose $K \neq \mathbb{Q}$ and $|\Delta_K| = 1$. Then, $\chi(\mathscr{O}_K) = \log\left(\frac{2}{\pi}\right)^{r_2}$. We want to use Riemann-Roch. Note that $-\chi(\mathscr{O}_K) \leq 0$ (with equality if $r_2 = 0$). Hence, if $\deg D \geq 0 \geq -\chi(\mathscr{O}_K)$ we can apply arithmetic Riemann-Roch. We now want to create a degree 0 divisor which is nontrivial; this will then have a section by Riemann-Roch, which is a contradiction (see second bullet point from before). Consider $D = (\mathscr{O}_K, (\lambda_\sigma))$. Then, $\deg D = \sum \lambda_\sigma$. We have $r_1 + r_2$ variables $\lambda_\sigma \in \mathbb{R}$, so as long as $r_1 + r_2 > 1$, we can choose λ_σ not all 0 such that $\sum \lambda_\sigma = 0$. Since $r_1 + 2r_2 = n$, we see that $r_1 + r_2 = 1 \iff r_0 = 0$ and $r_2 = 1$. Suppose we are not in this case, so then we have our non-trivial degree 0 divisor D and Riemann-Roch gives us our contradiction.

The only remaining case is that of imaginary quadratic fields, but this one can do by hand. None of them have discriminant ± 1. ■

This is an analogue of the classical theorem that $S^2 = \mathbb{CP}^1$ has no unramified nontrivial cover.

Theorem 2.4.4 (Hermite-Minkowski). *The set of number fields K such that $|\Delta_K| \leq X$ and $\deg K \leq N$, for any $X, N > 0$, is finite.*

Proof. We want to find $x \in \mathscr{O}_K$ such that $|x|_\sigma < \lambda_\sigma$ for every σ (use only finitely many such x of bounded degree).

Consider $D = (\mathscr{O}_K, (\lambda_\sigma)) \in \widehat{\operatorname{Div}}(\mathscr{O}_K)$. Choose $\lambda_{\sigma_1} \geq -\chi(\mathscr{O}_K) + \deg \cdot \log \frac{1}{2}$ but $\lambda_{\sigma_2}, \lambda_{\sigma_3}, \dots$ very small, say $\lambda_{\sigma_i} \leq \log \frac{1}{2}$ if $i \geq 2$. Hence,

$$\sum \lambda_\sigma \geq -\chi(\mathscr{O}_K)$$

so Riemann-Roch gives some $x \in \mathscr{O}_K$ such that $|x|_{\sigma_1} \leq e^{\lambda \sigma_1}$ and $|x|_{\sigma_i} \leq \frac{1}{2}$ for $i \geq 2$. This then implies that actually $K = \mathbb{Q}(x)$. We know that $\prod |x|_{\sigma_i} \geq 1$ since x integral. It has small absolute value at all but one embedding, so big absolute value at σ_1. If $\mathbb{Q}(x) \subsetneq K$, then there would be at least 2 absolute values on which x is big.

This is not quite true. We have an issue when K/K_0 quadratic sometimes (e.g. CM case like $\mathbb{Q}(i)/\mathbb{Q}$). I'm lost. He wrote

$$\deg K/K_0 = \sum_{\sigma | \sigma_0} \deg K_\sigma / K_0 \sigma_0.$$

Seems like this is a real issue (having a real place ramify into a complex place). At the very least, we've proved finiteness of the number of totally real fields.

Whatever, look at Szipiro's paper for the resolution. ■

Theorem 2.4.5 (Hermite). *Fix a finite set S of primes of $\mathbb{Z}$. Then,*

$$\#\{K : \deg K \leq N \text{ and } K \text{ unramified outside } S\} < \infty.$$

Question 2.4.6. *Can one bound Δ_K using ramification (and $\deg K \leq N$)?*

Answer. Yes, but one needs local fields. ⋆

2.4.2 Local fields

We've studied $\mathscr{O}_K$ using algebra and geometry. How about analysis?

Think of the situation of constructing $\mathbb{R}$ from $\mathbb{Q}$. One obtains $\mathbb{R}$ by completing $\mathbb{Q}$ with respect to some metric, but the choice of metric on $\mathbb{Q}$ is not unique. So maybe one should study what metrics there are.

Let's start with absolute values, which are basically multiplicative valuations.

Definition 2.4.7. Let K be a field. An **absolute value** is a group homomorphism $K^\times \to \mathbb{R}^\times_{>0}$ satisfying the**triangle inequality**: $|x+y| \leq |x| + |y|$ for all $x, y \in K$. Also, we set $|0| = 0$. ⋄

Example. The trivial absolute value is $|x| = 1$ for $x \in K^\times$ △

Note that the image of an absolute value has to be a subgroup of $\mathbb{R}^\times_{>0}$. If it is nontrivial, it has to contain at least countably many elements.

Example. The simplest nontrivial case is when $\operatorname{im}(K^\times) \cong \mathbb{Z}$. For example, the **$p$-adic absolute value** ($p$ rational prime). First note that $\mathbb{Q}^\times \cong \bigoplus_p p^{\mathbb{Z}} \oplus \{\pm 1\}$ as an abelian group, so enough to specify absolute value of generators. $\mathbb{R}^\times_+$ has no torsion, so $|\pm 1| = 1$. To finish, for $x = p^n y$ with $(p, y) = 1$, we set $|x|_p = p^{-n}$. One checks that this satisfies the triangle inequality.

In fact, it satisfies the **strong triangle inequality**

$$|x+y| \leq \max(|x|, |y|).$$

An absolute value satisfying the above is called **non-archimedean**. △

Lemma 2.4.8. *An absolute value on K (any field, not just number fields) is non-archimedean iff $|\mathbb{Z}| \leq C$ for some $C > 0$ (in fact can take $C = 1$), i.e. the absolute value of the integers is bounded.*

Proof. ($\to$) When $|\cdot|$ is non-archimdean, $|m| = |1 + 1 + \cdots + 1| \leq \max(|1|, \ldots, |1|) = 1$ for all $m \in \mathbb{Z}$.

($\leftarrow$) We have

$$|x+y|^N = \left|(x+y)^N\right| \leq \left|\sum_{k=0}^{N} x^k y^{N-k} \binom{N}{k}\right| \leq C \sum_{k=0}^{\infty} \left|x^k y^{N-K}\right| \leq NC \max(|x|^N, |y|^N)$$

for all N. Taking Nth roots, we get

$$|x+y| \leq N^{1/N} C^{1/N} \max(|x|, |y|).$$

Take the limit as $N \to \infty$ to win. ■

Corollary 2.4.9. *An absolute value in positive characteristic is non-archimedean.*

Remark 2.4.10. Given an absolute value $|\cdot|$, we can define a metric $d : K \times K \to \mathbb{R}_{\geq 0}$ via $d(x, y) = |x - y|$. This induces a topology on K. ∘

Definition 2.4.11. Two absolute values $|\cdot|_1, |\cdot|_2$ are **equivalent**, denoted $|\cdot|_1 \sim |\cdot|_2$, iff they define the same topology. ◇

Theorem 2.4.12 (Ostrowski). *Up to equivalence, the only absolute values on $\mathbb{Q}$ are the usual one $|\cdot|_\infty$ and the p-adic ones $|\cdot|_p$. Furthermore, these are pairwise non-equivalent.*

2.5 Lecture 15 (10/26): Product formula; Frobenius; Cebotarev density

2.5.1 Not Cebotarev density

Definition 2.5.1. A **global field** K is either

- a finite extension of $\mathbb{Q}$ (**number field**); or
- a finite extension of $\mathbb{F}_p(t)$ (**function field**)

◇

We will focus n the number field K.

Recall 2.5.2. Ostrowski's theorem classifies all possible absolute values of $\mathbb{Q}$. ⊙

We would like an analogous result for a general number field K. Recall that for a (finite?) separable extension L/K of *local fields*, the absolute value on K extends uniquely to one on L.

Now, say K is a number field (so $K/\mathbb{Q}$ finite), and write $K = \mathbb{Q}(\alpha)$ where α has minimal polynomial $f(x) \in \mathbb{Q}[x]$. For a rational prime p, how can we extend the p-adic absolute value on $\mathbb{Q}$ to one on K?

Theorem 2.5.3. *There are natural bijections between the sets*

(a) *Extensions of absolute values $|\cdot|_p$ to K.*

(b) *irreducible factors of f in $\mathbb{Q}_p[X]$.*

(c) *prime ideals of $\mathscr{O}_K$ above p.*

Remark 2.5.4. Write $f(x) = \prod f_i(x) \in \mathbb{Q}_p[x]$ as s product of irreducible factors.[21] Then,

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_i \underbrace{\mathbb{Q}_p[x]/(f_i(x))}_{K_i}.$$

Above, $K_i/\mathbb{Q}_p$ is a finite extension. This is how one does **(b)** $\to$ **(a)**. ○

Remark 2.5.5. Say $\mathscr{O}_K = \mathbb{Z}[\alpha]$ and α has minimal poly $f(x) \in \mathbb{Z}[x]$. Recall that $p\mathscr{O}_K = \prod_i \mathfrak{p}_i^{e_i}$ where $\overline{f} = \prod_i \overline{g}_i^{e_i} \in \mathbb{F}_p[x]$ and $\mathfrak{p}_i = (p, g_i(\alpha))$.

If $f = \prod f_i \in \mathbb{Z}_p[x]$ (with f_i irreducible), then Hensel's lemma or Newton polygon shows us that $\overline{f}_i = \overline{g}_i^{e_i}$ for some irreducible $\overline{g}_i$ (if $\overline{f}_i$ had two factors, could lift both of them and then contradict f_i being irreducible over $\mathbb{Z}_p$). This gives the bijection **(b)** $\leftrightarrow$ **(c)** (under the extra hypothesis that $\mathscr{O}_K$ is monogenic). ○

[21] No repeated factors follows from f being irreducible over $\mathbb{Q}$

Remark 2.5.6. Let's finish with **(a)** $\to$ **(c)**. If we have an extension of $|\cdot|_p$ to K, then we get a valuation val : $K \to \mathbb{Z} \cup \{\infty\}$, and so can form $A = \{x : \mathrm{val} \geq 0\}$ which is local with unique maximal $\mathfrak{p} = \{x : \mathrm{val} > 0\}$. From this, we get the prime $\mathfrak{p} \cap \mathscr{O}_K$ of $\mathscr{O}_K$. ◦

Theorem 2.5.7. *There are natural bijections*

$$\left\{\begin{matrix}\textit{non-arch abs value}\\ \textit{of } K\end{matrix}\right\} / \sim \longleftrightarrow \left\{\begin{matrix}\textit{prime ideal}\\ \textit{of } \mathscr{O}_K\end{matrix}\right\}$$

and

$$\left\{\begin{matrix}\textit{arch abs value}\\ \textit{of } K\end{matrix}\right\} / \sim \longleftrightarrow \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) / \sim$$

where two embeddings $K \rightrightarrows \mathbb{C}$ are considered equivalent if they differ by complex conjugation.

Definition 2.5.8. A **place** is an equivalence class of absolute values. If v is a place of K, then we write K_v to denote the completion of K with respect to v. ⋄

For each place v of a number field K, we would like a canonical choice of representative absolute value.

- When $K_v = \mathbb{R}$, we choose $|z|_v = |z|$ as our canonical representative.
- When $K_v = \mathbb{C}$, we choose $|z|_v = |z|^2 = z\overline{z}$ as our canonical representative.[22]
- When v is non-archimedean, let $\pi_v \in \mathscr{O}_{K_v}$ be a uniformizer, and let $k_v = \mathscr{O}_{K_v}/(\pi_v)$ be the residue field. We choose our canonical representative so that

$$|\pi_v|_v = \frac{1}{\# k_v}.$$

Remark 2.5.9. More intrinsically, these representatives are chosen because of their connection to Haar measures. If μ_v is a Haar measure on K_v and $\alpha \in K_v^\times$, then $\mu_{\alpha,v}(S) := \mu_v(\alpha S)$ (S a Borel set) is also a Haar measure, and $\mu_{\alpha,v} = |\alpha|_v \, \mu_v$. ◦

Theorem 2.5.10 (Product Formula). *Let K be a number field. For any $x \in K^\times$, $\prod_v |x|_v = 1$.*

Proof. First case is $K = \mathbb{Q}$. Here can reduce to the case $x = \pm 1$ or $x = p$ is prime. If $x = \pm 1$, this is obvious. If $x = p$, then the only non-unit absolute values are $|p|_\infty \cdot |p|_p = p \cdot \frac{1}{p} = 1$.

In the general case, we use the following fact:

Fact.

$$\prod_{w|v} |x|_w = |\mathrm{Nm}(x)|_v$$

where the product is taken over all places w above v.

Norm is constant term of minimal polynomial. Apply previous lemma bijecting places above v with irreducible factors of minimal poly

This fact let's us reduce to the case of $K = \mathbb{Q}$ as

$$\prod_w |x|_w = \prod_v \left(\prod_{w|v} |x|_w \right) = \prod_v |\mathrm{Nm}(x)|_v = 1$$

[22]Technically speaking, $|z|_v$ defined here is not an absolute value, since it does not satisfy triangle inequality. This is not really that much of an issue for what we'll do with it.

where $x \in K^\times$, w ranges over places of K, and v ranges over places of $\mathbb{Q}$. ■

Remark 2.5.11. Compare the product formula with the following: $\mathbb{C}(t)$ is the field of meromorphic functions on $\mathbb{P}^1$. For $f \in \mathbb{C}(t)^\times$, one has $\deg \operatorname{div}(f) = 0$. ○

2.5.2 Cebotarev density

We can't prove this right, but we can give the statement, and maybe this is secretly more useful. Let L/K be a Galois extension of number fields with Galois group $\mathrm{Gal}(L/K) = G$. Consider some non-archimedean place v on K, and extend it to a place $w \mid v$ on L. We have the **decomposition group** $D(w \mid v) = \{\sigma \in G : \sigma \cdot w = w\}$. This sets in a short exact sequence

$$1 \longrightarrow I(w \mid v) \longrightarrow D(w \mid v) \longrightarrow \mathrm{Gal}(k_w/k_v) \longrightarrow 1$$

whose kernel is called the **Inertia group** (one has to show that the map on the right is surjective). Let's assume for now that w is unramified (i.e. $I(w \mid v) = 1$) so $D(w \mid v) \simeq \mathrm{Gal}(k_w/k_v) = \langle \mathrm{Frob}_w \rangle$ (extensions of finite fields are cyclic), where

$$\begin{array}{rccc} \mathrm{Frob}_w : & k_w & \longrightarrow & k_w \\ & x & \longmapsto & x^{q_v} \end{array}$$

and $q_v = \# k_v$.

Abuse of Notation 2.5.12. We write $\mathrm{Frob}_w \in D(w \mid v) \subset G$ to denote the (unique) lift of $\mathrm{Frob}_w \in k_w$ to the decomposition group.

Notation 2.5.13. One may also denote Frobenius by

$$\mathrm{Frob}_w = (w, L/K) = (\mathfrak{p}, L/K)$$

where $\mathfrak{p} \subset \mathscr{O}_L$ is the prime corresponding to w. This defines a map Art from unramfied primes of L to $\mathrm{Gal}(L/K)$. called the **Artin map**.

Example. Let $K = \mathbb{Q}(\sqrt{D})$.

- Say p is split, so $p\mathscr{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. Then, $(\mathfrak{p}, K/\mathbb{Q}) = \mathrm{id} \in \mathrm{Gal}(K/\mathbb{Q})$. This is because $k_{\mathfrak{p}} = k_p$, so the residue extension is trivial.
- Say p is inert, so $p\mathscr{O}_K$ is prime. Then, $k_p \cong \mathbb{F}_{p^2}$ is degree 2 over $\mathbb{F}_p$. Hence, $(p\mathscr{O}_K, K/\mathbb{Q}) = c$ is the unique non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$.

△

Remark 2.5.14. If $\sigma \in \mathrm{Gal}$, then $(\sigma(w), L/K) = \sigma(w, L/K)\sigma^{-1}$. This is basically just because $\sigma D(w \mid v)\sigma^{-1} = D(\sigma(w) \mid v)$ (check things by hand or just say the phrase "transfer of structure"). In particular, if G is abelian, then the Artin map does not depend on the choice of place above v. ○

Example. Say $K = \mathbb{Q}(\mu_n)$ is a cyclotomic extension. Then, $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ where $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to the unique $\sigma \in G$ sending $\sigma(\mu_n) = \mu_n^m$. The Artin map in this case is

$$\begin{array}{rccc} \mathrm{Art}_{K/\mathbb{Q}} : & \{\text{primes } p \text{ of } \mathbb{Q} : p \nmid n\} & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ & p & \longmapsto & p \bmod n \end{array}.$$

This is simply because Frobenius is characterized by the fact that it induces the pth power map on the residue field. Well, $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to the Galois action which raises the generator to the pth power. △

Definition 2.5.15. Let Σ be a set of primes of $\mathscr{O}_K$. Then, its **natural density** is

$$\operatorname{den}(\Sigma) := \lim_{X\to\infty} \frac{\#\{\mathfrak{p} : \mathfrak{p} \in \Sigma, \operatorname{Nm}\mathfrak{p} < X\}}{\#\{\mathfrak{p} : \operatorname{Nm}\mathfrak{p} < X\}}.$$

⋄

Theorem 2.5.16 (Cebotarev Density). *Let L/K be Galois with Galois group G, and let $C \subset G$ be a conjugacy class. Then, the set of places v of K such that* $\operatorname{Frob}_w \in C$ *(for $w \mid v$) has natural density $\#C/\#G$.*

Remark 2.5.17. In particular, this is saying that Artin map is surjective, and that alone is non-trivial. ∘

Example. Say G is abelian, so every conjugacy class has size 1. Even more specifically, say $K = \mathbb{Q}(\mu_n)$ as an extension of $\mathbb{Q}$. For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have

$$\{p : p \nmid n \text{ and } \operatorname{Frob}_p = a \bmod n\} = \{p : p \equiv a \pmod n\},$$

with both sets having natural density $1/\#G$. In particular, Cebotarev density implies Dirichlet's theorem on primes in arithmetic progressions. △

2.6 Lecture 16 (10/28): Cebotarev density; Dedekind zeta function

2.6.1 Cebotarev, continued

Last time we introduced Cebotarev density. We want to say more about this, and then introduce Dedekind zeta functions.

Recall 2.6.1. Say L/K is some Galois extension, and let v be a (non-archimedean) place of K which is unramified. Let $w \mid v$ be a place of L above v. Then, we can define the Artin map

$$\begin{array}{rccc} \operatorname{Art}: & \left\{\begin{matrix}\text{unram primes}\\ \text{in } \mathscr{O}_L\end{matrix}\right\} & \longrightarrow & \operatorname{Gal}(L/K) \\ & w & \longmapsto & (w, L/K) \end{array}$$

where $(w, L/K) = \operatorname{Frob}_w$ is the unique element $\sigma \in \operatorname{Gal}(L/K)$ satisfying both

- $\sigma w = w$; and
- $\sigma(x) \equiv x^{q_v} \mod \mathfrak{p}_w$ for all $x \in \mathscr{O}_L$. Here, $q_v = \#(\mathscr{O}_L/\mathfrak{p}_v)$ and $\mathfrak{p}_v$ is the prime corresponding to v.

Note that the conjugacy class of Frob_w in $\operatorname{Gal}(L/K)$ only depends on v. Hence the Artin map can be viewed as

$$\operatorname{Art}: \left\{\begin{matrix}\text{unram primes}\\ \text{in } \mathscr{O}_K\end{matrix}\right\} \longrightarrow \left\{\begin{matrix}\text{conj classes}\\ \text{in } \operatorname{Gal}(L/K)\end{matrix}\right\}.$$

When $\mathrm{Gal}(L/K)$ is abelian, this is really

$$\mathrm{Art} : \left\{ \begin{matrix} \text{unram primes} \\ \text{in } \mathscr{O}_K \end{matrix} \right\} \longrightarrow \mathrm{Gal}(L/K).$$

$\odot$

The density theorem is about the fiber of this map.

Theorem 2.6.2 (Cebotarev)**.** *Fix a conjugacy class $C \subset G$. Then,*

$$\mathrm{Den}\left\{v : (w, L/K) \in C \,\forall w \mid v\right\} = \frac{\#C}{\#G}.$$

Corollary 2.6.3. *There exists infinitely many v with* Frob *in a given conjugacy class.*

Example. Consider $K = \mathbb{Q}$ and $L = \mathbb{Q}(\mu_n)$, the nth cyclotomic extension. Then, the Galois group is canonically $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, and the Artin map sends $\mathrm{Art}(p) = (p \mod n)$. Hence, in this case, Cebotarev density gives Dirichlet's theorem on primes in APs. $\triangle$

Example (**Quadratic reciprocity**)**.** Let p, q be odd primes. We aim to show that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Let $L = \mathbb{Q}(\mu_p)$. By Galois theory + considering discriminants, $L/\mathbb{Q}$ has a unique quadratic intermediate field which is $K = \mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right)$. Frobenius behaves well in towers, so $(q, K/\mathbb{Q}) = (q, L/\mathbb{Q})|_K \in \mathrm{Gal}(K/\mathbb{Q})$. When is this trivial? Let $d = \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p$, so $K = \mathbb{Q}(\sqrt{d})$. Then, $(q, K/\mathbb{Q})$ is trivial iff q is split in K, i.e. $(q, K/\mathbb{Q}) = \left(\frac{d}{q}\right)$. We know that

Note q unramified since $q \neq p$

$$\mathrm{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \ni (q \mod p) \mapsto \left(\frac{q}{p}\right) \in \mathbb{Z}/2\mathbb{Z} = \mathrm{Gal}(K/\mathbb{Q}),$$

so using $(q, K/\mathbb{Q}) = (q, L/\mathbb{Q})|_K \in \mathrm{Gal}(K/\mathbb{Q})$ now gives

$$(-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{d}{q}\right) = \left(\frac{q}{p}\right).$$

This is quadratic reciprocity (note $\left(\frac{p}{q}\right)^{-1} = \left(\frac{p}{q}\right)$). $\triangle$

Let

$$\mathrm{Spl}(L/K) := \left\{\mathfrak{p} \text{ split completely in } L\right\} = \left\{\mathfrak{p} : (\mathfrak{p}, L/K) = \mathrm{id}\right\}.$$

Note that

$$\mathrm{Den}\,\mathrm{Spl}(L/K) = \frac{1}{[L:K]}$$

by Cebotarev.

Application. Consider L/K Galois. Can we determine L from its set $\mathrm{Spl}(L/K) \subset \{\text{primes in } \mathscr{O}_K\}$ of split primes? Yes.

Theorem 2.6.4. *Let L, L' be Galois over K. If $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$, then $L = L'$.*

Proof. We will show that

$$\mathrm{Spl}(L/K) \subset \mathrm{Spl}(L'/K) \implies L \supset L'.$$

Consider $M = LL'$. If $L \not\supset L'$, then we will get $M \supsetneq L$. A prime splits completely iff its Frobenius vanishes; from this, one quickly sees that[23]

$$\mathrm{Spl}(LL'/K) = \mathrm{Spl}(L/K) \cap \mathrm{Spl}(L'/K).$$

Hence, $\mathrm{Spl}(M/K) = \mathrm{Spl}(L/K)$. Take the density of both sides, this gives $[M : K]^{-1} = [L : K]^{-1}$, so $L = M \supset L'$ as desired. ■

Note that, since the proof relies on density, we can strengthen the claim by only requiring $\mathrm{Spl}(L/K), \mathrm{Spl}(L'/K)$ to differ by *finitely many* primes.

Example. $\mathrm{Spl}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = \{p : p \equiv 1 \pmod{n}\}$ determines cyclotomic extensions of $\mathbb{Q}$ (among Galois extensions of $\mathbb{Q}$). △

In general, class field theory will tell us that this set of split primes is "linear" – defined by congruence conditions – for abelian extensions. For non-abelian extensions, things are messier.

Relevant blog post

Apparently there was a homework problem about showing that $\mathbb{Q}_p$ has no nontrivial field automorphisms $\sigma : \mathbb{Q}_p \to \mathbb{Q}_p$ (no continuity assumption).

Claim 2.6.5. *Let $U = 1 + p\mathbb{Z}_p$. Then,*

$$U = \left\{x \in \mathbb{Q}_p^\times : x^{1/n} \in \mathbb{Q}_p \text{ for all } p \nmid n\right\} =: U'.$$

This gives an algebraic characterization of a neighborhood of unity, so $\sigma(U) \subset U$.

Proof. ($\supset$) Choose $x \in U'$. First, $x \in \mathbb{Z}_p^\times$. If $v_p(x) \neq 0$, then good luck taking nth roots in $\mathbb{Q}_p$. There's some $y \in \mathbb{Q}_p$ such that $y^{p-1} = x$. Taking valuations, we see $v_p(y) = v_p(x)/(p-1) = 0$, so $y \in \mathbb{Z}_p^\times$. Thus, $x \equiv y^{p-1} \equiv 1 \pmod{p}$, so $x \in 1 + p\mathbb{Z}_p = U$.

($\subset$) We want to show that the "multiplication by n-map" $U \xrightarrow{n} U, a \mapsto a^n$ is surjective, i.e. U is n-divisible. Use Hensel's lemma. We want to show that if $x \equiv 1 \mod p$, then $a^n = x$ has a solution $a \in \mathbb{Z}_p$. Mod p, we want a solution to $a^n \equiv 1 \pmod{p}$. This is separable precisely when $p \nmid n$, so Hensel's lemma gives us a solution in $\mathbb{Z}_p$ when $p \nmid n$. ■

The same proof applies in general to show that automorphisms of local fields are automatically continuous.

2.6.2 Dedekind Zeta

We won't prove Cebotarev density, but its proof involves introducing various L-functions. We can at least introduce one of those.

[23]Uses $\mathrm{Gal}(LL'/K) \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$ is always injective

Definition 2.6.6. For any number field K, its **Dedekind zeta function** is

$$\zeta_K(s) = \sum_{\mathfrak{a}} (N\mathfrak{a})^{-s},$$

where the sum is taken over nonzero (integral) ideals $\mathfrak{a} \subset \mathscr{O}_K$. ⋄

When $K = \mathbb{Q}$, this recovers the usual Riemann zeta function. In general, this series converges whenever $\mathrm{Re}(s) > 1$. Unique factorization of ideals allows one to write

$$\zeta_K(s) = \prod_{\mathfrak{p} \text{ prime}} \frac{1}{1 - N\mathfrak{p}^{-s}} = \prod_p \prod_{\mathfrak{p}|p} \frac{1}{1 - N\mathfrak{p}^{-s}}.$$

Recall that $N\mathfrak{p} = p^f$ where f is the residue degree over $\mathbb{F}_p$, so ζ_K is encoding splitting behavior.

Example. If $p \in \mathrm{Spl}(K/\mathbb{Q})$, then $(1 - p^{-s})^n$ appears in the Euler product for ζ_K.

If p is inert (i.e. $p\mathscr{O}_K$ prime), then $(1 - p^{-ns})^{-1}$ appears in the Euler product. △

Definition 2.6.7. Say two number fields K, K' are **arithmetically equivalent** if $\zeta_K = \zeta_{K'}$. ⋄

Lemma 2.6.8. $K \sim K' \iff$ *for all rational primes p, the local factors of $\zeta_K, \zeta_{K'}$ are equal.*

Remark 2.6.9. If $K \sim K'$ are both Galois over $\mathbb{Q}$, then $\mathrm{Spl}(K/\mathbb{Q}) = \mathrm{Spl}(K'/\mathbb{Q})$, so $K = K'$. ∘

What is we look at non-Galois field? Does splitting behavior still determine the field?

Theorem 2.6.10. *There exists non-isomorphic number fields K, K' with $K \sim K'$.*

The construction here is surprisingly elementary.

Suppose $L/\mathbb{Q}$ is Galois with Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. We will construct subextensions $K, K'/\mathbb{Q}$, so these will correspond to subgroups $\mathrm{Gal}(L/K) = H$ and $\mathrm{Gal}(L/K') = H'$. The factorization of an (unramified) prime is determined already by its Frobenius conjugacy class.

Remember: Frobenius generates the Decomposition group (which has size f)

Fact. K, K' are isomorphic $\iff$ H, H' are conjugate in G.

Fact. $K \sim K'$ $\iff$ H, H' are "**locally conjugate**" in G in the sense that for any conjugacy class $C \subset G$, $\#C \cap H = \#C \cap H'$.

Definition 2.6.11. A **Gassmann triple** (G, H, H') is a group G with subgroups $H, H' \leq G$ which are locally conjugate, but not conjugate. ⋄

Example. There's a triple with $G = S_6$ and H, H' two certain subgroups, both abstractly isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. △

Existence of such a triple proves the theorem (modulo inverse Galois issues. Luckily there is a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_6$).

Up next is class field theory, followed by a survey on what we should spend the end of the class on.

2.7 Lecture 17 (11/2): Local class field theory

Break from global stuff to talk about (the statements of?) global class field theory. Afterwards, we'll go back to the global theory and introduce adeles and whatnot.

Class field theory is about understanding abelian extension of (global or local) fields. The original proofs of the main statements were completely circa 1930. At the time, it was very difficult to learn.

- "Class field theory has a reputation for being difficult, which is partly justified. But it is necessary to make a distinction: there is perhaps nowhere in science a theory in which the proofs are so difficult but at the same time the results are of such perfect simplicity and of such great power." – J. Herbrand, 1936
- "I have been reviewing a little class field theory, of which I finally have the impression that I understand the main results (but not the proofs, of course!)" – Grothendieck, letter to Serre, 19.9.56.1
- "(Salomon Bochner) He encouraged me in a number of ways, above all by suggesting that I give a course on class field theory. This was a terrifying suggestion. In the early 1960s class field theory was unknown outside of Germany and the circle of Artin's students in Princeton, and not regarded as otherwise accessible." – Langlands, in An Appreciation, 2013.

Proving the main results of class field theory today is still not easy, but it it more accessible than it used to be. In the 60s, say, there was no good reference for class field theory; because of this there was a conference to remedy the situation which was recorded in the book (edited) by Cassels and Fröhlich. Now there multiple references for class field theory.

Today, we just try to state the main results. Let K be a non-archimedean local field (e.g. $K/\mathbb{Q}_p$ finite).[24] Let K^{ab} be the maximal abelian extension of K, so

$$K^{\text{ab}} = \bigcup_{\substack{L/K \\ \text{fin ab.}}} L$$

where the union is taken inside a given algebraic closure of K. Hence, $\text{Gal}(K^{\text{ab}}/K) = \varprojlim \text{Gal}(L/K)$ where the inverse limit is taken over L/K finite abelian.

Wei spent some time introducing profinite groups, of which $\text{Gal}(K^{\text{ab}}/K)$ is an example

Exercise. $\text{Gal}(\overline{K}/K)^{\text{ab}} \xrightarrow{\sim} \text{Gal}(K^{\text{ab}}/K)$

Question 2.7.1. *Can we describe* $\text{Gal}(K^{\text{ab}}/K)$ *by "only using* K*"?*

The answer will be related the $K^\times$. Recall that

$$1 \longrightarrow \mathscr{O}_K^\times \longrightarrow K^\times \xrightarrow{\nu} \mathbb{Z} \longrightarrow 0.$$

We can choosing a splitting (i.e. a uniformizer π), to get an isomorphism

$$K^\times \simeq \pi^{\mathbb{Z}} \times \mathscr{O}_K^\times.$$

[24]One can also treat archimedean local fields, but understanding their abelian extensions is much easier

Example. When $K = \mathbb{Q}_p^\times$, then p is a natural choice of uniformizer, so

$$\mathbb{Q}_p^\times \simeq p^{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

Furthermore, we know that

$$\mathbb{Z}_p^\times \simeq \varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times.$$

$\triangle$

Example. When $K = \mathbb{Q}_p$, we have certain easy examples of abelian extensions, the cyclotomic ones. Let μ_n be the nth roots of unity (in $\overline{K}$). Then, $K_n = \mathbb{Q}_p(\mu_n)$ is abelian, as we have $\mathrm{Gal}(K_n/K) \hookrightarrow \mathrm{Aut}(\mu_n) = (\mathbb{Z}/n\mathbb{Z})^\times$. This map may not be surjective in the local setting. For example, $K_{p-1} = \mathbb{Q}_p(\mu_{p-1}) = \mathbb{Q}_p$ (Hensel's lemma/Teichmuller lifts) so $\mathrm{Gal}(K_{p-1}/K) = 1$ is trivial.

Note that when n is a p-power, we have $\mathrm{Gal}(K_{p^n}/K) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$ since $K_{p^n}/\mathbb{Q}_p$ is totally ramified of degree $\varphi(p^n)$ (it's generate by the roots of an Eisenstein polynomial).

The upshot is that we know $\mathbb{Q}_p^{\mathrm{ab}} \supset \mathbb{Q}_p(\mu_\infty) = \bigcup_n \mathbb{Q}_p(\mu_n)$. $\triangle$

Let's continue this $K = \mathbb{Q}_p$ example, but now outside of the example block to emphasize its importance. We can form $\mathbb{Q}_p(\mu_\infty)$ in two steps. Think of it as

$$\mathbb{Q}_p(\mu_\infty) = \mathbb{Q}_p(\mu_m, \mu_{p^n} : p \nmid m \text{ and } m, n \geq 1)$$

so we get

$$\begin{array}{c} \mathbb{Q}_p(\mu_\infty) \\ | \\ \mathbb{Q}_p(\mu_m : p \nmid m) = \mathbb{Q}_p^{\mathrm{un}} \\ | \\ \mathbb{Q}_p \end{array}$$

Remark 2.7.2. Unramified extensions are determined by the extension of residue fields. For $\mathbb{Q}_p$, the residue field is $\mathbb{F}_p$ which is finite. All extensions of finite fields are formed by adjoining further roots of unity, so we easily see that $\mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p(\mu_m : p \nmid m)$ is the maximal unramified extension of $\mathbb{Q}_p$. $\circ$

Fact (Kronecker-Weber). $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_\infty)$. In fact, even globally, $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty)$ (this is implied by the local result).

We'll prove, assuming the statement of local class field theory, in a bit. In the meantime, here's another quote.

- "I should perhaps add that until the Brighton conference in 1965, published as [8] (Cassels–Fröhlich), the apparatus of class field theory was much more forbidding than was Weber's Algebra" – Bryant Birch, 2002, when recalling Heegner's famous article.

Recall we've fixed a local field K (possibly in positive characteristic).

Theorem 2.7.3 (Main Theorem of Local Class Field Theory). *There is a unique homomorphism*

Can't be an isomophism of topological groups since RHS compact but LHS noncompact

$$\varphi_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

called the ***local Artin map*** *such that*

(a) *For L/K finite unramified and π a uniformizer, one has*

$$\varphi_K(\pi)|_L = \mathrm{Frob}_{L/K} \in \mathrm{Gal}(L/K).$$

(note $u\pi$ is a uniformizer for any $u \in \mathscr{O}_K^\times$, so we are implicitly saying that $\varphi_K(u)$ acts trivially on unramified extensions).

(b) *For L/K finite abelian, we consider*

$$\begin{tikzcd} K^\times \arrow[r, "\varphi_K"] \arrow[dr, "\varphi_K|_L"'] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, two heads] \\ & \mathrm{Gal}(L/K) \end{tikzcd}$$

and $\ker \varphi_K|_L = \operatorname{Nm} L^\times$. *The is, we have a commutative square*

$$\begin{tikzcd} K^\times \arrow[r, "\varphi_K"] \arrow[d, two heads] \arrow[dr, "\varphi_K|_L"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, two heads] \\ K^\times / \operatorname{Nm} L^\times \arrow[r, "\sim"] & \mathrm{Gal}(L/K) \end{tikzcd}$$

Remark 2.7.4. There's a hidden extra condition in part **(b)** above that we've not made completely explicit. This condition can be given in any of the following equivalent forms

- The induced $K^\times / \operatorname{Nm} L^\times \hookrightarrow \mathrm{Gal}(L/K)$ is surjective when L/K finite abelian.
- $\varphi_K|_L K^\times \to \mathrm{Gal}(L/K)$ is surjective when L/K finite abelian.
- The Artin map $\varphi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ has dense image.
- We have an equality $[L : K] = [K^\times : \operatorname{Nm} L^\times]$ when L/K finite abelian. ○

Definition 2.7.5. A subgroup of $K^\times$ is called a **norm group** if it is of the form $\operatorname{Nm} L^\times$ for some finite abelian L/K. ◇

The main theorem above tells us that this are in (inclusion-reversing?) bijection with Galois groups of finite abelian extensions of K.

Example. We have $\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\mu_{p^\infty}) \cdot \mathbb{Q}_p^{\mathrm{un}}$ with one factor totally ramified and the other unramified. These overlap trivially, so

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \times \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_p^\times \times \widehat{\mathbb{Z}}.$$

These isomorphisms are all canonical (once you fix this decomposition). Similarly, we have $\mathbb{Q}_p^\times \simeq \mathbb{Z}_p^\times \times$

$p^{\mathbb{Z}} \simeq \mathbb{Z}_p \times \mathbb{Z}$ and the Artin map is what you might now expect

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \arrow[r, "\sim"] & \mathbb{Z}_p^\times & \times & \widehat{\mathbb{Z}} \\
\mathbb{Q}_p^\times \arrow[u, "\varphi_K"] \arrow[r, "\sim"] & \mathbb{Z}_p^\times \arrow[u, equal] & \times & \mathbb{Z} \arrow[u, hook]
\end{tikzcd}$$

△

For general K, one can always consider the tower $K^{\mathrm{ab}}/K^{\mathrm{un}}/K$ and one has $\mathrm{Gal}(K^{\mathrm{un}}/K) \simeq \widehat{\mathbb{Z}}$ and $\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{un}}) \simeq \mathscr{O}_K^\times$.

Proposition 2.7.6. *Let $L, L'/K$ be finite abelian extensions. Then,*

(1) $L \subset L' \iff \mathrm{Nm}\,(L')^\times \subset \mathrm{Nm}\, L^\times$

(2) $\mathrm{Nm}(L \cdot L')^\times = \mathrm{Nm}\, L^\times \cap \mathrm{Nm}(L')^\times$

(3) $L \rightsquigarrow \mathrm{Nm}\, L^\times$ *defines a bijection (really, an equivalence of categories) from finite abelian extensions of K to Norm groups in $K^\times$.*

Proof. (**(2)** $\implies$ **(1)**) Suppose $\mathrm{Nm}\,(L')^\times \subset \mathrm{Nm}\, L^\times$. Then, $\mathrm{Nm}(L' \cdot L)^\times = \mathrm{Nm}\, L' \cap \mathrm{Nm}\,(L')^\times = \mathrm{Nm}\,(L')^\times$. On the other hand, CFT tells us that $[K^\times : \mathrm{Nm}\,(L')^\times] = [L' : K]$ and the same thing with $L \cdot L'$ in place of L. Thus, $[L' : K] = [L' \cdot L : K]$ so $L' = L' \cdot L$ which means $L \subset L'$.

(**(2)**) We know $\mathrm{Nm}(L \cdot L')^\times \subset \mathrm{Nm}\, L^\times \cap \mathrm{Nm}\,(L')^\times$. Need to show other direction. We have

$$\begin{tikzcd}
 & \mathrm{Gal}(L \cdot L'/K) \arrow[r, hook] & \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K) \\
\mathrm{Nm}\, L^\times \cap \mathrm{Nm}\,(L')^\times \arrow[r] \arrow[urr, bend left, "\varphi_K|_L \times \varphi_K|_{L'}"] & K^\times / \mathrm{Nm}(L'L)^\times \arrow[u, "\wr", "\varphi_K|_{LL'}"'] &
\end{tikzcd}$$

We want the bottom left map to be 0. This is equivalent to the map $\mathrm{Nm}\, L^\times \cap \mathrm{Nm}\,(L')^\times \to \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K)$ being the zero map, but this is true by **(b)** of CFT. ■

This shows that classifying finite abelian extensions is the same as classifying norm groups.

Theorem 2.7.7 (theorem of local existence). *The norm groups are precisely the open subgroups $U \subset K^\times$ of finite index.*

Corollary 2.7.8. *We have a bijection (really, an equivalence of categories)*

$$\left\{ \begin{array}{c} \textit{finite abelian} \\ \textit{extensions of } K \end{array} \right\} \overset{\sim}{\longleftrightarrow} \left\{ \begin{array}{c} \textit{open subgroups } U \subset K^\times \\ \textit{of finite index} \end{array} \right\}.$$

Remark 2.7.9.

$$K^\times \supset \mathscr{O}_K^\times \supset 1 + (\pi)^n$$

with $1 + (\pi)^n$ open for all n. ∘

2.8 Lecture 18 (11/4): Some applications of local class field theory

Fix K a non-archimedean local field.

Recall 2.8.1. There is a unique homomorphisms $\varphi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that

- For L/K finite unramified and for any uniformizer π, $\varphi_K(\pi)|_L = \mathrm{Frob}_{L/K}$
- For L/K finite abelian, $\ker(\varphi_K|_L) = \mathrm{Nm}\, L^\times$ and

$$K^\times / \mathrm{Nm}\, L^\times \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

$\odot$

We saw last time that there's a bijection between finite abelian extensions of K and norm groups. We also saw a the norm groups are precisely the open, finite index subgroups of $K^\times$.

Proof of local existence. ($\Longrightarrow$) $[K^\times : \mathrm{Nm}\, L^\times] = [L : K]$ so if of finite index. To show that it is open, it suffices to show that $\mathrm{Nm}\, \mathscr{O}_L^\times \subset \mathscr{O}_K^\times$ is open. Note that $\mathrm{Nm}\, \mathscr{O}_L^\times = \mathrm{Nm}\, L^\times \cap \mathscr{O}_K^\times$, so we have an injection

$$\mathscr{O}_K^\times / \mathrm{Nm}\, \mathscr{O}_L^\times \hookrightarrow K^\times / \mathrm{Nm}\, L^\times$$

between *finite* sets. Now, $\mathrm{Nm}\, \mathscr{O}_L^\times \subset \mathscr{O}_K^\times$ is compact in a Hausdorff space, so closed; since it is also of finite index (its complement is a union of finitely many closed cosets), it is open.

($\Longleftarrow$) Harder. ■

Example (Cyclotomic extension)**.** $\mathbb{Q}_p(\mu_\infty) \subset \mathbb{Q}_p^{\mathrm{ab}}$. We can show this inclusion is an equality, assuming local class field theory. It suffices to show that any finite abelian $L/\mathbb{Q}_p$ must be contained inside $\mathbb{Q}_p(\mu_\infty)$. Note that finite abelian extensions are in (order-reversing) bijection with open, finite index subgroups of $\mathbb{Q}_p^\times$. To show $L \subset \mathbb{Q}_p(\mu_N) \subset \mathbb{Q}_p(\mu_\infty)$ for some N, it suffices to show that

$$\mathrm{Nm}\, L^\times \supset \mathrm{Nm}\, \mathbb{Q}_p(\mu_N)^\times \text{ for some } N.$$

Since $\mathrm{Nm}\, L^\times$ is finite index, open, we know it must contain $(1 + p^n\mathbb{Z}_p) \times p^{m\mathbb{Z}}$ for some n, m. We just need to choose N large enough to have norm contained in this subgroup. Here's a fact:

$$\mathrm{Nm}\, (\mathbb{Z}_p[\mu_{p^n}])^\times = 1 + p^n\mathbb{Z}_p.$$

We say $\{\mathrm{Nm}\, \mathbb{Q}_p(\mu_N)^\times : N\}$ is *commeasurable* with $\{\mathrm{Nm}\, L^\times : L/\mathbb{Q}_p \text{ fin. abel}\}$. $\triangle$

Theorem 2.8.2 (Kronecker-Weber Theorem). $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty)$

Lemma 2.8.3. *Let $K/\mathbb{Q}$ be finite abelian. Then, $G := \mathrm{Gal}(K/\mathbb{Q})$ is generated by I_p for all ramified primes p.*

Proof. Let $G' = \langle I_p : \forall p \rangle$. By Galois theory, there is some field $L = K^{G'}$ which is Galois over $\mathbb{Q}$ (since $\mathrm{Gal}(K/\mathbb{Q})$ abelian) with Galois group G/G'. Hence, $L/\mathbb{Q}$ is unramified everywhere, so $L = \mathbb{Q}$, i.e. $G = G'$. ■

Above secretly works for any base field with trivial class group, but maybe we don't know that yet.

Proof of Global Kronecker-Weber. First observe that

$$\mathbb{Q}(\mu_N) = \prod \mathbb{Q}(\mu_{p_i^{m_i}}) \text{ when } N = \prod_i p_i^{m_i}$$

so this N can be recovered by local ramification. Now, consider $K/\mathbb{Q}$ finite abelian. Let p be a ramified (rational) prime, and choose some place $v \mid p$, so we get a finite abelian extension $K_v/\mathbb{Q}_p$. By local Kronecker-Weber, we know $K_v \subset \mathbb{Q}_p(\mu_{p^{m_p}}, \mu_{m'_p})$ where $p \nmid m'_p$. Define,

$$N = \prod_{p \text{ ram in } K} p^{m_p}.$$

We claim that $K \subset \mathbb{Q}(\mu_N)$, i.e. $K(\mu_N) = \mathbb{Q}(\mu_N)$, i.e. $\mathrm{Gal}(K(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. For this, its enough to check cardinality. We know the Galois group is generated by local inertia, so

$$\# \mathrm{Gal}(K(\mu_N)/\mathbb{Q}) \le \prod_{p|N} \# I_p = \prod_{p|N} \# \left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times = \# \left(\mathbb{Z}/N\mathbb{Z}\right)^\times.$$

This finishes the proof since the inclusion $\mathbb{Q}(\mu_N) \subset K(\mu_N)$ tells us that we have a surjection $\mathrm{Gal}(K(\mu_N)/\mathbb{Q}) \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ (which is an iso by above cardinality bound). ∎

Remark 2.8.4 (Hilbert 12th problem). Can you do explicit class field theory for general base fields? So far, we can really only do it for $K = \mathbb{Q}$ or K imaginary quadratic. Locally though, for K non-archimedean local field, one has Lubin-Tate theory; you use (roots of?) certain formal power series to obtain extensions. ○

Recall the local Artin map

$$\varphi_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Claim 2.8.5. *This map is continuous and injective with dense image.*

Proof. It is continuous because all maps $\varphi_{K/L} : K^\times \to \mathrm{Gal}(L/K)$ for L/K finite abelian are continuous. This is because norm subgroups are open.

For injectivity, this is just the statement $\bigcap \mathrm{Nm}\, L^\times = \{1\}$.

Finally, it has dense image since it surjects onto each finite quotient of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, i.e. each $\mathrm{Gal}(L/K)$ with L/K finite abelian. ∎

In fact, we have an isomorphism

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\sim} \varprojlim_{L/K} K^\times / \mathrm{Nm}\, L^\times$$

with the RHS above the completion of $K^\times$ with respect to the norm topology.

Lemma 2.8.6. *When* $\mathrm{char}\, K = 0$ *(so $K/\mathbb{Q}_p$ finite), every finite index subgroup of $K^\times$ is automatically open.*

Proof Sketch. It is enough to prove that $(\mathscr{O}_K^\times)^n \subset \mathscr{O}_K^\times$ is open for all n. In characteristic p, one runs into issues when $n = p^k$. We don't run into issues in the characteristic 0 case. For example, one can prove that

$$(1+(\pi))^{p^n} \supset 1 + p^{n+1}(\pi).$$

The LHS is a group and the RHS is open, so the LHS is open too. To prove this, you want to use *Newton's Lemma*, a sup'd up version of Hensel's lemma. ■

Hence, $\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \varprojlim_{U \subset K^\times} K^\times/U$ where U ranges over all finite index subgroups. In particular, picking a uniformizer so $K^\times \simeq \mathscr{O}_K^\times \times \pi^{\mathbb{Z}}$, one sees that

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \simeq \mathscr{O}_K^\times \times \widehat{\mathbb{Z}}$$

as topological groups. The local Artin map then fits in the diagram

$$\begin{tikzcd} \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r, "\sim"] & \mathscr{O}_K^\times \arrow[d, equal] & \times & \widehat{\mathbb{Z}} \\ K^\times \arrow[u, "\varphi_K"] \arrow[r, "\sim"] & \mathscr{O}_K^\times & \times & \mathbb{Z} \arrow[u, hook] \end{tikzcd}$$

2.8.1 Alternative formulation of class field theory

Maybe you don't like profinite groups. Can we still state class field theory without them? The answer is yes, and in fact, this formulation better generalizes to the non-abelian case. However, we will we see that it also only gives a "partial" formulation.

Consider finite order characters $\chi : K^\times \to \mathbb{C}^\times$? Why finite order? Because the Galois group (what we're trying to get after) is profinite, so any continuous character $\chi' : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathbb{C}^\times$ has finite image.

Lemma 2.8.7. *Let G be a profinite group. Then, any continuous character $\chi : G \to \mathbb{C}^\times$ has finite image.*

Proof. Since G is compact, $\chi(G)$ is a compact subgroup of $\mathbb{C}^\times$, so we really have $\chi : G \to S^1$. We don't actually need this, but why not mention it?

Taking some small open disc $D(1,\varepsilon) \subset \mathbb{C}^\times$ around 1 of radius $\varepsilon > 0$. Then, $\chi^{-1}(D(1,\varepsilon)) \subset G$ is open. At the same time, we claim that

$$D(1,\varepsilon) \cap \operatorname{Im} G = \{1\}.$$

This is because the LHS is a group, but the "**no small subgroup argument**" tells us that $D(1,\varepsilon)$ has no subgroup other than $\{1\}$ (take powers to leave the disc otherwise). Thus, $\ker\chi \supset \chi^{-1}(D(1,\varepsilon))$ is open, so χ factors through a finite quotient. ■

Question: Why?

Answer: Not an answer, but alternate take. $\chi^{-1}(D(1,\varepsilon)) \subset$ G is open, so contains an (open) subgroup $H \leq G$ since G profinite. Now,

Theorem 2.8.8. *There exists a natural bijection*

$$\left\{ \begin{matrix} \chi : K^\times \to \mathbb{C}^\times \\ \textit{continuous w/ finite order} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \chi' : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathbb{C}^\times \\ \textit{continuous} \end{matrix} \right\}.$$

Note that, above, we can replace $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ *with* $\mathrm{Gal}(\overline{K}/K)$.

Proof. If you know class field theory, this is just composition with the Artin map $\varphi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. ■

Warning 2.8.9. Just saying there is a bijection is kinda cheap. Like, you can prove there's a bijection just be showing these sets have the same cardinality. To get a complete statement, you need a way of characterizing the bijection you want. •

The point of this perspective is that it may be better to use representations to formulate class field theory. The above says that 1-dim representations of the Galois group are naturally bijective to 1-dim representations of $K^\times$.

Now it's more natural to consider non-abelian extensions. Just think about higher dimensional representations.

Conjecture 2.8.10 (**Local Langlands Conjecture**).

$$\left\{\begin{matrix} \textit{Certain representations} \\ \textit{of } \mathrm{GL}_n(K) \end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix} \rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C}) \\ \textit{continuous} \end{matrix}\right\}$$

When $n = 1$, we have $\mathrm{GL}_1(K) = K^\times$ and recover the previous theorem. However, proving this for $n > 1$ (and even stating it correctly in that case) is no small feat. First, there is no "Artin map" $\mathrm{GL}_n(K) \to \mathrm{Gal}(\overline{K}/K)$, so your bijection has to arise in some other fashion. Second, one does not consider all representations of $\mathrm{GL}_n(K)$, and figuring out the right ones is nontrivial.

2.9 Lecture 19 (11/9): Global class field theory

We spent the last two lectures on local class field theory, so let's move onto global class field theory. Recall that local CFT was about the existence of the Artin map

$$\varphi_K = \mathrm{Art}_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

for a local field K, which satisfies a couple of characterizing properties.

For global class field theory, we'll want to fix a global field K. For simplicity, assume $\operatorname{char} K = 0$ (so $K/\mathbb{Q}$ a number field). The statements in the end will apply also for function fields.

In the case of local class field theory, understanding the maximal unramified extension of K is even easier than the maximal abelian extension. The Artin map restricts to a map

$$\{\text{fraction ideals}\} \simeq \left(K^\times/\mathscr{O}_K^\times\right) \to \mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \widehat{\mathbb{Z}}.$$

We are looking for the right analogue of $K^\times$ in the global case. The above tells us that maybe it should somehow be related to fractional ideals.

2.9.1 Adeles and Ideles

Historically, ideles (ideal elements) were introduced before adeles (additve ideles), potentially by Chevalley. Let $\mathscr{O}_K$ be the ring of integers. Then, the group of fractional ideals

$$\{\text{fraction ideal}\} \xrightarrow{\sim} \bigoplus_{\mathfrak{p}} \mathbb{Z}\mathfrak{p} \xrightarrow{\sim} \bigoplus_{v\nmid\infty} K_v^\times/\mathscr{O}_{K_v}^\times$$

is the free abelian group generated by the prime ideals (i.e. finite places).

Definition 2.9.1. Let $\Sigma_K = \{\text{all places of } K\}$. Let $\{G_v\}_{v\in\Sigma_K}$ be a collection of topological groups with open, compact subgroups $\{H_v\}$ given for all but finitely many places. Given this data, the **restricted direct product** is

$$\prod_{v\in\Sigma_K}{}' G_v = \prod_{v\in\Sigma_K}{}'(G_v : H_v) := \left\{(g_v)_{v\in\Sigma_K} \in \prod_v G_v : g_v \in H_v \text{ for almost all } v \in \Sigma_K\right\} \subset \prod_v G_v$$

where "almost all" means "all but finitely many." ◇

Remark 2.9.2. For any finite subset $S \subset \Sigma_K$, can consider

$$G(S) := \prod_{v\in S} G_v \cdot \prod_{v\notin S} H_v.$$

Then,

$$\prod_v{}' G_v = \bigcup_{\substack{S\subset\Sigma_K\\ \text{finite}}} G(S).$$

○

Adeles and ideles are (elements of) certain restricted direct products.

Definition 2.9.3. Take $G_v = K_v^\times$ and $H_v = \mathscr{O}_{K_v}^\times$ (when v non-arch). Then, the restricted direct product

$$\mathbb{I}_K := \prod_v{}'(K_v^\times : \mathscr{O}_{K_v}^\times) = \prod_v{}' K_v^\times$$

is called the group of **ideles**. ◇

Remark 2.9.4. Restricted direct products are topological groups. Give $G(S)$, defined in previous remark, the product topology and then require that it be open in $\prod'_v G_v$. The topology of $\prod'_v G_v$ is the smallest such that these $G(S)$'s are open with induced topology equal to their product topology; if G_v is locally compact for all v, then $\prod'_v G_v$ is locally compact too. Note that $\prod_v G_v$ is usually *not* locally compact though. ○

Note that

$$\mathbb{I}_K \Big/ \prod_{v\mid\infty} K_v^\times \simeq \prod_{v<\infty}{}' K_v^\times =: \mathbb{I}_{K,f}$$

and the above is called the group of **finite ideles**. One also observes that

Lemma 2.9.5.

$$\mathbb{I}_{K,f} \Big/ \prod_v \mathscr{O}_{K_v}^\times \simeq \bigoplus_{v<\infty} K_v^\times / \mathscr{O}_{K_v}^\times = \{\textit{fractional ideals}\}.$$

Proof. This is

$$\frac{\bigcup_{\substack{S\subset \Sigma_{K,f}\\ \text{finite}}} \left(\prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathscr{O}_{K_v}^\times\right)}{\prod_{v<\infty} \mathscr{O}_{K_v}^\times} \xrightarrow{\simeq} \bigcup_S \bigoplus_{v\in S} \left(K_v^\times / \mathscr{O}_{K,v}^\times\right) = RHS.$$

■

We won't really need the adeles for class field theory, but it's good to introduce them as well.

Definition 2.9.6. The (topological) ring of **adeles** is

$$\mathbb{A}_K := \prod_{v\in\Sigma_K}{}' (K_v : \mathscr{O}_{K_v}).$$

Concretely, its $(x_v) \in \prod_v K_v$ s.t. $x_v \in \mathscr{O}_{K_v}$ for almost all v. ◇

2.9.2 Back to GCFT

Remark 2.9.7. $\mathbb{I}_K \simeq \mathbb{A}_K^\times$ as groups, but $\mathbb{I}_K$ does not carry the subspace topology. ○

Question: Does it carry the subspace topology with respect to $\mathbb{A}_K^\times \subset \mathbb{A}_K \times \mathbb{A}_K$ via $x \mapsto (x, x^{-1})$?

Answer: Probably, but even better: it carries the direct limit topology $\mathbb{A}_F^\times := \lim_{S \text{ finite}} \prod_{v\in S} F_v^\times \prod_{v\notin S} \mathscr{O}_{F_v}^\times$.

We've see that

$$\left\{\begin{matrix}\text{fractional ideals}\\ \text{in K}\end{matrix}\right\} \xrightarrow{\simeq} \mathbb{I}_K \Big/ \left(\prod_{v\mid\infty} K_v^\times \times \prod_{v<\infty} \mathscr{O}_{K_v}^\times\right)$$

as (topological) groups (the RHS is discrete since quotienting by something open). For any place (archimedean or not) $v \in \Sigma_v$, can consider (K^s = separable closure, K^{ab} = maximal abelian extension)

$$\begin{tikzcd} K^s \arrow[r, hook] \arrow[d, dash] & K_v^s \arrow[d, dash] \\ K^{\mathrm{ab}} \arrow[r, hook] \arrow[d, dash] & K_v^{\mathrm{ab}} \arrow[d, dash] \\ K \arrow[r, hook] & K_v \end{tikzcd}$$

so get a natural map $\mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \hookrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ via restriction. This depends on the choice of $K^s \subset K_v^s$, but it is still well-defined up to conjugation. Hence, in the abelian case it is just outright well-defined, so we can use local class field theory without worrying about compatibility issues. We stitch together the local Artin maps to get

$$\begin{tikzcd} K_v^\times \arrow[r, "\varphi_{K_v}"] \arrow[d] & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \arrow[d] \\ \prod_v{}' K_v^\times \arrow[r, "\varphi_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{tikzcd}.$$

We need to make sure that the **global Artin map**

$$\varphi_K((x_v)) := \prod_v \varphi_{K_v}(x_v)$$

makes sense, i.e. that $\varphi_{K_v}(x_v) = 1$ for almost all v.

Claim 2.9.8. *This is true: $\varphi_{K_v}(x_v) = 1$ for almost all v.*

Proof. It will actually be easier[25] to show a finite version of this. Choose L/K a finite abelian extension as well as $w \mid v$, a place of L, and consider instead

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\varphi_{L_w/K_v}|_L} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \prod_v{}' K_v^\times & \xrightarrow{\varphi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

and we want to show that $\varphi_{L/K}(x_v) = 1$ for almost all v.

Wei started talking about the last problem on homework 7. Something about counting degree n extensions of Local fields (apparently only finitely many in char 0, but infinitely many in char p).

I think he's wanting to count degree p extensions of K, a char p local field. Artin-Schrier apparently tells us that all such extensions are of the form $L_a = K[x]/(f_a)$ where (a chosen so that) $f_a(x) = x^p - x - a$ is irreducible, separable. If α is a root of f_a, then so is $\alpha + i$ with $i \in \mathbb{F}_p$, so this gives all roots.

Let K^s be the separable closure and consider

$$\begin{array}{cccc} \sigma: & K^s & \longrightarrow & K^s \\ & x & \longmapsto & x^p - x \end{array},$$

a $G = \mathrm{Gal}(K^s/K)$-equivariant homomorphism of abelian groups. The short exact sequence

$$0 \longrightarrow \mathbb{F}_p \longrightarrow K^s \xrightarrow{\sigma} K^s \longrightarrow 0$$

induces

$$K \xrightarrow{\sigma} K \longrightarrow \mathrm{H}^1(G; \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p)$$

in cohomology, so we have $K/\sigma(K) \hookrightarrow \mathrm{Hom}(G; \mathbb{F}_p)$. Artin-Schrier tells us that this is actually an isomorphism. One can describe this map without cohomology via

$$\begin{array}{ccc} K/\sigma(K) & \longrightarrow & \mathrm{Hom}(G, \mathbb{F}_p) \\ \alpha & \longmapsto & \tau \mapsto \tau(\alpha) - \alpha \end{array}$$

since we saw that all roots differ by elements of $\mathbb{F}_p$. This is called the Artin-Schrier map AS_K. Note that $\mathrm{Hom}(G, \mathbb{F}_p)$ gives the space of degree p extensions of K, so $\alpha, \beta \in K$ give the same Artin-Schrier extension precisely when they agree in $K/\sigma(K)$. Thus, to get infinitely many inequivalent extensions,

[25]What we stated as the claim might not actually be true. Unclear

just nee to show that $\#K/\sigma(K) = \infty$. In another perspective, we have $K/\sigma(K) = \mathrm{Gal}(L/K)^\vee$ where $L = \bigcup(\text{degree } p \text{ extensions of } K)$.

Note that K can be any field of char p, even $K = \mathbb{F}_p$. In this case, $K/\sigma(K) = \mathbb{F}_p$ is a 1-dim vector space, so there's only one degree p extension.

What does this have to do with class field theory? Say K is a local field. Then, $\mathrm{Gal}(L/K) \simeq K^\times/\left(K^\times\right)^p$ when $L = \bigcup(\text{degree } p \text{ extensions of } K)$, by CFT. This quotient is big.

Back to the proof. Scroll up to remember what we're doing.

Note that w is unramified over v for almost all v since there are only finitely many ramified primes. Recall that local CFT tells us that $\varphi_{L_w/K_v}(\mathscr{O}_{K_v}^\times) = 1$ if v is unramified, so we win by definition of the ideles. ∎

Remark 2.9.9. We only proved the claim in the finite extension case. Taking inverse limits, we do get a map to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Unclear, to me at least, if this really is the product of the local Artin maps. ○

Theorem 2.9.10 (**Main Theorem of Global CFT**). *Still in the finite extension case L/K. We've seen that local CFT let's us define*

$$\varphi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

with $\varphi_{L/K} = \prod_v \varphi_{L_w/K_v}$.

(i) $\varphi_{L/K}(K^\times) = 1$ *with* $K^\times \hookrightarrow \prod'_{v\in\Sigma_K} K_v^\times$ *via the diagonal embedding* $x \mapsto (x_v = x)_v$ ***(reciprocity)****. Hence, we really have a map*

$$\varphi_{L/K} : \mathbb{I}_K/K^\times \longrightarrow \mathrm{Gal}(L/K)$$

from the ***idele class group*** $C_K = \mathbb{I}_K/K^\times$.

(ii) $\varphi_{L/K}$ *is surjective with kernel*

$$\ker \varphi_{L/K} = \mathrm{Nm}(C_L) \subset C_K,$$

i.e. it induces an isomorphism $C_K/\mathrm{Nm}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$. *Note that* $\mathrm{Nm}(C_L)$ *is open (by local CFT. See following remark) and of finite index.*

Remark 2.9.11. To form the norm map $\mathrm{Nm} : C_L \to C_K$, write

$$\mathbb{I}_L = \prod_{w\in\Sigma_L}{}' L_w^\times = \prod_{v\in\Sigma_K}{}' \left(\prod_{w|v} L_w^\times\right).$$

The norm map is induced by the coordinate wise maps

$$\prod_{w|v} L_w^\times \xrightarrow{\prod_{w|v}\mathrm{Nm}_{L_w/K_v}} K_v^\times$$

for $v \in \Sigma_K$. Note that local CFT tells us that if v is unramified, then $\mathrm{Nm}\,\mathscr{O}_{L_w}^\times = \mathscr{O}_{K_v}^\times$. Hence, $\mathrm{Nm}\,\mathbb{I}_L$ is an open subgroup in $\mathbb{I}_K$. ○

Let's compare global and local CFT.

Local	Global
$K^\times/\operatorname{Nm} L^\times \xrightarrow{\sim} \operatorname{Gal}(L/K)$	$C_K/\operatorname{Nm} C_L \xrightarrow{\sim} \operatorname{Gal}(L/K)$
$K^\times$	$C_K = \mathbb{I}_K/K^\times$

Note that

$$\operatorname{Cl}_K = \frac{\left\{\substack{\text{fractional ideals}\\ \text{in K}}\right\}}{\{\text{principal ideals}\}} \xrightarrow{\sim} K^\times \Big\backslash \mathbb{I}_K \Big/ \left(\prod_{v\mid\infty} K_v^\times \times \prod_{v<\infty} \mathscr{O}_{K_v}^\times\right) = C_K \Big/ \left(\prod_{v\mid\infty} K_v^\times \times \prod_{v<\infty} \mathscr{O}_{K_v}^\times\right)$$

No class on Wednesday for some reason. We'll spend a little more time (half-lecture?) on global CFT.

2.10 Lecture 20 (11/16)

Including today, we have 6 lectures left. Wei sent out a survey with possible topics for the remaining lectures.

2.10.1 Global CFT, Continued

Last time we introduced the ideles and used them to state the main results of global class field theory.

Recall 2.10.1. Let K be a global field (so included function field case). Can define a global Artin map for L/K finite, abelian. This is

$$\varphi_{L/K} : \mathbb{A}_K^\times \to \operatorname{Gal}(L/K)$$

which combines the local Artin maps in the sense that

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\varphi_{L_w/K_v}} & \operatorname{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^\times & \xrightarrow{\varphi_{L/K}} & \operatorname{Gal}(L/K) \end{array}$$

commutes for any place v of K and place $w \mid v$ of L. One writes

$$\varphi_{L/K} = \prod_v \varphi_{L_w/K_v}.$$

One uses local CFT to guarantee that this infinite product is indeed well-defined. This global Artin map satisfies (and is determined by?)

(a) $\varphi_{L/K}(K^\times) = \mathrm{id} \in \operatorname{Gal}(L/K)$, i.e. one really has

$$C_K := \mathbb{A}_K^\times/K^\times \xrightarrow{\varphi_{L/K}} \operatorname{Gal}(L/K).$$

The Artin map is really a homomorphisms from the **idèle class group** C_K. This group is the right analogue for the group of units $K_v^\times$ in the local case.

(b) $\varphi_{L/K}$ induced an isomorphism

$$C_K/\operatorname{Nm} C_L \xrightarrow{\sim} \operatorname{Gal}(L/K).$$

$\odot$

Definition 2.10.2. Any group of the form $\operatorname{Nm} C_L$ for a finite extension L/K is called a **norm group**. $\diamond$

Theorem 2.10.3 (**global existence theorem**)**.** *The norm groups of a global field K are precisely the finite index, open subgroups of $\mathbb{A}_K^\times$.*

Remark 2.10.4. The $\implies$ direction follows from local existence (for open) + second part of global CFT (for finite index). The other direction is nontrivial. $\circ$

The upshot is we have

$$\left\{\begin{matrix}\text{finite abelian}\\ L/K\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{open, finite index}\\ \text{subgroups of } C_K\end{matrix}\right\}.$$

Example (**Kronecker-Weber Theorem**)**.** Recall we showed before that $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_N : N \geq 2)$ using local CFT. Say $L = \mathbb{Q}(\mu_N)$ is a cyclotomic field (and $K = \mathbb{Q}$). We want to understand

$$\varphi_{L/K} : C_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \longrightarrow \operatorname{Gal}(L/\mathbb{Q}).$$

Note that $\mathbb{A}_L^\times = \prod'_w L_w^\times$. Any archimedean place w of L is complex, so the local norm map $L_w^\times \to \mathbb{Q}_v^\times$ looks like $\mathbb{C}^\times \to \mathbb{R}^\times$. For a non-archimedean place $w \mid p$, the image of the norm map $\mathscr{O}_{L_w}^\times \to \mathbb{Z}_p^\times$ is everything if $p \nmid N$ (i.e. w is unramified) by local CFT. If $p \mid N$ (the ramified case), then $\mathbb{Z}_p[\mu_{p^n}]^\times \to 1 + (p^n) = 1 + N\mathbb{Z}_p$ where $N = p^n m$ (and $p \nmid m$). Hence,

$$\operatorname{Nm} C_L \supset \mathbb{Q}^\times \left(\underbrace{\mathbb{R}_+^\times \cdot \prod_{p\nmid N} \mathbb{Z}_p^\times \cdot \prod_{p\mid N}(1 + N\mathbb{Z}_p)}_{\widetilde{\operatorname{Nm} L}}\right)$$

Exercise. $\mathbb{A}_{\mathbb{Q}}^\times/\widetilde{\operatorname{Nm} L} = \mathbb{Q}^\times\backslash\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{R}_+^\times \cdot \prod_{p\nmid N} \mathbb{Z}_p^\times \cdot \prod_{p\mid N}(1 + N\mathbb{Z}_p) \xrightarrow{\sim} \operatorname{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. In this double coset thing, people like to write discrete groups on the left and open ones on the right

$\triangle$

For that exercise, may be better to consider a more general situation.

Recall 2.10.5. For fixed global field K, the **finite ideles** are $\mathbb{A}_f^\times = \prod'_{v<\infty} K_v^\times$, and the ideal class group is

$$K^\times\backslash\mathbb{A}_f^\times \Big/ \prod_{v<\infty} \mathscr{O}_{K_v}^\times \simeq \mathrm{Cl}_K.$$

In particular, this double coset space is finite. $\odot$

Example. When $K = \mathbb{Q}$, one has

$$\mathbb{A}_{\mathbb{Q},f}^\times = \mathbb{Q}^\times \left(\prod_{p<\infty} \mathbb{Z}_p^\times\right).$$

Looking at all ideles,

$$\mathbb{A}_{\mathbb{Q}}^\times = \mathbb{Q}^\times \left(\mathbb{R}_+^\times \prod_{p<\infty} \mathbb{Z}_p^\times\right).$$

This gives the $N = 1$ case of the exercise? $\triangle$

For notational convenience, define

$$\left(1+N\widehat{\mathbb{Z}}\right)^{\times} := \cdot \prod_{p\nmid N} \mathbb{Z}_p^{\times} \cdot \prod_{p\mid N}(1+N\mathbb{Z}_p),$$

so

$$\mathbb{Q}^{\times}\backslash\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{R}_{+}^{\times}(1+N\widehat{\mathbb{Z}})^{\times} \simeq \frac{\mathbb{Q}^{\times}\backslash\mathbb{Q}^{\times}(\mathbb{R}_{+}^{\times}\prod_p \mathbb{Z}_p^{\times}}{\mathbb{Q}^{\times}\backslash\mathbb{Q}^{\times}(\mathbb{R}_{+}^{\times}(1+N\widehat{\mathbb{Z}})\times} \simeq \prod_{p\nmid N} \mathbb{Z}_p^{\times}/(1+N\mathbb{Z}_p) \simeq (\mathbb{Z}/N\mathbb{Z})^{\times}.$$

What are we doing and why?

2.10.2 Hilbert Class field

Recall that

$$K^{\times}\backslash\mathbb{A}_f^{\times} \Big/ \prod_{v<\infty} \mathscr{O}_{K_v}^{\times} \simeq \mathrm{Cl}_K,$$

so the ideal class group is a quotient of the idele class group $C_K = K^{\times}\backslash\mathbb{A}_K^{\times}$:

$$K^{\times}\backslash\mathbb{A}_K^{\times}/\prod_{v\mid\infty} K_v^{\times} \cdot \prod_{v<\infty} \mathscr{O}_{K_v}^{\times} \xrightarrow{\sim} \mathrm{Cl}_K.$$

Thus, associated to the norm group (i.e open, finite index subgroup) $K^{\times}\left(\prod_{v\mid\infty} K_v^{\times} \cdot \prod_{v<\infty} \mathscr{O}_{K_v}^{\times}\right) \subset C_K$ is a **Hilbert class field** H_K which is abelian over K with Galois group

$$\mathrm{Gal}(H_K/K) \simeq \mathrm{Cl}_K.$$

The property alone does not characterize the field (e.g. imagine $\mathrm{Cl}_K = \mathbb{Z}/2\mathbb{Z}$). What does characterize it is that H_K is the *maximal unramified abelian extension* of K. Note that this includes being **unramified at the archimedean places** $v \mid \infty$, i.e. $\mathrm{Nm}_v : L_w^{\times} \twoheadrightarrow K_v^{\times}$ is surjective (i.e. the extension is not $\mathbb{C}/\mathbb{R}$).

For any unramified extension, its norm must contain all integral units at non-archimedean places and must contain everything at archimedean places, i.e. you must mod out by $\prod_{v\mid\infty} K_v^{\times} \cdot \prod_{v<\infty} \mathscr{O}_{K_v}^{\times}$ at least.

Survey topics: what to do with the time we have left? One of

- (Introduction to) Iwasawa theory (for $\mathbb{Z}_p$-extensions).

  Consider $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$. This has Galois group isomorphic to $\mathbb{Z}_p$ (coming from $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^{\times} \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$). Turns out studying this $\mathbb{Z}_p$-extension let's you understand $\mathrm{Cl}_{\mathbb{Q}(\mu_{p^n})}[p^\infty]$ (Sylow p-subgroup), e.g. you can get asymptotics for its size.

- Theorem of Tate on $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}}_p}$ (which is algebraically closed).

  $\mathbb{C}_p$ has an action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})$ by isometrics. Tate showed that the "p-adic $2\pi i$" does not belong to $\mathbb{C}_p$. Consider **the cyclotomic character**

$$\omega : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^{\times}.$$

Is there some $x \in \mathbb{C}_p^\times$ which is an eigenvector for this character, i.e.

$$\sigma(x) = \omega(\sigma)x?$$

Tate proved that the answer is no. This is a starting point of p-adic Hodge theory.

- Tate's thesis.

  For a continuous character
  $$\chi : C_K = K^\times \backslash \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times,$$
  one can define an L-function $L(\chi, s)$, e.g. given a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ get an idele class character
  $$C_K \twoheadrightarrow \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / \mathbb{R}_+^\times \cdot (1 + N\widehat{\mathbb{Z}})^\times \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times$$
  whose L-function is the corresponding Dirichlet L-function. Tate's thesis proved that, in general, these L-functions have meromorphic continuations, functional equations, etc.

- Analytic Methods in zeta functions.

  Description here seem muddled. Somethings related to explicit formula for primes, siegal (spelling?) zeros, and/or other stuff?

Remark 2.10.6. Class field theory tells you when primes ramify as well as the ramification behavior, e.g. if $\varphi_{L/K} : C_K \to \mathrm{Gal}(L/K)$ is the Artin map, then v is unramified iff $\varphi_{L/K}$ kills $\mathscr{O}_{K_v}^\times$. ○

2.10.3 Ray class groups

Recall once more that
$$K^\times \backslash \mathbb{A}_K^\times / \prod_{v\mid\infty} K_v^\times \cdot \prod_{v\nmid\infty} \mathscr{O}_{K_v}^\times \simeq \mathrm{Cl}_K .$$
We can relax what we mod out by. Fix some
$$N = \prod_{v<\infty} \mathfrak{p}_v^{m_v} \text{ with } m_v \geq 0,$$
an (integral) ideal (in particular, we require this to be a finite product). Can define
$$\left(1 + N\widehat{\mathscr{O}}\right)^\times := \prod_{v\nmid N} \mathscr{O}_{K_v}^\times \cdot \prod_{v\mid N} (1 + \varpi_v^{m_v})$$
with products taken only over *finite places*. Then, we can define the **Ray class group of modulus** N to be
$$\mathrm{Cl}_{K,N} := K^\times \backslash \mathbb{A}_K^\times / \prod_{v\mid\infty} K_v^\times \left(1 + N\widehat{\mathscr{O}}\right)^\times .$$
One can interpret this as certain isomorphism classes of ideals. Something like "fractional ideals prime to N modulo principal ideals with support away from N" but, you know, more precise. The point is this

enlarges the class group a little. One can even modify the factors as the archimedean places (if $K_w = \mathbb{R}$, $\mathbb{R}_+^\times \subset \mathbb{R}^\times$ is an open, finite-index subgroup, so could mod out by this instead). These ray class groups have corresponding Hilbert fields just like the class group did.

2.10.4 Injectivity/Surjectivity of the Artin map

Remark 2.10.7. For K local and non-archimedean, recall that

$$K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

is injective, but not surjective (e.g. target compact/profinite while source is not).

For K global,

$$C_K = K^\times \backslash \prod\nolimits' K_v^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

is neither necessarily injective nor necessarily surjective (it does have dense image though). When K is a number field, it is surjective, but not injective (e.g. the kernel contains the connected components of the archimedean places). If K is a function field it is injective, but not surjective. ◦

Let's take a closer look at injectivity. Note that

$$\ker \varphi_K = \bigcap_{\substack{L/K \\ \text{finite}}} \mathrm{Nm}\, C_L.$$

Wei said why this is (or should be?) trivial in the function field case, but I was distracted so I missed it. In the Archimedean case, the smallest subset of $\mathbb{R}^\times$ you can get comes from the norm map $\mathbb{C}^\times \to \mathbb{R}^\times$ (i.e. it is $\mathbb{R}_+^\times$).

Here's another perspective. There is an absolute value map

$$\begin{array}{rccc} |\cdot|: & \mathbb{A}_K^\times & \longrightarrow & \mathbb{R}_+^\times \\ & (x_v) & \longmapsto & \prod_v |x_v|_v \end{array}$$

The product formula tells us that this descends to the idele class group $C_K = \mathbb{A}_K^\times / K^\times$. This map has a splitting, e.g. take

$$\mathbb{R}_+^\times \ni t \longmapsto \Big(\underbrace{t^{1/N}, \dots, t^{1/N}}_{v|\infty}, \underbrace{1, \dots 1}_{v\nmid\infty}\Big) \in \mathbb{A}_K^\times$$

with N depending on the number of archimedean places. Thus, $\mathbb{A}_K^\times \cong \mathbb{R}_+^\times \times \mathbb{A}_K^1$. Similarly,

$$C_K = \mathbb{R}_+^\times \times \mathbb{A}_K^1 / K^\times.$$

Clearly, we will have $\varphi_K(\mathbb{R}_+^\times) = 1$ so the Artin map will have non-trivial kernel. Really, one should consider the Artin map as a map

$$\varphi_K : \mathbb{A}_K^1 / K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

This is still not injective in general (it is when $K = \mathbb{Q}$). The issue is we've only taken out one archimedean place, but there are others. We call the kernel $\ker\varphi_K$ the **universal norm** since it is $\bigcap_{L/K}\operatorname{Nm} C_L$. It is non-trivia in general (when K a number field).

What about surjectivity? In the number field case, we have the following.

Lemma 2.10.8. *$\mathbb{A}_K^1/K^\times$ is compact.*

Proof. It is enough to find a compact subgroup of $\mathbb{A}_K^A$ whose translations (under $K^\times$) cover $\mathbb{A}_K^1$. We know that

$$K^\times\backslash\mathbb{A}_K^1/\left(\prod_{v\mid\infty}K_v^\times\right)^1\cdot\prod_{v\nmid\infty}\mathscr{O}_{K_v}^\times\simeq\mathrm{Cl}_K$$

and that $\prod_{v\nmid\infty}\mathscr{O}_{K_v}^\times$ is compact. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & \frac{\left(\prod_{v\mid\infty}K_v^\times\right)^1}{K^\times\cap\prod_{v\nmid\infty}\mathscr{O}_{K_v}^\times} \arrow[r] \arrow[d, "\wr"] & \frac{\mathbb{A}_K^1}{K^\times} \arrow[r] \arrow[d, equal] & \frac{\mathbb{A}_K^1}{K^\times\left(\left(\prod K_v^\times\right)^1\right)\prod_{v\nmid\infty}\mathscr{O}_{K_v}^\times} \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \frac{\left(\prod_{v\mid\infty}K_v^\times\right)^1}{\mathscr{O}_{K_v}^\times} \arrow[r] & \frac{\mathbb{A}_K^1}{K^\times} \arrow[r] & \mathrm{Cl}_K \arrow[r] & 0
\end{tikzcd}$$

Thus, we win by finiteness of class group + Dirichlet's unit theorem. In other words, this lemma gives us another statement combining these two fundamental results. ■

Thus, the image of $\varphi_K:\mathbb{A}_K^1/K^\times\to\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is compact. We already knew it was dense, so now its image is a closed, dense subgroup. This says the map is surjective.

2.11 Lecture 21 (11/18): Iwasawa Theory

There were 10 responses for the final topic. The top two were Iwasawa theory and Tate's thesis, but Iwasawa theory was slightly ahead, so this is what we'll spend the remaining lectures on.

Our main reference will be "Introduction to Cyclotomic Fields" by Lawrence Washington. Mainly just chapter 13 + section 7.1.

Why study Iwasawa theory? One early motivation for Iwasawa was earlier work by André Weil on the zeta function for curves over finite fields. Say $X/\mathbb{F}_q$ is an algebraic curve. Say $k_n/\mathbb{F}_q$ is the unique extension of degree n (i.e. $k_n=\mathbb{F}_{q^n}$), and note that $\overline{k}=\bigcup_n k_n$. Even if you are only interested in the $\mathbb{F}_q$-points $X(\mathbb{F}_q)$, it can still be useful to study the points $X(k_n)$ or $X(\overline{k})$ over field extensions. We know $\mathrm{Gal}(\overline{k}/k)\simeq\widehat{\mathbb{Z}}$ with distinguished generator

$$\mathrm{Gal}(\overline{k}/k)\ni\mathrm{Frob}_q\longmapsto 1\in\widehat{\mathbb{Z}}$$

given by Frobenius. Thus, we can recover $X(k)=X(\overline{k})^{\mathrm{Frob}_q}$. So, instead of considering the set $X(k)$, we can instead consider $X(\overline{k})$ which is not only a set, but also has a Galois action $\mathrm{Frob}_q\curvearrowright X(\overline{k})$.

Another perspective: consider the function field $K=k(X)$. Recall that the "right" analogue of the class group in this setting is the divisor class group $\operatorname{Pic}X$ or even the the degree 0 divisor class group $\operatorname{Pic}^0(X)\simeq\operatorname{Jac}(X)(k)$ which is all the k-points of the Jacobian variety. This is a (finite?) abelian group, so we can consider its Sylow ℓ-subgroup. As before, we have

$$\mathrm{Jac}(X)(k) = \mathrm{Jac}(X)(\overline{k})^{\mathrm{Frob}} \text{ and } \mathrm{Jac}(X)(k) \otimes \mathbb{Z}_l \simeq (\mathrm{Jac}(X)(\overline{K}) \otimes \mathbb{Z}_\ell)^{\mathrm{Frob}}.$$

In doing either of this, we are basically considering the tower

$$\begin{tikzcd}
 & K_\infty = \overline{k}(X) \arrow[d, dash] \\
 & K_n = k_n(X) \\
K = k(X) \arrow[ur, dash] \arrow[uur, dash, bend left, "\widehat{\mathbb{Z}}"] &
\end{tikzcd}$$

This is the basic picture that inspired Iwasawa.

Now consider making an analogue of this for number fields. There's the issue that there's no "constant field" (e.g. $k = \mathbb{F}_q$ above). So we need to produce extensions in another way; we want them to be as simple as possible (i.e. pro-cyclic Galois groups).

Iwasawa considered the following situation. Let K be a number field, and fix a prime p. We want to consider $\mathbb{Z}_p$-extensions. Write $\Gamma = \mathbb{Z}_p$ (this is just notation). We want an extension K_∞/K with $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, and then study the "class group" of K_∞, suitably defined; we hope that this + the $\mathbb{Z}_p$-action will allow us to recover information on Cl_K.

Any $\mathbb{Z}_p$-extension will have a few nice properties, coming from the group theory of $\mathbb{Z}_p$. Recall that $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is a profinite abelian group, and one can enumerate all its closed subgroups (i.e. intermediate fields extensions $K_\infty/L/K$). They are precisely $p^n\mathbb{Z}_p$ for $n \geq 0$ as well as 0 (think of as $n = \infty$); show this as an exercise. In particular, there is a unique closed subgroup (i.e. intermediate field extension) of index p^n (over K). We let K_n denote the corresponding intermediate field, so we have a tower

$$\begin{tikzcd}
K_\infty \arrow[d, dash, "\Gamma^{p^n}"] \\
K_n \arrow[d, dash, "\Gamma_n"] \\
K \arrow[uu, dash, bend left, "\Gamma"]
\end{tikzcd}$$

with $\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$ and the group operation on Γ written multiplicatively.

Example. Every number field has at least one $\mathbb{Z}_p$ extension. Here is one for $\mathbb{Q}$. One then we have the extension $\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}$ with Galois group $\left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times$. In the limit, we have $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ with Galois group $\mathbb{Z}_p^\times$. This is not quite what we want, we recall that

$$\mathbb{Z}_p^\times \simeq \mu_{p-1} \times (1 + p\mathbb{Z}_p) \simeq \mu_{p-1} \times \mathbb{Z}_p.$$

Thus, there is a unique subextension $\mathbb{Q}_\infty \subset \mathbb{Q}(\mu_{p^\infty})$ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \Gamma$. This is our desired extension.

For a number field K, can consider $K \cdot \mathbb{Q}_\infty =: K_\infty$ as an extension of K. This gives an injection

$$\mathrm{Gal}(K_\infty/K) \hookrightarrow \Gamma \simeq \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}).$$

The image of this is not finite, so of the form Γ^{p^m} for some m, but this is still abstractly isomorphic to Γ, so K_∞/K is a $\mathbb{Z}_p$-extension. △

Given K, let $K^{\max-p}$ be its maximal abelian pro-p extension. We can determine this using class field theory.

Lemma 2.11.1. *Any $\mathbb{Z}_p$-extension K_∞/K is unramified output of p.*

Proof. Let v be a prime of K above a rational prime $\ell \neq p$. Let L/K be a finite p-extension (i.e. $\mathrm{Gal}(L/K)$ is a p-group, i.e. has order a p-power). We want to show that v is unramified. By class field theory, we have the Artin map

$$\varphi_{L/K} : K^\times \backslash \mathbb{A}_K^\times \longrightarrow \mathrm{Gal}(L/K)$$

whose kernel is the norm group. By comparison with the local Artin map

$$K_v^\times \longrightarrow \mathrm{Gal}(L_w/K_v)$$

(with $w \mid v$ any place of L over v), we see that v is unramified iff the norm group contains $\mathscr{O}_v^\times$. We know

$$\ker \varphi_{L/K} \simeq \mathrm{Nm}(C_L) \supset (C_K)^{p^N}$$

where $\#\,\mathrm{Gal}(L/K) = p^N$. At v,

$$\left(K_v^\times\right)^{p^N} \supset \left(\mathscr{O}_{K_v}^\times\right)^{p^N} \supset 1 + \varpi_v \mathscr{O}_{K_v}$$

with last inclusion coming from $v \nmid p$ (so $p \nmid \operatorname{char} \kappa(v)$, the characteristic of the residue field at v; use Hensel's lemma or whatever).

Upon further thought, this may not be true at the finite level. Seems you really need use the fact that our finite extensions K_n fit inside a $\mathbb{Z}_p$-extension.

Consider

$$\varphi_{K_\infty/K} : K^\times \backslash \mathbb{A}_K^\times \longrightarrow \mathrm{Gal}(K^\infty/K) \simeq \Gamma$$

whose image is torsion-free. We've seen above already that

$$\ker \varphi_{K_\infty/K} \supset (1 + \varpi_v \mathscr{O}_{K_v})$$

Thus, we win using that $\mathscr{O}_{K_v}^\times = \left\langle (\mathscr{O}_{K_v}^\times)_{\mathrm{tors}}, 1 + \varpi_v \mathscr{O}_v \right\rangle$ is generated by its torsion along with $1 + \varpi \mathscr{O}_{K_v}$. ■

What about primes above p?

Lemma 2.11.2. *Say* $\mathrm{Gal}(K_\infty/K) \simeq \Gamma$. *Then, there exists $n \geq 0$ s.t. all primes v of K_n above p are either totally ramified or unramified. Furthermore, there exists at least one prime which is totally ramified.*

Example. If $\mathbb{Q}_\infty/\mathbb{Q}$ constructed earlier, p is totally ramified. △

We won't prove this lemma. We will see the same proof strategy in the next lemma we write down. Recall that we were interested in

$$K^{\max-\mathbb{Z}_p} = \bigcup \text{all } \mathbb{Z}_p\text{-extensions}.$$

This field contains $K \cdot \mathbb{Q}_\infty =: K_{\text{cycl}}$.

Question 2.11.3. *What is* $\mathrm{Gal}(K^{\max-\mathbb{Z}_p}/K)$*?*

We use class field theory. This is asking what the maximal pro-p quotient of $\mathrm{Gal}(K^{\text{ab}}/K)$ is. It will necessarily be a quotient of

Question: For non-arch v, why do we only kill $\mathscr{O}_v^\times$ and not all of K_v?

$$K^\times \backslash \mathbb{A}_K^\times / \prod_{v|\infty} K_v^\times \cdot \prod_{v\nmid p} \mathscr{O}_{K_v}^\times \twoheadrightarrow \mathrm{Gal}(K^{\max-\mathbb{Z}_p}/K).$$

Recall, the the class group is

$$K^\times \backslash \mathbb{A}_K^\times / \prod_{v|\infty} K_v^\times \cdot \prod_{v\nmid p} \mathscr{O}_{K_v}^\times \cdot \prod_{w|p} \mathscr{O}_{K_w}^\times = \mathrm{Cl}_K\,.$$

In the present case, we are excluding the factors above p. We more-or-less have something like

The exact connection to the bottom line is lost on me

$$\prod_{v|p} \mathscr{O}_{K_v}^\times \Big/ \mathscr{O}_K^\times \to \mathrm{Gal}(K^{\max-\mathbb{Z}_p}/K).$$

Conjecture 2.11.4 (Leopoldt Conjecture). *Consider*

$$\mathbb{Z}^{r_1+r_2-1} \simeq \mathscr{O}_K^\times \hookrightarrow \prod_{v|p} \mathscr{O}_{K_v}^\times.$$

The conjecture is that

$$\mathrm{rank}_{\mathbb{Z}_p} \overline{\mathscr{O}_K^\times} = r_1 + r_2 - 1$$

where the closure is taken in the RHS of the map considered above.

Definition 2.11.5. We define the **Leopoldt defect** to be $\delta = r_1 + r_2 - 1 - \mathrm{rank}_{\mathbb{Z}_p} \overline{\mathscr{O}_K^\times}$. ⋄

Then,

$$\mathrm{Gal}(K^{\max-\mathbb{Z}_p}/K) \simeq \mathbb{Z}_p^{[K:\mathbb{Q}]-(r_1+r_2-1)+\delta} = \mathbb{Z}_p^{r_2+1+\delta}.$$

It is conjectured (above) that $\delta = 0$ always, and this is known when $K/\mathbb{Q}$ is abelian.

Example. When $K = \mathbb{Q}$, the rank is 1. When K is real quadratic, the rank is still 1. When it is imaginary quadratic, the rank jumps to 2. △

This calculation also shows that there must be a ramified place above p (part of earlier lemma). For $v \mid p$, consider the induced $\mathscr{O}_{K_v}^\times \to \Gamma \simeq \mathbb{Z}_p$. If it is trivial, then v is unramified; else, the image of the form Γ^{p^n} so it will be totally ramified from the nth stage onwards. This map is induced from a surjective map, so it can't be trivial on all factors.

Consider K_∞/K a $\mathbb{Z}_p$-extension. Let's consider the p-Sylow subgroups $\mathrm{Cl}(K_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p =: X_n$ of the class groups of the finite intermediate extensions. Note that $\Gamma_n \curvearrowright X_n$ for all n, Furthermore, the norm maps $X_{n+1} \xrightarrow{\mathrm{Nm}} X_n$ are equivariant, so the limit $X := \varprojlim X_n$ has a Γ-action. This is why we prefer the notation Γ over $\mathbb{Z}_p$. This X is a $\mathbb{Z}_p$-module ($\mathbb{Z}_p$ the ring) since it is built from p-groups, but it is also separately a (continuous) Γ-module ($\Gamma \simeq \mathbb{Z}_p$ the (profinite) group) because of the Galois action.

This motivates the study of objects which are both $\mathbb{Z}_p$-modules and Γ-modules. These objections are modules over the group algebra $\mathbb{Z}_p[\![\Gamma]\!]$. One has to be careful about what this means because of the limiting going on. At the finite level, X_n is a $\mathbb{Z}_p[\Gamma_n]$-module with $\mathbb{Z}_p[\Gamma_n]$ the usual group algebra. We let

$$\mathbb{Z}_p[\![\Gamma]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma_n]$$

with transition maps $\mathbb{Z}_p[\Gamma_{n+1}] \twoheadrightarrow \mathbb{Z}_p[\Gamma_n]$ induced by

$$\Gamma_{n+1} \twoheadrightarrow \Gamma_n.$$

Theorem 2.11.6. *There is a canonical isomorphisms*

$$\mathbb{Z}_p[\![\Gamma]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!].$$

Therefore one should try to classify modules over this power series ring. This ring is called the **Iwasawa algebra**.

2.12 Lecture 22 (11/30)

4 lectures left. Last time we introduced $\mathbb{Z}_p$-extensions. Say K_∞/K_0 is Galois with Galois group $\Gamma \simeq \mathbb{Z}_p$. For each n, there is a unique subgroup Γ^{p^n} (written multiplicatively) of Γ whose quotient is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, i.e. unique

$$0 \longrightarrow \Gamma^{p^n} \longrightarrow \Gamma \longrightarrow \Gamma_n \longrightarrow 0$$

with $\Gamma_n \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Recall 2.12.1. Every place $v \mid p$ of K_0 above p are either totally ramified or totally unramified. The other (finite?) places of K_0 are unramified. ⊙

What is the basic question/philosophy of Iwasawa theory? We're interested in the behavior of the class group. One historic motivation for this is understanding the p-part of the class group of cyclotomic fields for application to Fermat.

Let $X_n = \mathrm{Cl}_{K_n}[p^\infty] = \mathrm{Cl}_{K_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ be the p-Sylow subgroup of the class group of K_n (K_n unique intermediate field with $\mathrm{Gal}(K_n/K_0) \simeq \Gamma_n$). We will package these together by forming an inverse limit. Recall that there is a norm map

$$X_{n+1} \xrightarrow{\mathrm{Nm}^{K_{n+1}}_{K_n}} X_n,$$

and use these to form $X = \varprojlim_n X_n$.

Note that X_n is a Γ_n-module and the norm maps are equivariant with respect to the natural projection $\Gamma_{n+1} \twoheadrightarrow \Gamma_n$. Thus, the limit X defined above is a module over the Iwasawa algebra $\mathbb{Z}_p[\![\Gamma]\!] = \varprojlim_n \mathbb{Z}_p[\Gamma_n]$.

Iwasawa identified this algebra with something more familiar, and he showed that X has nice finiteness properties as a $\mathbb{Z}_p[\![\Gamma]\!]$-module. One studies the general structure of (nice) modules over this algebra, and uses this knowledge to understand X and extract information at the finite level (i.e. about X_n).

This is what we discussed last time. Where are we going with it today?

2.12.1 Iwasawa algebra

Theorem 2.12.2. *There exists a natural isomorphism of $\mathbb{Z}_p$-algebras*

$$\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![\Gamma]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma_n].$$

Remark 2.12.3. Γ_n is cyclic of order p^n, so $\mathbb{Z}_p[\Gamma_n] \simeq \mathbb{Z}_p[X]/(X^{p^n}-1)$. Hence, $\varprojlim_n \mathbb{Z}_p[\Gamma_n] = \varprojlim_n \mathbb{Z}_p[X]/(X^{p^n}-1)$, but this iso is maybe a bit misleading. The transition map on the RHS is not so simple; it is given by $X \mapsto X^p$, so maybe not so obvious that you still end up with the formal power series ring in the end. ◦

We can actually prove this theorem is slightly more generality once we know a bit of the structure of $\mathbb{Z}_p[\![T]\!]$ (and rings like it).

Theorem 2.12.4. *Let $\mathscr{O}$ be a p-adic complete dvr (i.e. complete dvr which is a $\mathbb{Z}_p$-algebra). Then,*

$$\mathscr{O}[\![T]\!] \xrightarrow{\sim} \mathscr{O}[\![\Gamma]\!].$$

Lemma 2.12.5 (Euclidean algorithm). *Let $f \in \mathscr{O}[\![T]\!]$ and write $f = \sum_{i\geq 0} a_i T^i$ with $a_i \in \mathscr{O}$. Suppose that $a_i \in \mathfrak{m}$ for $i = 0, 1, \dots, n-1$ and $a_n \in \mathscr{O}^\times$. Then, for any $g \in \mathscr{O}[\![T]\!]$, there is a unique $g \in \mathscr{O}[\![T]\!]$ and $r \in \mathscr{O}[T]$ s.t.*

$$g = fq + r$$

and $\deg r \leq n-1$.

Can always put f in this form by scaling

Proof. Omitted. ■

I think this is sometimes called being *n-distinguished*

TODO: Actually add a proof

Definition 2.12.6. A polynomial $P \in \mathscr{O}[T]$ is called **distinguished** of degree n if

$$P = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \text{ with } a_i \in \mathfrak{m}.$$

The **Weierstrass degree** of $f = \sum_{i\geq 0} a_i T^i \in \mathscr{O}[\![T]\!]$ is the minimal (i.e. first) $n \in \mathbb{Z}_{\geq 0}$ such that a_n has minimal valuation (among the coefficients) and is denoted $\deg_W f$ (if no a_i is a unit then $\deg_W f = \infty$). ◇

Theorem 2.12.7 (Weiestass preparation Theorem). *Let $f \in \mathscr{O}[\![T]\!]$. We can uniquely write $f = uP$ where $u \in \mathscr{O}[\![T]\!]^\times$ (i.e. $u(0) \in \mathscr{O}^\times$) and P is a distinguished polynomial of degree $\deg_W f$.*

Proof. Say $n = \deg_W f$. Then we can (uniquely) divide

$$X^n = fq + r \text{ where } \deg r < n.$$

The coefficient of X^n on each side gives

$$1 \equiv a_n q(0) \pmod{\mathfrak{m}}$$

where $f = \sum_{i \geq 0} a_i T^i$ and $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{m}$ since $\deg_w f = n$. Thus, $q \in \mathscr{O}[\![T]\!]^\times$ is a unit, so $f = (X^n - r)q^{-1}$ is in the desired form. ■

Corollary 2.12.8. *Say $f \in \mathbb{Z}_p[\![T]\!]$ so $f(x)$ converges if $x \in \mathbb{C}_p$ with $|x| < 1$. Then, f has only finitely many zeros in $|x| < 1$ ($x \in \mathbb{C}_p$).*

Question: Does it have $\deg_w f$ zeros?

Corollary 2.12.9. *$\mathbb{Z}_p[\![T]\!]$ is a UFD (In fact, it is noetherian and regular local of Krull dimension 2).*

Remember: Any regular local ring is a UFD

Note 5. There will be an optional problem set 11.

Let's finally prove that we have an isomorphism

$$\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![\Gamma]\!] = \varprojlim \mathbb{Z}_p[\Gamma_n].$$

Note that, for fixed n, we have

In turning this group rings in poly algebras, we need to pick a generator in a consistent way. This is possible because we use $1 \in \mathbb{Z}_p = \Gamma \twoheadrightarrow \Gamma_n$

$$\mathbb{Z}_p[\Gamma_n] \simeq \mathbb{Z}_p[X]/(X^{p^n} - 1) \simeq \mathbb{Z}_p[T]/((T+1)^{p^n} - 1)$$

where the last isomorphism comes from setting $X = 1 + T$. Let $P_n(T) = (T+1)^{p^n} - 1$ which is a distinguished polynomial of degree p^n. We then get a map

$$\mathbb{Z}_p[\![T]\!] \overset{\varphi_n}{\twoheadrightarrow} \mathbb{Z}_p[\![T]\!]/(P^n) \simeq \mathbb{Z}_p[T]/(P^n) \simeq \mathbb{Z}_p[\Gamma_n]$$

with the fist iso above more-or-less coming from the Euclidean algorithm.

We claim these φ_n induce an isomorphism $\mathbb{Z}_p[\![T]\!] = \varprojlim \mathbb{Z}_p[\![T]\!]/(P^n)$ and that we have commutative squares

$$\begin{tikzcd}
\mathbb{Z}_p[\![T]\!]/P_{n+1} \arrow[r, "\sim"] \arrow[d] & \mathbb{Z}_p[\Gamma_{n+1}] \arrow[d] \\
\mathbb{Z}_p[\![T]\!]/P_n \arrow[r, "\sim"] & \mathbb{Z}_p[\Gamma_n]
\end{tikzcd}$$

so we have an induced iso $\mathbb{Z}_p[\![T]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![\Gamma]\!]$ as desired.

The first claim is easy. It essentially says that $\bigcap (P_n) = 0$ (this is the kernel of $\mathbb{Z}_p[\![T]\!] \to \varprojlim_n \mathbb{Z}_p[\![T]\!]/(P_n)$). You also need to know the map is surjective. Well, it has dense image and both sides are compact, Hausdorff so it is surjective.

2.12.2 $\mathbb{Z}_p[\![\Gamma]\!]$-modules

Notation 2.12.10. Let $\Lambda = \mathbb{Z}_p[\![T]\!] \simeq \mathbb{Z}_p[\![\Gamma]\!]$ using the specific isomorphism given above. Recall that Λ is a UFD.

Definition 2.12.11. Let M, M' be modules over Λ. We say they are **pseudo-equivalent**, denoted $M \sim M'$, iff there exists $M \xrightarrow{f} M'$ s.t. $\ker f, \operatorname{coker} f$ are finite. ◇

Warning 2.12.12. This is not an equivalence relation. It is not symmetric. •

Example. $\mathfrak{m} = (p, T) \hookrightarrow \Lambda$ is injective with finite cokernel ($= \mathbb{F}_p$), so $\mathfrak{m} \sim \Lambda$. However, $\Lambda \not\sim \mathfrak{m}$.

Lemma 2.12.13. *For any $f \in \Lambda$, $\#\Lambda/(f) = \infty$.*

Reflection of the fact that Λ is two-dimensional

In particular, $\mathfrak{m}$ is not principal. △

Fact. If M, M' are f.g. torsion Λ-modules, then

$$M \sim M' \iff M' \sim M$$

so you do get an equivalence relation on these.

Theorem 2.12.14 (**Classification of f.g. Λ-modules up to psuedo-equivalence**)**.** *Any f.g. Λ-module M is pseudo-equivalent an elementary one:*

$$M \sim \Lambda^r \oplus \bigoplus_{1 \le i \le n} \Lambda/(f_i^{m_i})$$

where f_i are irreducible and $m_i \in \mathbb{Z}_{>0}$. Moreover, (r, f_i, m_i) are unique (up to obvious caveats[26])

Definition 2.12.15. For a f.g. torsion Λ-module M, we can define its **characteristic polynomial**

$$\operatorname{charpoly}(M) = \prod_{i=1}^{n} f_i^{m_i} \in \Lambda.$$

◇

Lemma 2.12.16. *Say $f, g \neq 0$ are coprime (i.e. no common irreducible factor). Then, $\Lambda/(f, g)$ is finite (Hence, $(f, g) \sim \Lambda$).*

Lemma 2.12.17. *If f, g are coprime, then*

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g).$$

This are both torsion, so we also have $\Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$.

Note that Lemma 2.12.16 implies Lemma 2.12.17. Consider the sequence

$$0 \longrightarrow \Lambda/(fg) \longrightarrow \Lambda/(f) \oplus \Lambda/(g) \longrightarrow \Lambda/(f, g) \longrightarrow 0$$

whose cokernel is finite. For the reverse pseudo-equivalence, fix a distinguished polynomial P, prime to f, g, and consider the map

$$\Lambda/(f) \oplus \Lambda/(g) \xrightarrow{\times P^k} \Lambda/(f) \oplus \Lambda/(g).$$

One shows that the image of this map contains $\Lambda/(fg)$ when $k \gg 0$. For some reason, this implies the other direction?

2.13 Lecture 23 (12/2)

Last time we identified the Iwasawa algebra with the power series algebra in one variable. Then, we described the structure of finitely generated $\Lambda \simeq \mathbb{Z}_p[\![T]\!]$-modules M. Any such this is pseudo-equivalent

[26] e.g. reordering or multiplying f_i by a unit

(i.e. there's a map with finite (co)kernel) to

$$M \sim \Lambda^r \oplus \left(\bigoplus_i \Lambda/(f_i^{m_i}) \right)$$

with the f_i irreducible, for some unique $r, \{f_i\}$.

Remark 2.13.1. Here's a heuristic. Recall Λ is regular local of dimesnion 2, and consider $X = \operatorname{Spec}\Lambda$. Consider the Grothendieck group of coherent $\mathscr{O}_X$-modules $\mathscr{F}$. In this group, given $0 \to \mathscr{F}_1 \to \mathscr{F}_2 \to \mathscr{F}_3 \to 0$, one has $\mathscr{F}_2 \sim \mathscr{F}_1 + \mathscr{F}_3$. Given a coherent $\mathscr{F}$, one has

$$\dim \operatorname{supp}(\mathscr{F}) \in \{0, 1, 2\},$$

and in fact $\dim \operatorname{supp} \mathscr{F} = 0 \iff \mathscr{F}$ is supported on the unique closed point (maximal ideal) of the (local) ring Λ. Our pseudo-isomorphism is essentially ignoring the sheaves with 0-dimensional support, we only care about those with 1 or 2-dimensional support. The 2-dimensional case looks like $\mathscr{O}_X^{\oplus r}$ while the 1-dimensional case looks like $\mathscr{O}_X/(f^m)$ with f irreducible (the 0-dimensional case is a skyscraper sheaf at the closed point). ○

If M is torsion (think support at most 1 dimension), then $M \sim \bigoplus_i \Lambda/(f_i^{m_i})$ with f_i irreducible. We define the **characteristic polynomial**

$$\operatorname{charpoly}(M) := \prod f_i^{m_i}.$$

Warning 2.13.2. We do not, in general, have

$$\bigoplus_i \frac{\Lambda}{(f_i^{m_i})} \sim \frac{\Lambda}{\prod f_i^{m_i}}.$$

For example, the f_i may not be coprime (might have $f_i = f_j$ but $m_i \neq m_j$). •

Given a module, how do you know it is finitely generated?

Lemma 2.13.3 (**Nakayama's Lemma**). *Let M be a (topological) Λ-module which is compact (this is the assumption that replace finite generation in the usual Nakayama's lemma). Then,*

(i) *$M = 0 \iff \mathfrak{m}M = M$ (i.e. $M \otimes \Lambda/\mathfrak{m} = 0$)*

(ii) *$M \otimes_\Lambda \Lambda/\mathfrak{m}$ f.g. over $\Lambda/\mathfrak{m}$ (i.e. finite) $\iff$ M f.g. over Λ.*

Let's state one of Iwasawa's big theorems. To do so, we will need some setup. Consider the diagram of field extensions

$$\begin{tikzcd}[arrows=-]
 & & & L_\infty & = & \bigcup_n K_\infty L_n \\
 & & K_\infty L_n \arrow[ur] & & & \\
 & K_\infty L_0 \arrow[ur] & & L_n \arrow[ul] & & \\
 K_\infty \arrow[ur] & & & & & \\
 & K_n \arrow[ul] \arrow[uurr] & & L_0 \arrow[uull] & & \\
 & & K \arrow[ul] \arrow[ur] & & &
\end{tikzcd} \tag{2.1}$$

where K_∞/K is a $\mathbb{Z}_p$-extension, and L_n is the Hilbert class field of K_n ($K_0 = K$). Let

Question: Shouldn't that say $\mathrm{Gal}(L_n/K_n)[p^\infty]$ on the right?

$$X_n = \mathrm{Cl}(K_n) \otimes \mathbb{Z}_p \xrightarrow{\sim} \mathrm{Gal}(L_n/K_n).$$

Answer: I think the real issue is that L_n is not the Hilbert class field, but like the "p-Hilbert class field"

Theorem 2.13.4 (**Iwasawa Theorem**). *There exists some μ, λ, ν such that*

$$\#X_n = p^{\mu p^n + \lambda n + \nu}$$

for all $n \gg 0$ (i.e. $n \geq n_0$ for some finite n_0). That is,

$$\log_p \#X_n = \mu p^n + \lambda n + \nu.$$

Definition 2.13.5. μ above is called the **μ-invariant** for K_∞/K. ◇

How does one prove this? It will follow from the fact that $X = \varprojlim X_n$ is a torsion Λ-module, and so pseudo-isomorphic to $\bigoplus_i \Lambda/f_i^{m_i}$. Hence its characterstic polynomial will be $\mathrm{char}(X) = \prod f_i^{m_i}$. We will prove a "control theorem" saying that $X_n = X \otimes_\Lambda \Lambda/P_n$ where $P_n = (1+T)^{p^n} - 1$ and $n \gg 0$ (recall $\Lambda/P_n \cong \mathbb{Z}_p[T_n]$). It will turn out that

$$\mathrm{char}(X) = \prod f_i^{m_i} = p^\mu \cdot f_X$$

with f_X prime to p, and this μ will be the μ-invariant.

This μ-invariant is actually expected to vanish in many cases.

Conjecture 2.13.6 (Kummer-Vandiver). *$\mu = 0$ for $K(\mu_{p^\infty})^+/K(\mu_p)^+$ (the $+$ here means take the maximal totally real subfield). In this case, the p-part of the class group grows linearly.*

Fun fact: this is allegedly equivalent to $K_{4n}(\mathbb{Z}) = 0$, the algebraic K-theory of the integers vanishing in degrees multiple of 4

Iwasawa theory just gives existence of μ; actually calculating it is a different matter...

So to prove this, we'll need to prove the control theorem and compute

$$X \otimes \Lambda/(P^n)$$

at least for $X = \Lambda/(f^m)$.

Recall that in K_∞/K, all primes away from p are unramified. Some primes above p are unramified and the rest (at least 1) are totally ramified. For simplicity, we make the following assumption.

Assumption. assume there is only one prime above p in $K = K_0$, and that it is totally ramified in K_n for all n.[27]

Under this hypothesis, $K_n \cap L_0 = K$ for all n. The point is that p is totally ramified in one direction, but unramified in the other (recall diagram (2.1). Hence,

$$\mathrm{Gal}(K_\infty L_0/K_\infty) \simeq \mathrm{Gal}(L_0/K) = X_0$$

This allows us to restate the control theorem (under our working assumption).

Theorem 2.13.7 (Control Theorem). *$X_n \xrightarrow{\sim} X \otimes_\Lambda \Lambda/(P_n) = X \otimes_{\mathbb{Z}_p[\Gamma]} \mathbb{Z}_p[\Gamma_n]$ for all n.*

Proof. In fact, it is now enough to prove this only when $n = 0$ (for arbitrary n, just let K_n play the role of K_0!), i.e. we only need show ($P_0 = T$)

$$X_0 \simeq X \otimes_\Lambda \Lambda/T \simeq X/TX.$$

Let $\Gamma = \mathrm{Gal}(K_\infty/K) = \langle\gamma\rangle$ (γ a topological generator). Then we want to prove $X_0 \simeq X/(\gamma-1)X$. How does γ act on X? Let $G = \mathrm{Gal}(L_\infty/K_0)$, and note $X = \mathrm{Gal}(L_\infty/K_\infty)$. We have a short exact sequence

$$0 \longrightarrow X \longrightarrow G \longrightarrow \Gamma \longrightarrow 0,$$

and this exactly induces the action of Γ on X. That is,

$$\gamma \cdot x = \widetilde{\gamma} x \widetilde{\gamma}^{-1} \in X$$

where $\widetilde{\gamma} \in G$ is a lift of $\gamma \in \Gamma$.

This group theoretic thing + the unique prime above p being totally ramified is enough to prove the claim. The key is to characterize L_0 as a subfield of L_∞. It is the maximal abelian, unramified (over K_0, i.e. above p) of L_∞. This tells us that $\mathrm{Gal}(L_\infty/L_0) = \overline{\langle [G,G], I_v : v \mid p\rangle}$ where $I_v \subset G = \mathrm{Gal}(L_\infty/K_0)$ is inertia at v (this is true without our running hypothesis. It just tells us there's only one v among p). We now want to show that

$$\overline{\langle [G,G], I_v : v \mid p\rangle} = (\gamma-1)X.$$

Lemma 2.13.8. $\overline{[G,G]} = (\gamma-1)X$

Proof. Recall the exact sequence $0 \longrightarrow X \longrightarrow G \longrightarrow \Gamma \longrightarrow 0$. Fix some $\widetilde{\gamma} \in G$ lifting γ. Any element of $g \in G$ can be written in the form $g = \widetilde{\gamma}^i x$ where $x \in X$ for some i. Then (recall, X is commutative),

$$\begin{aligned} \widetilde{\gamma}^i x \widetilde{\gamma}^j y x^{-1} \widetilde{\gamma}^{-i} y^{-1} \widetilde{\gamma}^{-j} &= (\widetilde{\gamma}^i x \widetilde{\gamma}^{-i})(\widetilde{\gamma}^{i+j} y x^{-1} \widetilde{\gamma}^{-i-j})(\widetilde{\gamma}^j y^{-1} \widetilde{\gamma}^{-j}) \\ &= (\gamma^i \cdot x) + (\gamma^{i+j} \cdot (y-x)) - (\gamma^j \cdot y) \end{aligned}$$

[27] This will eventually be the case, so can just replace K_0 with some slightly higher K_m

$$= \left[\gamma^i(1-\gamma^j)\cdot x\right] + \left[\gamma^j(\gamma^i - 1)\cdot y\right] \in (\gamma-1)X.$$

This gives $\overline{[G,G]} \subset (\gamma-1)X$ (RHS closed). For reverse inclusion, just set $i=0$ or $j=0$. ■

Back to the control theorem. In our case, we have a unique prime $v \mid p$. Its inertia group $I_v \subset G$ fits into (v totally ramified)

$$I_v \to G \twoheadrightarrow \Gamma (\twoheadrightarrow \Gamma_n)$$

with surjective composition $I_v \twoheadrightarrow \Gamma$. On the other hand, staring at (2.1), one sees that $I_v \cap X = 0$ (so $G = I_v X = X I_v$), so the composition $I_v \hookrightarrow \Gamma$ is also injective, and hence an isomorphism. Now,

$$\frac{G}{\overline{\langle [G,G], I_v\rangle}} \xrightarrow{\sim} \frac{G}{\overline{\langle (\gamma-1)X, I_v\rangle}} \simeq \frac{X}{(\gamma-1)X}$$

with the last isomorphism using $G = I_v X$. This completes the proof of the control theorem. ■

Remark 2.13.9. We didn't mention this explicitly before, but the isomorphisms $X_n \simeq \mathrm{Gal}(L_n)$ are compatible with the transition maps in

$$\varprojlim_n \mathrm{Gal}(L_n/K_n) = \mathrm{Gal}(L_\infty/K_\infty) = X = \varprojlim X_n.$$

This is not completely trivial, but is guaranteed by class field theory. ○

We'll next use Nakayama to see that X is finitely generated over Λ. Control theorem tells us that $X \otimes_\Lambda \Lambda/(p,T) \simeq X_0/p$ which is finite since $X_0 = \mathrm{Cl}(K_0)\otimes \mathbb{Z}_p$ is finite. Hence, X is f.g. We claim it is furthermore torsion. This is because X/TX is finite (again by Control) while $\Lambda/T \cong \mathbb{Z}_p$ which is not finite. Thus,

$$X \sim \bigoplus_i \frac{\Lambda}{f_i^{m_i}}.$$

The last thing to do is to compute

$$M \otimes_\Lambda \Lambda/(P_n) \text{ as } n \to \infty$$

for $M = (\Lambda/f^m)$ with f irreducible. There are two cases...

- $f = p \in \mathbb{Z}_p \subset \mathbb{Z}_p[\![T]\!] \simeq \Lambda$.
- Say $f = T^n + \sum_{i=0}^{n-1} a_i T^i$ is a distinguished polynomial (so $p \mid a_i$ for all i).

Neither case is too hard, but we'll just do the easier one, so assume $f = p$. We want to compute

$$\Lambda/(p^m)\otimes \Lambda/(P^n) = \Lambda/(p^m P_n) \text{ where } P_n = \left((T+1)^{p^n} - 1\right).$$

To make things even easier, assume $m = 1$, so we want

$$\Lambda/(p, P_n) = \mathbb{F}_p[T]/(\overline{P}_n).$$

This is an $\mathbb{F}_p$-vector space of dimension $\deg P_n = p^n$, so $\log_p \#\Lambda/(p,\mathbb{P}_n) = p^n$ contributes to the exponential term. In general, $\log_p \#\Lambda/(p^m, P_n) = p^{nm}$ (probably). This also contributes to the μ-invariant.

In the second case, argue by induction. You'll get a term contributing to the λ-invariant (and to the constant term).

In the remaining two classes, we'll talk about the other side of Iwasawa theory. What we've seen so far has been purely algebraic and gave some statistical behavior for class groups. The next two classes will be about L-functions and the Iwasawa Main conjecture

$$\mathrm{charpoly}(X) \overset{?}{=} \text{“}p\text{-adic } L\text{-function}'' \in \Lambda = \mathbb{Z}_p[\![T]\!] .$$

This is a deeper part of Iwasawa theory. We will not prove this in the last two classes, but will try to give an overview. It was proven, in the generality we'll talk about, by Mazur-Wiles.

2.14 Lecture 24 (12/7): Iwasawa Main Conjecture

This main conjecture is the highlight of classical Iwasawa theory. On the algebraic side, we want to understand class groups and class numbers. On the analytic side, we want to understand L-functions.

Remark 2.14.1 (**Class Number Formula**). Any number field F (e.g. $F = \mathbb{Q}(\mu_n)$) has a **Dedekind zeta function**

relevant notes

$$\zeta_F(s) = \sum_{\mathfrak{a} \subset \mathscr{O}_F} N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} \left(1 - N\mathfrak{p}^{-s}\right)^{-1},$$

where the sum is taken over nonzero ideals and the product over maximal ideals. A priori, this is convergent only when $\mathrm{Re}(s) > 1$; however, like the Riemann zeta function, this has a meromorphic continuation to all $s \in \mathbb{C}$ with a functional equation relating $s \leftrightarrow 1 - s$. This function also encodes arithmetic information about $\mathscr{O}_F$:

- $\mathrm{ord}_{s=0}\, \zeta(s) = \mathrm{rank}_{\mathbb{Z}}\, \mathscr{O}_F^\times = r = r_1 + r_2 - 1$.
- $\zeta_F^{(r)}(0) \sim h_F R_F$ where h_F is the class number, and R_F is the **regulator** $\mathrm{vol}(\mathbb{R}^r / \log \mathscr{O}_F^\times)$ (or something like this). Alternatively (using the functional equation), can express this as the residue at $s = 1$ of ζ_F.

I think this $\sim$ is supressing some relevant factors

$\circ$

Example. When $F = \mathbb{Q}$, $\zeta_{\mathbb{Q}} = \zeta$ is Riemann zeta, and $\zeta(0) = -\frac{1}{2}$.

Say $F = \mathbb{Q}(\sqrt(\Delta))$. If imaginary ($\Delta < 0$), then $\zeta_F(0) \sim h_F$ since $r = 0$. If real ($\Delta > 0$), then $\zeta_F^{(1)}(0) \sim h_F \log \theta_F$ where $\mathscr{O}_F^\times = \pm\theta_F^{\mathbb{Z}}$.

If $F = \mathbb{Q}(\mu_p)$, then $\mathrm{rank}\, \mathscr{O}_F^\times = \frac{p-1}{2} - 1 = r$ (only imaginary embeddings), and $\zeta_F^{(r)}(0) \sim h_F R_F$. $\triangle$

Recall (p odd)

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times \simeq (\mu_{p-1})^\times \times (1 + p\mathbb{Z}_p) \xrightarrow{\sim} \mu_{p-1} \times \mathbb{Z}_p$$

where the iso $(1 + p\mathbb{Z}_p) \xrightarrow{\sim} \mathbb{Z}_p$ is given by $\frac{1}{p}\log_p$ where

$$\log_p(1 + x) = -\sum_{n \geq 1}^{\infty} (-1)^n \frac{x^n}{n}$$

converges for $x \in 1+p\mathbb{Z}_p$. From this, we see that $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) \simeq \mathbb{Z}_p$. Let $X_n = \mathrm{Cl}_{\mathbb{Q}(\mu_{p^n})} \otimes \mathbb{Z}_p$, and let $X = \varprojlim X_n$. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \simeq \mu_{p-1}$ (so $\mathbb{Z}_p^\times \simeq \Delta \times \Gamma$).

We see that Δ acts on X_n, and hence on X. Thus, X is in fact a module over $\mathbb{Z}_p[\![\Gamma \times \Delta]\!] = \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Delta]$ where Λ is the Iwasawa algebra. This is slightly more complicated than usual Iwasawa theory since there's an additional, but not too much more complicated since Δ has order prime to p ($\#\Delta = p-1$), so you can decompose according to eigenspaces of the Δ-action.[28] That is,

$$X = \bigoplus_{\chi \in \widehat{\Delta}} X_\chi \text{ where } \widehat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times).$$

In fact, Teichmuller gives us a map

$$\varepsilon : \Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}_p^\times$$

sending a mod p to the unique $\widetilde{a} \in \mu_{p-1}$ s.t. $\widetilde{a} \equiv a \pmod{p}$. This character $\varepsilon \in \widehat{\Delta}$ generates the whole group, so $X = \bigoplus_i X_{\varepsilon^i}$. Each X_{ε^i} is now a module over $\Lambda \simeq \mathbb{Z}_p[\![\Gamma]\!] \simeq \mathbb{Z}_p[\![T]\!]$.

What are we doing, what's the central question? Notice that the class number formula does not reflect the group action (by Δ). We get a formula of the form

$$\zeta_F^{(r)}(0) \sim h_F R_F$$

which is "absolute." Can we make an equivariant version which reflects the action of $\mathrm{Gal}(F/\mathbb{Q})$ (when $F/\mathbb{Q}$ Galois) on both sides (e.g. makes use of the fact that the Galois group acts on the class group)? Can we decompose both sides according the the Galois action? Iwasawa theory takes care of the right hand side (the class group side), but what about the left?

Say $F/\mathbb{Q}$ is an abelian extension, so $F \subset \mathbb{Q}(\mu_n)$ for some n. Then one has

There's some subtlety with taking into account non-primitive characters that I think we're ignoring here

$$\zeta_{\mathbb{Q}(\mu_n)}(s) = \prod_{\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times} L(s, \chi),$$

where $L(s,\chi) = \sum_{n=1}^\infty \chi(n) n^{-s}$ is a Dirichlet L-series. Similarly, if $G = \mathrm{Gal}(F/\mathbb{Q})$ (so $(\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow G$), then

$$\zeta_F(s) = \prod_{\chi : G \to \mathbb{C}^\times} L(s, \chi).$$

Example. If F is quadratic, then $\zeta_F(s) = \zeta_{\mathbb{Q}}(s) L(s, \eta_{F/\mathbb{Q}})$, where $\eta_{F/\mathbb{Q}} : (\mathbb{Z}/d\mathbb{Z})^\times \to \{\pm 1\}$ is determined by $p \mapsto 1$ if it is split and $p \mapsto -1$ if it is inert. In this case, the class number formula says

$$\begin{cases} L(0, \eta_{F/\mathbb{Q}}) = h_F & \text{if } F = \text{imag} \\ L'(0, \eta_{F/\mathbb{Q}}) = h_F \log \theta_F & \text{if } F = \text{real}. \end{cases}$$

$\triangle$

What about more generally? Say $F/\mathbb{Q}$ abelian with Galois group G. Then, $G \curvearrowright \mathrm{Cl}_F$ as well as on $\mathscr{O}_F^\times$. Then, we have

$$\prod_{\chi : G \to \mathbb{C}^\times} L(s,\chi) = \zeta_F(s) \sim h_F R_F,$$

[28] We're doing (simple) rep theory of Δ over $\Lambda \simeq \mathbb{Z}_p[\![\Gamma]\!]$

so one naturally wonders...

Question 2.14.2. *Can we decompose*

$$\mathrm{Cl}_F = \bigoplus_\chi \mathrm{Cl}_F[\chi] \text{ and } \mathscr{O}_F^\times = \bigoplus_\chi \mathscr{O}_F^\times[\chi]$$

so that $L^{(r_\chi)}(0,\chi) = h_{F,\chi} R_{F,\chi}$ *where* $r_\chi := \operatorname{rank} \mathscr{O}_F^\times[\chi]$ *and also* $\operatorname{rank} \mathscr{O}_F^\times[\chi] = \operatorname{ord}_{s=0} L(s,\chi)$*?*

As stated, the answer is no. It would be hard to get such a decomposition e.g. if $\gcd(\# \mathrm{Cl}_F, \# G) \neq 1$. At least the part of rank equally the order of vanishing of the L-function is a still-open conjecture, the **Stark Conjecture**. He formulated this for Artin L-functions more generally; so far, only the case of abelian extensions of $\mathbb{Q}$ is understood.

Let's return to the Iwasawa setting. Recall we had the decomposition $X = \bigoplus_i X_{\varepsilon^i}$, and each X_{ε^i} is a torsion $\mathbb{Z}_p[\![T]\!]$-module, so

$$X_{\varepsilon^i} \sim \bigoplus_j \Lambda/f_j^{n_j}.$$

We want to connect this to L-functions.

Let's correct our question.

(algebraic side) $\operatorname{charpoly}(X_{\varepsilon^i}) \in \Lambda$

(analytic side) "p-adic L-function" $L_p(s,\varepsilon^i) \in \Lambda$ attached to each character $\varepsilon^i : \Delta \to \mathbb{Z}_p^\times$.

We want to relate these to as a sort of refinement of the class number formula.

Conjecture 2.14.3 (Iwasawa Main Conjecture).

$$\operatorname{charpoly}(X_{\varepsilon^i}) = u L_p(s,\varepsilon^i)$$

for some unit $u \in \Lambda^\times$*, i.e. they generate the same ideal.*

This is actually a theorem now.

What are these p-adic L-functions? We want $L_p(s,\varepsilon^i) \in \Lambda = \mathbb{Z}_p[\![\Gamma]\!] \simeq \mathbb{Z}_p[\![T]\!]$. The '$s$' may be a little confusing; it's really a 'T'. It should somehow "contain" $\{L(0,\chi)\}$ for $\chi : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ (odd) finite order.

Warning 2.14.4. Thinking in terms of the class number formula, the Iwasawa main conjecture seems to be missing a contribution from the regulator. This is the case. It does not actually take into account all characters, but only those which do not contribute to the regulator. These are the "odd" characters satisfying $\chi(-1) = -1$. •

Here's a "1st approximation to $L(s,\varepsilon^i)$." Recall $\mathbb{Z}_p^\times \simeq \Delta \times \Gamma$, so each character $\mathbb{Z}_p^\times \to \mathbb{C}$ can be decomposed as $\chi_0\chi$ where $\chi_0 : \Delta \to \mathbb{C}^\times$ and $\chi : \Gamma \to \mathbb{C}^\times$ of finite order. The first factor χ_0 is kinda minor, so let's just ignore it. We consider

$$\widehat{\Gamma}_{\mathrm{tor}} = \left\{ \begin{matrix} \text{fin order} \\ \text{char of } \Gamma \end{matrix} \right\} \simeq \mu_{p^\infty}$$

as well as $\widehat{\Gamma} = \operatorname{Hom}_{\mathrm{cts}}(\Gamma, \mathbb{C}_p^\times)$, where $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$. These are both (topological) abelian groups.

Lemma 2.14.5.
$$\widehat{\Gamma} \simeq \{x \in \mathbb{C}_p : |x-1| < 1\} = D(1,1),$$
the open unit disk centered at 1*. The isomorphism is given by*
$$\begin{array}{ccc} \widehat{\Gamma} & \longrightarrow & D(1,1) \\ \chi & \longmapsto & \chi(\gamma_0) \end{array}$$
once you fix a generator $\langle \gamma_0 \rangle = \Gamma$.

Remark 2.14.6. Let 1 be a choice of generator for $\mathbb{Z}_p$. Given any $x \in D(1,1)$, we can define
$$\begin{array}{cccc} \chi: & \mathbb{Z}_p & \longrightarrow & \mathbb{C}_p^\times \\ & a & \longmapsto & x^a \end{array}.$$
Write $x = 1+t$ with $|t| < 1$; then to make sense of x^a, we use
$$x^a = (1+t)^a = \sum_{n \geq 0} \binom{a}{n} t^n$$
where
$$\binom{a}{n} = \frac{a(a-1)(a-2)\dots(a-(n-1))}{n!} \in \mathbb{Z}_p.$$
Hence $x^a = \sum_{n\geq 0} \binom{a}{n} t^n$ converges since $|t| < 1$ (so $\lim \left|\binom{a}{n} t^n\right| = \lim |t|^n = 0$). ○

What does this have to do with the Iwasawa algebra. Remember, $\Lambda \simeq \mathbb{Z}_p[\![T]\!]$, so it is in some sense "functions on $\widehat{\Gamma} \simeq D(1,1)$." Given, $f \in \Lambda$, it makes sense to pair/evaluate $f(\chi)$ on $\chi \in \widehat{\Gamma}$.

Theorem 2.14.7. *For i odd, there exists unique $f_i \in \Lambda$ such that*
$$f_i(\chi) = (*)L(0, \chi\varepsilon^i),$$
where we view $\chi\varepsilon^i$ as a character $\mathbb{Z}_p^\times \to \mathbb{C}_p^\times$. Above, $(*)$ is some slight modification.

Warning 2.14.8. In the above theorem, we need to be more careful. First of all, what does it mean to write $L(0, \chi\varepsilon^i)$ when $\chi\varepsilon^i$ is valued in $\mathbb{C}_p$? In general, it does not mean anything, but it can make sense when $\chi \in \widehat{\Gamma}_{\text{tor}}$ is torsion, so $\chi\varepsilon^i$ lands in $\mu_{p^\infty} \times \mu_{p-1}$ (in the background, we fix a field iso $\mathbb{C}_p \simeq \mathbb{C}$). Further, it is a fact that actually $L(0, \chi\varepsilon^i) \in \overline{\mathbb{Q}}$, so we have hope of comparing p-adic and analytic things. •

Remark 2.14.9. The (*) appearing in the theorem is essentially the local Euler factor at p of $L(0, \chi\varepsilon^i)$. This is a technical point, so we don't pay it too much attention. ○

We've specified f_i at some subset of $D(1,1)$, and the claim of the theorem is essentially that we can extend/interpolate this to a function on the whole open disk. That such an extension would be unique is easy, but existence is much harder.

Lemma 2.14.10. *If $f \in \Lambda$ with $f(\chi) = 0$ for all $\chi \in \widehat{\Gamma}_{\text{tor}}$, then $f = 0$.*

Proof. Given a generator $\gamma_0 \in \Lambda$, so $\Lambda \simeq \mathbb{Z}_p[\![T]\!]$ via $\gamma_0 \mapsto (1+T)$. Say $f \in \Lambda$ corresponds to $\widetilde{f} \in \mathbb{Z}_p[\![T]\!]$. Then,

$$f(\chi) = \widetilde{f}(\chi(\gamma_0) - 1).$$

Hence, $\widetilde{f}$ vanishes at $\mu_{p^\infty} - 1 \subset D(0,1)$, so it has infinitely roots in the open unit disk centered at the origin. We have shown previously (Corollary 2.12.8) that any nonzero element of $\mathbb{Z}_p[\![T]\!]$ only has finitely many zeros in this disk, so $\widetilde{f} = 0$. ■

2.15 Lecture 25 (12/9): Last Class

Note 6. I have not watched Monday's lecture yet, so this will be interesting

Assumption. Say p is an odd prime.[29]

"I don't want to talk about the unique even prime number"

We keep the setup from last time. Have $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$ as our $\mathbb{Z}_p$-extension. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. This acts on $X_n = \mathrm{Cl}(\mathbb{Q}(\mu_{p^n})) \otimes \mathbb{Z}_p$ as well as $X = \varprojlim X_n$, so these are modules over $\mathbb{Z}_p[\![\Gamma \times \Delta]\!] = \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\Delta]$. Let

$$\omega : \Delta \to \mu_{p-1} \subset \mathbb{Z}_p^\times$$

be the **Teichemuller character** (spelling). Note that

$$\mathbb{Z}_p[\![\Gamma \times \Delta]\!] \simeq \prod_{\widehat{\Delta}} \mathbb{Z}_p[\![\Gamma]\!]$$

where $\widehat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$ is the group of characters of $\Delta \simeq \mathbb{Z}/p-1\mathbb{Z}$. Hence, we can decompose

$$X = \bigoplus_{\chi \in \widehat{\Delta}} X[\chi],$$

and we only need understand the pieces.

Note that each $\chi \in \widehat{\Delta}$ is of the form $\chi = \omega^i$ for some $i \in \mathbb{Z}/p-1\mathbb{Z}$. Let $f_i = \mathrm{charpoly}(X_i) \in \Lambda \simeq \mathbb{Z}_p[\![T]\!]$; note that this is only well-defined up to units. However, the ideal is generates is well-defined on the nose, and that's what really matters.

Last time we discussed the existence of p-adic L-functions/zeta functions

$$L_p(\omega^i) \in \Lambda = \mathbb{Z}_p[\![T]\!].$$

Unlike f_i, this guy is defined as a power seires on the nose.

Theorem 2.15.1 (**Iwasawa Main Conjecture**, Mazur-Wiles)**.** *For $\omega^i \in \widehat{\Delta}$ with i odd. Then,*

$$L_p(\omega^i) = u \cdot \mathrm{charpoly}(X_i) \in \mathbb{Z}_p[\![T]\!]$$

for some unit $u \in \mathbb{Z}_p[\![T]\!]^\times$.

[29]This is a version of what we talk about for $p = 2$

This was proved circa 1980, and the proof is like 200 pages long. After Kolyvagin's discovery of Euler systems, a simplified proof was found. However, this is still quite a deep statement.

One should really think of this as a family of identifies involving class numbers and special values of L-function, i.e. think of this as a refinement of the class number formula. The LHS involves "$L(0, \chi\omega^i)$" for many χ and the RHS involves class numbers of $\mathbb{Q}(\mu_{p^n})$, taking into account the action by $\Gamma_n \times \Delta$.

Remark 2.15.2. $\widehat{\Gamma} = \mathrm{Hom}_{\mathrm{cts}}(\mathbb{Z}_p, \mathbb{Q}_p) \simeq D(1,1)$ is apparently the units disk centered at 1? Further, $\widehat{\mathbb{Z}_p^\times} \cong \widehat{\Delta} \times \widehat{\Gamma}$. ○

I'm not sure why this remark was made...

2.15.1 p-adic L-function/zeta function

Constructing this roughly involves 3 steps.

- Connect L-values with Bernoulli numbers. For uniquely determining the power series we want, it suffices to specify its value at infinitely many points. This is because we've seen earlier that power series have only finitely many zeros in the unit disc. We'll specify $\zeta(-n) \in \mathbb{Q}$ for integers $n \geq 0$. Recall the usual Riemann zeta function is

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s},$$

so

I think the below (up to next bullet point) is not technically correct as written, but the correct argument should be recoverable from it

$$\begin{aligned}
\Gamma(s)\zeta(s) &= \left(\sum_{n \geq 1} \frac{1}{n^s}\right) \int_0^\infty e^{-t} t^s \frac{\mathrm{d}t}{t} \\
&= \int_0^\infty \left(\sum_{n \geq 1} e^{-tn}\right) t^s \frac{\mathrm{d}t}{t} \\
&= \int_0^\infty \frac{e^{-t}}{1 - e^{-t}} t^s \frac{\mathrm{d}t}{t} \\
&= \int_0^\infty \frac{1}{e^t - t} t^s \frac{\mathrm{d}t}{t}
\end{aligned}$$

What are Bernoulli numbers? They are the B_n defined by

$$f(t) := \frac{t}{e^t - 1} = \sum_{n \geq 0} B_n \frac{t^n}{n!}.$$

From what we did above, one sees that

$$\zeta(-n) = (-1)^n f^{(n)}(0) \text{ for } n \in \mathbb{Z}_{\geq 0}.$$

This is because

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty f(t) t^{s-1} \frac{\mathrm{d}t}{t}.$$

Seems like something is maybe off somewhere, but the point is that $\Gamma(s)$ has a simple pole at $s = -n$, and so calculating the above quantity should only depend on the value of $f(t)$ near $t = 0$.

After cleaning this up, one should conclude that $\zeta(-n) = (-1)^n B_{n+1}/(n+1)$ or something like that. The upshot is that $\zeta(-n)$ is indeed rational.

- The next step is to do p-adic interpolation. We have

$$\mathbb{Z}_{\leq 0} \ni n \mapsto \zeta(-n) \in \mathbb{Q},$$

and we want to interpolate this to a continuous (or even analytic) function $\mathbb{Z}_p \to \mathbb{Q}_p$.

Proposition 2.15.3. *There is a continuous function φ on $\mathbb{Z}_p$ so that*

$$\varphi(-n) = (\textit{simple fudge factor})\zeta(-n)$$

for all $n \geq 1$.

It will be helpful to discuss some measure theory on $\mathbb{Z}_p$ (another interpretation of $\mathbb{Z}_p[\![T]\!]$). Let

$$C(\mathbb{Z}_p, \mathbb{Q}_p) = \{f : \mathbb{Z}_p \to \mathbb{Q}_p \text{ continuous}\}.$$

We give this the L^∞-norm $\|f\| := \sup_{x\in\mathbb{Z}_p} |f(x)|$ (that sup is really a max since $\mathbb{Z}_p$ compact). We also define the valuation

$$v(f) = \min_{x\in\mathbb{Z}_p} v(f(x)).$$

Let $\mathcal{D} = \mathrm{Hom}_{cts}(C(\mathbb{Z}_p, \mathbb{Q}_p), \mathbb{Q}_p)$ be the space of **distributions**. Inside $\mathcal{D}$ is the subset $\mathcal{D}_0 \subset \mathcal{D}$ consisting of **bounded distributions**, which we also call **measures**, i.e. $\mu \in \mathcal{D}_0$ if exists $C > 0$ such that $|\mu(\mathbf{1}_U)|_p \leq C$ for all $U \subset \mathbb{Z}_p$ compact open (enough to have $\left|\mu(\mathbf{1}_{i+p^n\mathbb{Z}_p})\right|_p \leq C$ for all $n \geq 1$ and $i \in \mathbb{Z}/p^n\mathbb{Z}$).

Example.

$$\delta_0(1_U) = \begin{cases} 0 & \text{if } 0 \notin U \\ 1 & \text{if } 0 \in U \end{cases}.$$

We write

$$\int_{\mathbb{Z}_p} f\delta_0 := \delta_0(f) = f(0)$$

where the integral above is just notation. △

Example. The "Haar measure" assigns $\mu(1_{i+p^n\mathbb{Z}_p}) = p^{-n}$. This is not bounded, so it is a p-adic distribution, but not a p-adic measure. △

Theorem 2.15.4 (**Mahler Theorem**). *We have $C(\mathbb{Z}_p, \mathbb{Q}_p) \xrightarrow{\sim} \ell^\infty(\mathbb{Q}_p) := \{(a_n) : v(a_n) \to \infty\}$. Any continuous function can be uniquely expressed in the form*

$$f(x) = \sum_{n\geq 0}^{\infty} a_n \binom{x}{n} \quad \textit{with } a_n \in \mathbb{Q}_p$$

such that $v_p(a_n) \to \infty$ as $n \to \infty$.

I think ℓ^∞ usually denotes bounded sequences, and what we have here is sometimes denoted $\perp_{n\geq 0,0}$ $\mathbb{Q}_p$ or something like that

Note 7. I really messed up in the beginning by putting these notes in an \itemized. Oh well...

2.15.2 Measure on $\mathbb{Z}_p$

This is still part of step 2 from before, but I just had to escape that \itemized.

Let $\mu \in \mathcal{D}_0$ be a p-adic measure. The **Amice transform** is

$$A_\mu := \int_{\mathbb{Z}_p} (1+T)^x \mu(x) = \sum_{n\geq 0} \left(\int_{\mathbb{Z}_p} \binom{x}{n} \mu(x) \right) T^n$$

Recall 2.15.5.

$$\left(\int_{\mathbb{Z}_p} \binom{x}{n} \mu(x) \right)$$

is just notation for evaluating the measure μ on the continuous function $x \mapsto \binom{x}{n} = \frac{x(x-1)\ldots(x-n+1)}{n!}$. ⊙

The Amice transform turns a measure into a power series with bounded coefficients. It gives a bijection

$$\mathcal{D}_0(\mathbb{Z}_p) \xrightarrow{\sim} \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

One can even define a norm on each side so that this becomes an isometry. On the RHS, the valuation of a power series is the minimal valuation of any of its coefficients, I think.

This is our reinterpretation of the Iwaswa algebra. It is more-or-less the algebra of $\mathbb{Q}_p$-valued measures on $\mathbb{Z}_p$.

Theorem 2.15.6. *Given $a \in \mathbb{Z}_p^\times$, there is a measure λ_a such that*

$$\int_{\mathbb{Z}_p} x^n \lambda_a = (-1)^n (1 - a^{n+1}) \zeta(-n)$$

for all $n \geq 1$.

Corollary 2.15.7 (Kummer's congruence). *Let $n_1, n_2 \geq m \geq 1$ be positive integers such that $n_1 \equiv n_2 \pmod{p^{m-1}(p-1)}$. Then,*

$$(1 - a^{n_1+1})\zeta(-n_1) \equiv (1 - a^{n_2+1})\zeta(-n_2) \pmod{p^m}.$$

In some sense, the ζ-values have a lot of redundancy. As a special case, say $m = 1$ and that $n_1 \equiv n_2 \not\equiv -1 \pmod{p-1}$, then we can remove the a-dependency and get

$$\zeta(-n_1) \equiv \zeta(-n_2) \pmod{p}.$$

(we want then not -1 mod $(p-1)$ so the exponent $n_1 + 1$ of a is not divisible by $p-1$, and you can divide).

Proof Sketch of Theorem. The Amice transform of λ_a will be

$$A_{\lambda_a}(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1}.$$

The $1/T$ term (corresponding to $a = 1$) is a little worrisome since we want this to be a power series. However, expanding the right term, it cancels out so indeed $A_{\lambda_a}(T) \in \mathbb{Z}_p[\![T]\!]$, and even one can show

$v(A_{\lambda_a}) = 0$. Now,

$$\begin{aligned}
\int_{\mathbb{Z}_p} x^n \lambda_a &= \left(\frac{\partial}{\partial t}\right)^n \left(\int_{\mathbb{Z}^p} e^{tx}\lambda_a\right)\Bigg|_{t=0} \\
&\overset{T=e^t-1}{=} \left(\frac{\partial}{\partial t}\right)^n A_{\lambda_a}(e^t-1)\Bigg|_{t=0} \\
&= \left(\frac{\partial}{\partial t}\right)^n \left(\frac{1}{e^t-1} - \frac{a}{e^{ta}-1}\right)\Bigg|_{g=0} \\
&= (-1)^n(1-a^{n+1})\zeta(-n).
\end{aligned}$$

■

This is telling you something like you can interpolate the ζ function into a p-adic measure.

2.15.3 Step 3

Do some kind of "Mellin-transform". Let $i \in \mathbb{Z}/(p-1)\mathbb{Z}$ odd.

Unclear if i odd or p odd

Theorem 2.15.8. *There exists unique $\zeta_{p,i}(s)$, an analytic function on $\mathbb{Z}_p$ (when $i = 1$, $(s-1)\zeta_{p,1}(s)$ is analytic), s.t.*

$$\zeta_{p,i}(-n) = (1-p^n)\zeta(-n) \text{ for all } n \equiv -i \pmod{p-1}.$$

This is maybe more appropriately termed a p-adic zeta function.

Theorem 2.15.9 (Maybe continuation of above theorem?)**.** *There exists $f_i \in \Lambda$ s.t. for all $n \geq 1$ with $-n \equiv i \pmod{p-1}$*

$$f_i\left((1+p)^{-n}-1\right) = (blah)\zeta(-n).$$

We can view $(f_i)_i$ as a function on $\widehat{\Gamma} \times \widehat{\Delta} = \mathrm{Hom}_{cts}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times) \supset \mathbb{Z}$. This is or is related to an interpolation of $(1-p^n)\zeta(-n)$. This space $\mathrm{Hom}_{cts}(\mathbb{Z}_p^\times, \mathbb{C}_p^\times)$ is called **weight space**, and the $\mathbb{Z}$ canonically embedded in it consists of "**classical points**." So we want to extend our zeta function from classical points to all of weight space. There is a second type of classical points consisting of torsion points μ_{p^∞}.

The Mazur-Wiles proof follows ideas of Ribet (he proved a sort of first approximation), and their proof uses Eisenstein series, so the theory of modular forms. Their proof techniques can also be used to study the BSD conjecture. For E an elliptic curve, BSD claims its L-function $L(E,s)$ is connected to the rank of $E(\mathbb{Q})$. This is a sort of generalization of the class group, and of the connection between $L(s,\chi)$ and class groups. There's a 300 page proof of a version of Iwasawa Main conjecture for elliptic curves.

3 18.919 (Kan Seminar)

Instructor: Haynes Miller

Course Site: click here

3.1 First Meeting (9/2)

What is the seminar about and how does it work? This is a "literature seminar" in algebraic topology. Assumes basic homotopy theory and tries to go further from a historical point of view. We'll be reading many classic papers. There's a list on the website, but we won't read all, and others can be suggested.

Each participant gives 2 or 3 talks about different papers, depending on the number of people. Right now there are 11 participants (33 papers is a lot, so may do 2 talks for some people or may do 2 talks on same paper by different people or other things). Talks are usually 50 minutes.

In preparation for talks, Haynes will try to meet with each in preparation each week to talk about scheduling and talk topics.

You should read the papers you don't talk about, but of course is less detail. Get good at skimming/reading papers quickly.

Email Miller a reading response before lecture on each paper you don't talk about. What puzzles you? What interests you? What connections you see? Historically, people give practice talks before the official seminar talk; this generally works well and is organized by the participants (i.e. not by Haynes).

"Every good piece of mathematics really deserves to be heard twice."

Between reading papers, giving talks, etc. this class involves quite a time commitment, so keep that in mind.

"I'm teaching graduate students, and I'm teaching freshman this year. They are my two favorite groups of people" (paraphrase)

Apparently, Dan Kan was born in the Netherlands and never really switched off of European time, even after coming to the US.

Might want to subscribe to the MIT topology list and/or attend Monday topology seminar (4:30, I think).

With 11 people in the seminar, seems more likely we do 2 talks each for 22 papers total. This means there will be quite a gap between the two talks you give (like 5 or 6 weeks). During first meeting (likely Friday or next week), you'll pick a first paper.

Haynes recommends looking at construction of Steenrod operations before first talk.

Seems like there will be 2 papers a week, so make sure to allot time to skim them all in advance.

The first few papers are in French. Borel and Serre's French is very simple. Thom's is more complicated French. There is a Russian-made English translation of it available, but parts of it are also difficult to read.

First practice talk Monday (Labor Day) during this time (11:00 am). Cameron talking about Serre.

3.1.1 How I'll organize these notes

Seems like there should be 3 looks at each paper: one skim through on your own, once during the practice talk, and once during the actual talk. I think for each paper, I'll take some light notes when I skim, will

It seems, in practice, taking notes while skimming is more work than I take *no* notes during the practice talk, and then will take more notes during the actual talk.

3.2 Cameron: Cohomologie modulo 2 des complexes d'Eilenberg-Maclane, Serre

The focus in on parts 7 and 8 in section 2.

3.2.1 Skimmed Notes

3.2.2 Talk Notes

Plan of the talk Paper starts with calculation of $\mathrm{H}^*(K(\pi, q); \mathbb{Z}_2)$ where π is abelian of finite type, via induction on q and using Borel's transgresssion theorem. He then discusses Poincaré series, and ends with applications to homotopy groups.

Spectral sequence comparison Good to know the following result.

Theorem 3.2.1 (**Comparison Theorem for Spectral Sequences**). *Let $f : E \to \overline{E}$ be a morphism of 1st quadrant spectral sequences s.t. there exist short exact sequences of the form*

$$0 \longrightarrow E_2^{p,0} \otimes E_2^{0,q} \longrightarrow E_2^{p,q} \longrightarrow \mathrm{Tor}_1(E_2^{p+1,0}, E_2^{0,q}) \longrightarrow 0$$

and the same for $\overline{E}$. Then, any two of the following imply the third.

- $f_2^{p,0} : E_2^{p,0} \xrightarrow{\sim} \overline{E}_2^{p,0}$ *for all $p \geq 0$ ("iso on base")*
- $f_2^{0,q} : E_2^{0,q} \xrightarrow{\sim} \overline{E}_2^{0,q}$ *for all $q \geq 0$ ("iso on fiber")*
- $f_\infty^{p,q} : E_\infty^{p,q} \xrightarrow{\sim} \overline{E}_\infty^{p,q}$ *for all $p, q \geq 0$ ("iso on total space")*

Proof. See MacLane's book "Homology" (pp 355–57), or McCleary "User's guide to spectral sequences" (sect 3.3). ■

Remark 3.2.2. For the Serre spectral sequence, the desired short exact sequences are just the universal coefficients theorem. ○

Remark 3.2.3. This theorem is dealing with additive structure. Even when your spectral sequences have multiplicative structure, you can apply this theorem to a map f not preserving this structure. ○

Borel's Transgression theorem

Definition 3.2.4. For X a space and $A = \mathrm{H}^*(X; \mathbb{Z}_2)$, a **simple system of generators** for A is a family (x_i) such that each x_i is homogeneous, and the products

$$x_{i_1} \cdot \dots \cdot x_{i_r} \text{ with } i_1 < i_2 < \dots < i_r$$

(and $r > 0$) form an additive basis for A. ⋄

Example. Generators for an exterior algebra work. △

Definition 3.2.5. A **transgression** is a differential $d_n : E_n^{0,n-1} \to E_n^{n,0}$ going all the way from the fiber to the base. We may denote this as τ. ◇

See 18.906 notes for some facts/results about/on transgressions.

Theorem 3.2.6 (Transgression). *Let $F \to E \to B$ be a fibration with path-connected base such that $E_2 = \mathrm{H}^*(B;\mathbb{Z}_2) \otimes \mathrm{H}^*(F;\mathbb{Z}_2)$, $\mathrm{H}^i(E;\mathbb{Z}_2) = 0$ for all $i > 0$, and $\mathrm{H}^*(F;\mathbb{Z}_2)$ has a simple system of transgressive generators (x_i). Then if $y_i = \tau(x_i)$, we get that*

$$\mathrm{H}^*(B;\mathbb{Z}_2) = \mathbb{Z}_2[y_1, \dots, y_m].$$

Remark 3.2.7. The transgression is not a function (on $\mathrm{H}^*(F;\mathbb{Z}_2)$, but a relation. The y_i's above are not well-defined, but exist in some coset. The theorem says that any choice of representative will get a polynomial basis. In Serre's application, we'll choose particular, well-defined y_i's though. ○

Proof Sketch.
- Define an **elementary spectral algebra of degree** s, called $E(s)$, to be such that $E(s)_2 := F(s) \otimes B(s)$, where $F(s) := \bigwedge(\eta)$ where $|\eta| = s$ and $B(s) := \mathbb{Z}_2[\zeta]$ where $|\zeta| = s+1$. This looks like

$$\begin{array}{c|cccc}
s & \eta & \eta\zeta & & \\
\vdots & & & & \\
0 & 1 & & \zeta & \zeta^2 \\
\hline
 & 0 & \dots & s+1 &
\end{array}$$

  with $\tau(\eta) = \zeta$. One can use Liebniz to calculate $\tau(\eta\zeta) = \tau(\eta)\zeta + \eta\tau(\zeta) = \eta^2 + 0$, and so one. In particular, these transgressions are isomorphisms so the E_∞-page has a 1 (generator of $\mathbb{Z}_2$) in the lower left, and is 0 everywhere else.

- Create a candidate spectral sequence $\overline{E} = E(s_1) \otimes \cdots \otimes E(s_n)$ for $s_i = |x_i|$ and see that $\overline{F} = \Lambda(\eta_1, \dots, \eta_n)$, $\overline{B} = \mathbb{Z}_2[\zeta_1, \dots, \zeta_n]$. This is what we want, so you now want to use comparison theorem. Define a map $f : E \to \overline{E}$ sending $x_i \mapsto \eta_i$ and $y_i \mapsto \zeta_i$.

- The comparison theorem applies since we have (additive) isomorphisms on the total space and on the fiber. This gives $\overline{B} \cong B$. After checking that f is an algebra map on the base, this gives $\mathrm{H}^*(B;\mathbb{Z}_2) \simeq \mathbb{Z}_2[y_1, \dots, y_n]$ as desired.

■

Serre's induction We look at $\mathrm{H}^*(\mathbb{Z}_2; q, \mathbb{Z}_2) := \mathrm{H}^*(K(\mathbb{Z}_2, q); \mathbb{Z}_2)$.

Theorem 3.2.8 (Serre). *Let $u_q \in \mathrm{H}^q(\mathbb{Z}_2; q, \mathbb{Z}_2)$ be the generator coming from Hurewicz + UCT. Then,*

$$\mathrm{H}^*(\mathbb{Z}_2; q, \mathbb{Z}_2) = \mathbb{Z}_2\left[\left\{\mathrm{Sq}^I u_q \mid I \textit{ admissible and } e(I) < q\right\}\right].$$

Recall 3.2.9. A sequence $I = \{0, \dots, i_n\}$ is **admissible** if $i_1 \geq 2i_2, \dots, i_{n-1} \geq 2i_n$. The **excess** of I is $e(I) = i_n + \sum_{j=1}^{n-1}(i_j - 2i_{j+1})$. ⊙

Proof Sketch. Induct on q. When $q = 1$, $K(\mathbb{Z}_2, 1) \simeq \mathbb{RP}^\infty$ has $\mathrm{H}^*(\mathbb{RP}^\infty;\mathbb{Z}_2) = \mathbb{Z}_2[u_1]$ so we're good.

We'll do an example of the inductive step, going from $q = 1$ to $q = 2$. Have the path space fibration

$$\mathbb{RP}^\infty \longrightarrow * \longrightarrow X := K(\mathbb{Z}_2, 2).$$

The Serre spectral sequence is $E_2^{p,q} = \mathrm{H}^p(X; \mathrm{H}^q(\Omega X)) \implies \mathrm{H}^{p+q}(*)$. E_2-page looks like

$$\begin{array}{c|ccc}
2 & u_2 & & \\
1 & u_1 & & \\
0 & pt & ? & ? \\
\hline
 & 0 & 1 & 2
\end{array}$$

and the E_∞-page looks like

$$\begin{array}{c|ccc}
2 & 0 & 0 & \\
1 & 0 & 0 & \\
0 & pt & 0 & 0 \\
\hline
 & 0 & 1 & 2
\end{array}$$

We know $d_2(u_1) = u_2$ since they have to die in the E_∞-page. We can use this to calculate $d_2(u_1^2) = d_2(u_1)u_2 + u_1 d_2(u_1) = 2u_1u_2 = 0 \in \mathbb{Z}_2$. Similarly,

$$d_2(u_1^{2n}) = 0 \text{ and } d_2(u_1^{2n+1}) = u_1^{2n}u_2.$$

Picture now looks like

TODO: Fix these pictures

$$\begin{array}{c|ccc}
2 & u_2 & & \\
1 & u_1 & & \\
0 & pt & ? & ? \\
\hline
 & 0 & 1 & 2
\end{array}$$

What about on the E_3-page? Recalling that Sq^I commutes with τ (ultimately because τ comes from coboundary map), we calculate

$$d_3(u_1^2) = d_3(\mathrm{Sp}^1(u_1)) = \mathrm{Sp}^1(d_2(u_1)) = \mathrm{Sp}^1 u_2.$$

So on E_3-page, things that are $2 \pmod 4$ don't die while things that are $0 \pmod 4$ do die (recall that all odd exponents died on the E_2-page).

Note that the fiber has a simple system given by the 2^ith powers of u_1 (express everything else in binary). Hence, the Transgression Theorem will give

$$\mathrm{H}^*(\mathbb{Z}_2; 2, \mathbb{Z}_2) = \mathbb{Z}_2\left[\left\{\tau(u_1^{2^n}) \mid n \geq 0\right\}\right].$$

It still remains to compute these transgressions $\tau(u_1^{2^n})$ and check against the $\mathrm{Sq}^I(u_2)$'s. We saw above that $\tau(u_1) = u_2$, $\tau(u_1^2) = \mathrm{Sq}^1 u_2$. One can induct to show in general that

$$\tau(u_1^{2^n}) = \mathrm{Sp}^{2^{k-1}} \circ \cdots \circ \mathrm{Sq}^2 \mathrm{Sq}^1 u_2.$$

Finally, one checks these are the only admissible sequences of excess < 2. This finishes the first inductive step. ■

Applications Serre calculates the Poincaré series

$$\vartheta(\pi; q, t) := \sum_{n=0}^{\infty} \dim(\mathrm{H}^n(\pi; q, \mathbb{Z}_2))t^n.$$

Better to instead modify these to functions $\varphi(x)$ to compare growth rates (See Serre sect. 3 for details).

Theorem 3.2.10 (Serre)**.** *Let X be path connected and simply connected. Assume*

- $\mathrm{H}_i(X; \mathbb{Z})$ *is abelian of finite type for all $i > 0$.*
- $\mathrm{H}_i(X; \mathbb{Z}_2) = 0$ *for $i \gg 0$.*
- $\mathrm{H}_i(X; \mathbb{Z}_2) \neq 0$ *for at least one $i \neq 0$.*

Then, $\pi_i(X)$ contains a subgroup isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_2$ for infinitely many i's.

Proof Idea. Use contradiction, so suppose there's a maximum q such that $\pi_q(X) \otimes \mathbb{Z}_2 \neq 0$. Get a fibration of Whitehead towers on X, and use facts about growth rates of their cohomologies to get a contradiction.

End up looking at a fibration

Potentially this is the wrong fibration

$$K(\pi_{q-1}(X), q-2) \longrightarrow (X, q) \longrightarrow (X, q-1)$$

giving

Serre allegedly proves some result relating Poincare series for (X, q) to one for $\vartheta(\pi; q, t)$

$$\vartheta(\pi; q, t) < \vartheta(\pi; q-1, t)\vartheta(\pi_{q-1}(X); q-2, t).$$

(RHS is E_2-page and LHS is E_∞-page. Get to latter from former by taking homology, so dimensions decrease, giving above). After plugging in growth rates from section 3, get a contradiction. ■

3.3 Jiakai: La cohomologie mod 2 de certains espace homogènes, Borel

The focus is on sections $4, 5, 7, 10$.

3.3.1 Skimmed Notes

Introduction We want to study the mod 2 cohomology of certain homogeneous spaces or principal G-bundles for G an orthogonal group. So we'll use classifying spaces, spectral sequences, and the like.

One knows that the Steifel manifold $V_{n+1+k,n}$ of n-frames (ordered, orthonormal collctections of n vectors) in $\mathbb{R}^{n+1+k}$ is a universal space $E(k, O(n))$. Its base, a $B(k, O(n))$ is given by the grammannian $G_{n+1+k,n}$ for n-dimensional subspaces of $\mathbb{R}^{n+1+k}$. Hence, studying $\mathrm{H}^*(B_{O(n)}; \mathbb{Z}_2)$ up to k corresponds to studying $\mathrm{H}^*(G_{n+1+k,n}; \mathbb{Z}_2)$ up to k; for this, once can use the cellular decomposition of the grassmannian.

Notation 3.3.1. We'll let $Q(n) \subset O(n)$ denote the subgroup of (orthogonal) diagonal matrices.

Note that $Q(n) \cong (\mathbb{Z}_2)^n$, and so $B_{Q(n)} \simeq (\mathbb{RP}^\infty)^n$. Hence,

$$\mathrm{H}^*(B_{Q(n)}; \mathbb{Z}_2) \cong \mathbb{Z}_2[x_1, \ldots, x_n]$$

with x_i in degree 1. In section 5, we will show that the map

$$\mathrm{H}^*(B_{O(n)};\mathbb{Z}_2) \to \mathrm{H}^*(B_{Q(n)};\mathbb{Z}_2),$$

induced by the inclusion $Q(n) \subset O(n)$, is injective sending the ith Stiefel-Whitney class w^i to the ith elementary symmetric polynomial in $x_1, \dots, x_n$. To show this, we'll study the cohomology of the homogeneous space $O(n)/Q(n)$ in section 4.

Notation 3.3.2. We let $\rho^*(H,G)$ denote the homomorphism $\mathrm{H}^*(B_G;\mathbb{Z}_2) \to \mathrm{H}^*(B_H;\mathbb{Z}_2)$ induced by the inclusion $H \subset G$ of topological groups.

Sect 4: Cohomologie de F_n We want to study the homomorphism $\rho^*(Q(n), O(n))$, and this is "the transpose of the projection in the fibration"

$$F_n \hookrightarrow BQ(n) \twoheadrightarrow BO(n)$$

and this motivates studying $F_n = O(n)/Q(n) = \mathrm{SO}(n)/SQ(n)$.

Lemma 3.3.3. *The dimension of $\mathrm{H}^1(F_n)$ is $\geq n-1$ (for $n \geq 2$).*

Proof sketch. Look at the spectral sequence for $F_n \hookrightarrow BSQ(n) \twoheadrightarrow BSO(n)$. ∎

Proposition 3.3.4. *$\mathrm{H}^*(F_n)$ is generated by elements in degree ≤ 1 and it's Poincaré series is*

$$P(F_n, t) = (1-t^2)(1-t^3)\dots(1-t^n)(1-t)^{1-n}$$

for $n \geq 2$.

Proof Sketch. Induct on n. When $n = 2$, $F_2 = \mathrm{SO}(2)/\mathbb{Z}_2$ is a circle, so the proposition holds. In the inductive step, use the fibration

$$O(n-1)/Q(n-1) \hookrightarrow O(n)/Q(n) \twoheadrightarrow O(n)/(\mathbb{Z}_2 \times O(n-1))$$

where $O(n)/\mathbb{Z}_2 \times O(n-1) \cong \mathbb{RP}^{n-1}$. Hence, the above looks like

$$F_{n-1} \hookrightarrow F_n \twoheadrightarrow \mathbb{RP}^{n-1}\,.$$

Analyze the Serre spectral sequence. ∎

Corollary 3.3.5. *$\mathrm{H}^*(\mathrm{SO}(n)/SQ(n))$ is equal to its "characteristic subalgebra". The Poincaré series of $\mathrm{H}^*(B_{\mathrm{SO}(n)})$ is*

$$P(B_{\mathrm{SO}(n)}, t) = (1-t^2)^{-1}(1-t^3)^{-1}\cdots(1-t^n)^{-1}\,.$$

Question: What is that?

Answer: See talk notes for a definiton

Sect 5: Cohomologie de $B_{O(n)}$; classes caractéristiques réduites One knows that the first cohomology groups (mod 2) of the Steifel variety $V_{n,n-i} = O(n)/O(i)$ are given by

$$\mathrm{H}^j(V_{n,n-i}) = 0 \text{ for } j < i \text{ and } \mathrm{H}^i(V_{n,n-i}) = \mathbb{Z}_2.$$

Lemma 3.3.6. *The degree $i+1$ Stiefel-Whitney class of $B_{O(n)}$, denoted w^{i+1}, is the unique nonzero element of degree $i+1$ in the kernel of $\rho^*(O(i), O(n)) : \mathrm{H}(B_{O(n)}) \to \mathrm{H}(B_{O(i)})$.*

Above, $B_{O(n)}$ can be taken to be a classifying space for any sufficiently large dimension, e.g. $> n$.

Theorem 3.3.7. *The map $\rho^*(Q(n), O(n))$ from $H(B_{O(n)})$ to $H(B_{Q(n)}) = \mathbb{Z}_2[x_1, \ldots, x_n]$ ($Dx_i = 1$) is injective with image the algebra of symmetric functions in $x_1, \ldots, x_n$. It sends w^i to the ith elementary symmetric function $\sigma^i = \sigma^i(x_1, \ldots, x_n)$.*

Sect 7: Les i-carrés des classes caractéristiques réduites Recall that w^j denotes the characteristic classes of $H(B_{O(n)})$, and in particular that $w^j = 0$ if $j > n$.

Theorem 3.3.8. *One has*

$$\mathrm{Sq}^i w^j = \sum_{0 \le t \le i} \binom{j-i+t-1}{t} w^{i-t} w^{j+t}.$$

Sect 10: Remarques générales

3.3.2 Talk Notes

Note 8. Internet being extremely spotty, so may miss more than usual. Already missed interesting stories about Borel and Serre when they were learning spectral sequences...

Notation 3.3.9.

Definition 3.3.10. Let $G \to E \to B$ be a principal bundle. E is pulled back from a map $\sigma : B \to B_G$ which induces the **characteristic homomorphism**

$$\sigma^* : \mathrm{H}^*(B_G, \Gamma) \to \mathrm{H}^*(B, \Gamma).$$

The image is the **characteristic subalgebra**. The characteristic subalgebgra of the cohomology $\mathrm{H}^*(G/H)$ is that of the fibration $H \to G \to G/H$. ◇

Proposition 3.3.11. $\mathrm{H}^*(G/H)$ *is equal to its characteristic subalgebra iff the fiber of $G/H \to B_H \to B_G$ is totally non-homologous to zero in* $\mathrm{H}^*(B_H)$.

Note $B_H = E_G/H$ and $B_G = E_G/G$.

Definition 3.3.12. The fiber is **totally non-homologous to zero** if the induced map $\mathrm{H}^*(B_H) \to \mathrm{H}^*(G/H)$ is surjective. ◇

Remark 3.3.13. This definition (because of finite type assumptions) is the same as the homology of the fiber injecting into the homology of the total space, so nothing becomes non-homologous. ○

Theorem 3.3.14 (Leray-Hirsch). *Let $F \to E \to B$ be a fibration (with B path-connected) and K a field. Then, the spectral sequence associated to $F \to E \to B$ collapses at E_2 iff F is totally non-homologous to zero. In this case, $\rho^* : \mathrm{H}(B) \to \mathrm{H}(E)$ is injective, and $\iota^* : \mathrm{H}(E) \to \mathrm{H}(F)$ identifies* $\mathrm{H}^*(F) \cong \mathrm{H}^*(E)/(\operatorname{im} \rho^*)^{>0}$.

Proposition 3.3.15. *Let $F \to E \to B$ be a fibration with B locally connected and F connected. Then F is totally nonhomologous to zero (over K) iff $P_K(E,t) = P_K(B,t)P_K(F,t)$. In either case, the local coefficients system is automatically trivial.*

Lemma 3.3.16. *Let $F_n = O(n)/Q(n) = \mathrm{SO}(n)/SQ(n)$. Then,* $\dim \mathrm{H}^1(F_n) \geq n-1$.

Proof. Look at $F_n \to B_{SO(n)} \to B_{SQ(n)}$. Since $B_{SO(n)}$ is imply connected, we see $E_2 = \mathrm{H}^*(B_{SO(n)}) \otimes \mathrm{H}^*(F_n)$. Hence,

$$n-1 = \dim \mathrm{H}^1(B_{SQ(n)}) = \dim^1 E_\infty \leq \dim^1 E_2 = \dim E_2^{0,1} + \dim E_2^{1,0} = \dim \mathrm{H}^1(F_n).$$

■

Theorem 3.3.17. $P(F_n,t) = (1+t)(1+t+t^2)\dots(1+t+\dots+t^{n-1})$ *and* $\mathrm{H}^*(F_n)$ *is generated by eleemnts of degree* ≤ 1.

Remark 3.3.18. Recall that any orthogonal transformation is given by a product of reflections, and a choice of hyperplane is a choice of reflection which is a degree 1 thing. ○

Proof. Induct. When $n=2$, $F_n = S^1$ and we win. So assume claim for $n-1$. Get fibration

$$F_{n-1} \longrightarrow F_n \longrightarrow \frac{O(n)}{\mathbb{Z}_2 \times O(n-1)} = \mathbb{RP}^{n-1}.$$

We want to show that the Serre spectral sequence collapses at E_2 so that F_n is, as far as cohomoogy is concerned, a product of projective spaces. Note that

$$n-1 \geq \dim^1 E_2 \geq \dim^1 E_\infty = \dim \mathrm{H}^1(F_n) \geq n-1,$$

so

$$n-1 = \dim^1 E_2 = \dim E_2^{1,0} + \dim E_2^{0,1} = \dim \mathrm{H}^1(\mathbb{P}^{n-1}) + \dim \mathrm{H}^0(\mathbb{P}^{n-1}; \mathrm{H}^1(F_{n-1}))$$

where $\dim \mathrm{H}^0(\mathbb{P}^{n-1}; \mathrm{H}^1(F_{n-1})) = \dim \mathrm{H}^1(F_{n-1})^{\pi_1(\mathbb{P}^{n-1})}$. Hence, everything is fixed by π_1. Since the image of $\iota^* : \mathrm{H}^q(F_n) \to \mathrm{H}^q(F_{n-1})$ is identified with $E_\infty^{0,q}$, we see that this image contains $\mathrm{H}^1(F_{n-1})$ and, by hypothesis that deg ≤ 1 elements generate all of $\mathrm{H}^*(F_{n-1})$.

Something something, use Leray-Hirsch to write $E_\infty = E_2$ page as a tensor product. Both factors are generated in degree ≤ 1, so their product is too, and we win. ■

To study cohomology of $B_{O(n)}$, we look at various maps between classifying spaces. First, we have $O(m) \hookrightarrow O(n)$ (when $m < n$) by inserting into lower diagonal block.

Notation 3.3.19.

$$\rho^*(H,G) : \mathrm{H}^*(B_G) \to \mathrm{H}^*(B_H).$$

Our first goal is showing Stiefel-Whitney classes are symmetric polynomials in the cohomology generators of $B_{Q(n)}$. To do this, we make use of the following convenient definition/proposition of Stiefel-Whitney classes.

Definition 3.3.20. The ith **Stiefel-Whitney class** w_i is the unique nonzero element of degree i in the kernel of $\rho^*(O(i-1), O(n))$. ◇

Let's describe the map $\rho^*(Q(i), Q(n))$ more carefully. Can set things up so that

$$E_{Q(n)}/Q(i) = S^\infty \times \ldots \times S^\infty \times \mathbb{P}^\infty \times \ldots \times \mathbb{P}^\infty$$

with $(n-i)$ factors of S^∞ and i factors of $\mathbb{P}^\infty$.

He had much more written down, but I didn't really follow...

Theorem 3.3.21.

$$\rho(Q(n), O(n)) : \mathrm{H}^*(B_{O(n)}) \xrightarrow{\sim} \mathrm{H}^*(B_{Q(n)})^{\Sigma_n}.$$

Maybe Jiakai will share his notes...

A while later, get result of Steenrod squares of SW classes.

$$\mathrm{Sq}^i w_j = \sum_{0 \le t \le i} \binom{j-i+t-1}{t} w_{i-t} w_{j+t}.$$

The proof is combinatorial, using that SW classes are symmetric polynomials and the Cartan formula for Steenrod squares.

Talks ends with flag varieties. There are analogies between maximal tori and maximal subgroups of type $(2, \ldots, 2)$ (i.e. of the form $(\mathbb{Z}_2)^n$).

Let G be a Lie group and $Q(n)$ the maximal abelian subgroup of form $\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$. These are always conjugate when $G = O(n)$, but not so in general. This causes some general. The classical theorem is that $\mathrm{H}^*(BG; \mathbb{Q})$ is precisely $\mathrm{H}^*(BT; \mathbb{Q})^{W_G}$ where W_G is the Weyl group; Borel has proven the analogue mod 2 for $O(n)$ (but this needed $O(n)$ being special).

History (Miller)**.** The number of generators for cohomology of G over $\mathbb{Q}$ is equal to its rank (i.e. rank of its maximal torus). One can hope that the same is true for mod 2 cohomology where rank is replaced by 2-rank (i.e. rank of maximal abelian subgroup of type $(2, 2, \ldots, 2)$). This was proved by Quillen (using equivariant techniques?)

See Jae's second talk

Can compute Poincaré polynomial of $\mathrm{H}^*(G/U)$. We say that $\mathrm{H}^*(G/U)$ satisfies the **Hirsch formula mod 2** if

$$P(G/U, t) = \frac{(1-t^{m-1})(1-t^{m-2}) \ldots (1-t^{m_n})}{(1-t^{q_1})(1-t^{q_2}) \ldots (1-t^{q_n})}$$

where $m_1, \ldots, m_n$ and $q_1, \ldots, q_n$ are degrees of generators of $\mathrm{H}^*(B_G)$ and $\mathrm{H}^*(B_U)$.

More stuff I missed..

Theorem 3.3.22.

$$\rho^*(O(n_1) \times \ldots \times O(n_k), O(n))$$

is injective, and $\mathrm{H}^*(G(n_1, \ldots, n_k))$ *is equal to its characteristic subalgebra.*

$$\mathrm{H}^*(G(n_1, \ldots, n_k)) \cong \mathrm{H}^*(B_{O(n_1) \times \ldots \times O(n_k)})/(\operatorname{im} \rho^*)^{>0} \cong \mathbb{Z}_2[w_1^{(1)}, \ldots, w_{n_1}^{(1)}] \otimes \cdots \otimes \mathbb{Z}_2[w_1^{(k)}, \ldots, w_{n_k}^{(k)}]/(1 = w^{(1)} \ldots w^{(k)}).$$

with Poincare series

$$P(G(n_1, \ldots, n_k), t) = \frac{(1-t)(1-t^2) \ldots (1-t^{n-1})(1-t^n)}{\prod_{i=1}^k (1-t)(1-t^2) \ldots (1-t^{n_i})}$$

Above, in paticular applies to Grassmianians $G_{m,n} = G(n, m-n)$.

3.4 Deeparaj: A topological proof of Bott periodicity, Dyer-Lashof

3.4.1 Talk Notes

The goal is

Theorem 3.4.1 (**Bott Periodicity**)**.** *Let $U = \varinjlim U(n)$. Then, $\Omega U \simeq \mathbb{Z} \times BU$.*

Here are some consequences.

Corollary 3.4.2. *$\pi_i(U) = \pi_{i+2}(U)$, $\pi_0(U) = 0$, and $\pi_1(U) = \mathbb{Z}$, so we know all homotopy groups of U.*

Corollary 3.4.3. *$K(X) := [X^+, \mathbb{Z} \times BU]_*$ gives a cohomology theory.*

Corollary 3.4.4. *BU is an ∞-loop space.*

Remark 3.4.5. $BU = \Omega^n X_n$ where X_n should be some highly connected cover of BU. $\circ$

How will we prove this? Note that $\mathrm{SU}(n) \subset U(n)$ is compatible with the inclusions $U(n) \subset U(n+1)$ and $\mathrm{SU}(n) \subset \mathrm{SU}(n+1)$. Hence, in the limit we get $\mathrm{SU} \subset U$. Furthermore, at the finite level, $U(n) \cong S^1 \times \mathrm{SU}(n)$ via a choice of splitting of

$$0 \longrightarrow \mathrm{SU}(n) \longrightarrow U(n) \xrightarrow{\det} S^1 \longrightarrow 0.$$

Hence, $U \cong S^1 \times SU$, so $\Omega U \simeq \mathbb{Z} \times \Omega SU$, and Bott Periodicity is equivalent to $\Omega SU \simeq BU$.

This is what we will show. We will find a map $BU \to \Omega SU$, and then show that it is a weak equivalence.

Motivation from Morse Theory $E : \Omega SU(2n)[I; -I] \to \mathbb{R}$ given by $E(\gamma) = \int_I |\gamma'|^2 \, dt$ is a Morse-Bott map. By Magic, this gives $\Omega\,\mathrm{SU}(2n)[I; -I] = \mathrm{Gr}_n(2n) \cup \{\text{cells of higher dimension}\}$. The upshot is you get a map $\varphi_n : \mathrm{Gr}_n(2n) \to \Omega\,\mathrm{SO}(2n)$ which is $2n+1$ connected. Taking colimits, gets us a map $\varphi : BU \to \Omega SO$ which is a weak equiv because of connectectivity.

Remark 3.4.6. $\mathrm{Gr}_n(2n) = U(2n)/(U(n) \times U(n))$. $\circ$

Proof without Morse Theory We first want an H-space structure on BU and on U.

Lemma 3.4.7. *Let $f : X \to Y$ be an H-map between H-spaces. Then, $H_*(f)$ an iso implies that f is a weak equivalence.*

Intuition. The H-space structure $X \times X \to X$ shows that $\pi_1(X)$ acts trivially on $\pi_i(X)$. The H-space action $X \times M(f) \to M(f)$ should mean that the local system in above situation in trivial (think proof of Hurewicz via Serre spectral sequence).

Now, recall $U(n) \curvearrowright \mathbb{C}^n \subset \mathbb{C}^\infty = \bigoplus_{i=1}^\infty \mathbb{C} e_i$ (not a Hilbert space). Note that $\mathbb{C}^\infty \oplus \mathbb{C}^\infty \xrightarrow{\sim} \mathbb{C}^\infty$ via $e_i \mapsto e_{2i}$ and $\widetilde{e}_j \mapsto e_{2j-1}$. This gives a map $U(n) \times U(m) \to U(n+m)$ which "interweaves rows". Thinking of BU as $\varinjlim U(2n)/(U(n) \times U(n))$, we get $BU \times BU \to BU$ as desired. From the moduli perspective, this induces the map $[X, BU] \times [X, BU] \to [X, BU]$ given by addition of (stable) vector bundles (in particular, the H-space structure is homotopy commutative).

From this moduli perspective, we see that the identity of the map is given by the trivial bundle $\mathbf{1} = [\mathbb{C}]$ and also we know that if $E \oplus F \cong \underline{\mathbb{C}}^r$, then $-[E] = [F]$.

Note that the maps $U(n) \times U(m) \to U(n+m)$ also give an H-space structure $U \times U \to U$ on U. This (we will see) is also homotopy commutative.

We want to show φ induces an isomorphism on homology, so what is $\mathrm{H}_*(BU)$?

Remark 3.4.8. If X is an H-space, then $\mathrm{H}_*(X)$ is a ring. In particular, given $X \times X \to X$, this induces $\mathrm{H}_*(X \times X) \to \mathrm{H}_*(X)$. Composing this with the Künneth map (which may not be an isomorphism) $\mathrm{H}_*(X) \otimes \mathrm{H}_*(X) \to \mathrm{H}_*(X \times X)$, we get our multiplication. ○

Theorem 3.4.9. *$\mathrm{H}_*(BU) = \mathbb{Z}[d_1, d_2, \dots]$ where $d_k = f_*(\alpha_k)$ where $(\alpha_k, \alpha^k) = 1$ and $\alpha \in \mathrm{H}^2(BU(1))$ is a generator. Above, f is the map $BU(1) \to BU$ induced by $U(1) \to U$.*

Remark 3.4.10. d_k "is" $\sum_i x_i^k$ with x_i the Chern roots.

Also, both homology and cohomology of BU are polynomial algebras. Even beyond this, it is self-dual as a Hopf algebra. ○

This is great, but what's the plan here? Have diagram

$$\begin{tikzcd}
 & \mathrm{Gr}_n(2n) \arrow[r, "\varphi_n"] & \Omega\,\mathrm{SU}(2n) \\
\mathbb{CP}^n \arrow[r, equal] & \mathrm{Gr}_n(n+1) \arrow[u, "\bar{j}_n"] \arrow[r, "\widetilde{\varphi}_n"] & \Omega\,\mathrm{SU}(n+1) \arrow[u, "\Omega j_n"']
\end{tikzcd}$$

where $j_n : U(n+1) \to U(2n)$ is inclusion as top left block.

Fact. The induced map $\bar{j} : \mathbb{CP}^\infty \to BU$ has images, on homology, which generate $\mathrm{H}_*(BU)$ as a ring.

This map j_n is highly connected. In particular, the fibration $U(n) \hookrightarrow U(n+1) \to S^{2n+1}$ is $2n$-connected, which shows

$$U(n+1) \subset U(n+2) \subset \cdots \subset U(2n)$$

is at least $2n$-connected. Thus, $j = \varinjlim j_n$ is a weak equivalence, so induces an isomorphism on homology (I think even the identity map).

The upshot is that if $\widetilde{\varphi} : \mathbb{CP}^\infty \to \Omega SU$ sends the (additive) generators of $\mathrm{H}_*(\mathbb{CP}^\infty)$ to the (algebra/-multiplicative) generators of $\mathrm{H}_*(\Omega SU)$, then we can conclude by commutativity that the same is true about $\varphi : BU \to \Omega\,\mathrm{SU}$, showing that it is a weak equivalence.

Computation of $\mathrm{H}_*(\mathrm{SU})$ Recall that $[\Sigma X, Y] \cong [X, \Omega Y]$. Consider the map of pairs

$$(\varphi_n, \varphi_{n-1}) : \left(\Sigma\,\mathbb{CP}^n, \Sigma\,\mathbb{CP}^{n-1}\right) \to (\mathrm{SU}(n+1), \mathrm{SU}(n)).$$

Claim 3.4.11. *The composition*

$$\left(\Sigma\,\mathbb{CP}^n, \Sigma\,\mathbb{CP}^{n-1}\right) \to (\mathrm{SU}(n+1), \mathrm{SU}(n)) \to (S^{2n+1}, *)$$

induces an isomorphism on homology.

Intuition. $\Sigma\,\mathbb{CP}^n / \Sigma\,\mathbb{CP}^{n+1} \cong \Sigma(\mathbb{CP}^n / \mathbb{CP}^{n-1}) \cong \Sigma(S^{2n}) \cong S^{2n+1}$

The actual proof if very hands on/computational.

What does this give us? It tells us that, homologically, "$\mathrm{SU}(n+1) = \mathrm{SU}(n) \times S^{2n+1}$." We have a fibration

$$\mathrm{SU}(n) \to \mathrm{SU}(n+1) \to S^{2n+1}.$$

This gives rise to the Serre spectral sequence, which, since these are H-spaces, let's us talk about multiplication (this is a spectral sequence of modules over the homology of the fiber). This gives rise to an "homological Euler class" $[\xi]$, and we will show that $[\xi] = 0$. This will be what we mean by "$\mathrm{SU}(n+1) = \mathrm{SU}(n) \times S^{2n+1}$." Explicitly, this will give $\mathrm{H}_*(\mathrm{SU}(n+1)) \cong \mathrm{H}_*(\mathrm{SU}(n)) \otimes \mathrm{H}_*(S^{2n+1})$, additively.

What is this air quotes Euler class? We have a composition

$$\rho : (D^{2n+1}, S^{2n}) \to (\Sigma\,\mathbb{CP}^n, \Sigma\,\mathbb{CP}^{n-1}) \to (\mathrm{SU}(n+1), \mathrm{SU}(n)) \to (S^{2n+1}, *)$$

which is an isomorphism on homology (at each step). This composition includes a map $S^{2n} \to \mathrm{SU}(n)$ and Hurewicz applies to this map gives the Euler class $[\xi] \in \mathrm{H}_{2n}(\mathrm{SU}(n))$. Note that this Euler class, or the map is comes from anyways, factors through $\Sigma\,\mathbb{CP}^{n-1}$ which has no even-dimensional homology, so $[\xi] = 0$.

One can use this to show that

$$\mathrm{H}_*(\mathrm{SU}(n)) = \bigwedge(x_3, \dots, x_{2n-1}) \implies \mathrm{H}_*(\mathrm{SU}(n+1)) \cong \bigwedge(x_3, \dots, x_{2n-1})$$

by saying the words "comparison theorem" and/or "transgression." The new generator x_{2n+1} is coming from the S^{2n+1} in the fibration. These homology rings are commutative because $\mathrm{SU}(n) \hookrightarrow \mathrm{SU}$ with homology injecting, and we know that SU is a commutative H-space.

Deeparaj said more about showing the above implication, but I was distracted so I did not write anything down. See the paper.

Remark 3.4.12. At some point the phrase "transgressively generated" is used, but this does not mean what it sounds like. It means "generated by elements which transgress" where "transgress" means survive/are not killed by the transgression map (which, in homology, goes from base to fiber). ○

Main Proof Recall our diagram

$$\begin{tikzcd} BU \arrow[r] & \Omega SU \\ \mathbb{CP}^\infty \arrow[u] \arrow[r] & \Omega\,\mathrm{SU} \arrow[u] \end{tikzcd}$$

Everything have done so far shows that these maps (injectively) sends the additive generators of $\mathrm{H}_*(\mathbb{CP}^\infty)$ to algebra generators for $\mathrm{H}_*(BU)$ and $\mathrm{H}_*(\Omega SU)$, while the right vertical map induces the identity on homology. By commutativity, we win.

3.5 Jae: Quelques propriétés globales des variétés différentiables, Thom

3.5.1 Paper Notes

TODO: Read this paper

3.5.2 Talk Notes

Results from this paper (won't have time to talk about all).

- Motivating Question: Steenrod's problem (representing cohomology classes by submanifolds)
- Pontryagin-Thom construction + Notion of transversality
- Algebraic topology of Thom spaces $MO(k)$
- Computation of the additive structure of cobordism ring

Steenrod's problem Two intuitions for homology: cycles in simplicial complexes and fundamental classes of manifolds.

Question 3.5.1 (Steenrod)**.** *Is any homology class represented by a singular manifold? Given a homology class $z \in \mathrm{H}_k(X)$ is there a smooth manifold W with a map $W \xrightarrow{f} X$ so that $f_*[W] = z$.*

Answer (Thom)**.** Unoriented case ($\mathbb{Z}/2\mathbb{Z}$-coefficients): Yes
oriented case ($\mathbb{Z}$-coefficients): No. Counterexamples in dimension ≥ 7 ⋆

We'll focus talk on unoriented case.

Thom's approach Reduce to submanifold realization problem and use Poincaré duality.

Let $G \leq O(k)$ be a closed subgroup, so rank k real vector bundles over X with structure groups which can be reduced to G are the same things as maps $X \to BG$. Can construct **Thom space** $D(EG)/S(EG) =: MG$ (Technically, should write $D(EG \times_G \mathbb{R}^k)/S(EG \times_G \mathbb{R}^k)$) where $D(\cdot), S(\cdot)$ are the unit disk and sphere bundles.

Given $\xi \to X$ pulled back fro $X \to BG$, can consider its Thom space $T(\xi) = D(\xi)/S(\xi)$, and this has a natural map $T(\xi) \to MG$.

Fact (**Thom isomorphism**)**.** There's an iso $\mathrm{H}^*(BG) \to \widetilde{\mathrm{H}}^{*+k}(MG)$ and the image of $1 \in \mathrm{H}^0(BG)$ is the **Thom class** $U \in \mathrm{H}^k(MG)$. (All with $\mathbb{Z}/2\mathbb{Z}$-coefficients)

Theorem 3.5.2. *submanifold realizaion $\iff$ maps to MG.*

Definition 3.5.3. We call $u \in \mathrm{H}^k(V)$ G**-realizable** if $\exists f : V \to MG$ s.t. $f^*U = u$. ◇

Fact. $z \in \mathrm{H}_{n-k}(V^n)$ is realized by $W^{n-k} \subset V^n$ submanifold with normal bundle with structure group $G \iff PD(z) \in \mathrm{H}^k(V^n)$ is G-realizable.

How do we reduce Steenrod problem to the submanifold case? Start with W a smooth manifold with map $W \to K$. Embed $K \subset \mathbb{R}^n$, and enlarge K to a neighborhood $M \subset \mathbb{R}^n$ (which deformation retracts onto K). Collapse the boundary $M/\partial M = V^n$ to get a closed manifold with same dimension as ambient Euclidean space.

Question: Is this always a manifold? When K a manifold, get use tubular neighborhood and are happy, but K does not have to

Note 9. Thom uses different construction. He takes the "double of M" which is always a manifold. Take two copies of M and glue them together by identifying their boundaries.

Now, W is an embedded (after a pertubation of f) submanifold of V^n which is homotopy equivalent to K.

Pontryagin-Thom Construction Instance of duality between geometric/covariant objects and algebraic/contravariant ones. In geometric side, start with

$$W \xrightarrow{f} K \hookrightarrow M \subset \mathbb{R}^n$$

(and get V from M). On the algebraic side, have

$$V^n \to \mathcal{V}/\partial\mathcal{V} \to MG.$$

To get this, let $\mathcal{V} \subset V^n$ be a tubular neighborhood of W in V. It's Thom space is $\mathcal{V}/\partial\mathcal{V}$ to this maps into universal Thom space MG (the map $V^n \to \mathcal{V}/\partial\mathcal{V}$ is inclusion of zero section).

If you start with the algebraic data, you can also recover the geometric one. Have pullback diagram

$$\begin{tikzcd} W \arrow[r] \arrow[d] & V^n \arrow[d] \\ BG \arrow[r] & MG \end{tikzcd}$$

We want $W \to V^n$ to be an actual embedding of submanifolds. Start by removing points at infinity

$$\begin{tikzcd} W \arrow[r] \arrow[d] & V^n \setminus F^{-1}(\infty) \arrow[d, "F"] \\ BG \arrow[r] & MG \setminus \infty \end{tikzcd}$$

Now, F is an actual map between smooth manifolds (technically, should take some finite dimensional model of MG), and then perturb F to be transversal to the image of BG. Then, $W = W^{n-k} \hookrightarrow V^n \setminus F^{-1}(\infty)$ really is an embedded submanifold, and its normal bundle in V will have G as its structure group (and $PD(W)$ will coincide with pullback of Thom class.)

Missed something. Essentially, this construction ignores anything "away from K", so you can take a local (deformation?) retract from V^n to K, and then the composition $W^{n-k} \to V^n \setminus F^{-1}(\infty) \dashrightarrow K$ gives your singular manifold.

Question 3.5.4 (Audience)**.** *Is there a complex analogue?*

Answer. Yes, can take $G = U(k) \hookrightarrow O(2k)$. Also, the G-structure on the normal bundle is a much weaker condition that requiring submanifolds to be holomorphic, so don't need to worry about lack of transversality for complex analytic manifolds. ⋆

Remarks about the Pontryagin-Thom duality

- Works for any structure group $G \le O(k)$
- $M/\partial M \to MG$ is determined by map near $F^{-1}(BG)$
- Ambient cobordisms (L-equivalences) in $V \times I$ correspond to homotopies of maps to $MO(k)$ under this duality, i.e. $L_{n-k}(V^n) \cong [V^n, MO(k)]$.
- One can "stabilizer," $BO(k) \to BO(k+1)$ classifies $\xi \oplus \underline{\mathbb{R}}$, so get

Remember: $T(\xi \oplus \underline{\mathbb{R}}^n) = \Sigma^n T(\xi)$.

$$\Sigma MO(k) \to MO(k+1).$$

We (really Thom) have (really has) reduced Steenrod's problem to understanding cohomology of Thom spaces.

Topology of $M(O(k))$ Main observation is a square

$$\begin{array}{ccc} SEO(k) & \longrightarrow & DEO(k) \\ \downarrow & & \downarrow \\ BO(k-1) & \longrightarrow & BO(k) \end{array}$$

whose vertical maps are homotopy equivalences. For the left vertical map, the data of a point of $SEO(k)$ is a k-place along with a unit vector. The complement of this vector is a $(k-1)$-plane, so get a map to $BO(k-1)$. The fibers of this map are the spheres complementary to this $(k-1)$-plane so fiber basically S^∞.

Now see $MO(k)$ as mapping cone of $BO(k-1) \to BO(k)$ so cohomologically $(BO(k), BO(k-1))$.

Remark 3.5.5. Maybe easier to see $BO(k-1) \simeq SEO(k)$ by doing something like $BO(k-1) = EO(k)/O(k-1)$. ◦

Fact (Borel)**.** $\mathrm{H}^*(BO(k); \mathbb{Z}_2)$ generated by Stiefel-Whitney classes.

Can use this to see that $\widetilde{\mathrm{H}}^*(MO(k)) \hookrightarrow \mathrm{H}^*(BO(k))$ with image equal to the ideal generated by the top SW class $w_k \in \mathrm{H}^k(BO(k))$.

Computing the homotopy type of $MO(k)$ Two ingredients: cohomology of $K(\mathbb{Z}_2, k)$ (Serre) and cohomology of $BO(k)$ (Borel).

Recall 3.5.6. For $h < k$, $\mathrm{H}^{k+h}(\mathbb{Z}_2, k; \mathbb{Z}_2)$ is generated by $\mathrm{Sq}^I u$ where I is an admissible sequence and $u \in \mathrm{H}^k(\mathbb{Z}_2, k; \mathbb{Z}_2)$ is universal class. The number of admissible sequences, rank of cohomology in $k+h$ is

$$c(h) = \#\text{dyadic decompositions of } h$$

where **dyadic decomposition** means partitions into sum of integers of form $2^j - 1$. ⊙

Lemma 3.5.7 (in Thom's paper but due to Serre)**.** *For $h \le k$, Sq^I act freely on $w_k \in \mathrm{H}^k(BO(k))$, i.e. $\mathrm{Sq}^I w_k$ are linearly independent.*

Keep in mind that this top SW class generates cohomology of $MO(k)$.

Fact (Serre-Thom)**.** For $h \le k$, let

$$X^h_{\omega_h} = \sum W_k x_1^{a_1} \dots x_r^{a_r} \in (w_k) \subset \mathrm{H}^{k+h}(BO(k))$$

for $\omega_h = (a_1, \dots, a_r)$ a *non-dyadic decomposition* of h (so no integers of form $2^j - 1$.)

Using Serre's lemma, can show that for fixed $m \leq k$,

$$X^m_{\omega_m}, \mathrm{Sq}^1 X^{m-1}_{\omega_{m-1}}, \dots, \mathrm{Sq}^{I_k} X^h_{\omega_h}, \dots, \mathrm{Sq}^I w_K$$

for $|I_h| = m - h$, ω_h as above, are linearly independent.

Let $p(m) = \#$ partitions of m, so

$$p(m) = \sum_{h=0}^{m} c(m-h)d(h).$$

Above linear independence + dimension counting show that those X's form a basis of $\mathrm{H}^{k+m}(MO(k))$.

Using this explicit basis and knowledge of Steenrod squares, can prove the following (also show this spaces are simply connected).

Theorem 3.5.8.

$$MO(k) \to \prod_{h=0}^{k} K(\mathbb{Z}_2, k+h)^{d(h)}$$

induces the same homotopy $2k$-type ($d(h) = \#\omega_h = \#$ generators in $H_k(MO)$ as Steenrod module). Stably,

$$MO \xrightarrow{\sim} \prod_h \left(\Sigma^h H\mathbb{F}_2\right)^{d(h)}.$$

This gives solution to Steenrod's problem. It's asking if we can lift

$$\begin{tikzcd} & MO(k) \arrow[d] \\ V^n \arrow[r] \arrow[ur, dashed] & K(\mathbb{Z}_2, k) \end{tikzcd}$$

However, Thom's results says that there is a factor of $K(\mathbb{Z}_2, k)$ in $MO(k)$, su get section of the vertical map.

3.6 Jordan: Bordisms and Cobordisms, Atiyah

3.6.1 Talk Notes

First, a remark.

Remark 3.6.1. For $(X, x_0), (Y, y_0)$ pointed spaces, we get a suspension sequence

$$[X, Y] \to [\Sigma X, \Sigma Y] \to [\Sigma^2 X, \Sigma^2 Y] \to \dots$$

with the first object a set, the second a group, and every other an abelian group. Using Freudenthal suspension, the maps $[\Sigma^n X, \Sigma^n Y] \to [\Sigma^{n+1} X, \Sigma^{n+1} Y]$ are isomorphisms for large n, where large here means

$$n + 2(\text{connectivity of } Y) \geq \dim X$$

if X a finite-dimensional CW-complex.

As you suspend X its dimension goes up, but the connectivity of Y is going up at the same rate, so twice the connectivity of Y is increasing more quickly. ○

Notation 3.6.2. We let

$$\{X,Y\} = \varinjlim [\Sigma^n X, \Sigma^n Y]$$

be the eventual value of these groups.

Recall 3.6.3. Given a topological group G (e.g. $G = \mathrm{SO}(n)$), get an associated classifying space BG. Can form the Thom space $MG = D(EG)/S(EG)$. In Thom's paper, he shows that the natural map

$$\Sigma MSO(n) \to MSO(n+1)$$

induces isomorphisms on π_{n+r} for $n > 2r$. ⊙

Question: Is $MSO(n)$ n-connected?

Answer: Yes. This is part of the Thom isomorphism (+ Hurewicz + arguing that it is simply connected)

The upshot is that the induced map $[X, \Sigma MSO(n)] \to [X, MSO(n+1)]$ is bijective for $n \gg 0$. So, if X is a CW-complex with subcomplex $Y \subset X$, the composition

$$[\Sigma^{n-k}(X/Y), MSO(n)] \to [\Sigma^{n+1-k}(X/y), \Sigma MSO(n)] \to [\Sigma^{n+1-k}(X/Y), MSO(n+1)]$$

will be an iso for $n \gg 0$ (suspension sequence + Thom).

Notation 3.6.4. We define

$$MSO^k(X,Y) := \varinjlim [\Sigma^{n-k}(X/Y), MSO(n)].$$

(Stable maps from X/Y into spectrum MSO). When $Y = \emptyset$, we write $MSO^k(Y)$ and interpret $Y/\emptyset$ as Y_+.

Fact. This construction satisfies all the Eilenberg-Steenrod axioms except for dimension.

An interesting case is $X = *$. Then,

$$MSO^{-k}(*) = \varinjlim [\Sigma^{n+k} S^0, MSO(n)] = \varinjlim [S^{n+k}, MSO(n)] = \varinjlim \pi_{n+k} MSO(n) \cong \Omega_k$$

is Thom's cobordism group.

Alternate perspective (spectra) Recall the map $\Sigma MSO(n) \to MSO(n+1)$. This gives a spectrum MSO with $MSO_n = MSO(n)$ and structure/transition/whatever maps given by the ones we just recalled. Given a space X, we can then define

Remember: The natural map $X \to \Sigma X$ ("inclusion as belt") is nullhomotopic

$$[X, MSO]_k := \varinjlim_{n\to\infty} [\Sigma^{n+k}, MSO(n)] = \varinjlim_{n\to\infty} [\Sigma^n X, \Sigma^k MSO(n)]$$

Back to Atiyah Fix a "suitable" category $\mathcal{A}$ (e.g. countable, finite-dimensional CW-complexes). Consider the category $\mathcal{B}$ of pairs (X,α) where $X \in \mathcal{A}$ and α a principal $\mathbb{F}_2$-bundle over X (i.e. a double cover). The maps/homotopies in $\mathcal{B}$ are usual bundle maps/homotopies. For example, a map $F : (Y,\beta) \to (X,\alpha)$ consists of a map $f : Y \to X$ along with an iso $\beta \cong f^*\alpha$.

Notation 3.6.5. We define $\mathcal{M}_k \subset B$ to be the full subcategory of pairs (M, τ) where M is a compact, smooth manifold (possibly with boundary) of dimension k, and τ is its orientation bundle. We also consider $M_k^0 \subset M_k$ consisting of closed manifolds (i.e. compact, no boundary).

Definition 3.6.6. Given $(X, \alpha) \in \mathcal{B}$, we define $C_k(X, \alpha)$ to be the set

$$C_k(X, \alpha) := \left\{((M, \tau), F) : (M, \tau) \in \mathcal{M}_k^0 \text{ and } F : (M, \tau) \to (X, \alpha)\right\}.$$

On this set, we define an equivalence relation. We say $((M, \tau), F) \sim ((M', \tau'), F')$ iff there exists $(N, \sigma) \in M_{k+1}$ and $G : (N, \sigma) \to (X, \alpha)$ such that

Can think of $C_k(X, \alpha)$ as being the space of cycles (not chains), and then we mod out by boundaries, giving a homology theory

- $\partial N = M \sqcup M'$
- $G|_M = F$ and $G|_{M'} = F'$

We let $MSO_k(X, \alpha)$ denote this set of equivalence classes. $\diamond$

The space $MSO_k(X, \alpha)$ are abelian groups with addition given by disjoint union.

Notation 3.6.7. If α is the trivial bundle $X \times \mathbb{F}_2$, we just write $MSO_k(X) := MSO_k(X, X \times \mathbb{F}_2)$. In this, the manifolds mapping in must be oriented.

Remark 3.6.8. When $X = *$, we get

$$MSO_k(*) = C_k(*, * \times \mathbb{F}_2)/\sim.$$

Every (oriented) $M \in \mathcal{M}_k^0$ has a map $M \xrightarrow{f} *$. Checking the equivalence relations, we get that $MSO_k(*) \cong \Omega_k$ is Thom's oriented bordism group. $\circ$

Spectra stuff

Claim 3.6.9. *$MSO_k(X) \cong \varinjlim \pi_{n+k}(MSO(n) \wedge X_+)$ where $n = \dim X$.*

Proof. Choose $((M, \tau), f) \in C_k(X, \alpha)$, and want to fix an embedding $i : M \hookrightarrow \mathbb{R}^{n+k}$. Since the codimension is n, the normal bundle ν gives us a map $f : M \to BO(n)$ with $f^*\xi \cong \nu$. I stopped paying attention for a second... do something and get a map between Thom spaces, and then do more things.... $\blacksquare$

Back to Atiyah

Proposition 3.6.10. *For large $n = \dim X$. We have an isomorphism*

$$\psi : L_k(X) \to MSO_k(X, \tau)(\cong \pi_k^S(MSO \wedge X_+))$$

Thom had shown that $\Omega_k \cong L_k(S^n)$ for $n \gg k$. So,

$$\Omega_k \cong L_k(S^n) \cong \pi_k^S(MSO \wedge S^n_+) \cong \pi_k^S(\Sigma^n MSO) \cong \pi_k^S(MSO)$$

(where there's maybe some cancellation in degree shifting that should be there).

3.7 Elia: Topological Methods in Algebraic Geometry, Hirzebruch

3.7.1 Talk Notes

The Plan

- $\Omega_k \otimes \mathbb{Q} \xrightarrow{\sim} \operatorname{Hom}(\mathrm{H}^n(BSO, \mathbb{Z}), \mathbb{Q})$
- $\{[\mathbb{CP}^{2n}]\}$ is a basis for $\Omega_k \otimes \mathbb{Q}$
- Signature, σ, is a multaplicative homomorphism from cobordism ring
- Signature theorem

The Talk

Theorem 3.7.1. *MSO_k is stably, rationally, $\prod_{m=0}^k K(Z, k+4m)^{c(m)}$*

Proof. $\varphi : H(MSO, \mathbb{Q}) \to H(bSO, \mathbb{Q})$ with $H_*(BSO, \mathbb{Q})$ a Hopf algebra. Hopf-Leray shows that its free, so of the form $\mathbb{Q}[y_1, y_2, \dots]$. One can show $y_i \in \mathrm{H}_{4i}(BSO, \mathbb{Q})$ (look at Poincaré series). ∎

Recall 3.7.2. $H(\mathbb{Z}, m; \mathbb{Q}) = \begin{cases} \mathbb{Q}[a_m] & \text{if } m \text{ even} \\ E[a_m] & \text{otherwise.} \end{cases}$. ⊙ Proved in 18.906?

Corollary 3.7.3. $\pi_n MSO \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{H}_n(MSO, \mathbb{Q})$

Proof. This map is injective and both sides have same dimensions. ∎

Keep in mind the diagram... (missed it)

Corollary 3.7.4. *For closed oriented manifold M, there's N such that $N[M]$ null-cobordant iff all Pontryagin numbers of M are* 0.

Corollary 3.7.5. $\dim_{\mathbb{Q}}(\Omega^{4k} \otimes \mathbb{Q}) = \pi(k) = \#$ *partitions of k.*

Definition 3.7.6. A **multiplicative sequence** over $\mathbb{Q}$ is a set of homogeneous polynomials $K_i(x_1, \dots, x_i) \in \mathbb{Q}[x_1, \dots, x_i]$ of degree i (with x_i in ith grading). Can put this together by setting

$$K\left(a_0 + a_1 t + a_2 t^2 + \dots\right) = \sum K_i(a_0, a_1, \dots, a_i) t^i.$$

We require these to satisfy

$$K(P(t)Q(t)) = K(P(t))K(Q(t)).$$

◇

Remark 3.7.7. Note that $Q(t) = K(1 + at)$ determines all the K_i since any polynomial will factor into a product of linear ones. ○

Example. $Q(t) = 1 + \lambda t$ gives $K_i(x_1, \dots, x_i) = \lambda^i x_i$, so

$$K(a_0, a_1, \dots) = \sum_{i \geq 0} \lambda^i a_i.$$

△

Theorem 3.7.8. *Ring homomorphisms from the rational cobordism ring are multiplicative sequences in the Pontryagin classes. These are in bijection with the coset* $1 + (t) \subset \mathbb{Q}[\![t]\!]$.

Let $\{V^{4i}\}$ be a sequence of $4i$-dimensional manifolds, and let $V_{(j)} = V^{4j_1} \times \ldots \times V^{4j_r}$ for all $(j) \in \pi(k)$. When are these $V_{(j)}$ a basis of $\Omega^{4k} \otimes \mathbb{Q}$?

Definition 3.7.9. Factor the Pontryagin polynomial

$$1 + p_1 t + p_2 t^2 + \cdots + p_k t^k = \prod_{i=1}^{k} (1 + \beta_i t).$$

Let $S(V^{4k}) = \left(\sum_i \beta_i^k\right) [V^{4k}]$. ◇

Lemma 3.7.10. *The* $V_{(j)}$ *are a basis iff* $S(V^{4i}) \neq 0$ *for all* i.

Proof. Enough to show independence since we already know dimensions. Suppose we find m-sequences K^t such that $K_i^t[V^{4i}] = y_i^t$ (ith indeterminant, to the tth power). Consider the map

$$\left(K_k^1, K_k^2, \ldots, K_k^{\pi(k)}\right) : \Omega^{4k} \otimes \mathbb{Q} \to \mathbb{Q}[y_1, \ldots].$$

This will map the $V_{(j)}$ to independent elements in the target ring, and so we would win.

Need to find these K^t. These are determined by $Q^t(z) = K^t(1 + az) = b_0 + b_1 z + b_2 z^2 + \ldots$. We'll find these b_i by induction. Suppose we know $b_1, \ldots, b_{k-1}$. Then, $K_k^t[V^{4k}]$ is the kth term in $(K^t)(V^{4k})$ and is equal to the kth term of

$$\prod K^t(1 + \beta_i) = \prod_i \left(b_0 + b_1 \beta_i + b_2 \beta_i^2 + \ldots\right)$$

which is

$$\left(\sum \beta_i^k\right) b_k + (\text{poly in } \beta_0, \ldots, \beta_{k-1}).$$

We can now solve for b_k. ■

Lemma 3.7.11. $S(\mathbb{CP}^{2k}) = 2k + 1$ *and so* $\{\mathbb{CP}^{2k}\}$ *give a basis for* $\Omega \otimes \mathbb{Q}$.

Proof. Need to compute S-invariants. Note that $W_{\mathbb{C}} = W \oplus \overline{W}$ for W a real vector bundle, so

$$1 - p_1 + p_2 - \cdots = c\bar{c}$$

where c is the Chern polynomial. The Chern polynomial is $c = (1 - a^2)^{2k+1}$. Thus,

$$1 + p_1 + p_2 + \cdots = (1 + a^2)^{2k+1}$$

where $a \in \mathrm{H}^2(\mathbb{CP}^{2k})$ is a generator. Thus, each Pontryagin root is a^2. Thus, $\beta\beta_i^k = (2k+1)a^{2k}$. ■

Remark 3.7.12. Suggest that if you don't work rationally, then may $[\mathbb{CP}^{2k}] \in \Omega$ is divisible by $(2k+1)$. ○

Signature Note that $T : \mathrm{H}^{2k}(V^{4k}) \otimes \mathrm{H}^{2k}(V^{2k}) \to \mathbb{Q}$ is a quadratic form, given by cup product. Let $\tau(V^{4k})$ denote its signature, pos def part - neg def part.

Lemma 3.7.13.

- τ *is* 0 *for null-cobordant* V
- τ *is additive on* $\Omega^{4k} \otimes \mathbb{Q}$
- τ *is multiplicative*

Proof. **(2)** is clear (once you know **(1)**). **(3)** follows from Kunneth formula + choice of a clever basis.

(1) is the interesting one. Have $f : V^{4k} \hookrightarrow X^{4k+1}$ with $\partial X = V$. Consider diagram

$$\begin{array}{ccccc} \mathrm{H}^{2k}(X) & \xrightarrow{f^*} & \mathrm{H}^{2k}(V) & \longrightarrow & \mathrm{H}^{2k+1}(X, v) \\ \downarrow & & \downarrow i & & \downarrow \\ \mathrm{H}_{2k+1}(X) & \longrightarrow & \mathrm{H}_{2k}(V) & \longrightarrow & \mathrm{H}_{2k}(X, V) \end{array}$$

Horizontals are LES of a pair, verticals are all isomorphisms (Poincaré duality). Compute image of f^*.

$$\dim \operatorname{im} f^* = \dim \operatorname{im}(if^*) = \dim \ker f_*.$$

$$\dim \operatorname{im} f^* = \dim \mathrm{H}_{2k}(V)/\ker f_*.$$

Thus, $\dim \operatorname{im} f^* = \frac{1}{2} \dim H_{2k}(V)$. We know T vanishes on $\operatorname{im} f^*$.

$$(f^* x)^2[V] = x^2[f_* x V] = 0$$

since $f_* V$ is a boundary in X. This implies that the signature of T is 0 via linear algebra. ∎

Let $Q(t) = \sqrt{t}/\tanh\sqrt{t}$ with associated multaplicative sequence $\{L_i(x_1, \ldots, x_i)\}$.

Theorem 3.7.14 (Singature Theorem). $\tau(V^{4k}) = L_k(p_1, \ldots, p_k)[V^{4k}]$

Proof. Enough to check this on a (multplicative) basis like $\{\mathbb{CP}^{2k}\}$. $\tau(\mathbb{CP}^{2k}) = 1$ is easy to see ($\mathrm{H}^*(\mathbb{CP}^k) = \mathbb{Q}[a]/(a^{2k+1})$). Let's now compute $L_k(\mathbb{CP}^{2k})$, the $2k$th term of $L(1 + p_1 t + \dots)$. This is the $(2k)$th term of

$$\left(\frac{\sqrt{a^2}}{\tanh\sqrt{a^2}}\right)^{2k+1}$$

Can compute this via complex analysis (substitute $u = \tanh z$ so $dz = du/(1-u^2) = \sum u^{2i} du$)

$$\frac{1}{2\pi i}\int \left(\frac{z}{\tanh z}\right)^{2k+1} \frac{1}{z^{2k+1}} \mathrm{d}z = \frac{1}{2\pi i}\frac{\sum u^{2i} du}{u^{2k+1}} = \frac{1}{2\pi i}\int \frac{\mathrm{d}u}{u} = 1.$$

(most terms vanish since they are holomorphic). Thus, the $(2k)$th coefficient is $1 \cdot a^{2k}$ which evaluates to 1 on $[\mathbb{CP}^{2k}]$. ∎

Applications

- $L_k[V^{4k}]$ is oriented homotopy, cobordism invariant
- Let V^4 be diff manifold which is a homotopy 4-sphere. The obstruction to TV being stably trivial is a class $a \in \mathrm{H}^4(V, \pi_3 \mathrm{SO}_5) = \pi_3 \mathrm{SO}_5$. This is $a = p_1(TM)$. Since $\tau(V^4) = 0$, TV is in fact stably trivial.
- If $f : V \to W$ is a degree d map, they have the same Pontryagin classes and the fundamental class upstairs gets mapped to d times the fundamental class downstairs. Hence, we can deduce $\tau(V) = 4\tau(W)$.
- Sig theorem imposes restrictions on poincaré polynomials.

  Example. No W with $P_W(t) = 1 + t^6 + t^{12}$. △

  Example. $p_1[V^4]/3$ is an integer. Get other integrality conditions as well. △

3.8 Junyao: On manifolds homeomorphic to the 7-sphere, Milnor

3.8.1 Talk Notes

Our goal is the following

Goal. There exists a differentiable manifold M^7 homeomorphic to S^7, but not diffeomorphic to S^7.

Proof strategy

- Find invariant λ on certain[30] (differentiable, oriented) 7-manifolds M^7 satisfying the following: $\lambda(M^7) \neq 0 \iff M^7$ has no orientation-reversing diffeo.
- Construct manifolds M_k^7 with invariant $\lambda(M_k^7) = k^2 - 1 \pmod 7$.
- Show that M_k^7 is homeomorphic to S^7

λ **Invariant** Fix a closed, differentiable M^7 with orientation $\mu \in \mathrm{H}_7(M^7, \mathbb{Z})$. Assume $\mathrm{H}_3(M^7) = \mathrm{H}_4(M^7) = 0$. Thom computed $\pi_7(MSO) = 0$, so every M^7 is the bounded of an oriented 8-manifold B^8. We'll define λ using invariants of B^8.

Recall 3.8.1 (Hirzebruch signature theorem)**.** For any closed 8-manifold C^8 with orientation ν,

$$\tau(C^8) = \left\langle \nu, \frac{1}{45}\left(7p_2(C^8) - p_1(X^8)^2\right) \right\rangle.$$

This gives

$$45\tau = \left\langle \nu, -p_1^2 \right\rangle \pmod 7$$

so we define $q(C^8) := \left\langle \nu, p_1^2 \right\rangle$. Note that $2q - \tau \equiv 0 \pmod 7$. ⊙

[30] $\mathrm{H}^3(M^7) = \mathrm{H}^4(M^7) = 0$

Definition 3.8.2. Let B^8 be a oriented manifold with boundary. We define $\tau(B^8)$ to be the index of the quadratic form on $\mathrm{H}^4(B^8, M^7)/tors$

$$\alpha \mapsto \langle \nu, \alpha^2 \rangle$$

where $\nu \in \mathrm{H}_8(B^8, M^7)$ is the orientation. ⋄

Definition 3.8.3. The Pontryagin number $q(B^8) = \langle \nu, (i^{-1}p_1)^2 \rangle$ where $i : \mathrm{H}^4(B^8, M^7) \xrightarrow{\sim} \mathrm{H}^4(B^8)$ since H_3, H_4 vanish. ⋄

Theorem 3.8.4. $2q(B^8) - \tau(B^8) \pmod 7$ *does not depend on the choice of* B^8 *(with* $\partial B^8 = M^7$*). Call this invariant* $\lambda(M^7)$*.*

Proof. Suppose B_1^8, B_2^8 both have boundary M^7 with orientations ν_1, ν_2. Get closed $C^8 = B_1^8 \cup_{M^7} B_2^8$ with orientation $(\nu_1, -\nu_2)$. We claim

$$\tau(C^8) = \tau(B_1^8) - \tau(B_2^8) \text{ and } q(C^8) = q(B_1^8) - q(B_2^8).$$

Since $2q - \tau(C^8) = 0$ from the signature theorem, this will prove the theorem.

Let's do the first one. We know τ index of $\langle \alpha^2, \nu \rangle$ with $\alpha \in \mathrm{H}^4(C)$ and $\nu = (\nu_1, -\nu_2)$. The Mayer-Vietoris sequence shows that

$$\mathrm{H}^3(B_1 \cap B_2) \longrightarrow \mathrm{H}^4(B_1 \cup B_2) \longrightarrow \mathrm{H}^4(B_1) \oplus \mathrm{H}^3(B_2) \longrightarrow \mathrm{H}^4(B_1 \cap B_2)$$

is exact. The outer terms are cohomology groups of M^7 which vanish, so get $\mathrm{H}^4(C^8) \xrightarrow{\sim} \mathrm{H}^4(B_1) \oplus \mathrm{H}^4(B_2)$. We can also use relative M-V to get $\mathrm{H}^4(C, M) \xrightarrow{\sim} \mathrm{H}^4(B_1, M) \oplus \mathrm{H}^4(B_2, M)$. These are isomorphic to the previous two things by LES of pair, so $\alpha \in \mathrm{H}^4(C)$ corresponds to $(\alpha_1, \alpha_2) \in \mathrm{H}^4(B_1, M) \oplus \mathrm{H}^4(B_2, M)$. We also have $\mathrm{H}^8(B, M) \xrightarrow{\sim} \mathrm{H}^8(B_1, M) \oplus \mathrm{H}^8(B_2, M)$ and all this nonsense respects the product structure. The up shot is we have $\alpha^2 \leftrightarrow (\alpha_1^2, \alpha_2^2)$ so

$$\langle \alpha^2, \nu \rangle = (\alpha_1^2, \alpha_2^2), (\nu_1, -\nu_2) = \langle \alpha_1^2, \nu_1 \rangle - \langle \alpha_2^2, \nu_2 \rangle$$

so the qudratic form splits which gives $\tau(C^8) = \tau(B_1^8) - \tau(B_2^8)$. ■

Theorem 3.8.5. *If the orientation* M^7 *is reversed, then* $\lambda(M^7) \rightsquigarrow -\lambda(M^7)$*.*

Construction of 7-manifolds M_k^7

Recall 3.8.6. S^7 is a principal S^3-bundle over S^4. ⊙

What about other principal S^3-bundles over S^4?

We can get this from 4-plane bundles over S^4 with structure group $\mathrm{SO}(4)$. This, via the clutching construction, correspond to elements of $\pi_3(\mathrm{SO}(4)) \cong \mathbb{Z} \oplus \mathbb{Z}$.

We can identify $\pi_3(\mathrm{SO}(4)) \cong \mathbb{Z} \oplus \mathbb{Z}$ explicitly via $(h, j) \mapsto f_{hj} : S^3 \to \mathrm{SO}(4)$ where

$$f_{hj}(v) \cdot v = v^h u v^j$$

thinking in terms of multiplication in $\mathbb{H}$.

Definition 3.8.7. Let M^7_k be the S^3-bundle over S^4 corresponding to $(h, j) \in \mathbb{Z} \oplus \mathbb{Z}$ such that $h + j = 1$ and $h - j = k$. ⋄

Notation 3.8.8. Let ξ_{hj} denote the 4-plane bundle over S^3 corresponding to $(h, j) \in \mathbb{Z}^2$.

Remark 3.8.9. Need $h + j = 1$ so $\mathrm{H}^3(M) = \mathrm{H}^4(M) = 0$. Look at spectral sequence $E^2_{p,q} = \mathrm{H}^p(S^3) \otimes \mathrm{H}^q(S^4) \implies \mathrm{H}^{p+q}(M^7_k)$. The E_4 page looks like

TODO: Draw this page

Need to kill the map $\mathrm{H}^3(S^3) \to \mathrm{H}^4(S^4)$ so need Euler class to get a generator for $\mathrm{H}^4(S^4)$. This Euler class (we'll show) is $(h + j)$·(generator) ○

Construction 3.8.10. Here's an explicit construction of ξ_{hj}. Glue two $\mathbb{R}^4 \times S^3$ along $(\mathbb{R}^4 \setminus 0) \times S^3$ via

$$(u, v) \sim (u', v') \iff u' = \frac{u}{\|u\|^2} \text{ and } v' = \frac{u^h v u^j}{\|u\|^{h+j}}$$

Note that if $h + j = 0$, then $\xi_{-h,h}$ has a section given by $v = 1$ for all u, u', so $e(\xi_{-h,h}) = 0$.

Remark 3.8.11. The Euler class $e : \mathrm{Bun}_{\mathrm{SO}(4)}(S^4) \to \mathrm{H}^4(S^4)$ is a group homomorphism $\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$. We've just seen that $(h, -h)$ is in the kernel (and we this map is surjective since $e(S^7 \to S^4)$ is a genrator), so $e(\xi_{hj}) = 1 \implies h + j = \pm 1$. ○

Lemma 3.8.12. $\lambda(M_k) = k^2 - 1 \pmod 7$

Proof. Choose B^8_k to be the corresponding D^4 bundle over S^4, so $\lambda(M^7_k) = 2q(B^8_k) - \tau(B^8_k)$. What is $\tau(B^8_k)$? Have

$$\mathrm{H}^4(B^8_k, M^7_k) \xrightarrow{\sim} \mathrm{H}^4(B^8_k) \xrightarrow{\sim} \mathrm{H}^4(^4) = \mathbb{Z}$$

so pick α mapping to $1 \in \mathbb{Z}$. We claim $\alpha^2 \in \mathrm{H}^8(B^8_k, M^7_k)$ is a generator. Look at the spectral sequence with fiber $F = (D^4, S^3)$ and base $B = S^4$.

Can think of α^2 as $\mathrm{Th}(\xi)$?

TODO: Draw sequence

This gives $\mathrm{H}^*(B_k, M_k) \cong \mathrm{H}^*(D^4, S^3) \otimes \mathrm{H}^*(S^4) \cong \mathrm{H}^*(S^4)$ (Thom isom).

Thom iso says that $- \smile \alpha : \mathrm{H}^*(S^4) \xrightarrow{\sim} \mathrm{H}^{*+4}(B_k, M_k)$ where $\alpha \mapsto \iota \in \mathrm{H}^4(S^4)$. This (via some natauirility/compatibility stuff) should then give α^2 as a generator in H^8 (since $\iota \smile \alpha$ is).

What is $q(B^8_k)$? Well, $\mathcal{T}_{B^8_k} =$ "$\mathcal{T}_{S^4} \oplus \xi_{hj}$", so use Whitney formula. Let $\mathcal{L}$ be the normal bundle of S^4 (inside what space?). Then,

$$p_1(\mathcal{T}_{S^4}) = -p_1(\mathcal{L}) = -c_2(\mathcal{L} \otimes_{\mathbb{R}} \mathbb{C}) = 0.$$

We claim $p_1(\xi_{hj}) = \pm 2(h - j) \cdot (\mathit{generator}) \in \mathrm{H}^4(S^4)$.

$p_1(\xi_{hj})$ is independent of the orientation of the fiber (look at bases of tangent$\otimes_{\mathbb{R}}\mathbb{C}$, get an even permutation). If orientation of the fiber S^3 is reversed, then $\xi_{hj} \rightsquigarrow \xi_{-j,-h}$. This is because reversing changes

$$(u, v) \sim \left(\frac{u}{\|u\|^2}, \frac{u^h v u^j}{\|u\|^{h+j}}\right) \rightsquigarrow (u, v^*) \sim \left(\frac{u}{\|u\|^2}, \left(\frac{u^h v u^j}{\|u\|^{h+j}}\right)^*\right)$$

but using $uu^* = \|u\|^2$, one sees that

$$\left(\frac{u^h v u^j}{\|u\|^{h+j}}\right)^* = \frac{u^{-j} v^* u^{-h}}{\|u\|^{-j-h}}.$$

Using that p_1 is a group homomorphism, we now conclude that $p_1(\xi_{hj}) = c(h-j)$ for some constant c. When $h = 1, j = 0$, we have $\xi_{hj} = \mathbb{P}^2(\mathbb{H})\backslash(\text{an 8-cell})$. Hirzebruch tells us that $p_1(\mathbb{P}^2(\mathbb{H})) = 2(\textit{generator}) \in \mathrm{H}^4(\mathbb{P}^2(\mathbb{H}))$, so $c = \pm 2$.

Putting these together, we've proven the lemma. ■

The last step is showing M^7_k is homeomorphic to S^7.

Proposition 3.8.13. *If there exists a differentiable function $f : M^n \to \mathbb{R}$ having only two critical points, which are both non-degenerate, then M^n is homeomorphic to S^n.*

Question 3.8.14. *Can we classify all differentiable structures on S^7 or even on S^n?*

Kervaire and Milnor, in a later paper, compute the number of differentiable structures on S^n for various n. For example, there are 28 differentiable structures on S^7.

Here's a construction. Consider the intersection of the hypersurface in $\mathbb{C}^5$ defined by

$$a^2 + b^2 + c^2 + d^3 + e^{6k-1} = 0$$

(for $k = 1, 2, \ldots, 28$) with a small unit sphere around the origin. This gives all smooth structures on the oriented 7-sphere.

Remark 3.8.15. In dimensions $4k-1$, the signature theorem can be used to get large cyclic subgroups of the group of differentiable structures on S^{4k-1}. ○

3.9 Niven: Cohomology Theories, Brown

3.9.1 Talk notes

Technical difficulties caused things to be kind of jank, but this is what I wrote down (The purple was written during the talk. All the other colored text was written beforehand or afterwards). It'd probably be somewhat more instructive to just read the paper; it's thankfully not too long.

3.10 Jiakai: K-theory, Atiyah

3.10.1 Talk Notes

Plan

- Definition of K^*, $\widetilde{K}^*$, $K^*(X, A)$
- Bott Periodicity
- (representability)
- Atiyah-Hirzebruch SS
- $\mathbb{CP}^n$, Riemann surfaces
- Alternative definition of $K(X, A)$, product structure

Assumption. Throughout, assume all spaces are compact, Hausdorff.

Notation 3.10.1. Let $\operatorname{Vect}(X)$ be the semigroup of iso classes of $\mathbb{C}$-vector bundles under $\oplus$.

The Grothendieck construction applied to $\operatorname{Vect}(X)$ gives us a group $K^0(X)$ whose elemnts are formal differences $[E]-[F]$ of vector bundles, up to stable equivalence. Can think of $K^0(X)$ as $(\operatorname{Vect}(X) \times \operatorname{Vect}(X))/\Delta$.

In K^0, $[E]=[F] \iff E \oplus \underline{n} \cong F \oplus \underline{n}$ for some n. Since every vector bundle E has a "complement" F so that $E \oplus F$ is trivial, we can write any element of $K^0(X)$ as the difference $[E]-[n]$ between a (stable) vector bundle and a trivial one (i.e. an integer).

Example. $K^0(*) = \{[m]-[n] : m,n \in \mathbb{N}\} \cong \mathbb{Z}$ with isomorphism given by virtual rank $m-n$. △

Example. $X = S^2$. A topological vector bundle on S^2 is determined by c_1 and its rank, so get iso $K^0(S^2) \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z}$ given by virtual rank $\oplus$ first Chern class. Under this iso $(0,1)$ corresponds to $[H]-[1]$ where $H = \mathscr{O}(1)$ is the hyperplane bundle on $S^2 = \mathbb{CP}^1$. Multiplicatively, one has $K(S^2) = \mathbb{Z}[x]/(x^2)$ where $x = [H]-1$. △

Definition 3.10.2. For a pointed space $(X,*)$, reduced K-theory is $\widetilde{K}(X) = \ker(K(X) \to K(*))$, so kill virtual rank. In general, we define

$$K^{-n}(X,Y) = \widetilde{K}(\Sigma^n(X/Y)).$$

◇

Bott Periodicity

Theorem 3.10.3. *Let L be a line bundle over X. Then, $K(\mathbb{P}(L \oplus 1))$ is a $K(X)$-algebra generated by $[H]$ (the tautological quotient bundle) subject to the relation $([H]-[1])([L][H]-[1]) = 0$.*

Remark 3.10.4. The Thom space of L is $\operatorname{Th}(L) = \mathbb{P}(L \oplus 1)/\mathbb{P}(L)$, so can think of above as related to a Thom isomorphism theorem. ○

Corollary 3.10.5. *$K(S^2)$ is generated by $[H]$ as a $K(*)$-module, with $([H]-1)^2 = 0$. Furthermore, $\widetilde{K}(S^2)$ is generated by $[H]-1$.*

Corollary 3.10.6. *$\widetilde{K}^0(X) \xrightarrow{\sim} \widetilde{K}^0(S^2X)$ given by $[E] \mapsto ([H]-[1])[E]$. Thus,*

$$\widetilde{K}^{\mathrm{even}}(X) = \widetilde{K}^0(X) \;\; \textit{and} \;\; \widetilde{K}^{\mathrm{odd}}(X) = \widetilde{K}^{-1}(X) = \widetilde{K}^0(\Sigma X).$$

The above result lets us extend K^n and $\widetilde{K}^n$ to positive degrees $n > 0$. It also let's us calculate the K-theory of spheres as $K^0(S^{\mathrm{even}}) = \mathbb{Z} \oplus \mathbb{Z}$ and $K^1(S^{\mathrm{even}}) = 0$ and $K^0(S^{\mathrm{even}}) = K^1(S^{\mathrm{even}}) = \mathbb{Z}$.

Note that we've seen in Deeparaj's talk that $\Omega^2 U \simeq \Omega U$ and $\Omega U \simeq \mathbb{Z} \times BU$. On compact X, one has $\widetilde{K}(X) = [X, BU \times \mathbb{Z}]_+$, so

$$\widetilde{K}(\Sigma^2 X) = [\Sigma^2 X, BU \times \mathbb{Z}]_+ = [X, \Omega^2(BU \times \mathbb{Z})]_+ = [X, BU \times \mathbb{Z}]_+ = \widetilde{K}(X).$$

Note that $\operatorname{Vect}(X) = [X, \coprod_{n \ge 0} BU(n)]$. One can show that $\Omega B\left(\coprod_{n \ge 0} BU(n)\right) \simeq BU \times \mathbb{Z}$ which you can think of as a topological version of "group completion" or of "Grothendieck's construction."

Apparently, the clutch construction shows that $[X, U] = \widetilde{K}^0(\Sigma X)$.

K-theory is a generalized cohomology theory We won't go over the details, but this is true. I guess the main point is Bott periodicity tells you that it is representable by an Ω-spectrum.

In particular, this gives us access to the Atiyah-Hirzebruch spectral sequence. Let X be a compact CW-complex. The **Atiyah-Hirzebruch spectrual sequence** is a spectral sequence

$$E_2^{p,q} = \mathrm{H}^p(X, K^q(*)) \implies K^{p+q}(X).$$

This has the same construction as the Serre spectral sequence.

$$\begin{array}{c|cccc}
p & & & & \\
2 & \mathrm{H}^0(X,\mathbb{Z}) & \mathrm{H}^1(X,\mathbb{Z}) & \mathrm{H}^2(X,\mathbb{Z}) & \\
1 & 0 & 0 & 0 & \\
0 & \mathrm{H}^0(X,\mathbb{Z}) & \mathrm{H}^1(X,\mathbb{Z}) & \mathrm{H}^2(X,\mathbb{Z}) & \\
-1 & 0 & 0 & 0 & \\
-2 & \mathrm{H}^0(X,\mathbb{Z}) & \mathrm{H}^1(X,\mathbb{Z}) & \mathrm{H}^2(X,\mathbb{Z}) & \\
\hline
 & 0 & 1 & 2 & q
\end{array}$$

Example. Apply to $\mathbb{RP}^2$ to get $K^0(\mathbb{RP}^2) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $K^1(\mathbb{RP}^2) = 0$. △

Example. Apply to Σ_g (genus g Riemann surface) to get $K^1(\Sigma_g) = \mathbb{Z}^{2g}$ and $K^0(\Sigma_g) = \mathbb{Z} \oplus \mathbb{Z}$. △

Example. Apply to $\mathbb{CP}^n$ to get $K^0(\mathbb{CP}^n) = \mathbb{Z}^{\oplus(n+1)}$. One can actually work out that the ring structure is $\mathbb{Z}[x]/(x^{n+1})$ with $x = [H] - 1$. △

Remark 3.10.7. If you ignore degrees, seems like we're getting no more info than one sees in singular cohomology. ∘

Note that the LES of a pair becomes a six-term long exact sequence.

$$\begin{tikzcd}
\widetilde{K}^0(X,A) \arrow[r] & \widetilde{K}^0(X) \arrow[r] & \widetilde{K}^0(A) \arrow[d] \\
\widetilde{K}^1(A) \arrow[u] & \widetilde{K}^1(X) \arrow[l] & \widetilde{K}^1(X,A) \arrow[l]
\end{tikzcd}$$

Let's apply this to study $\mathbb{RP}^2 \hookrightarrow \mathbb{RP}^3 \twoheadrightarrow S^3$ (cofiber sequence). This gives

$$0 \longrightarrow \widetilde{K}^0(\mathbb{RP}^3) \longrightarrow \widetilde{K}^0(\mathbb{RP}^2) \longrightarrow \widetilde{K}^1(S^3)$$

but $\widetilde{K}^0(\mathbb{RP}^2) = \mathbb{Z}/2\mathbb{Z}$ and $\widetilde{K}^1(S^3) = \mathbb{Z}$, so the last map above is the zero map, so $\widetilde{K}^0(\mathbb{RP}^3) \xrightarrow{\sim} \widetilde{K}^0(\mathbb{RP}^2)$. We also have

$$\widetilde{K}^0(\mathbb{RP}^2) \to \widetilde{K}^1(S^3) \to \widetilde{K}^1(\mathbb{RP}^3) \to \widetilde{K}^1(\mathbb{RP}^2) = 0.$$

The first map looks like $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ so is 0, and hence $\widetilde{K}^1(\mathbb{RP}^3) = \mathbb{Z}$.

Now let's study $\mathbb{RP}^3 \to \mathbb{RP}^4 \twoheadrightarrow S^4$. One now gets a sequence like

$$\widetilde{K}^1(\mathbb{RP}^2) \xrightarrow{2} \widetilde{K}^0(S^4) \to \widetilde{K}^0(\mathbb{RP}^4) \to \widetilde{K}^0(\mathbb{RP}^3) \to \widetilde{K}^1(S^4) = 0.$$

This tells us that $\widetilde{K}^0(\mathbb{RP}^4)$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$. This gives two possibilities, but it turns out to be $\mathbb{Z}/4\mathbb{Z}$, so K-theory does not always have the same info as cohomology.

Claim 3.10.8. *$\widetilde{K}^0(\mathbb{RP}^4) \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof idea. Find a complex vector bundle with nontrivial characteristic classes. Like, you have some $[L] - 1 \in \widetilde{K}(\mathbb{RP}^2)$ (take L the generator of $\mathrm{H}^2(\mathbb{RP}^2; \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$) which lifts to some $[\widetilde{L}] - 1 \in \widetilde{K}(\mathbb{RP}^4)$ and you can check that $2(\widetilde{L} - 1) \neq 0$ since $w_4(\widetilde{L} \oplus \widetilde{L}) = w_2(\widetilde{L})w_2(\widetilde{L}) \neq 0$ or something like that.

Or look at the AH spectral sequence and play around with elements/multiplicativity. ■

Remark 3.10.9. In general, $\widetilde{K}(\mathbb{RP}^{2n}) = \mathbb{Z}/2^n\mathbb{Z}$. ○

Haynes sent out an email explaining the spectral sequence approach to this calculation. Here's my attempt at explaining/understanding his email.

This argument is given in more detail and greater generality in the notes for my second talk.

$\mathbb{RP}^{2n}$ supports a unique nontrivial complex line bundle L with first Chern class given by the generator of $\mathrm{H}^2(\mathbb{RP}^{2n}; \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. The AHSS for $K^*(\mathbb{RP}^{2n})$ collapses on the E_2-page since $\mathrm{H}^*(\mathbb{RP}^{2n}; \mathbb{Z}) \simeq \mathbb{Z}[c]/(2c, c^{n+1})$ (with $c = c_1(L)$) is even.

Along the main diagonal $E_2^{p,-p} = \mathrm{H}^p(\mathbb{RP}^{2n}; K^{-p}(*))$ you find an algebra isomorphic to $\mathrm{H}^*(\mathbb{RP}^{2n}; \mathbb{Z})$ ($E_2^{p,-p} = 0$ when p odd since $K^{\mathrm{odd}}(*) = 0$ and $E_2^{p,-p} = \mathrm{H}^p(\mathbb{RP}^{2n}; \mathbb{Z})$ when p even since $K^{\mathrm{even}}(*) = 0$. The multiplicative structure is basically cup product).

The class $x = 1 - L \in K^0(\mathbb{RP}^{2n}, *) = \widetilde{K}^0(\mathbb{RP}^{2n})$ is in filtration 2 (because its virtual dimension is 0) and reduces mod filtration 3 to a generator for $E_2^{2,-2}$, that is, to c.

This is $K^*((\mathbb{RP}^{2n})^2, ($ $K^*(\mathbb{RP}^2, \mathbb{RP}^1)$ $\widetilde{K}(S^2)$, right?

First index is filtration, and sum of indices $2 - 2 = 0$ is the degree

Now, $2c_1(L) = 0$ implies that $L^2 = 1$, so

$$x^2 = (1 - L)^2 = 1 - 2L + 1 = 2(1 - L) = 2x.$$

This solves the additive extension problem.

$x = 1 - L$ is the K-theoretic Chern class of $-L$, so $(-L)^2 = 1$ tells us that $2x - x^2 = 0$ since K-theory has the multiplicative formal group law

Since $x = 1 - L$ is in filtration 2, x^{n+1} is in $F^{2(n+1)} = 0$ (as $2(n+1) > 2n = \dim \mathbb{RP}^{2n}$), so

$$K(\mathbb{RP}^{2n}) = \mathbb{Z}[x]/(x^2 - 2x, x^{n+1}).$$

As a group, this is $\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z}$. Also, $K^1(\mathbb{RP}^{2n}) = 0$, so the Milnor sequence implies that

$$K(\mathbb{RP}^\infty) = \frac{\mathbb{Z}[\![x]\!]}{(x^2 - 2x)} = \mathbb{Z} \oplus \mathbb{Z}_2$$

where $\mathbb{Z}_2$ is the 2-adic integers.

Alternative definition of relative K-theory Consider triples (E_1, E_2, α) where E_1, E_2 vector bundles over X and $\alpha : E_1|_A \to E_2|_A$ is an isomorphism. Can think of this as a two term exact sequence

$$0 \longrightarrow E_1|_A \xrightarrow{\sim} E_2|_A \to 0.$$

We now impose the following equivalence relation:

- $(E_1, E_0, \alpha_1) \sim (E_1 \oplus G, E_0 \oplus G, \alpha_1 \oplus \mathrm{id}_G|_A)$.

- If you have a commutative square (τ an iso)

$$\begin{tikzcd} E_1|_A \arrow[r, "\alpha"] \arrow[d, "\tau_1"'] & E_0|_A \arrow[d, "\tau_0"] \\ F_1|_A \arrow[r, "\beta"] & F_0|_A \end{tikzcd}$$

  then $(E_i, \alpha) \sim (F_i, \beta)$.

When $A =$, these equiv classes map to $\widetilde{K}(X)$ via $(E_1, E_0, \alpha) \mapsto [E_1] - [E_0]$. In general, we can map equiv classes to $\widetilde{K}(X, A) = \widetilde{K}(X/A)$. Starting by finding G s.t. $E_0 \oplus G \cong \underline{m}$ so $(E_1, E_0, \alpha) \sim (E_1 \oplus G, \underline{m}, \alpha_1 \oplus \mathrm{Id}_{G|A})$ and we obtain trivialization of $E_1 \oplus G$ over A which defines a bundle over X/A.

Example. When $(X, A) = (D^2, S^1)$, we can take $E_1 = E_0 = \underline{\mathbb{C}}$ with map $\alpha_z : v \mapsto zv$ ($z \in D^2$) which is an iso outside the origin. This gives the generator of $\widetilde{K}(D^2, S^1) = \widetilde{K}(S^2)$. △

One can use this chain complex description to define the product structure on relative K-groups. See Atiyah's book; I don't want to write down the formula.

3.11 David: Vector Fields on Spheres, Adams

3.11.1 Talk I Notes

Notation 3.11.1. Throughout, we write $n = (2a + 1)2^b \in \mathbb{Z}_{>0}$ and $b = c + 4d$ (with $0 \le c \le 4$). Also, $\rho(n) = 2^c + 8d$ is the **Radon-Hurwitz number**.

Our goal is the following.

Theorem 3.11.2. *There exists at most $\rho(n) - 1$ linearly independent vector fields on S^{n-1}.*

Remark 3.11.3. Note that $\rho(16n) = \rho(n) + 8$. ○

Let $\varphi(k) = \#$ of positive integers at most k which are 0,1,2,4 $\pmod 8$, and let $a_k := 2^{\varphi(k)}$. The main theorem is equivalent to the following.

Proof. If S^{n-1} admits k vector fields, then $a_k \mid n$. ■

Let's make some observations.

- Gram-Schmidt let's us make our vector fields orthonormal at each point
- Under standard embedding $S^{n-1} \hookrightarrow \mathbb{R}^n$, the tangent space at $x \in S^{n-1}$ can be identified with $x^\perp$. Hence, need to find $v_1, \ldots, v_k : S^{n-1} \to S^{n-1}$ such that $\{x, v_1(x), \ldots, v_k(x)\}$ is orthnormal for all x.
- S^{n-1} admits k vector fields iff Stiefel manifold projection $V_{n,k+1} \to V_{n,1} = S^{n-1}$ has a section where $V_{n,k+1}$ is $(k + 1)$-frames in $\mathbb{R}^n$
- If S^{n-1} admits k vector fields, then so does S^{pn-1} for all $p \in \mathbb{Z}_{>0}$.

Parrallelizable spheres

Corollary 3.11.4. *The only parallelizable spheres are S^0, S^1, S^3, S^7.*

Note the implications: division algebra structure on $\mathbb{R}^n \implies$ parallelizability of $S^{n-1} \implies H$-space structure on $S^{n-1} \implies$ Hopf invariant one elment in $\pi_{2n-1}(S^n)$ (these all turn out to be equivalences).

Construction of vector fields The numbers $\rho(n) - 1$ appearing in the mai theorem are optimal.

Goal. Construct k vector fields on $S^{a_k - 1}$.

Definition 3.11.5 (Clifford algebra). $C_{p,q}$ is an associative $\mathbb{R}$-algebra generated by $e_1, \dots, e_{p+q}$ satisfying

$$e_1^2 = \cdots = e_p^2 = -1 \text{ and } e_{p+1}^2 = \cdots = e_{p+q}^2 = 1$$

and $e_i e_j = -e_j e_i$. ◇

Proposition 3.11.6. *If $C_{k,0}$ acts linearly on $\mathbb{R}^n$, then there exist k vector fields on S^{n-1}.*

Proof. Take any inner product $\langle -, - \rangle$ on $\mathbb{R}^n$ and averate it wih the group $\{\pm e_{i_1} \dots e_{i_s} : i_1 < \cdots < i_s\}$ of monomials to get an invariant inner product $(-,-)$. Can check that for $v \in S^{n-1}$, we have $(v, e_i v) = 0$ for all i (multipliy both by e_i) and $(e_i v, e_j v) = 0$ for all $i \neq j$. Thus,

$$(e_1 \times -), (e_2 \times -), \dots, (e_k \times -) : S^{n-1} \to S^{n-1}$$

gives an orthonormal vector field. ■

Example. $C_{0,0} \simeq \mathbb{R}, C_{1,0} \simeq \mathbb{C}$, and $C_{2,0} \simeq \mathbb{H}$.

$C_{0,1} \simeq \mathbb{R} \oplus \mathbb{R}$ and $C_{0,2} \simeq \mathbb{R}(2)$, 2x2 real matricies. △

Proposition 3.11.7. $C_{0,k+2} \simeq C_{k,0} \otimes C_{0,2}$ *and* $C_{k+2,0} \simeq C_{0,k} \otimes C_{2,0}$.

* David has a table of these for $k \leq 8$, but I can't tex that fast enough *

Note that $C_{k+8,0} \simeq C_{k,0}(16)$. One can show that $C_{k,0}$ acts on $\mathbb{R}^{a_k}$ (assuming I heard correctly).

Reduction of main theorem to Adams' Theorem 1.2

Notation 3.11.8 (Stunted Projective Spaces). Set $\mathbb{RP}^a_b := \mathbb{RP}^a / \mathbb{RP}^{b-1}$.

Theorem 3.11.9 (Adams' Theorem 1.2)**.** *There is no map $r : \mathbb{RP}_m^{m+\rho(m)} \to S^m$ such that*

$$S^m \simeq \mathbb{RP}^m_m \hookrightarrow \mathbb{RP}_m^{m+\rho(m)} \xrightarrow{r} S^m$$

has degree 1.

Proof Sketch. Suppose there exists $\rho(n)$ vector fields on S^{n-1} and assume $n \gg \rho(n)$ (multiply it by a large odd number). Recall that is equivalent to saying that $V_{n,\rho(n)+1} \to S^{n-1}$ has a section.

- THe first step is showing there is a $2(n - \rho(n) - 1)$-connected map

$$\mathbb{RP}^{n-1}_{n-\rho(n)-1} \to V_{n,\rho(n)+1}.$$

We have

$$\begin{tikzcd}
 & \mathbb{RP}^{n-1}_{n-\rho(n)-1} \arrow[r] \arrow[d] & \mathbb{RP}^{n-1}_{n-1} \arrow[r, "\sim"] & S^{n-1} \\
S^{n-1} \arrow[r] \arrow[ur, dashed] & V_{n,\rho(n)+1} \arrow[r] & V_{n-1} \arrow[ur, "\sim"] &
\end{tikzcd}$$

If $2(n-\rho(n)-1) \geq n$, then the dashed arrow above exists, and the left triangle commutes up to homotopy.

- Take the Spanier-Whitehead dual. The duals of $S^{n-1}, \mathbb{RP}^{n-1}_{n-\rho(n)-1}$ are $S^{1-n}, \Sigma\,\mathbb{RP}^{\rho(n)-n}_{-n}$, so we get a retract

  $$S^{1-n} \simeq \Sigma\,\mathbb{RP}^{-n}_{-n} \to \Sigma\,\mathbb{RP}^{\rho(n)-n}_{-n} \dashrightarrow S^{1-n}$$

  or

  $$S^{-n} \to \mathbb{RP}^{\rho(n)-n}_{-n} \to S^{-n}.$$

- Suspend these to come back to actual spaces. It is plausible that $\Sigma^r S^{-n} = S^{r-m}$, but what about stunted projective spaces?

  Theorem 3.11.10 (James Periodicity). *There is an integer $r \in \mathbb{Z}_{>0}$ depending on k such that*

  $$\Sigma^r\,\mathbb{RP}^{n+k}_{n} \simeq \mathbb{RP}^{n+r+k}_{n+r}$$

  for all $n \in \mathbb{Z}$.

  Using this, we can suspend our preious map to get

  $$S^{qr-n} \to \mathbb{RP}^{qr-n+\rho(n)}_{qr-n} \to S^{qr-n}.$$

  Take $2n \mid q$ and define $m := qr-n = n \times \text{odd}$, so $\rho(m) = \rho(n)$. This then gives

  $$S^m \to \mathbb{RP}^{m+\rho(m)}_{m} \to S^m$$

  of degree 1, a contradiction.

■

Let's revisit these steps in more detail.

Step 2 of the reduction We need a suitable category for negative suspensions.

Definition 3.11.11. The **Spanier-Whitehead Category** SW has objects (X, n) with X a pointed finite CW-complex and $n \in \mathbb{Z}$. We also denote this as $\Sigma^{-n}X$. The morphisms are

$$\{(X,n),(Y,m)\} := \varinjlim_{\varepsilon}[\Sigma^{\varepsilon+n}X, \Sigma^{\varepsilon+m}Y].$$

This is a symmetric monoidal category with respect to smash product $\wedge$. ◇

Remark 3.11.12. $(X,n) \wedge (Y,m) = (X \wedge Y, n+m)$ and the identity is $S^0 = (S^0, 0)$. ○

Fact. $\mathrm{Th}(V+\varepsilon) \simeq \Sigma T(V)$ where ε is a trivial real line bundle.

Definition 3.11.13. Given a finite CW-complex X and a virtual vector bundle $V = [E] - m \in KO(X)$, we define its **Thom space** $\mathrm{Th}(X, V)$ (or $\mathrm{Th}(V)$) in SW as $\Sigma^{-m}\,\mathrm{Th}(E)$. $\diamond$

Proposition 3.11.14.

$$\mathbb{RP}^{n-1}_{n-k} \simeq \mathrm{Th}(\mathbb{RP}^{k-1}, (n-k)L)$$

where L is the tautological line bundle.

Proof. Note $L \simeq S^{k-1} \times_{\mathbb{Z}_2} \mathbb{R}$ and consider the inclusion $S^{k-1} \hookrightarrow S^{n-1}$. Let N be a tubular neighborhood of S^{k-1}, so $N \simeq$ normal bundle, which is trivial in this case. The complement $S^{n-1} \setminus N \simeq S^{n-k-1}$ (deformation retracts).[31] Now, we have $(n-k)L \simeq S^{k-1} \times_{\mathbb{Z}_2} \mathbb{R}^{n-k}$. To construct $\mathrm{Th}(\mathbb{RP}^{k-1}, (n-k)L)$, quotient everything by $\mathbb{Z}_2$ (so $N \rightsquigarrow (n-k)L$) and then quotient everything outside of N. However, this is the same process as gets us the stunted projective space

$$\mathbb{RP}^{n-1}_{n-k} = \mathbb{RP}^{n-1} / \mathbb{RP}^{n-k-1}$$

so they are homeomorphic. ■

Remark 3.11.15. We can now define $\mathbb{RP}^a_b$ for any integers $a \geq b$ as $\mathrm{Th}(\mathbb{RP}^{a-b}, bL)$ (i.e. b can be negative). $\circ$

Definition 3.11.16. We say Y is a **Spanier-Whitehead dual** of X is there are maps $S^0 \to Y \wedge X$ and $X \wedge Y \to S^0$ such that

$$X \simeq X \wedge S^0 \to X \wedge Y \wedge X \to S^0 \wedge X \simeq X$$

(and similarly for Y) are identities. Hence, we have adjunctions

$$\{W \wedge X, Z\} \simeq \{W, Z \wedge Y\}$$

and similarly with X, Y swapped. Write DX for the dual of X. $\diamond$

Example. $DS^n \simeq S^{-n}$. $\triangle$

Theorem 3.11.17. *Duals exist (note we're only considering finite complexes)*

Let's compute some duals.

Theorem 3.11.18 (**Alexander Duality**). *If $X \subset S^n$ and $S^n \setminus X \simeq A$, then $DX \simeq \Sigma^{1-n} A$.*

We won't prove this, but why Σ^{1-n}? If $A \hookrightarrow S^n \setminus X$, we can define a map $\Sigma(X \wedge A) \simeq X * A \to S^n$ using geodesics ($*$ for join here). Desuspending, we get a map $X \wedge \Sigma^{1-n} A \to S^0$ and adjunction now gives $\Sigma^{1-n} A \to DX$.

Theorem 3.11.19 (**Atiyah Duality**). *Let M be a compact manifold with boundary. Then,*

$$D(M/\partial M) \simeq \mathrm{Th}(M, -TM).$$

[31] e.g. remove equation of S^2 and result deformation retracts onto S^0

Proof. Find a smooth embedding $M \hookrightarrow D^N$ such that $\partial D^N \cap M = \partial M$ transversally. Let N be a tubular neighborhood of M, so $N \simeq \nu$, the normal bundle. Then, $M/\partial M \hookrightarrow D^N/\partial D^N = S^N$ and $S^N - M\partial M \simeq D^N - M \simeq D^N - N$. Also, $\Sigma(D^N - N) \simeq N/\partial N = \mathrm{Th}(M, \nu)$.

Attach a disk D^N to one half of the suspension and homotopy the contraction to inclusion in D^N to get a space that looks like mapping cone of inclusion

Apply Alexander duality to conclude that

$$D(M/\partial M) \simeq \Sigma^{1-N}(D^N - N) \simeq \Sigma^{-N}(\mathrm{Th}(M, \nu)) \simeq T(M, \nu - N\varepsilon) \simeq T(M, -TM).$$

■

Now let M be a closed manifold without boundary, and let $V \to M$ be a vector bundle. Apply Atiyah duality to $(B(V), S(V))$ to get

$$D\,\mathrm{Th}(V) \simeq \mathrm{Th}(B(V), -TB(V)) \simeq \mathrm{Th}(B(V), -V - TM) \simeq \mathrm{Th}(M, -TM - V).$$

Corollary 3.11.20. $D\,\mathbb{RP}^{n-1}_{n-k} \simeq \Sigma\,\mathbb{RP}^{-n+k-1}_{-m}$

Step 3 in the reduction We want stunted projective spaces to suspend to other stunted projective spaces.

Theorem 3.11.21. *There's some $r > 0$, depending on k, such that $\Sigma^r\,\mathbb{RP}^{n+k}_n \simeq \mathbb{RP}^{n+k+r}_{n+r}$ in* SW.

Proof. It suffices to have $nL + r = (n+r)L$ in $KO(\mathbb{RP}^n)$. So the question is, does $L - 1 \in \widetilde{KO}(\mathbb{RP}^k)$ have finite order? Yes it is by AHSS. ■

This just leaves step 1 and Adams' theorem 1.2. More on this next time.

3.11.2 Talk II Notes

Let's prove Adam's theorem 1.2. We'll need K-theory to do this.

Notation 3.11.22. KO is real K-theory and K is complex K-theory.

We will construct Adams operations using the method in Atiyah's book, not the one Adams uses.

Proposition 3.11.23. *There is a map* $\mathrm{Vect}(X) \to 1 + k(X)[\![t]\!]^+$ *(power series with constant term* 1 *and coefficients in* $K(X)$*) given by*

$$E \mapsto 1 + \sum_{i \geq 1} \left[\bigwedge^i E\right] t^i.$$

This is a homomorphism of monoids, but the RHS is an abelian group, so it extends to a group homomorphism $\lambda_t : K(X) \to 1 + K(X)[\![t]\!]^+$.

Proof. To show $\lambda_t(E \oplus F) = \lambda_t(E)\lambda_t(F)$, use

$$\bigwedge^n (E \oplus F) = \bigoplus_{i+j=n} \bigwedge^i E \otimes \bigwedge^j F.$$

■

For $x \in K(X)$, we can now consider the power series

The log power series does not make sense in K-theory since it involves derivation. Hence, we

$$\psi_t(x) = -t\frac{\partial}{\partial t}\lambda_{-t}(x) = -t\frac{\frac{\partial}{\partial t}\lambda_{-t}(x)}{\lambda_{-t}(x)} = \sum_{k\geq 1}\psi^k(x)t^k.$$

The k**th Adams operation** $\psi^k : K(X) \to K(X)$ is the kth coefficient in the above power series (when $k \geq 1$). Here are some properties

- ψ^k is natural
- ψ^k is a ring homomorphism

  We used log in the definition in the hopes of getting something additive. However, we got even more than that for free; these operations are also multiplicative

  Proof. We'll prove additivity at least. Have have $\lambda_{-t}(x+y) = \lambda_{-t}\lambda_{-y}$. Taking the derivative of log, we get

  $$\frac{\partial}{\partial t}(\log\lambda_{-t}(x+y)) = \frac{\partial}{\partial t}\left(\log\lambda_{-t}(x) + \log\lambda_{-t}(y)\right)$$

  ■

- For a line bundle L, $\psi^k([L]) = [L]^k$

  Proof. $\lambda_{-t}([L]) = 1 - t[L]$. We can just compute this by hand

  $$\sum\psi^k([L])t^k = -t\frac{\frac{\partial}{\partial t}\lambda_{-t}([L])}{\lambda_{-t}([L])} = \frac{(-t)(-[L])}{1-t[L]} = t[L] + t^2[L]^2 + \dots.$$

  ■

- $\psi^k \cdot \psi^\ell = \psi^{k\ell}$
- For any prime p, $\psi^p(x) \equiv x^p \mod p$.

Most of what we did not prove explicitly follows from the splitting principle and checking in the case of a sum of line bundles.

Remark 3.11.24 (**Splitting Principle**). For each $E \to X$, there is a $p : Y \to X$ such that p^*E is a sum of line bundles and $p^* : K^*(X) \hookrightarrow K^*(Y)$ is monic/injective. ∘

Proposition 3.11.25. *If $u \in \widetilde{K}(S^{2n}) \cong \mathbb{Z}$, then $\psi^k(u) = k^n u$.*

Proof. $\widetilde{K}(S^2)$ is generated by $h := [H] - 1$ with $h^2 = 0$. Hence,

$$\psi^k(h) = \psi^k(1+h) - \psi^k(1) = (1+h)^k - 1 = kh$$

using $h^2 = 0$.

In general, $\widetilde{K}(S^{2n}) = \widetilde{K}(S^2\wedge\cdots\wedge S^2) \simeq \widetilde{K}(S^2)\otimes\cdots\otimes\widetilde{K}(S^2)$ generated by $h^{\otimes n}$. Adams operations are still multiplicative on this exterior tensor product (which is just interior tensor product on the product space), so

$$\psi^k(h^{\otimes n}) = (\psi^k h)^{\otimes n} = (kh)^{\otimes n} = k^n h^{\otimes n}.$$

■

Remark 3.11.26. The Adams operation is very not stable. It does not commute with Bott periodicity. ○

We can define λ_t and ψ^k for KO-theory in the same way. However, we do not have the splitting principle to prove the properties, so need a different approach.

- Can use representation theory defintion of operations as Adams does
- Can use Atiyah's KR-theory

The point is that the same properties hold.

Proposition 3.11.27. *ψ^k commutes with complexification $c : KO(-) \to K(-)$.*

Proposition 3.11.28. *If $u \in \widetilde{KO}(S^{4n}) \simeq \mathbb{Z}$, then $\psi^k(u) = k^{2n}u$.*

Since Adams operations commute wtih complexification, suffices to show that complexification is injective.

Lemma 3.11.29. *$\widetilde{KO}(S^{4n}) \xrightarrow{c} \widetilde{K}(S^{4n})$ is an iso if n is even, and is a monomorphism with image $2\mathbb{Z}$ if n is odd.*

Proof. Complexification is the map $c : O \to U$. The above is just the LES

$$\pi_{4n}(U/O) \to \pi_{4n-1}(O) \to \pi_{4n-1}(U) \to \pi_{4n-1}(U/O) \to \pi_{4n-2}(O)$$

$+$ Bott periodicity ■

Computation of some K-groups Recall our new favorite spectral sequence

$$E_2 = \mathrm{H}^p(X, K^q(*)) \implies K^{p+q}(X)$$

for X a (finite) CW-complex.

Theorem 3.11.30. *Let $\mu = \eta - 1 \in \widetilde{K}(\mathbb{CP}^n)$ where η the tautological line bundle.*

- $K(\mathrm{SP}^n) \simeq \mathbb{Z}[\mu]/\mu^{n+1}$, $\widetilde{K}(\mathbb{CP}^n) \simeq \mathbb{Z}^n$
- $\widetilde{K}(\mathbb{CP}^n \,/\, \mathbb{CP}^m) \simeq \mathbb{Z}^{n-m}$

More precisely,

$$\widetilde{K}(\mathbb{CP}^n \,/\, \mathbb{CP}^m) \simeq \ker(\widetilde{K}(\mathbb{CP}^n) \to \widetilde{K}(\mathbb{CP}^m)) \simeq \mathbb{Z}\left\langle \mu^{m+1} \right\rangle + \cdots + \mathbb{Z}\left\langle \mu^{m} \right\rangle$$

Write $\mu^{(m+1)} \mapsto \mu^{m+1}$.

Proof. The AHSS is trivial. Why does μ represent a generator of $E^{2,-2}$? Consider

$$E^{2,-2}(\mathbb{CP}^n) \xrightarrow{\sim} E^{2,-2}(\mathbb{CP}^1)$$

which sends $\mu \mapsto \mu$, but we know $\mu \in E^{2,-2}(\mathbb{CP}^1)$ is a generator. ■

Let $\pi : \mathbb{RP}^n \to \mathbb{CP}^{\lfloor n/2 \rfloor}$ be the natural map. This exists by lookinag at the diagram

$$\begin{tikzcd}
 & S^{2k+1} \arrow[d, two heads] \arrow[dr, two heads] & \\
\mathbb{RP}^{2k} \arrow[r, hook] & \mathbb{RP}^{2k+1} \arrow[r, dashed, "\pi"] & \mathbb{CP}^k
\end{tikzcd}$$

Theorem 3.11.31.
- *$\widetilde{K}(\mathbb{RP}^n) \simeq \mathbb{Z}_{2^{\lfloor n/2 \rfloor}}$ generated by $\nu = \pi^*\mu$. Also $\nu^2 = -2\nu$ and $\nu^{\lfloor n/2 \rfloor + 1} = \pm 2^{\lfloor n/2 \rfloor}\nu = 0$.*

- *$\widetilde{K}(\mathbb{RP}^n \,/\, \mathbb{RP}^{2t}) \simeq \mathbb{Z}_{2^{\lfloor n/2 \rfloor - t}}$. More precisely,*

$$\widetilde{K}(\mathbb{RP}^n \,/\, \mathbb{RP}^{2t}) \simeq \ker(\widetilde{K}(\mathbb{RP}^n) \to \widetilde{K}(\mathbb{RP}^{2t})) \simeq \left\langle \nu^{t+1} \right\rangle \simeq \left\langle 2^t \nu \right\rangle.$$

This is the case iff $\widetilde{K}(\mathbb{RP}^n \,/\, \mathbb{RP}^{2t}) \to \widetilde{K}(\mathbb{RP}^n)$ is monic. Wrtie $\nu^{(t+1)} \mapsto \nu^{t+1}$.

- *$\widetilde{(}\mathbb{RP}^n \,/\, \mathbb{RP}^{2t-1}) \simeq \mathbb{Z} \oplus \mathbb{Z}_{2^{\lfloor n/2 \rfloor - t}}$ More precisely,*

$$0 \longrightarrow \widetilde{K}(\mathbb{RP}^n \,/\, \mathbb{RP}^{2t}) \longrightarrow \widetilde{K}(\mathbb{RP}^n \,/\, \mathbb{RP}^{2t-1}) \longrightarrow \widetilde{K}(\mathbb{RP}^{2t} \,/\, \mathbb{RP}^{2t-1}) \longrightarrow 0$$

is split exact. Note that the quotient above is $\widetilde{K}(S^2) \simeq \mathbb{Z}$. We have the following picture

TODO: Add Diagram

- *Let $\varepsilon = 0$ if k even and $\varepsilon = 1$ if k odd. Then,*

$$\psi^k \nu^{(t+1)} = \varepsilon \nu^{(t+1)}$$

and

$$\psi^k \overline{\nu}^{(t)} = k^t \overline{\nu}^{(t)} + \frac{k^t - \varepsilon}{2} \nu^{(t+1)}$$

This will all come from the AHSS, so first calculate ordinary comohomology of stunted projective spaces, and then use that. The spectral sequence will be trivial (on E_2-page); most of everything is concentrated on even degrees, except when n is odd, we get $\mathbb{Z}$'s at $E^{n,2i}$ only at the last column (and there's no nontrivial map $\mathbb{Z}_2 \to \mathbb{Z}$). Also need to compare to complex projective space.

We now want KO-group of real projective space. Let ξ be the topological line bundle on $\mathbb{RP}^n$ and $\lambda = \xi - 1$.

Lemma 3.11.32. *$c\lambda = \nu$.*

Proof. Only two complex line bundles on $\mathbb{RP}^n$, so just need to check that $c\lambda$ is nontrivial. Its Chern class is the nontrivial Stiefel-Whitney class. ∎

Theorem 3.11.33.
- *$\widetilde{KO}(\mathbb{RP}^n) \simeq \mathbb{Z}_{2^{\varphi(n)}}$ generated by λ. Also, $\lambda^2 = -2\lambda$.*

Question: What is φ?

- *... (3 fast 5 me)*

Theorem 3.11.34. *There is no map*

$$r : \mathbb{RP}^{m+\rho(m)} \,/\, \mathbb{RP}^{m-1} \to S^n$$

such that $S^m = \mathbb{RP}^m \,/\, \mathbb{RP}^{m-1} \hookrightarrow \mathbb{RP}^{m+\rho(m)} \,/\, \mathbb{RP}^{m-1} \xrightarrow{r} S^m$ *has degree* 1*. Write* $m = (2a+1)2^b$ *with* $b = ...$

3.12 Deeparaj: The Geometry of Iterated Loop Spaces, May

3.12.1 Talk Notes

Operads

Definition 3.12.1. An **operad** is $\{C(j), \gamma\}$ with $C(j)$ spaces and γ as below

$$: \gamma : C(k) \times C(j_1) \times \ldots \times C(j_k) \to C(j) \text{ with } j = \sum_i j_i.$$

This operation is meant to be "associative" in the expected way that's annoying to write down formally. Furthermore, $C(0) = *$ and $\exists 1 \in C(1)$ such that

$$\gamma(1; d) = d \text{ and } \gamma(c; 1, 1, \ldots, 1) = c.$$

There's a permutation group acting on inputs which has some some sort of equivariance property. ◇

Example. The N operad with $C(j) = *$ for all j, Σ-action trivial, γ trivial. △

Example. The M operad. $C(j) = \Sigma_j$ with obvious Σ_j action. $\gamma(e_k; e_{j_1}, e_{j_2}, \ldots, e_{j_k}) = e_j$ with e_r the basepoint/identity in $\Sigma_r = C(r)$. △

Example. For a pointed space X, get endo operad $\mathrm{End}_X(j) = C^0(X^j, X)_*$. We set

$$\gamma(f; g_1, g_2, \ldots, g_k)(x_1, x_2, \ldots, x_j) = f(g_1(x_1, \ldots), g_2(x_{j_1}, \ldots), \ldots)$$

and Σ_j acts by permuting X^j. △

Definition 3.12.2. An **action of an operad** C **on a space** X is a "morphism" of operads $\Theta : C \to \mathrm{End}_X$, i.e. $\Theta_j : C(j) \times X^j \to X$ such that $\Theta_j(-, *) = *$ and all associativity and equivariance conditions you expect. ◇

Example. $\Theta : N \to \mathrm{End}_X$ gives a unique n-ary operation for every n. If $x_1 \cdot x_2$ is the 2-ary operation, then

$$(x_1 \cdot x_2) \cdot x_3 = x_1(\cdot x_2 \cdot x_3) = x_2 \cdot (x_1 \cdot x_3)$$

and $(* \cdot x) = x$, i.e. X is a commutative monoid with $* = 1$, e.g. $X = (\mathbb{Z}_{\geq 0}, +)$. The converse holds as well, N acts on $X \iff X$ is a commutative monoid. △

Example. $\Theta : M \to \mathrm{End}_X$ with 2-ary op $x_1 \cdot x_2 = \theta_2(e_2; x_1, x_2)$. As

$$x_1 \cdot (x_2 \cdot x_3)\gamma(e_2; e_1, e_2) = e_3 = \gamma(e_2, e_2, e_1) = (x_1 \cdot x_2) \cdot x_3$$

we have associativity, e.g. $X = (\mathrm{End}_k(V), \cdot)$. Think of $M(j) = \Sigma_j$ as reflecting the fact that order matters. $\triangle$

Example. Let C_n denote the **little n-cube operad** which has $C_n(j) = \{j \text{ disjoint, ordered } n\text{-cubes in a fixed } n\text{-cube}\}$. The composition operation is by placing all your cubes together in a another cube (resizing allowed). $\triangle$

Example. C_n acts on $\Omega^n X$ thinking of $\Omega^n X$ as maps $(I, \partial I^n) \cong (S^n, *) \to X$.

In fact, if X is connected and there is a C_n-action on X, then there exists a Y such that $X \simeq \Omega^n Y$. $\triangle$

> Haynes called this an n-fold classifying space

Definition 3.12.3. A **monad** (C, μ, η) is a functor with nat transformations $\eta : 1 \to C$ and $\mu : C^2 \to C$ satisfying associativity and identity, e.g.

$$\begin{tikzcd} C^3X \arrow[r, "C\mu"] \arrow[d, "\mu C"'] & C^2X \arrow[d, "\mu"] \\ C^2X \arrow[r, "\mu"] & CX \end{tikzcd}$$

and the obvious identity diagram commute. $\diamond$

Remark 3.12.4. An operad C gives a monad C as follows:

$$CX = \bigsqcup C(j) \times X^j$$

...

Alternative voidpoint. Say a C-space is a space X with action $C \to \mathrm{End}_X$. Then the construction CX is a left adjoint to the forgetful functor. Then abstract nonsense tells us that we get a monad. $\circ$

In general, if you have a pair of adjoint functors L, R, then LR (or RL, can't remember) is a monad.

Example. $L = C$ and $R =$forgetful or $L = \Sigma^n$ and $R = \Omega^n$. $\triangle$

An action of operad C on X is $\xi : CX \to X$ such that $\xi \circ \eta = 1$ and

$$\begin{tikzcd} C^2X \arrow[r, "C\xi"] \arrow[d, "\mu"'] & CX \arrow[d, "\xi"] \\ CX \arrow[r, "\xi"] & X \end{tikzcd}$$

commutes.

We have a morphism of monads from little n-cubes to $\Omega^n S^n$. This is the composition

$$\alpha_n : C_n \xrightarrow{C_n \eta} C_n \Omega^n S^n \xrightarrow{\xi} \Omega^n S^n$$

where ξ is the action of C_n of nth loop spaces mentioned earlier.

Note that $\Omega^n S^n X = C^0(S^n, S^n \wedge X)_*$.

Theorem 3.12.5 (Approximation Theorem). *If X is connected, $\alpha_n : C_n X \to \Omega^n S^n$ is a weak equivalence. This is also works if $n = \infty$.*

What is C_∞? We have a morphism of operads $C_n \to C_{n+1}$ which stretches rectangles (take $R \rightsquigarrow R \times [0, 1]$) and so we can and do set $C_\infty = \varinjlim_n C_n$. Alternatively, we can think of $C_n(j)$ as the configuration of j points in $\mathbb{R}^n$ (they're homotopy equivalent). With this perspective, can think of $C_n(j) \to C_{n+1}(j)$ as being induced from $\mathbb{R}^n \to \mathbb{R}^{n+1}$. Hence, $C_\infty(j) \simeq \mathrm{Conf}_j(\mathbb{R}^\infty) = E\Sigma_j$.

While we're at it, recall that we have $\Omega^n S^n \to \Omega^{n+1} S^{n+1}$ via "smashing with S^1" (the (co)unit of the adjunction) so $\Omega^\infty S^\infty = \varinjlim_n \Omega^n S^n$.

Consequences Think of MX as the free associative monoid containing X with $1 = *$ (the **James construction**), so basically (not literally) $MX = \bigcup X^j$. The theorem tells us that $MX \simeq_w \Omega X$ if X is connected.

Deeparaj has a nice example of describing the map $\alpha_1 : C_1 S^1 \to \Omega S(S^1)$, but it was very pictorial so hard to tex. Basically, an element of $C_1 S^1$ is 3 points (technically, intervals) on a line, so these correspond to 3 points on the equator of S^2 and so you get a loop on S^2 by taking the great circles between these points in the order they appear on the line.

THe proof strategy is to induct on n. We want a diagram (TX is the reduced cone on X)

$$\begin{tikzcd}
C_n X \arrow[r] \arrow[d, "\alpha_n"] & E_n(TX, X) \arrow[r, "\pi_n"] \arrow[d, "\widetilde{\alpha}_n"] & C_{n-1}(SX) \arrow[d, "\kappa_n"] \\
\Omega^n S^n X \arrow[r] & P\Omega^{n-1} S^n X \arrow[r] & \Omega^{n-1} S^{n-1}(SX)
\end{tikzcd}$$

with top map a quasi-fibration and bottom map a fibration. We will show that $E_n(TX, X) \simeq_w *$ and then this let's us conclude that α_n is a weak eq.

Note that $E_n(X, A) = [c, x_1, x_2, \ldots, x_n] \subset C_n(X)$ such that if $x_i \notin A$, then the "shadow" of C_i should be unobstructed. The map $\pi_n : E_n(X, A) \to C_{n-1}(X/A)$ is taking the shadow (think, "A is transparent; you can see through it").

We show that $E_n(X, A)$ is contractible if X is compact and contractible. Filter $F_j E_n(X, A) = [c; x_1, x_2, \ldots, x_j]$. Now, $G : I \times (F_j E_n \setminus F_{j-1} E_n) \to F_j E_n$

$$G(t, [c, x_1, \ldots, x_j]) = [c, g(t_1, x_1), \ldots, g(t_j, x_j)]$$

(none of the x_i are the basepoint) with $g_i : I \times X \to X$ a contracting homotopy and

$$t_i = \begin{cases} t & \text{if } \; v_i(c) \leq 0 \\ t(1 - v_i(c)) \;\text{ if }\; v_i(c) \in [0,1] \\ 0 \;\text{ if }\; v_i(c) \geq 1 \end{cases}$$

and

$$v_i(c) = 2 \frac{\text{distance between rightmost cube an innermost cube}}{size of smallest cube}$$

satisfies

$$G_1(F_j E_n \setminus E_{j-1} E_n) \subset F_{j-1} E_n.$$

We can extend this to $F_{j-1}E_n$ by

$$H(t,[c,x_1,\dots,x_j]) = \begin{cases} 1 & \text{on } F_{j-1}E_n \\ G\left(t\frac{U(x_1,\dots,x_j)}{\varepsilon/2},[c,x_1,\dots,x_j]\right) \end{cases}$$

where U "meausres" how far x_i is from $*$ (there's some "good pair" nonsense going on here).

The says F_jE_n deformation retracts to $F_{j-1}E_n$ and $F_0E_n = *$, so we're essentially done. This gives weakly contractible immediately (compare with mapping telescope?), and then some more work gives contractibility on the nose.

I'm so lost. I'm gonna stop with the notes.

3.13 Jae: Spectrum of an Equivariant Cohomology Ring I, Quillen

3.13.1 Talk Notes

The goal is to study $\mathrm{H}^*(BG;\mathbb{F}_p)$ for G a compact Lie group, and p a prime.

- This is a natural followup to Borel ($\mathrm{H}^*(BO(n);\mathbb{F}_2)$)
- Resolved the Atiyah-Swan conjecture that $\dim \mathrm{H}^*(BG;\mathbb{F}_p)$ (Krull dimension) is equal to the rank of a maximal elementary abelian p-subgroup of G

The main result is that $\mathrm{H}^*(BG;\mathbb{F}_p)$ can be upderstood (up to nilpotence) in terms of the elementary abelian p-subgroups of G.

Key ingredients include

- Equivaraiant cohomology
- H^*_G as a sheaf = compatible family of functions over orbits
- Reduction to orbits for elementary abelian subgroups (faithfully flat descent)

Something came up and I missed 5 minutes. Not sure what material was said

Say $G \curvearrowright X$.

Slogan. Consider G-orbits instead of points. Moreally, $\mathrm{H}^*_G(X) \sim \mathrm{H}^*(X/G)$.

This does not work literally as said.

- remembers nothing about isotropy
- X/G is not well-behaved if the G-action is not free

The way to resolve this is to replace X with a homotopy equivalent space on which G acts freely.

Replace X with $EG\times X$ (on which G acts freely) and replace X/G with $EG\times_G X = EG\times X/(e,x) \sim (gx, gx) = X_{hG}$, the **homotopy orbit space**.

Definition 3.13.1. Borel Equivariant Cohomology is

$$\mathrm{H}^*_G(X;F) := \mathrm{H}^*(EG\times_G X;R).$$

This is functorial under equivariant pairs of maps $G \to G'$ and $X \to X'$ (i.e. these induce $\mathrm{H}^*_{G'}(X') \to \mathrm{H}^*_G(X)$) ⋄

Remark 3.13.2. This is not the finest equivariant cohomology theory one can define. For example, you have have an equivariant homotopy equivalence whose inverse is not equivariant, but this will still induce an isomorphism on Borel equivariant cohomology. ∘

Example. $X = * \implies \mathrm{H}^*_G(*) = \mathrm{H}^*(EG/G) = \mathrm{H}^*(BG) =: \mathrm{H}^*_G$ △

Example. If G acts freely on X, then $\mathrm{H}^*_G(X) = \mathrm{H}^*(EG \times_G X) \simeq \mathrm{H}^*(X/G)$ so the naive definition works. △

Example. If G acts trivially on X, then $\mathrm{H}^*_G(X) = \mathrm{H}^*(BG \times X) = \mathrm{H}^*_G \otimes \mathrm{H}^*(X)$ by Kunneth △

Remark 3.13.3. For $x \in X$ fixed by $K \le G$ (closed subgroup). Then, get a map $\mathrm{H}^*_G(Gx) \xrightarrow{\sim} \mathrm{H}^*_K$. (Quillen calls this the induction formula) ∘

What's Quillen's idea for understanding equivariant cohomology. We have two projection maps

$$BG \leftarrow EG \times_G X \to X/G.$$

The left projection is a fibration with fibers equal to X. The right projection is not a fibration; the fiber above a point $x = Gx \in X/G$ is $BG_x = B\,\mathrm{Stab}_G(x) = BK$ where $K \le G$ is the stabilizer of x under the G-action. Thus, we get the leray spectral sequences

$$\mathrm{H}^p(BG; \mathrm{H}^q(X)) \implies \mathrm{H}^{p+q}_G(X) \text{ and } \mathrm{H}^p(X/G; \mathcal{H}^q_G) \implies \mathrm{H}^{p+q}_G(X)$$

where $\mathcal{H}^q_G$ is the sheafification of

$$V \mapsto \mathrm{H}^q_G(\pi^{-1}V) \text{ for } X \xrightarrow{\pi} X/G$$

We'll use the second of these two projections/spectral sequences to study $\mathrm{H}^*_G(X)$.

Remark 3.13.4. The stalks of $\mathcal{H}^q_G$ are exactly equivariant cohomology of the fibers which, by the induction formula, is cohomology of the stabilizer. ∘

Theorem 3.13.5. *Now coefficients in $\mathbb{F}_p$ and X compact. The edge homomorphism*

$$\mathrm{H}^*_G(X) \longrightarrow \mathrm{H}^0(X/G; \mathcal{H}^*_G)$$

*has nilpotent kernel/cokernel. Quillen calls this an F-**isomorphism**.*

Proof. Multiplicative structure in spectral sequence + finite width. Edge homomorphism maps into 0th column. Being in the kernel means you have something living in column > 0. But the sequence has finite width, so the multiplicative structure says that high enough powers of it are 0 (go beyond the width). This gives nilpotent kernel.

For the cokernel, note that $\mathrm{d}_r s^p = p s^{p-1} \mathrm{d}_r s = 0$. Hence, if d is large enough, s^{p^d} will survive all the differentials and so end up surviving until the E_∞-page, so the cokernel is nilpotent as well. ■

Quillen gives a reinterpretation of $\mathcal{H}_G^*$ or at least, of its global sections. The key idea is to organize $s \in \mathrm{H}^0(X/G, \mathcal{H}_G^q)$ into the collection of data of (locally constant $s_K : X^K \longrightarrow \mathrm{H}_K^q$) fo family of subgroups $\mathscr{F} = \{K \leq G\}$. s_K forms a compatible family of maps $\mathscr{F}^q(X)$.

Given $s \in \mathrm{H}^0(X/G; \mathcal{H}_G^q)$, and $K \in \mathscr{F}$, get $s_K : X^K \to \mathrm{H}_K^q$ defined by

$s(Gx)$ is just looking at the image of s in the stalk (or fiber probably?) associated to $Gx \in X/G$

$$s_K(x) = s(Gx) \in \mathrm{H}_G^q(Gx) \xrightarrow{\sim} \mathrm{H}_K^q .$$

In what sense is this family "compatible"?

Fact. Inner automorphisms $G \to G$ and $X \to X$ via

$$g \mapsto g_0^{-1} g g_0 \text{ and } x \mapsto g_0^{-1} x$$

induce $\mathrm{id} : \mathrm{H}_G^*(X) \xrightarrow{\sim} \mathrm{H}_G^*(X)$.

Given a family $(f_K : X^K \longrightarrow \mathrm{H}_K^q)_{K \in \mathscr{F}}$, ask for $\Theta : K \to K'$ of form $\theta(k) = g_0^{-1} k g_0$ such that

$$f_K(g_0 x') = \Theta^* f_{K'}(x') \in \mathrm{H}_K^q$$

for all $x' \in X^{K'}$.

Note 10. Something like changing conjugacy classes via algebra (pulling back along Θ) is the same as doing it via topology (multiplying by g_0)

Question 3.13.6 (Audience)**.** *What if X is a point?*

Answer. This basically ends up saying you get a commuting triangle

$$\begin{tikzcd} & \mathrm{H}_G^* \arrow[dl] \arrow[dr] & \\ \mathrm{H}_{K'}^* \arrow[rr] & & \mathrm{H}_K^* \end{tikzcd}$$

so you see than you approximate H_G^* as a limit of the cohomology of subgroups. ⋆

Let $\mathscr{F}$ be a family of subgroups $K \leq G$ (orbit types). Then $\mathscr{F}$ becomes a category whose morphisms are $\Theta : K \to K'$ given by $[G/K, G/K']_G = \pi_0\left((G/K")^K\right)$ (both sides of $f_K(gx') = \Theta^* f_{K'}(x')$ only depend on this data, not the actual choice g_0 for $\Theta : K \to K', k \mapsto g_0^{-1} k g_0$)

Given $\mathscr{F}$, let $\mathscr{F}^q(X)$ be the group of compatible families of locally constant $f_K : X^K \to \mathrm{H}_K^q$, i.e. it is the equilizer

$$\mathscr{F}^q(X) \to \prod_{K \in \mathscr{F}} \mathrm{Map}(X^K, \mathrm{H}_K^q) \rightrightarrows \prod_{\Theta \in \mathrm{Mor}(\mathscr{F})} \mathrm{Map}(X^{K'}, \mathrm{H}_K^q)$$

with one arrow $(f_K) \mapsto (\Theta^* f_{K'})$ and the other arrow $(f_K) \mapsto (x' \mapsto f_K(g_\Theta x'))$.

We have defined a functor $X \mapsto \mathscr{F}^q(X)$ as a limit, for a family $\mathscr{F}$ of closed subgroups in G.

Theorem 3.13.7. *If the collection $\mathscr{F}$ exhaust the isotropy types of $G \curvearrowright X$ up to conjugacy, then $\mathrm{H}^0(X/G, \mathcal{H}_G^q) \to \mathscr{F}^q(X)$ is an isomorphism.*

Question: It seems I can think of this as sending a section to a collection of stalks, so

In practice, discussion so far not too useful unless we can control the complexity of $\mathscr{F}$. The key idea is that one can reduce to the case when $\mathscr{F}$ is take to be the family of elementary abelian subgroups $\mathscr{A}$ via faithfully flat descent.

Theorem 3.13.8. *Let $\mathcal{A}_G$ be the family of elementary abelian p-subgroups of G. Then, ...*

Proof Sketch. Embed $G \hookrightarrow U$ for unitary U (Peter-Weyl). Take a maximal torus $T \leq U$ and a subgroup $S \leq T$ or order p elements (e.g. Borel's "$Q(n)$")... ■

3.14 Cameron: On the cohomology and K-theory of the general linear groups over a finite field, Quillen

3.14.1 Talk Notes

Out goal is to calculate $K_*(\mathbb{F}_q)$ for $q = p^d$ where this is **algebraic K-theory** $K_i(R) = \pi_i(BGL(R)^+)$ of a ring.

To do this, we'll study $F\Psi^q = \text{hofiber}(1 - \Psi^q)$, the "homotopy fixed points of the adams operations." We then define $\Theta : BGL(\mathbb{F}_q) \longrightarrow F\Psi^q$ using the Brauer lift. We won't spend too much time on this, but Quillen calculates $\mathrm{H}_*(\mathrm{GL}(\mathbb{F}_q))$ and $\mathrm{H}_*(F\Psi^q)$ to see that these are (almost) homotopy equivalent (they are after applying the $+$ construction).

Algebraic K-Theory Let R be a commutative ring. We want a graded ring $K_*(R)$ that "resembles topological K-theory in definition." Recall that for a space X, we have $K^0(X) = \mathrm{Gr}(\mathrm{Vect}(X), \oplus)$, the group completion of vector bundles under addition. Similarly, we define

$$K_0(R) := \mathrm{Gr}(\mathrm{Proj}(R), \oplus)$$

where $\mathrm{Proj}(R)$ is the monoid of iso classes of f.g. projective R-modules.

Example. Let $\mathbb{F}$ be a field. Then, $K_0(\mathbb{F}) \simeq \mathbb{Z}$ since all modules over a field are free (in particular, projective), so rank : $\mathrm{Proj}(\mathbb{F}) \to \mathbb{N}$ is an iso and group completing gives the integers. △

What about K_1? We define

$$K_1(R) := \mathrm{GL}(R)^{\mathrm{ab}} = \mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)] = \mathrm{GL}(R)/E(R)$$

where $\mathrm{GL}(R) = \varinjlim_{n\to\infty} \mathrm{GL}_n(R)$. Also, $E(R)$ above is $E(R) = \varinjlim_{n\to\infty} E_n(R)$ where $E_n(R)$ are the $n \times n$ **elementary matrices** which differ by the identity in one entry.

Here's some motivation. One can calculate $K^0(\Sigma X)$ using **clutching functions**, linear maps $X \to \mathrm{GL}_n(\mathbb{C})$ specifying how fibers glue together above equator (like, $\Sigma X = CX \cup CX$ so a vector bundle on it is to trivial bundles glued above $CX \cap CX = X$). The matrices in $E_n(R)$ are connected to identity.

Example. Let $\mathbb{F}$ be a field. Then, $K_1(\mathbb{F}) = \mathbb{F}^\times$. We have $\mathrm{GL}_1 \mathbb{F} = \mathbb{F}^\times \hookrightarrow \mathrm{GL}(\mathbb{F})$ and the inverse map is $\det : \mathrm{GL}(\mathbb{F}) \to \mathbb{F}^\times$. Hence, $\mathrm{GL}\,\mathbb{F} = \mathrm{SL}\,\mathbb{F} \rtimes \mathbb{F}^\times$ and abelinizing kills the $\mathrm{SL}\,\mathbb{F}$ factor. △

Definition 3.14.1. A group P is **perfect** if $P^{\mathrm{ab}} = 0$. ⋄

Fact. $E(R)$ is a perfect normal subgroup of $\mathrm{GL}(R)$.

Let's define higher K_i.

Remark 3.14.2. $\pi_1(BGL(R)) \simeq \pi_0(GL(R)) \simeq GL(R)$ is almost K_1. ○

To fix the deficiency above, Quillen give the plus construction.

Definition 3.14.3. A **plus construction** X^+ for X has the universal property that for all maps $f : X \to Y$ such that the induced map kills perfect normal subgroups in $\pi_1(X)$, there exists a unique map f' (up to pointed homotopy) such that

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d] & Y \\ X^+ \arrow[ur, dash, "f'"] & \end{tikzcd}$$

Secretly, you can just kill a particular normal subgroup. We'll soon kill $[\mathrm{GL}(R), \mathrm{GL}(R)]$. ◇

Construction 3.14.4. Attach 2-cells to $BGL(R)$ to kill perfect normal subgroup ($[\mathrm{GL}(R), \mathrm{GL}(R)]$) in π_1, then attach 3-cells to correct for homology introduced in dim 2.

Now Quillen defines the higher algebraic K-theory groups as $K_i(R) := \pi_i(BGL(R)^+)$. This is visibly compatible with our definition of K_1 (but not with K_0).

Recall out goal is to compute $K_i(\mathbb{F}_q)$, and now we know what this means.

The Space $F\Psi^q$ The idea is to compare $BGL(\mathbb{F}_q)$ to an easier sapce, $F\Psi^q$.

Claim 3.14.5. *Since $\widetilde{K}(X) = [X, BU]$, any n-ary operations on $\widetilde{K}$ are represented by maps $BU \times \ldots \times BU \longrightarrow BU$.*

Proof. Yoneda Lemma + Milnor exact sequence (to get claim for infinite complexes). ■

Let $\sigma : BU \to BU$ represent the Adams operation Ψ^q on $\widetilde{K}$. We define $F\Psi^q$ as the pullback

$$\begin{tikzcd} F\Psi^q \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & BU^I \arrow[d] \\ BU \arrow[r, "\mathrm{id} \times \sigma"] & BU \times BU \end{tikzcd}$$

where the right vertical arrow is $p \mapsto (p(0), p(1))$. So $F\Psi^q$ is paris (x, p) with $x \in BU$ and p a path from x to $\sigma(x)$.

Lemma 3.14.6.

- $F\Psi^q$ = *homotopy fixed points of* Ψ^q
- *Furthermore, for X s.t. $[X, U] = 0$, one has*

$$[X, F\Psi^q] \xrightarrow{\sim} [X, BU]^{\Psi^q}.$$

- $F\Psi^q = \mathrm{hofiber}(1 - \sigma)$.

Above 3 above gives LES

TODO: Finish this

$$\begin{tikzcd}
\pi_{2j}(BU) \arrow[r, "1-\Psi^q"] \arrow[d, equal] & \pi_{2j}(BU) \arrow[r] \arrow[d, equal] & \pi_{2j-1}(F\Psi^q) \arrow[r] \arrow[d, equal] & \pi_{2j-1}(BU) \arrow[d, equal] \\
\mathbb{Z} \arrow[r, "(1-q^i)"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/(1-q^i)\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

with calculations given by Bott periodicity.

Cohomology of $F\Psi^q$ Pick a prime $\ell \neq p = \operatorname{char} \mathbb{F}_q$ and r minimal s.t. $q^r \equiv 1 \pmod{\ell}$.

Lemma 3.14.7.

$$\operatorname{gr} \mathrm{H}^*(F\Psi^q; \mathbb{F}_\ell) \simeq \mathbb{F}_\ell[c_r, c_{2r}, \dots] \otimes \bigwedge[e_r, e_{2r}, \dots]$$

with $\deg c_r = 2r$ *and* $\deg e_r = 2r-1$.

Proof. Using Eilenberg-Moore spectral sequence associated to a pullback square

Think of this as a Kunneth theorem over cohomology of B, but not over a PID

$$\begin{tikzcd}
E_f \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & E \arrow[d, "p"] \\
X \arrow[r, "f"] & B
\end{tikzcd}$$

(use B simply connected)

$$E_2^{s,t} = \operatorname{Tor}^{s,t}_{\mathrm{H}^*(B)}(\mathrm{H}^*(X), \mathrm{H}^*(E)) \implies \mathrm{H}^*(E_f)$$

See paper for details. Ultimately, the spectral sequence will collapse on E_2. ■

Theorem 3.14.8. *There is an algebra iso*

$$\mathbb{F}_\ell[c_r, c_{2r}, \dots] \otimes \bigwedge[e_r, e_{2r}, \dots] \simeq \mathrm{H}^*(F\Psi^q; \mathbb{F}_\ell).$$

Where do these generators come from? THe c_{jr}'s come from characterstic clases of complex representations, and the e_{jr}'s are related to Bocksteins.

Recall 3.14.9. Given a complex representation of a group G, we can get a vector bundle. From $E : G \to \mathrm{GL}_n(\mathbb{C})$, get associated bundle

$$EG \times_G \mathbb{C}^n \longrightarrow BG.$$

This then gives a classifying map $BG \to BU$. If $\Psi^q E = E$, we actually get a map $BG \to F\Psi^q$. ⊙

The Representation W Write $C = \mathbb{Z}/(q^r-1)\mathbb{Z}$ and let $\zeta : C \to \mathbb{C}^\times$ embed the roots of unity. Set $W = \zeta \oplus \zeta^q \oplus \cdots \oplus \zeta^{q^{r-1}}$, an r-dim representation.

Fact. Adams operations are also defined on $R(G)$ s.t. on 1-dim reps, $\Psi^q V = V^{\otimes q}$, and there is an analog of the splitting principle.

We see that $\Psi^q W = W$. Hence, W gives us a map $BC \to F\Psi^q$.

The classes $c_{jr}, e_{jr} \in \mathrm{H}^*(F\Psi^q)$ come from characteristic classes of a vector bundle associated to a sume of representations $\bigoplus_{i=1}^m W_i$ of C^m.

Back to $BGL(\mathbb{F}_q)$

Question 3.14.10. *How does $F\Psi^q$ relate to $BGL(\mathbb{F}_q)^+$*

Answer. These two spaces turn out to be homotopy equivalent. Quillen shows this by seeing an iso on integral homology and applying Whitehead. ⋆

Question 3.14.11. *How do we get a map $\Theta : BGL(\mathbb{F}_q) \to F\Psi^q$?*

Answer. Define a map $BGL(\overline{\mathbb{F}}_q) \to BU$ and look at fixed points of Ψ^q. ⋆

Write $k = \mathbb{F}_q$ and $G = \mathrm{GL}_n\, k$. We have a natural representation $\mathrm{GL}_n\, k \curvearrowright k^n$. Let E be a k-rep of G. We would like to turn this into a complex rep.

Recall 3.14.12. For G a finite group and $E : G \to \mathrm{GL}_n\, k$ a representation, the character of E is $\chi_E := \operatorname{tr} E(g) \in k$. ⊙

So now choose an embedding $\rho : \overline{k}^\times \hookrightarrow \mathbb{C}^\times$. This let's us define the **Brauer character** of a $\overline{k}$-rep of E as $\rho(\chi_E) : g \mapsto \sum_i \rho(\lambda_i)$. This character will then correspond to a unique virtual complex representation of G, so we get a map

$$R_{\overline{k}}(G) \longrightarrow R(G), E \mapsto \rho E.$$

Fact. On characters, Ψ^q acts by Frobenius $g \mapsto g^q$, i.e. $\Psi^q\chi(g) = \chi(g^q) = \chi(g)^q$.

Hence, we get $R_k(G) \to R(G)^{\Psi^q}$. Note that $[BG, U] = 0$ via the completion theorem in equivariant K-theory. Hence, given $E \in E_k(G)$, we get $EG\times)G\rho E \longrightarrow BG$ a complex vector bundle, and so get a map $\Theta = \Theta_E : BG \longrightarrow F\Psi^q$.

Question 3.14.13. *What representation do we pick to get Θ that induces an iso?*

Answer. We can take the standard rep $\mathrm{GL}_n\, k \curvearrowright k^n$. It decomposes into pieces L_i whose Brauer lifts are W_i, copies of W. ⋆

Skipping to the end Quillen shows that $\mathrm{H}_*(F\Psi^q; \mathbb{F}) \cong \mathrm{H}_*(BGL(\mathbb{F}_q); \mathbb{F})$ when $\mathbb{F} \in \{\mathbb{F}_\ell, \mathbb{F}_p, \mathbb{Q}\}$ which gives an iso on integral cohomology via universal coefficients.

We defined $K_i(R) = \pi_i(BGL(R)^+)$. We calculated pretty easily that

$$\pi_{2i-1}(F\Psi^q) = \mathbb{Z}/(q^i - 1)\mathbb{Z} \text{ and } \pi_{2i}(F\Psi^q) = 0.$$

We saw how to get a map $\Theta : B\,\mathrm{GL}\,\mathbb{F}_q \longrightarrow F\Psi^q$ using the Brauer lift. We have our iso on integral homology. Let's wrap it up.

The universal property of the $+$-construction says that $[BGL(R)^+, Z] \simeq [BGL(R), Z]$ for Z s.t. $\pi_1(Z)$ has no nontrivial perfect subgroups. Whitehead's theorem now gives us a homotopy equivalence $\Theta' : BGL\mathbb{F}_q^+ \xrightarrow{\sim} F\Psi^q$. Thus, for $i \geq 1$, we have

$$K_{2i}(\mathbb{F}_q) \simeq 0 \text{ and } K_{2i-1}(\mathbb{F}_q) \simeq \mathbb{Z}/(q^i - 1)\mathbb{Z}.$$

3.15 Jordan: The localization of spaces with respect to homology, Bousfield

3.15.1 Talk notes

Jordan included a nice dependency diagram for the sections of the paper, not reproduced here

There are two main results. Given a generalized homology theory h_*, Bousfield shows that h_*-localization functors exist. He all characterizes h_*-local spaces when h_* is connective.

Model Category Structure We want simplicial homotopy theory where are weak equivalences induce isomorphisms on h_*, instead of on π_*.

We are working in the category of simplicial sets.

Definition 3.15.1. A map $f : X \to Y$ is a **weak h_*-equivalence** if $f_* : h_*(X) \xrightarrow{\sim} h_*(Y)$, is an **$h_*$-cofibration** if it is a usual cofibration (i.e. injection), and is an **h_*-fibration** if it has the right lifting property against trivial cofibrations (i.e. maps $i : A \to B$ which is both a cofibration and a weak h_*-equivalence), i.e.

$$\begin{tikzcd} A \arrow[r] \arrow[d, "i"'] & X \arrow[d, "f"] \\ B \arrow[r] \arrow[ur, dashed, "\exists e"] & Y \end{tikzcd}$$

◇

Definition 3.15.2. A **closed model category** $\mathcal{C}$ is a category with classes of maps "fibrations," "cofibrations," and "weak equivalences" satisfying

(CM1) $\mathcal{C}$ is closed under finite (co)limits.

(CM2) If f, g are maps with gf defined, then if two of f, g, gf are weak equivalences, then so is the third.

(CM3) If f is a retract of g and g is a weak equivalence, fibration, or cofibration, then so if f.

(CM4) Given a commutative square

$$\begin{tikzcd} A \arrow[r] \arrow[d, "i"'] & X \arrow[d, "f"] \\ B \arrow[r] \arrow[ur, dashed, "e"] & Y \end{tikzcd}$$

where i is a cofibration, f is a fibration, and either i or f is also a weak equivalence, there exists a lift $e : B \to X$ making the diagram commute.

(CM5) Any map f can be factored in 2 ways (unclear if these factorizations have to be functorial)

- **(i)** $f = ui$, where i is a cofibration and u is a trivial fibration
- **(ii)** $f = ui$, where i is a trivial cofibration and i is a fibration

◇

Theorem 3.15.3. SSet *has a closed model category structure given by h_*-equivalences, -cofibrations, and -fibrations.*

Proof sketch. You want to show that $f : X \to Y$ is h_*-fibration and weak h_*-equivalence iff f is a Kan fibration and a weak equivalence. One you have this, most all the axioms follow except **(CM5(ii))**. That axiom is shown in section 11 of the paper. ■

Localizations Given a class W of morphisms in $\mathcal{C}$, an object $D \in \mathcal{C}$ is **W-local** if each $w : X \to Y$ in W induces a bijection

$\mathcal{C}$ here should be a homotopy category, not a model category

$$\mathrm{Hom}(Y, D) \xrightarrow{\sim} \mathrm{Hom}(X, D).$$

A **W-localization** of $A \in \mathcal{C}$ is the data of $w : A \to D$ with D being W-local and $w \in W$; this satisfies two different universal properties (consequences of the part before the semicolon)

- w is initial among morphisms $f : A \to X$ with X being W-local.
- w is terminal among morphisms $f : A \to X$ with $f \in W$.

Definition 3.15.4. A morphism class W **admits a calculus of left fractions** if

(i) W is closed under finite compositions and contains all identities (so its a subcategory containing all the objects)

(ii) W is closed under pushouts, given a pushout square

$$\begin{tikzcd} X_1 \arrow[r, "f"] \arrow[d, "w"'] & X_3 \arrow[d, "v"] \\ X_2 \arrow[r, "g"] & X_4 \end{tikzcd}$$

with $w \in W$, we get that $v \in W$ as well.

(iii) Given $X_1 \xrightarrow{w} \rightrightarrows^f_g X_3$ such that $fw = gw$ and $w \in W$, there exists some $X_3 \xrightarrow{v} X_4$ such that $v \in W$ and $vf = vg$.

$\diamond$

Lemma 3.15.5. *If W admits a calculus of left fractions, TFAE*

(i) *D is W-local*

(ii) **something unimportant for this talk**

(iii) *Each morphism $D \to Y$ in W has a left inverse (note if W satisfies 2/3, e.g. if its weak equivalences of some model category, then the left inverse will also be in W)*

In case it was not clear before, h_* is a generalized homology theory.

Remark 3.15.6. Usually, one would consider h_* as a functor on CW pairs. However, we can define h_* on simplicial pairs (K, L) using geometric realization, $h_*(K, L) = h_*(|K|, |L|)$. Let Ho denote the pointed homotopy category of Kan complexes (i.e. Kan fibrant objects) or of CW complexes; these two homotopy categories are equivalent via the geometric realization functor. Hence, there is nothing lost in working with simplicial sets. $\circ$

Lemma 3.15.7. *The class $h_* = \{$weak h_*-equivalences$\}$ admits a calculus of left fractions in* Ho.

Note that, given a space X, we can factor the terminal map $X \to *$ it functorially[32] as

$$X \overset{\sim}{\hookrightarrow} C_{h_*}X \twoheadrightarrow *$$

[32]The construction given in the paper turns out to be functorial

(i.e. trivial cofibration followed by fibration). In fancier terminology, we have a functor $C_{h_*} : \mathcal{C} \to \mathcal{C}$ ($\mathcal{C} = \mathrm{SSet}$) and a natural transformation $i : 1 \to C_{h_*}$ such that

(i) for all $X \in \mathcal{C}$, $i_X : X \to C_{h_*}X$ is an injection with $h_*(C_{h_*}X, X) = 0$

(ii) for all $X \in \mathcal{C}$, $C_{h_*}X$ is an h_*-Kan complex.

The utility of this is the following lemma.

Lemma 3.15.8. *For pointed Kan complex X, $i_X : X \to C_{h_*}X$ represents the h_*-localization of X in* Ho*.*

Characterizing Local Spaces

Assumption. Assume h_* is a connective homology theory.

Proposition 3.15.9. *If h_* is a connective homology theory, then h_* has the same acyclic spaces (vanishing h_*-homology) as $\mathrm{H}_*(-; R)$, where*

$$R \cong \mathbb{Z}[J^{-1}] \quad or \quad R \cong \bigoplus_{p \in J} \mathbb{Z}_p$$

where J is a set of primes and $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

Allegedly, this means that we get all local spaces by reducing to these two cases. Don't ask me why.

Let R be as above. Define

$$HR := \left\{ \alpha : A \to B \,\middle|\, \begin{array}{c} \alpha_* : \mathrm{H}_i(A; R) \to \mathrm{H}_i(B; R) \\ \text{iso for } i = 1 \text{ and epi for } i = 2 \end{array} \right\}$$

where A, B are groups.

Theorem 3.15.10. *The class HR admits a calculus of left fractions, and every group has an HR-localization.*

This is proven in section 7 of the paper.

We define an analogous thing for modules. Let π be a fixed group, M_π be the category of left π-modules. Define (unclear of what Z typeface Bousfield intended)

$$HZ = H\mathbb{Z} := \left\{ \alpha : A \to B \,\middle|\, \begin{array}{c} \alpha_* : \mathrm{H}_i(\pi; A) \to \mathrm{H}_i(\pi; B) \\ \text{iso for } i = 0, \text{ epi for } i = 1 \end{array} \right\}$$

where A, B are π-modules.

Theorem 3.15.11. *The class HZ admits a calculus of left fractions, and every π-module has an $H\mathbb{Z}$-localization.*

This is proved in section 8.

Theorem 3.15.12. *A connected object $X \in$ Ho is $\mathrm{H}_*(-; R)$-local iff $\pi_n X$ is HR-local for $n \geq 1$ and $\pi_n X$ is HZ-local over π_1 for $n \geq 2$.*

This is proven in section 9.

Realization theorems Bousfield studies these $H\mathbb{Z}, HR$ classes by connecting them back to topology.

Lemma 3.15.13. *$\alpha \in HR$ iff $\exists$ a map $f : X \to Y \in \mathrm{Ho}$ such that $f_* : \mathrm{H}_*(X;R) \xrightarrow{\sim} \mathrm{H}_*(Y;R)$ and $f_* : \pi_1 X \to \pi_1 Y$ is equivalent to α.*

Lemma 3.15.14. *$1 \otimes \alpha : R \otimes \pi_n X \to R \otimes M$ is in HZ iff exists a map $f : X \to Y \in \mathrm{Ho}$ s.t. $f_* : \mathrm{H}_*(X;R) \xrightarrow{\sim} \mathrm{H}_*(Y;R)$, $f_* : \pi_i X \xrightarrow{\sim} \pi_i Y$ for $i < n$, and $f_* : \pi_n X \to \pi_n Y$ is equivalent to α.*

3.16 Elia: Rational Homotopy Theory and Differential Forms, Griffiths and Morgan

3.16.1 Talk Notes

A *cdga* is a commutative differential graded algebra.

Slogan. For all 1-connected manifolds N, there is some cdga $\mathcal{M}_N$ which encodes all $\mathbb{Q}$-topological invariants.

Need a bridge between topology and commutative algebras. Let $\mathcal{A}^*(\Delta^n)$ be the $\mathbb{Q}$-poly forms on Δ^n. Let $\mathcal{A}^*(N)$ be the $\mathbb{Q}$-poly forms that are glued from forms on each simplex (N a simplicial complex). The point of this is that $\mathcal{A}^*(N)$ is a cdga, where as usual simplicial cochains are not commutative.

Fact. There's a map $\mathcal{A}^*(N) \otimes \mathbb{R} \to \Omega^*(N)$ inducing an isom on cohomology for PL manioflds.

Fact. For a general simplicial complex, $\mathcal{A}^*(N)$ computes the rational cohomology of N.

Not that we're working rationally throughout. We don't have something like the above if we were to work in positive characteristic.

Definition 3.16.1. A **Model for N** is A cdga over $\mathcal{M}_N/\mathbb{Q}$ with a map $f : \mathcal{M}_N \to \mathcal{A}^*(N)$ inducing an iso on cohomology. It is a **minimal model** if

- $\mathrm{d}\mathcal{M}_N \subset \mathcal{M}_N^{>0} \wedge \mathcal{M}_N^{>0}$ (decomposable)
- Free (as a graded commutative algebra[33]) on generators of degree ≥ 2
- $\mathrm{H}^0(\mathcal{M}_N) = \mathbb{Q}$ and $\mathrm{H}^1(\mathcal{M}_N) = 0$

$\diamond$

Theorem 3.16.2. *For any 1-connected N, $\exists!$ minimal model $\mathcal{M}_N$.*

Remark 3.16.3. Any cdga has a unique minimal model. We're just restricting to spaces because this is where our motivation for looking at this came from. $\circ$

Definition 3.16.4. A **Hirsch extension** of a cdga $\mathcal{A}$ is

$$\mathcal{A} \otimes_d \bigwedge \langle V^k \rangle,$$

where V is a vector space and $d : V \to \mathcal{A}^{k+1}$. We have V homogeneous in degree k and the $\bigwedge$ denotes a free commutative algebra (poly if k even and exterior if k odd). $\diamond$

[33] exterior in odd degrees, polynomial in even

Slogan. A Hirsh extension is like attaching k-cells to a CW-complex

Example. $\mathcal{M}_{S^2} = \langle x^{(2)}, y^{(3)} : \mathrm{d}y = x \wedge x \rangle$. Need $x^{(2)}$ for generate in degree 2, but then we need to kill $x^2 = x \wedge x$, so we introduce y in degree 3 (and $y^2 = 0$ since it lives in odd degree) △

Proof Sketch of Existence. Induct on grading. Say we have

$$p : \mathcal{M}(n) \longrightarrow \mathcal{A}^*(N)$$

the minimal model for elements of degree $\leq n$, i.e.

- $\mathcal{M}(n)$ min generators in deg $\leq n$
- p^* isom on H^k for $k \leq n$
- p^* inj on H^{n+1}

Let $V = \mathrm{H}^{n+1}(\mathcal{M}(n), \mathcal{A}(n))$ where this relative cohomology means closed forms in $\mathcal{M}(n)$ which p maps to exact forms in $\mathcal{A}(n)$.

Take $\mathcal{M}(n+1) = \mathcal{M}(n) \otimes_d \bigwedge \langle V^{n+1} \rangle$. Any $v \in V$ gives rise to some $m_v \in \mathcal{M}(n)$ and $a_v \in \mathcal{A}(N)$ with $\rho(m_v) = \mathrm{d}a_v$. Thus, we set $\mathrm{d}v = m_v$ and $\rho(v) = a_v$. Then one uses the 5-lemma. ■

Homotopy for cdga

Definition 3.16.5. $f, g : \mathcal{A} \to \mathcal{B}$ are **homotopic** if there exists $H : \mathcal{A} \to B \otimes \langle t, dt \rangle$ s.t. H commutes with d and $H|_{t=0} = f$ and $H|_{t=1} = g$. ⋄

Think of $\langle t, dt \rangle = \Lambda \langle t, dt \rangle$ as the cdga of an interval

Lemma 3.16.6. *Given $f : X \to Y$, $\exists \rho_f : \mathcal{M}_Y \to \mathcal{M}_X$ defined up to homotopy*

Question 3.16.7. *If $f \mapsto \rho_f$ an isomorphism? Is forming $\mathcal{M}_X$ fully faithful?*

We'll need some obstruction theory. Consider

$$\begin{tikzcd} & E \arrow[d] & K(\pi, n) \arrow[l] \\ X \arrow[r] \arrow[ur, dashed] & B & \end{tikzcd}$$

step in Postniokov tower. Then we get an "exact sequence"

$$\mathrm{H}^n(X, \pi) \longrightarrow [X, E] \longrightarrow [X, B] \longrightarrow \mathrm{H}^{n+1}(X, \pi)$$

so these cohomology groups on the end give obstructions to lifting maps and to lifting homotopies. Note that $\mathrm{H}^n(X; \pi) \curvearrowright [X, E]$. Given $\ell \in \mathrm{H}^n$ and $f \in [X, E]$, the action is $\ell \cdot f$ is ...

In CDGA world, have an analogous pictures

$$\begin{tikzcd} \mathcal{M} \arrow[r, "\rho"] \arrow[d] & \mathcal{A} \\ \mathcal{M} \otimes_d \bigwedge \langle V \rangle \arrow[r, equal] & \mathcal{M}' \arrow[u, dashed] \end{tikzcd}$$

get again

$$\mathrm{H}^n(A;V) \longrightarrow [\mathcal{M}',\mathcal{A}] \longrightarrow [\mathcal{M},\mathcal{A}] \longrightarrow \mathrm{H}^{n+1}(\mathcal{A};V)$$

where $\mathrm{Hom}(V,\mathrm{H}^n(\mathcal{A})) = \mathrm{H}^n(\mathcal{A};V)$. The idea is that $v \mapsto \rho(dv)$ must be exact in order to extend, so let $H : \mathcal{M} \to \mathcal{A} \otimes \langle t, dt\rangle$ be the homotopy between f, g. Then, $d\int_0^1 H(V) - \int_0^1 H\mathrm{d}v = f - g$ (chain homotopy condition), so

$$v \mapsto f - g + \int_0^1 H\mathrm{d}v$$

must be exact to extend H; this is a map $V \to \mathrm{H}^n(\mathcal{A})$.

Lemma 3.16.8. *For simply connected X, given minimal model $\mathcal{M}(n) \xrightarrow{\rho} \mathcal{M}_{(X_{\leq n})}$, a minimal model for n stage of Postnikov tower. Then there is a Hirsch extension of $\mathcal{M}(n)$ giving a minimal model for $X_{\leq n+1}$.*

One takes $V = \pi_{n+1}(X) \otimes \mathbb{Q}$ and d to be the **k-invariant**, the transgression map in the Serre spectral sequence for $K(\pi, n) \to X_{\leq n+1} \to X_{\leq n}$. We won't work out the details.

Corollary 3.16.9. $\mathcal{M}_X \simeq \mathcal{M}_{X_{(0)}}$

There's a natural map from the Postnikov tower of X to the Postnikov tower of $X_{(0)}$ from which we see that their minimal models have the same localization.

Now, comparing the obstruction theory on both sides with this comparision of Postnikov tower to nth stage minimal model, one uses the 5 lemma and obtains,

Theorem 3.16.10. *If X is (simply-connected with finitely generated homotopy groups? and) $\mathbb{Q}$-local (i.e. $\pi_*(X) \otimes \mathbb{Q} = \pi_*(X)$), then $[Y, X] \leftrightarrow [\mathcal{M}_X, \mathcal{M}_Y]$.*

Proof. $\mathrm{H}^{n+1}(\mathcal{M}_Y, V) \simeq \mathrm{H}^{n+1}(Y; \pi_{n+1}X)$ and then 5-lemma + induction. ■

Remark 3.16.11. Say X simply-connected with finitely generated homotopy groups. If it is $\mathbb{Q}$-local in the above sense, this it is $H\mathbb{Q}$-local in the sense of the last talk, so we get a bijection $[Y_{(0)}, X] \xrightarrow{\sim} [Y, X]$. This theorem is saying something like the subcategory of spaces equivalent to the category of CDGAs is the subcategory of $\mathbb{Q}$-local spaces. ○

Theorem 3.16.12. $\lambda_* : \pi_n(X) \otimes \mathbb{Q} \xrightarrow{\sim} I^n(\mathcal{M}_X)^\vee$ *where $I^n(\mathcal{M}_X)$ is indecomposables in degree n elements of $\mathcal{M}_X$.*

Proof. (surj) Given $f : I^n(\mathcal{M}_X) \to \mathbb{Q}$, extend to $\overline{f} : \mathcal{M}_X \to \mathcal{M}_{S^n}$. Then we get $\varphi : S^n \to X = X_{(0)} \in \pi_n(X) \otimes \mathbb{Q}$.

(inj) also easy. ■

Another perspective Look at cdgas and simplicial sets both as closed model categories. We have adjoint functors. $F : CDGAs \leftrightarrows$: SSet with $F(A) = \bigcup_p \mathrm{Hom}_{CDGA}(\mathcal{A}, \nabla_p)$ and $M(X) = \bigcup_p \mathrm{Hom}_{\mathrm{SSet}}(X, \nabla_p)$ or something like that. I'm not sure what ∇ is (something like ∇_p the cdga of p-simplex).

Theorem 3.16.13. $MF(X) \simeq X_{(0)}$.

Considering things as closed model categories helps simply things. e.g. Hirsch extensions are just (examples of?) cofibrations.

Applications Any $\mathbb{Q}$-topological invariant is given by an integral of forms.

Example (Hopf variant)**.** Start with $[f : S^3 \to S^2] \in \pi_3(S^2)$ and $\mathrm{d}\eta = f^*(\mathrm{d}\,\mathrm{vol}_{S^2})$. Then the Hopf invariant is

$$\int_{S^3} \eta \wedge f^* \mathrm{d}\,\mathrm{vol}_{S^2}\,.$$

△

Another result is that every manifold X^n is either *elliptic*, i.e. $\pi_k(X) \otimes \mathbb{Q} = 0$ for $k \geq 2n-1$, or *hyperbolic*, i.e.

$$\sum_{j \leq n} \dim(\pi_n(X) \otimes \mathbb{Q}) \geq C^n$$

for some $C > 1$ for all n.

Conjecture 3.16.14 (Bott)**.** *If X is a simply connected manifold with metric of non-negative sectional curvature, then it is rationally elliptic.*

3.17 Junyao: On the cobordism ring Ω_* and a complex analogue, part I, Milnor

3.17.1 Talk Notes

Outline

- Main result is that $\pi_*(MU)$ has no torsion, and $\pi_*(MSO)$ has no odd torsion.
- Structure of Steenrod algebra mod p
- Adams spectral sequence

Recall 3.17.1. $\mathrm{H}^*(MO; \mathbb{F}_2)$ is free over the mod 2 Steenrod algebra, which gives a splitting

$$MO \xrightarrow{\sim} \prod (\Sigma^* H\mathbb{F}_2)$$

as a product of Eilenberg-Maclane spectra. This let Thom calculate $\pi_*(MO)$. ⊙

However, $\mathrm{H}^*(MU; \mathbb{F}_p)$ is not free over the mod p Steenrod algebra. In particular, it is generated in even degree, but the mod p Steenrod algebra has the Bockstein $\beta = Q_0$ has had degree 1 (odd), so $\mathrm{H}^*(MU; \mathbb{F}_p)$ can't be free. In fact, this is the only issue. We'll see that $\mathrm{H}^*(MU; \mathbb{F}_p)$ is free over $\mathcal{A}/(\beta)$. This + an application of the Adams spectral sequence will allow us to conclude that $\pi_*(MU)$ is torsion-free.

Let $\mathcal{A}_0 \subset \mathcal{A}$ be the $\mathbb{F}_p$-subalgebra generated by $Q_0, Q_1, Q_2, \dots$ where

$$Q_n = [P^{p^{n-1}}, Q_{n-1}]$$

has degree $2p^n - 1$ and Q_0 is Bockstein.

Lemma 3.17.2.
- *$\mathcal{A}_0$ is an exterior algebra with generators Q_i*
- *$\mathcal{A}$ is free as a right $\mathcal{A}_0$-module (Milnor's basis)*

- $\mathcal{A}/(Q_0) \simeq \mathcal{A} \otimes_{\mathcal{A}_0} \mathbb{F}_p$ *where* $\mathbb{F}_p$ *is viewed as an* $\mathcal{A}_0$*-module with* Q_i *acting trivially.*

Theorem 3.17.3. $\mathrm{H}^*(MU;\mathbb{F}_p)$ *is a free module over* $\mathcal{A}/(Q_0)$ *with the basis elements given by* $s(\lambda)$*, where* λ *runs over all partitions which don't contain* $p^j - 1$*.*

If $\lambda = 1\lambda_1 + 2\lambda_2 + \dots$*, then* $s(\lambda)$ *is the smallest symmetric poly containing* $c_1^{\lambda_1} c_2^{\lambda_2} \dots$ *with* $c_i \in \mathrm{H}^*(BU;\mathbb{F}_p) = \mathrm{H}^*(MU;\mathbb{F}_p)$ *the mod* p *Chern classes.*

Recall 3.17.4. Recall in the case of $\mathrm{H}^*(MO;\mathbb{F}_2)$, we explicitly found a basis corresponding to a non-dyadic decomposition of n. $\odot$

Theorem 3.17.5. $\mathrm{H}^*(MSO;\mathbb{F}_p)$ *is a free module over* $\mathcal{A}/(Q_0)$ *for all odd primes* p*.*

Adams Spectral Sequence Let X, Y be finite CW compelxses with based points, so $\widetilde{\mathrm{H}}^*(X;\mathbb{F}_p)$ is a graded $\mathcal{A}$-module.

Definition 3.17.6. The **stable tack group** (for $n \in \mathbb{Z}$) is

$$\{X, Y\}_n := \varinjlim_m [\Sigma^{m+n} X, \Sigma^m Y].$$

This makes sense in the stable homotopy category with X, Y replaced by spectra. $\diamond$

The Adams spectral sequence looks like

$$E_2^{s,t} = \mathrm{Ext}_{\mathcal{A}}^{s,t}(\widetilde{\mathrm{H}}^*(Y), \widetilde{\mathrm{H}}^*(X)) \implies ?$$

where the something it converges to should contain "p-local information of $\{X, Y\}_*$." We'll need some finiteness conditions for convergence. Note that one can replace X, Y above with spectra.

The display of the Adams spectral sequence is a little different from what one usually does. We have a differential $d_r : E_r^{s,t} \to E_r^{s+r,t+r-1}$ of bidegree $(r, r-1)$ as usual, but now the total degree is $t - s$ and the filtration degree is s. We draw the spectral sequence as below, but with arrows going *up* r *units and to the left* 1 *unit.*

s (filtration)						
2	$E^{2,0}$	$E^{2,1}$	$E^{2,2}$	$E^{2,3}$	$E^{2,4}$	
1	$E^{1,-1}$	$E^{1,0}$	$E^{1,1}$	$E^{1,2}$	$E^{1,3}$	
0	$E^{0,-2}$	$E^{0,-1}$	$E^{0,0}$	$E^{0,1}$	$E^{0,2}$	
	-2	-1	0	1	2	$t - s$ (total degree)

In particular, the spectral sequence is concentrated in the upper half plane. From this, we can see why we have convergence worries. The arrows are never guaranteed to start hitting 0 since they just go higher and higher. Also, note that the total degree is $t - s$, so we expect vertical slices of the sequence to hold p-local information of $\{X, Y\}_*$.

Let's see some technical details. First

$$\mathrm{Ext}_{\mathcal{A}}^{0,t}(M, N) = \mathrm{Hom}_{\mathcal{A}}^t(M, N) = \text{graded } \mathcal{A}\text{-module maps of degree } -t,$$

and $\mathrm{Ext}_{\mathcal{A}}^{s,t}(-, N)$ are the right derived functors of $\mathrm{Hom}_{\mathcal{A}}^t(-, N)$.

For convergence issues, in our case "p-local info of $\{X,Y\}_*$" means $\{X,Y\}_* \otimes \mathbb{Z}_p$ where $\mathbb{Z}_p$ *is* the p-adic integers. In general, we need "boundedness" of S.S. for convergence $E_2 \implies \{X, \widehat{Y}_p\}$ where $\widehat{Y}_p$ is the p-completion of Y. Recall convergence means this space has a "natural" filtration whose graded pieces are given by the E_∞.

There's also the edge homomorphism

$$\{X,Y\}_t = \{X, \widehat{Y}_p\}_t \to \mathrm{Hom}^t_{\mathcal{A}}(\widetilde{\mathrm{H}}^* Y, \widetilde{\mathrm{H}}^* X).$$

Example. Let $Y = \Sigma^n H\mathbb{F}_p$, the mod P E-M spectrum. Then, $\mathrm{H}^* Y \cong \mathcal{A}$ as an $\mathcal{A}$-module. Hence,

$$\mathrm{Ext}^{s,t}_{\mathcal{A}}(\widetilde{\mathrm{H}}^* Y, \widetilde{\mathrm{H}}^* X) = \begin{cases} 0 & \text{if } s \geq 1 \\ \widetilde{\mathrm{H}}^{n-t}(X) & \text{otherwise.} \end{cases}$$

so the Adams SS degenerates at E_2, and we conclude that

$$\{X, \Sigma^n H\mathbb{F}_p\}_t = \widetilde{\mathrm{H}}^{n-t}(X)$$

which recovers representability of cohomology by the E-M spectrum. △

Example. $X = Y = S^0$ (i.e. $= \mathbb{S}$), so the Adams spectral sequence computes stable homotopy groups of spheres. Take an $\mathcal{A}$-resolution of $\widetilde{\mathrm{H}}^* S^0 = \mathbb{F}_p$

$$\cdots \longrightarrow \bigoplus_j \Sigma^{m_j}\mathcal{A} \longrightarrow \bigoplus_i \Sigma^{n_i}\mathcal{A} \longrightarrow \mathcal{A} \longrightarrow \mathbb{F}_p$$

Junyao goes over how to compute explicit generators for this start of the resolution.

The kernel of the first map $\mathcal{A} \to \mathbb{F}_p$ is the augmentation ideal with is generated as a left $\mathcal{A}$-module by $\beta, \beta P^1, \beta P^2, \dots$ (I think). From this you can cook up the second term, and then the third term, and it quickly becomes complicated.

The upshot is that you end us with $\mathrm{Hom}^t_{\mathcal{A}}(F_s, \mathbb{F}_p) = 0$ if $t < s$ (F_s is the sth free object resolving $\mathbb{F}_p$).[34] This tells us that $E_2^{s,t} = 0$ if $t < s$ and $E_2^{t,t} = \mathbb{F}_p$. Thus, the Adams spectral sequence is concentrated in the first quadrant (i.e. where the total degree $t - s \geq 0$). Also, everything along the zero column in $\mathbb{F}_p$ corresponding to the fact that $\pi_0^s(S_0) \otimes \mathbb{Z}_p = \mathbb{Z}_p$.

One can do a more careful analysis to say more things. Junyao said more I did not catch and so did not write down. △

What's the intuition for the Adams spectral sequence. The Hurewicz map gives a naive approximation of $\{-,-\}$:

$$\{X,Y\}_t \xrightarrow{d} \mathrm{Hom}^t_{\mathcal{A}}(\mathrm{H}^* Y, \mathrm{H}^* X) = E_2^{0,t}.$$

For $t = 0$, suppose some $f : X \to Y$ is in the kernel ($\mathrm{d}f = 0$). Then the LES induced by $X \to Y \to C(f)$ becomes a short exact sequence

$$0 \longrightarrow \mathrm{H}^{*-1}(X) \longrightarrow \mathrm{H}^*(C(f)) \longrightarrow \mathrm{H}^*(Y) \longrightarrow 0.$$

[34] In F_s, we raise the degree of every element by $\geq s$, but $\mathbb{F}_p$ lives in degree 0

This extension gives an element of $\operatorname{Ext}^{1,0}_{\mathcal{A}}(\mathrm{H}^* Y, \mathrm{H}^{*-1} X) = E_2^{1,1}$.

How we construct this spectral sequence. First resolve $\mathrm{H}^* Y$ be the Eilenberg-Maclane spaces. Let $Y = Y_0$. Let K_0 be a finite wedge of E-M spaces s.t. $Y_0 \to K_0$ induces a surjection $\mathrm{H}^* K_0 \twoheadrightarrow \mathrm{H}^* Y$. Let Y_1 be the homotopy cofiber[35] of $Y_0 \to K_0$. You can a spectral sequence, and in the stable range this gives a short exact sequence looking like

$$0 \longrightarrow \mathrm{H}^* Y_1 \longrightarrow \mathrm{H}^{*+1} K_0 \longrightarrow \mathrm{H}^{*+1} Y_0 \longrightarrow 0.$$

Repeat for $Y_s : Y_s \to K_s$ inducing a surjection $\mathrm{H}^* K_s \twoheadrightarrow \mathrm{H}^* Y_s$ and let Y_{s+1} be the (desuspension) of the cofiber. We can slice these short exact sequences together to get an "$\mathcal{A}$-resolution"

$$\cdots \longrightarrow \mathrm{H}^{*-2} K_2 \longrightarrow \mathrm{H}^{*-1} K_1 \longrightarrow \mathrm{H}^* K_0 \longrightarrow \mathrm{H}^* Y \longrightarrow 0.$$

The cofiber sequences $Y_{s+1} \to Y_s \to K_s \to \Sigma Y_{s+1} \longrightarrow$ induce an exact couple

$$\begin{tikzcd}
\bigoplus_{s,t}\{X, Y_s\}_{t-s} \arrow[rr, "i"] & & \bigoplus_{s,t}\{X, Y_s\}_{t-s} \arrow[dl, "j"] \\
& \bigoplus_{s,t}\{X, K_s\}_{t-s} \arrow[ul, "k"] &
\end{tikzcd}$$

This gives a spectral sequence with $E_1^{s,t} = \{X, K_s\}_{t-s} = \operatorname{Hom}^{t-s}_{\mathcal{A}}(\mathrm{H}^* K_s, \mathrm{H}^* X)$ a "free" $\mathcal{A}$-module (in the stable range)

The differential $d_1 = jk : \operatorname{Hom}^{t-s}_{\mathcal{A}}(\mathrm{H}^* K_S, \mathrm{H}^* X) \longrightarrow \operatorname{Hom}^{t-(s+1)}_{\mathcal{A}}(\mathrm{H}^* K_{s+1}, \mathrm{H}^* X)$ which turns out to be exactly the map induced by the resolution of $\mathrm{H}^* Y$. Hence, the E_2-page consists of Ext-groups.

Remark 3.17.7. We can replace Y be a spectrum when the following finiteness condition holds: $\mathrm{H}^*(Y)$ is bounded below and finitely generated for all $*$ (e.g. $Y = MU, MSO$,etc.). ◦

How do we use this spectral sequence?

Theorem 3.17.8. *If $\mathrm{H}^*(Y, \mathbb{F}_p)$ is a free $\mathcal{A}/(Q_0)$-module with even dimensional generators, and if it satisfies the finiteness conditions, then $\pi_n(Y) = \{S^0, Y\}_n$ contains no p-torsion.*

Let's sketch this proof. Consider the Moor space M with

$$\widetilde{\mathrm{H}}^i(M; \mathbb{Z}) = \begin{cases} \mathbb{F}_p & \text{if } i = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Get a UCT sequence

$$0 \longrightarrow \{S^1, Y\}_n \otimes \mathbb{F}_p \longrightarrow \{M, Y\}_n \longrightarrow \operatorname{Tor}_1^{\mathbb{Z}}(\{S^1, Y\}_{n-1}, \mathbb{F}_p) \longrightarrow 0.$$

Hence, If $\pi_*(Y)$ has p-torsion, then $\{M, Y\}_n$ will have p-torsion for two consecutive values of n.

We'll show this fails by showing that $\{M, Y\}_{\text{odd}} = 0$. To show this, we apply the Adams spectral sequence for $\{M, Y\}_*$. We want an $\mathcal{A}$-resolution of $\mathrm{H}^* Y$. Since Y is free over $\mathcal{A}/(Q_0) = \mathcal{A} \otimes_{\mathcal{A}_0} \mathbb{F}_p$, this corresponds to an $\mathcal{A}_0$-resolution of $\mathbb{F}_p$. One can do everything explicitly.

[35] Really, you should work completely in spectra and then take the desuspension of the cofiber

In the end, get that $\pi_*(MU)$ is torsion-free. Thus, the Hurewicz map $\pi_*(MU) \hookrightarrow \mathrm{H}_*(MU;\mathbb{Z})$ is an injection (so $\pi_*(MU)$ vanishes in odd degree) with finite cokernel (so you get the ranks of the even degree parts). Can then show $\pi_*(MU)$ is poly on even degree generators.

3.18 Niven: Quillen's work on formal group laws and complex cobordism, Adams

3.18.1 Paper Notes

I wrote up some notes on the reading which are (strictly) more detailed than the talk I give.

3.18.2 Talk Notes

For actual talk itself, this is what I wrote down.

3.19 David: Higher Algebraic K-theory, Quillen

3.19.1 Talk Notes

Classifying space of a category Let $\mathcal{C}$ be a small category. Its **nerve** $N\mathcal{C}$ the the simplicial set whose n-simplicials are diagrams

$$x_0 \to x_1 \to \cdots \to x_n$$

in $\mathcal{C}$, i.e. chains of n composable morphisms. The i face map drops x_i and composes the two arrows it was apart of; the ith degeneracy map adds an identity morphism $x_i \xrightarrow{\mathrm{id}} x_i$.

The nerve function $N : \mathrm{Cat} \to \mathrm{SSet}$ preserves all limits and filtered colimits. This construction lets you think of a category as a special kind of simplicial set.

The **classifying space** $B\mathcal{C} := |N\mathcal{C}|$ of the category is the geometric realization of the nerve. In practice, you may not need to worry about distinguishing the simplicial set from its geometric realization. We consider B as a functor $\mathrm{Cat} \to \mathrm{CG}$ to compactly-generated topological spaces; this target category allows B to preserve filtered colimits and pullbacks.

Let $\mathcal{C}, \mathcal{D}$ be small categories, and let $F : \mathcal{C} \to \mathcal{D}$ be a functor. Quillen's "Theorem A" gives a sufficient condition for the induced map $BF : B\mathcal{C} \to B\mathcal{D}$ to be a homotopy equivalence. His "Theorem B" gives a sufficient condition for

$$B(y/F) \longrightarrow B\mathcal{C} \longrightarrow B\mathcal{D}$$

to be a fiber sequence (where y/F is category with objects maps $y \to F(x)$ for $x \in \mathcal{C}$).

Remark 3.19.1. One condition for BF to be a homotopy equivalence is that it belong to an adjoint pair (since you have the unit, counit inducing homotopies to the identity). ○

Exact Category An **exact category** $\mathcal{C}$ is an additive category s.t. $\exists$ an abelian category $\mathcal{A}$ s.t. $\mathcal{C}$ is a full subcategory of $\mathcal{A}$ and $\mathcal{C}$ is closed under taking extensions in $\mathcal{A}$.

Given a SES

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

in $\mathcal{A}$ with objects in $\mathcal{C}$ ($\iff A, C \in \mathrm{ob}(\mathcal{C})$), we call i an **admissible monomorphism** (i.e. $\operatorname{coker} i \in \mathrm{ob}(\mathcal{A})$ actually lies in $\mathcal{C}$) and j an **admissible epimorphism**.

We would like a more intrinsic definition exact category without reference to some ambient abelian category. Such a definition exists (and is not scary), but we will not discuss it in this talk.

We'll always assume we have these ambient abelian category $\mathcal{A}$. In particular, when we say "kernel, cokernel, pullback, etc." we mean them in $\mathcal{A}$.

Proposition 3.19.2. *Admissible epimorphisms are stable under composition and pullback. Admissible monomorphisms are stable under composition and pushout.*

Proof. For the pullback case, stare at

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d] & A \times_B C \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & K \arrow[r] & A \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$

■

Definition 3.19.3. Given exact categories $\mathcal{C}, \mathcal{D}$, a functor $F : \mathcal{C} \to \mathcal{D}$ is **exact** if it sends SESs to SESs. ◇

Example. Let R be a ring. Then, $P(R) :=$ category of f.g. projective R-modules is an exact category (take $\mathcal{A}$ to be all R-modules). △

Example. Let $P_n(R)$ be R-modules of projective dimension $\leq n$. This is also exact. △

Q-construction Write $\twoheadrightarrow$ for admissible epimorphisms are $\hookrightarrow$ for admissible monomorphisms.

Definition 3.19.4. Let $\mathcal{C}$ be an exact category. The **Q-construction** is the category $Q\mathcal{C}$ with $\mathrm{ob}(Q\mathcal{C}) = \mathrm{ob}(\mathcal{C})$ and morphisms given by isom classes of diagrams of the form

$$M \twoheadleftarrow N \hookrightarrow M'$$

◇

Warning 3.19.5. A morphism also depends on the isomorphism class of N. For example $0 \twoheadleftarrow 0 \hookrightarrow M$ and $0 \twoheadleftarrow M \hookrightarrow M$ are different morphisms. •

Remark 3.19.6. Zoom has been periodically freezing so I missed some of this. But something like you may think of this construction as a way of defining multi-valued functions (e.g. $\sqrt{z}$ on $\mathbb{C}$) $M \to M'$. Like N is some covering of M, and then you consider $N \to M'$. Something along these lines was commented. ○

Proposition 3.19.7.

(1) $QC \simeq Q(C^{op})$

(2) *Missed it...*

How to compute morphisms. Given $M \twoheadleftarrow N \hookrightarrow M'$ and $M' \twoheadleftarrow N' \hookrightarrow M''$, let $N'' = N \times_{M'} N'$ be the pullback. Then, $N \twoheadleftarrow N''$ is admissible epi since it is pulled back from an epi. Furthermore, $N'' \hookrightarrow N'$ is admissible mono since it is pulled back *along an (admissible) epimorphism.*

Definition 3.19.8. Let $\mathcal{C}$ be an exact category. Its K-groups are

$$K_i\mathcal{C} := \pi_i(\Omega B(Q\mathcal{C}), 0) = \pi_{i+1}(B(Q\mathcal{C}), 0).$$

$\diamond$

Proposition 3.19.9. *If $C = \varinjlim C_i$ is a filtered colimit of exact categories and exact functors, then $K_*\mathcal{C} = \varinjlim K_*(\mathcal{C}_i)$.*

Definition 3.19.10. Let R be a ring. Then we define

$$K_i(R) := K_iP(R) \text{ and } K_i'(R) := K_i\mathrm{Modf}(R) =: G_i(R).$$

In the latter case, we assume R noetherian and $\mathrm{Modf}(R)$ is the category of f.g. left R-modules (which is already abelian). $\diamond$

Theorem 3.19.11. *There is a homotopy equivalence*

$$\Omega BQP(R) \simeq K_0R \times BGL(R)^+.$$

Basic Theorems

Theorem 3.19.12. *$K_0(\mathcal{C})$ is isomorphic to the Grothendieck group generated by a generator $[M]$ for each $M \in \mathrm{ob}(\mathcal{C})$ with a relation $[M] = [M''][M']$ for each SES*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

Note that this is abelian since $[M][N] = [M \oplus N$

Whelp, got kicked out of zoom and came back and am not sure what he's doing now... presumably proving the above theorem? Seems like one can show $\pi_1(\mathrm{sk}_1 BQ\mathcal{C}) = \langle [f] \,|[0 \hookrightarrow M] = 1\rangle$ where f ranges over $\mathrm{Mor}(\mathcal{C})$. Adding in 2-cells means adding in the relations $[f \circ g] = [g][f]$. What does this entail?

- $[M \hookrightarrow N] = [0 \hookrightarrow M][M \hookrightarrow N] = [0 \hookrightarrow N] = 1$ so all admissible mono are trivial.
- $[0 \twoheadleftarrow M][M \twoheadleftarrow N] = [0 \twoheadleftarrow N]$. Hence $[M \twoheadleftarrow N] = [0 \twoheadleftarrow M]^{-1}[0 \twoheadleftarrow N]$
- Given $0 \to M' \to M \to M'' \to 0$ a SES. Use above to get

  $$[0 \twoheadleftarrow M] = [0 \twoheadleftarrow M'][0 \twoheadleftarrow M''],$$

  the relationship from the Grothendieck group.

This allows one to show that $\pi_1(BQ\mathcal{C})$ is the Grothendieck group.

Theorem 3.19.13 (**Additivity theorem**)**.** *Let $\mathcal{C}, \mathcal{D}$ be exact categories. Let F', F, F'' be exact functors $\mathcal{C} \to \mathcal{D}$ s.t.*

$$0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0$$

is an exact sequence of functors. Then, $F_* = F'_* + F''_* : K_i(\mathcal{C}) \to K_i(\mathcal{D})$.

Theorem 3.19.14 (Resolution)**.** *Let $\mathcal{C}$ be an exact category. Let P be a full subcat of $\mathcal{C}$ closed under extensions (so P is exact). Suppose also that if $0 \to A \to B \to C \to 0$ is SES in $\mathcal{C}$ with $B, C \in P$, then $A \in P$. Finally, suppose that for any objection M in $\mathcal{C}$, there exists a finite P-resolution*

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

($P_i \in \mathrm{ob}(P)$). Then, $K_*P \simeq K_*\mathcal{C}$.

Corollary 3.19.15. *If every f.g. left R-module has a finite projective resolution, then the natural map $K_iR \to K'_iR$ is an isomorphism.*

3.20 Jiakai: Homotopical Algebra, Quillen

3.20.1 Talk Notes

Outline

- SSet
- model category: defns and examples
- the homotopic category associated to a model category
- Quillen equivalence

Most closely following Dyer's (?) chapter in "A handbook on homotopy theory" (?).

The motivating question is thus:

Question 3.20.1. *What is a homotopy theory?*

In trying to answer this, Quillen realized that the "homotopy theory" is really a secondary object; the primary thing is the model.

Simplicial sets Let Δ be the category whose objects are $[n] = \{0, 1, \ldots, n\}$ with morphisms given by order-preserving maps. The category SSet of simplicial sets is the category of functors $\Delta^{\mathrm{op}} \to \mathrm{Set}$.

There is an adjoint pair $|\cdot| : \mathrm{SSet} \leftrightarrows : \mathrm{Sing}$ given by geometric realization and the singular simplex. Recall,

$$\mathrm{Sing}(Y)_n = \{\Delta_n \to Y\}.$$

The geometric realization is

$$|X| = \left(\bigsqcup_{n \geq 0} \Delta^n \times X_n \right) / \sim \quad \text{where } (v, \varphi^* x) \sim (\varphi_* x, x) \text{ for all } \varphi : [m] \to [n].$$

Milnor showed that the natural map $|\mathrm{Sing}(X)| \to X$ is a weak equivalence. So "simiplicial sets give a combinatorial model for homotopy types of topological spaces."

Model categories A **model category** is a category $\mathcal{C}$ with three distinguished classes of maps: weak equivalences $\xrightarrow{\sim}$, fibrations $\twoheadrightarrow$, and cofibrations $\hookrightarrow$. An **acyclic (co)fibration** is a (co)fibration which is also a weak equivalence. We require 5 axioms.

(MC1) finite limits and colimits exist in $\mathcal{C}$

(MC2) If f, g, gf are defined and 2 are weak equivalences, then so is the third.

(MC3) If f is a retract of g, and g is a w.e, fib, or cofib, then so is f

(MC4) In the commutative diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "i"'] & X \arrow[d, "p"] \\ B \arrow[r, "g"] \arrow[ur, dashed] & Y \end{tikzcd},$$

a lift exists if

- i is a cofibration and p is an acyclic fibration; or
- i is an acyclic cofibration and p is a fibration

(MC5) Any map f can be factored in two ways:

$$X \hookrightarrow Z \overset{\sim}{\twoheadrightarrow} Y \text{ or } X \overset{\sim}{\hookrightarrow} Z \twoheadrightarrow Y.$$

An object $A \in \mathcal{C}$ is **cofibrant** if $\emptyset \to A$ is a cofibration ($\emptyset$ is initial). It is a **fibrant** object if $A \to *$ is a fibration.

Example. Topological spaces. The weak equivalences are weak homotopy equivalences. The fibrations are not necessarily surjective Serre fibrations. The cofibrations are retracts of maps $X \to Y'$ in which Y' is obtained from X by attaching cells.

Every object in Top is fibrant. The cofibrant objects are retracts of **generalized CW complexes**, i.e. spaces built from cells but necessarily ordered by dimension.

Note that if we factor $\emptyset \to X$ as $\emptyset \hookrightarrow X' \overset{\sim}{\twoheadrightarrow} X$, then X' is a CW approximation of X. In general, factoring $A \xrightarrow{f} X$ gives a "CW approximation of f." The other factorization $A \overset{\sim}{\hookrightarrow} A' \twoheadrightarrow X$ is like saying "every map can be replaced by a fibration." △

In general (including in the above example), verifying the axioms is a nontrivial task.

Example. Here's another model structure on Top (due to Strom). Take weak equivalences to be homotopy equivalences, cofibrations to be closed Hurewicz cofibrations, and fibrations to be Hurewicz fibrations. △

Example. (Bousfield). Let $\mathcal{C} = \mathrm{SSet}$ and h a generalized homology theory. Take weak equivalences to be h_*-equivalences, cofibrations to be the usual ones, and fibrations are maps which have the RLP with respect to acyclic cofibrations. △

Example. Simplicial sets. Weak equivalences are maps whose geometric realizations $|f|$ are weak homotopy equivalences in Top. The cofibrations are maps f with $f_n : X_n \to Y_n$ a monomorphism for all n, and the fibrations are **Kan fibrations**, i.e.

$$\begin{tikzcd} \Lambda^n_k \arrow[r, "s"] \arrow[d] & X \arrow[d, "f"] \\ \Delta_n \arrow[r, "y"] \arrow[ur, dashed, "x"] & Y \end{tikzcd},$$

for all $n \geq 1$ and $0 \leq k \leq n$, for any map $s : \Lambda^n_k \to X$ from the kth horn to X and map $y : \Delta_n \to Y$ s.t the diagram above commutes, the map y lifts to a map $x : \Delta_n \to X$. △

Remember: The kth horn is what you get from removing the k face (face opposite vertex k?)

Example. Model structure for nonnegatively graded chain complexes over R. The weak equivalences are quasi-isomorphisms, the cofibrations are: for each $k \geq 0$, $f_k : M_k \to N_k$ monic with projective kernel. The fibrations are: for all $k > 0$, $f_k : M_k \to N_k$ an epimorphism.

Every object is fibrant, and the cofibrant objects are complex where each M_k is projective. So here cofibrant replacement is like taking a projective resolution. △

Homotopy Category A **cylinder object** is an object $A \wedge I$ of $\mathcal{C}$ with diagram

$$\begin{tikzcd} A \sqcup A \arrow[r, "i"] \arrow[rr, bend right, "\mathrm{id}_A + \mathrm{id}_A"'] & A \wedge I \arrow[r, "\sim"] & A \end{tikzcd}$$

These are *not unique* when they exist, in general. We call it **good** if $A \sqcup A \to A \wedge I$ is a cofibration, and call it **very good** if *moreover*, $A \wedge I \to A$ is a (necessarily acyclic) fibration.

Two maps $f, g : A \to X$ in $\mathcal{C}$ are **left homotopic** if there exists a cylinder object $A \wedge I$ for A s.t. $f + g$ extends to $H : A \wedge I \to X$ with $H(i_0 + i_1) = f + g$.

Remark 3.20.2. $A \wedge I = A$ is always a cylinder object. usually not good. The factorization axiom guarantees that there's always a very good cylinder object. ○

Remark 3.20.3. In Top, $A \times I$ is a cylinder object, but usually not good when A is not a CW complex. ○

Remark 3.20.4. If A cofibrant, left homotopy gives an equiv relation. ○

A **path object** for $X \in \mathcal{C}$, usually denoted X^I, is an object together with a diagram

$$\begin{tikzcd} X \arrow[r, "\sim"] \arrow[rr, bend right, "(\mathrm{id}_X\,,\ \mathrm{id}_X)"'] & X^I \arrow[r] & X \end{tikzcd}$$

Two maps $f, g : A \to X$ are **right homotopic** if there's a path object X^I s.t. the product map $(f, g) : A \to X \times X$ lifts to X^I (or something).

Lemma 3.20.5. *If X is fibrant, then this is an equivalence relation on* $\mathrm{Hom}_{\mathcal{C}}(A, X)$.

Slogan. Mapping into fibrant objects is a good thing to do.

Remark 3.20.6. We really want objects which are both fibrant/cofibrant so both left and right homotopies are nice. When A cofibrant and X fibrant, left/right homotopies define the same equivalence relation. ○

Homotopy Category Ho$\mathcal{C}$ will be the category whose objects are those of $\mathcal{C}$, but with different morphisms. For $X \in \mathcal{C}$ factor

$$\emptyset \hookrightarrow QX \overset{\sim}{\twoheadrightarrow} X \text{ and } X \overset{\sim}{\hookrightarrow} RX \twoheadrightarrow *.$$

The morphisms are now

$$\mathrm{Hom}_{\mathrm{Ho}\mathcal{C}}(X, Y) = \pi\left(RQX, RQY\right),$$

homotopy classes of maps. Note that QX is cofibrant, RX is fibrant, and RQX is both. One gets a functor $\gamma\mathcal{C} \to \mathrm{Ho}(\mathcal{C})$ which is the identity on objects and morphisms are a little harder to show are well-defined but the upshot is you do end up with a well-defined homotopy class of maps $RQ(X) \to RQ(Y)$ given $f : X \to Y$.

Remark 3.20.7. Our factorizations are not required to be functorial (hence to annoyance), but some people do require this. Whether this can always be made to be the case is probably a set theoretic issue. ◦

Proposition 3.20.8. *If f is a morphism in $\mathcal{C}$, then $\gamma(f)$ is an isomorphic in* Ho($\mathcal{C}$) *if and only if f is a weak equivalence.*

Definition 3.20.9. Given a category $\mathcal{C}$ with $\mathcal{W} \subset \mathrm{Mor}(\mathcal{C})$. A functor $F : \mathcal{C} \to \mathcal{D}$ is a **localization of $\mathcal{C}$ with respect to $\mathcal{W}$** if

- $F(f)$ is an isomorphism for each $f \in \mathcal{W}$; and
- any functor $G : \mathcal{C} \to \mathcal{D}'$ inverting $\mathcal{W}$ factors through F (i.e. F is initial)

⋄

Theorem 3.20.10. *$\gamma : \mathcal{C} \to \mathrm{Ho}(\mathcal{C})$ is the localization of $\mathcal{C}$ w.r.t. weak equivalences.*

Remark 3.20.11. Fibrations and cofibrations are not mentioned in localization perspective above. ◦

Quillen Equivalence Let $\mathcal{C}$ and $\mathcal{D}$ be two model categories. A **Quillen equivalence** (F, G) is an adjoint pair

$$F : \mathcal{C} \leftrightarrows: \mathcal{D} : G$$

s.t.

(1) F preserves cofibrations and G preserves fibrations. Equivalently,

- F preserves cofibration and acyclic cofibrations; or
- G preserves fibrations and acyclic fibrations; or
- F preserves acyclic cofibrations and G preserves acyclic fibrations

(2) For each cofibrant object A of $\mathcal{C}$ and fibrant object X of $\mathcal{D}$, a map $f : A \to G(X)$ is a w.e. in $\mathcal{C} \iff$ its adjoint $f^\flat : F(A) \to X$ is a weak equivalence.

Proposition 3.20.12. *(2) above is equivalent to*

(2') The total left derived functor LF (and the total right derived functor RG) in the adjoint pair

$$LF : \mathrm{Ho}\mathcal{C} \leftrightarrows : \mathrm{Ho}\mathcal{D} : RG$$

is an equivalence of categories.

Example. $|\cdot| : \mathrm{SSet} \leftrightarrows : \mathrm{Top} : \mathrm{Sing}$ is a Quillen equivalence. △

Remark 3.20.13. Quillen equivalences have a "direction" (coming from participating in an adjoint pair). The notion is not symmetric. Furthermore, not any equivalence between homotopy categories can be lifted to a Quillen equivalence. ◦

The model category carries extra structure not captured by the homotopy category. What is this? One way of talking about this is that you can define an enrichment over spaces, i.e. turn $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is spaces whose π_0's are homotopy classes of maps. This only requires a notion of weak equivalences, and the construction was a predecessor to the notion of ∞-categories. There are more robust perspectives these days, but this is a good first pass; think of an ∞-category as a category enriched over topological spaces. (This paragraph heavily paraphrased).

3.21 Jae: Equivariant K-Theory and completion, Atiyah and Segal

3.21.1 Talk Notes

The goal is to compute K-theory of BG for compact Lie groups G.

Theorem 3.21.1 (Atiyah-Segal Completion). *For G a compact Lie group acting on X,*

$$\alpha : \widehat{K_G^*(X)}_I \longrightarrow K^*(X_{hG})$$

is an isomorphism.

Above $X_{hG} = (EG \times X)/G$ is the homotopy orbit space or "Borel construction," and K_G is the genuine/usual equivariant K-theory, the group completion of the group of (stable) G-vector bundles on the G-space X.

Corollary 3.21.2. *Taking $X = *$, we get*

$$\widehat{R(G)} \xrightarrow{\sim} K^*(BG),$$

the K-theory of BG is the completion of the representation ring G (at a certain ideal I).

Key ingredients include pro-objects and holomorphic induction.
Let's recall some basic properties of equivariant K-theory

- We write $K_G^*(X) := K_G^0(X) \oplus K_G^1(X)$ There's a equivariant Bott periodicity, $K_G^*(X) = K_G^*(X \times S^2)$ or whatever
- $K_G^*(*) = K_G^0(*) = R(G)$ is the representation ring
- If $G \curvearrowright X$ freely, then $K_G^*(X) = K^*(X/G)$.

- (functoriality) $G \xrightarrow{\varphi} G'$ with $X \xrightarrow{u} X'$ (a φ-equivariant map), then

$$K^*_{G'}(X') \to K^*_G(X).$$

- (induction) $G \hookrightarrow G'$ and $X' := G' \times_G X$ $(= (G' \times X)/G)$, then

$$K^*_{G'}(X') \cong K^*_G(X).$$

We can thing of the main theorem as a comparison between two forms of "equivariant K-theories."

$$\alpha : K^*_G(X) \longrightarrow K^*(X_{hG}) = K^*_G(X \times EG).$$

Example. When $X = *$, this is the usual associated bundle construction $R(G) = K_G(*) \to K(BG)$. $\triangle$

In the process of forming this map, we "lose" some information. K^*_G is a "fine equivariant theory" (it is an invariant up to G-equivalence) while $K^*(X_{hG})$ is a "coarse equivariant theory" (only up to hG-equivalence). The difference is that if two G-space X, Y are homotopy equivalent by a G-equivariant map, then $K^*(X_{hG}) = K^*(Y_{hG})$, but you *also need the inverse to be G-equivariant* in order to conclude that $K^*_G(X) = K^*_G(Y)$.

Recall 3.21.3. For a commutative ring R with ideal I, the **completion** of an R-module M is

$$\widehat{M}_I := \varprojlim M/I^n M.$$

$\odot$

In the statement of our main theorem, the ideal $I \subset K^*_G(*) = R(G)$ that we use is the **augmentation ideal** $I_G = \ker(R(G) \xrightarrow{\varepsilon} \mathbb{Z})$ where ε sends a virtual representation to its virtual rank. In fact, Atiyah-Segal prove a stronger statement than we gave before.

Theorem 3.21.4 (Atiyah-Segal)**.**

$$\alpha_n : K^*_G(X)/I^n_G \cdot K^*_G(X) \longrightarrow K^*_G(X \times EG_n)$$

is an isomorphism of pro-rings.

Above EG_n are successive, compact approximations of EG. We'll define them properly in a moment.

What are pro-objects? They're natural objects for dealing with inverse limits.

Definition 3.21.5. Let $\mathcal{C}$ be a category. Then, $\mathrm{Pro}(\mathcal{C})$ is a new category whose objects are functors

$$A : S^{\mathrm{op}} \to \mathcal{C}$$

with S a directed set, and whose morphisms are

$$\mathrm{Hom}_{\mathrm{Pro}(\mathcal{C})}(A, B) = \varprojlim_{\theta : T \to S} \left(\mathrm{Hom}_{\mathcal{C}}(A(-), B(-)) : S \times T^{\mathrm{op}} \to \mathrm{Set} \right).$$

Given $\theta : T \to S$... I didn't really follow this definition; see Atiyah-Segal $\diamond$

Let $EG_n = G * \cdots * G$ the nth iterated join of G with itself. Then, $EG = \varinjlim EG_n$ will be our chosen model for EG. With this model in mind, we have a composition

$$R(G) = K_G^*(*) \xrightarrow{\alpha_n} K_G^*(EG_n) = K^*(BG_n) \xrightarrow{\varepsilon} \mathbb{Z}$$

(second equality coming from the fact that G acts freely on EG_n) which is identified with the usual rank map. We'd like to show that α_n kills I_G^n. Since I_G is in the kernel of this composition, we see that $\alpha_n(I_G) \subset \widetilde{K}^*(BG_n)$. Now, one observes that BG_n is covered by n contractible sets (fixed point in each of the n factors of the join?), so any product of n elements of $\widetilde{K}^*(BG_n)$ vanishes. Thus, $\alpha_n(I_G^n) = 0$ as desired.

Functoriality then gives $K_G^*(X)/I_G^n \cdot K_G^*(X) \xrightarrow{\alpha_n} K_G^*(X \times EG_n)$ whenever $K_G^*(X)$ is finite over $K_G^*(*)$.

Example. Take $G = S^1$. Theorem gives a comparison

$$\mathbb{Z}[\rho, \rho^{-1}] = R(S^1) = K_{S^1}^*(*) \longrightarrow K^*(BS^1) \cong K^*(\mathbb{CP}^\infty) = \mathbb{Z}[\![t]\!] .$$

Can think of this as a map $\widehat{\mathbb{G}}_m \to \mathbb{G}_m$ from the formal multiplicative group to the usual multiplicative group.[36] This map is $\rho \mapsto 1 + t$ and $\mathbb{Z}[\![t]\!] \cong \mathbb{Z}[\rho, \rho^{-1}]^\wedge_{(\rho-1)}$. △ something something formal neighborhood something something

There are 4 steps to the proof of the main theorem

- $G = \mathbb{T}$ is a circle (use Thom isomorphism)
- $G = \mathbb{T}^m$ (induct on m)
- $G = U(m)$ (holomorphic induction)
- General G (embed in unitary group using Peter-Weyl). Here we need $K_G^*(X) \to K^*(X_G)$ for general X, not just $X = *$ (like in Quillen's paper we talked about before).

We'll focus on first and third steps.

Step 1 $G = \mathbb{T} = S^1$. Here, $ET_n = S^1 * \cdots * S^1 = S^{2n-1}$. Consider the pair $(X \times D^{2n}, X \times S^{2n-1})$. This gives

$$\begin{tikzcd}
K_T^*(X \times D^{2n}, X \times S^{2n-1}) \arrow[r, "\cdot \xi^n"] \arrow[d, "\wr"] & K_T^*(X \times D^{2n}) \arrow[r] & K_T^*(X \times S^{2n-1}) \arrow[ll, bend right] \\
K_T^*(X) & &
\end{tikzcd}$$

Above $\xi^n = (1 - \rho)^n$ is the Thom class. From this, we get a map of SESs

$$\begin{tikzcd}
0 \arrow[r] & K_T^*(X)/\xi^n \cdot K_T^*(X) \arrow[r, "\alpha_n"] \arrow[d] & K_T^*(X \times S^{2n-1}) \arrow[r] \arrow[d] & {}_{\xi^n} K_T^*(X) \arrow[r] \arrow[d, "\cdot \xi^{n-m}"] & 0 \\
0 \arrow[r] & K_T^*(X)/\xi^m \cdot K_T^*(X) \arrow[r] & K_T^*(X \times S^{2m-1}) \arrow[r] & {}_{\xi^m} K_T^*(X) \arrow[r] & 0
\end{tikzcd}$$

[36] I think so anyways; I'm not sure if dealing with formal schemes involves any relevant subtleties. What Jae actually said is that this gives a map from the ring of functions of $\mathbb{G}_m$ to the ring of functions of $\widehat{\mathbb{G}}_m$.

$(m \le n)$. Above, ${}_{\xi^m}K_T^*(X) = \{x : \xi^n x = 0\}$. Key observation is that $(1-\rho) = I_{S^1}$ is the augmentation ideal.

This gives one morphism of pro-objects. To get the inverse morphism, we really just need maps

$$\beta_{n,m} : K_T^*(X \times S^{2m-1}) \longrightarrow K_T^*(X)/\xi^m \cdot K_T^*(X).$$

Constructing this map is basically just a diagram chase.

One you have this, you can induct on dimension to get to the general torus case.

Step 3 Holomorphic induction. Let $j : \mathbb{T}^m \to U(m)$ be a maximal torus, so we get a restriction map $j^* : K_U^*(X) \to K_T^*(X)$.

Proposition 3.21.6 (Atiyah)**.** *j^* above admits a left inverse*

$$j_* : K_T^*(X) \to K_U^*(X).$$

That is, we can "induce" U-representations from T-representations (even relatively over a paracompact base space X).

Remark 3.21.7. (Irreducible) representations of U arise as holomorphic sections of line bundles over the flag variety U/T induced from T-representations for $T \subset U$ a maximal torus. $\circ$

The idea is that the natural projection $U \to U/T$ is a principal T-bundle. Starting with a T-rep $\mathbb{C}_\lambda$, you can glue it in to get a vector bundle over the flag variety U/T and then the unitary group acts on its space of global sections (something like this). One needs to be more careful (need holomorphic line bundles, so U/T needs to be a complex manifold for example).

The result in K theory is saying this can be done relatively over a base space X.

We now have a diagram

$$\begin{tikzcd}
K_U^*(X)/I_U^n \cdot K_U^*(X) \arrow[r, "\alpha_n"] \arrow[d, bend left] & K_U^*(X \times EU_n) \arrow[d, bend left] \\
K_T^*(X)/I_U^n \cdot K_T^*(X) \arrow[r] \arrow[u, bend left] \arrow[d, "\wr"] & K_T^*(X \times EU_n) \arrow[u, bend left] \arrow[d, "\wr"] \\
K_T^*(X)/I_T^n K_T^*(X) \arrow[r, "\alpha_n"] & K_T^*(X \times ET_n)
\end{tikzcd}$$

Note that to make the argument here work (i.e. have the maps going up), we need a compact base space. This is why we worked with pro-objects instead of the completions themselves.

Step 4 Embed $G \hookrightarrow U$ and consider $Y = U \times_G X$. Then $K_U^*(Y) = K_U^*(U \times_G X) \xrightarrow{\sim} K_G^*(X)$ and $K_U^*(Y \times EU_n) = K_U^*(U \times_G (X \times EU_n))$. This gives

$$K_G^*(X)/I_G^n \cdot K_G^*(X) \longrightarrow K_G^*(X \times EG_n).$$

This gives pro-object version of main theorem. To pass to completed version, we use the Milnor sequence to see that taking inverse limits gives cohomology of EG. It's not a priori obvious our system satisfies Mittag-Leffler, but it's identified with the LHS above which has surjective transition maps.

3.22 Jordan: The localization of spectra with respect to homology, Bousfield

3.22.1 Talk Notes

One big takeaway is that localization will be easier in the stable setting. Here are some key results/ideas:

- Bousfield classes
- SG-localizations
- arithmetic fiber squares
- E-(pre)nilpotence and consequences
- K-theory localizations

Notation/conventions We work with spectra in the stable homotopy category Ho^s .

Definition 3.22.1. Say X is **E_*-acyclic** if $E_*X = 0$, and X is **E_*-local** if every E_*-equivalence $f : A \to B$ induces a bijection

$$[B, X] \xrightarrow{\sim} [A, X].$$

Equivalently, $[A, X] = 0$ whenever A is E_*-acyclic. ⋄

Last time we mentioned that there was a connection between acyclic spaces and local spaces, but it was not easy to say exactly what it is. In the stable setting, there's a more concrete connection.

Theorem 3.22.2 (Theorem 1.1)**.** *Given $E, A \in \mathrm{Ho}^s$, there is a natural (in A) triangle*

$${}_EA \to A \to A_E \to \Sigma({}_EA)$$

where ${}_EA$ is the E_*-acyclization and A_E is the E_*-localization.

Definition 3.22.3. Given $E, G \in \mathrm{Ho}^s$, we say that $E \sim G$ iff E and G have the same acyclics. We can further define a partial order on these equivalence classes of spectra: we say $\langle E\rangle \le \langle G\rangle$ iff each G_*-acyclic is E_*-acyclic. ⋄

The idea is that E has more acyclic spaces than G, and so sees less homotopy-theoretic information. The equiv classes above are called **Bousfield classes**.

Proposition 3.22.4. *If $\langle E\rangle \le \langle G\rangle$, then*

(i) *X E_*-local $\Longrightarrow$ X G_*-local.*[37]

(ii) *For all $X \in \mathrm{Ho}^s$,*

$$(X_G)_E \simeq X_E \simeq (X_E)_G$$

(iii) *Other relation similar to **(ii)**, but these aren't important for this talk.*

Definition 3.22.5. We say X is a **Moore spectrum** SG if $\pi_i X = 0$ for $i < 0$, $H_0X \cong G$, and $H_iX = 0$ for $i \neq 0$. ⋄

[37] Get this by making use of the triangles from before

Note 11. Can construct by taking a presentation $0 \to \mathbb{Z}^{\oplus A} \xrightarrow{f} \mathbb{Z}^{\oplus B} \to G \to 0$ of G, and then letting SG be the cofiber of the corresponding map $\bigvee_A S \to \bigvee_B S$ where S is the sphere spectrum.

Definition 3.22.6. Two abelian groups G_1, G_2 **have the same type of acyclicity** if

(i) G_1 torsion iff G_2 torsion.

(ii) For all primes p, G_1 is unique p-divisible iff G_2 is.

$\diamond$

Proposition 3.22.7 (Proposition 2.3)**.** *TFAE:*

(i) *G_1, G_2 have the same type of acyclicity*

(ii) *$\langle SG_1 \rangle = \langle SG_2 \rangle$, i.e. SG_1 an SG_2 have exactly the same acyclics*

(iii) *SG_1, SG_2 give equivalent localization functors*

Proposition 3.22.8 (Propositions 2.4 + 2.5)**.** *Let $G \cong \mathbb{Z}_{(J)}$, for J a set of primes. Then $X_{SG} \simeq SG \wedge X$, and*

$$\pi_* X_{SG} \simeq G \otimes \pi_* X$$

for all spectra $X \in \mathrm{Ho}^S$.

Now let $G \cong \mathbb{Z}/p\mathbb{Z}$. Then, $X_{SG} \simeq F(\Sigma^{-1} S\mathbb{Z}/p^\infty\mathbb{Z}, X)$. If $\pi_* X$ are finitely generated, then

$$\pi_* X_{SG} \cong \widehat{\mathbb{Z}}_p \otimes \pi_* X.$$

Remark 3.22.9. Above, $F(-,-)$ is the **function spectrum**. It satisfies the following "hom-tensor" type adjunction

$$[X \wedge Y, Z] \cong [X, F(Y, Z)].$$

Note that you can prove $F(Y, Z)$ exists via Brown representability since the LHS above is a cohomology theory in X. In particular, if $Z = S$ (and X, Y are finite complexes), then $F(Y, S) = Y^\vee$ is the **Spanier-Whitehead dual** of Y.

I don't know what the actual notation for this usually is

In prop 2.5, Bousfield claims that $F(\Sigma^{-1} S\mathbb{Z}/p^\infty\mathbb{Z}, X)$ can be constructed as a homotopy inverse limit of

$$S\mathbb{Z}/p\mathbb{Z} \wedge X \leftarrow S\mathbb{Z}/p^2\mathbb{Z} \wedge X \leftarrow \dots$$

in analogy with the construction of $\widehat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. $\circ$

Remark 3.22.10. Bousfield also gives conditions for how to tell if a spectrum is SG-local $\circ$

Proposition 3.22.11 (Prop 2.1)**.** *For all $E, X \in \mathrm{Ho}^s$, we have an "arithmetic fiber square"*

or 2.9?

$$\begin{tikzcd} X_E \arrow[r] \arrow[d] & \prod X_{E\mathbb{Z}/p\mathbb{Z}} \arrow[d] \\ X_{E\mathbb{Q}} \arrow[r] & \left(\prod X_{E\mathbb{Z}/p\mathbb{Z}}\right)_{E\mathbb{Q}} \end{tikzcd}$$

where, for an abelian group G, we define $EG := E \wedge SG$ ("spectra with coefficients").

Remark 3.22.12. If $E = S$ is the sphere spectrum, then the above lets you recover X itself from its localizations at various Moore spectra. $\circ$

Definition 3.22.13 (Definition 3.7)**.** For ring spectrum E, the ***E*-nilpotent** spectra form the smallest class $\mathcal{C}$ satisfying

Remember: A ring spectrum is a monoid is the (symmetric monoidal) homotopy category of spectra

(i) $E \in \mathcal{C}$

(ii) For $N \in \mathcal{C}$, $X \in \mathrm{Ho}^s$, we have $N \wedge X \in \mathcal{C}$

(iii) Triangles $X \to Y \to Z \to \Sigma X$ in Ho^S satisfy 2-out-of-3. In particular, it is closed under (finite) sums/wedges.

(iv) If $N \in \mathcal{C}$ and M is a retract of N, then $M \in \mathcal{C}$.

We say Y is ***E*-prenilpotent** if there exists an E_*-equivalence $Y \to N$ with N being E-nilpotent (i.e. Y_E is E-nilpotent). $\diamond$

"Let Nlab sink to the bottom of the ocean" – Haynes, 2020

Proposition 3.22.14 (Proposition 3.9)**.** *If S is E-prenilpotent for ring spectrum E, then*

(i) $S_E \wedge Y \xrightarrow{\sim} Y_E$ *for all* $Y \in \mathrm{Ho}^S$*. Might say that "E is* ***smashing-local****."*

(ii) *Every* $Y \in \mathrm{Ho}^S$ *is E-prenilpotent, and E-nilpotent = E_*-local.*

K-theory We start by noting/asserting that $\langle K \rangle = \langle KO \rangle$, so we will only look at localization with respect to complex K-theory.

Proposition 3.22.15 (Corollary 4.6)**.**

$$\pi_i S_K \cong \begin{cases} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } i = 0 \\ \mathbb{Q}/\mathbb{Z} & \text{if } i = -2 \\ \bigoplus_p \left(\mathbb{Z}_{(p)} \otimes \pi_i S_K\right) & \text{if } i \neq 0 \end{cases}$$

The last case is a bit strange. I think he's saying that when $i \neq 0$, $\pi_i S_k$ is a finite abelian group and so splits into a sum of its Sylow-p subgroups. One can be more specific about what these groups are since Bousfield gives a description for S_K.

Corollary 3.22.16 (Corollary 4.7)**.** *S is K-prenilpotent. Hence,* $S_K \wedge Y \xrightarrow{\sim} Y_K$ *for all* $Y \in \mathrm{Ho}^S$.

Remark 3.22.17. Mod p singular homology $H\mathbb{Z}/p\mathbb{Z}$ does not have this property, so this is one way in which K-theory is better. $\circ$

Theorem 3.22.18 (Theorem 4.8)**.** *For a spectrum* $X \in \mathrm{Ho}^S$*, TFAE:*

(i) *X is K_*-local.*

(ii) $A_p^* : [M_p, X]_* \xrightarrow{\sim} [M_p, X]_{*+d}$ *for all p.*

(iii) $A_{p,*} : \pi_* M_P \wedge X \xrightarrow{\sim} \pi_{*+d} M_p \wedge X$ *for all p.*

Above, A_p, M_p are constructed in Adams' $J(X)$ IV paper. In particular $M_p = S\mathbb{Z}/p\mathbb{Z}$ is a Moore spectrum, and $A_p : \Sigma^d M_p \to M_p$ ($d = 2p-1$ if p odd and $d = 8$ if p is even) a certain map inducing an isomorphism $A_p^* : K^*(M_p) \xrightarrow{\sim} K^*(M_p)$.

Remark 3.22.19. This is maybe a little like checking that you have a rational spectrum if its homotopy is rational. ○

Remark 3.22.20 (Haynes). There is a neat thing that you can recover K from KO. K is "KO with coefficient" is some respect: specifically, $K = KO \wedge \Sigma^{-2}\mathbb{CP}^2$. I didn't get everything he said, but sounds like $\Sigma^{-2}\mathbb{CP}^2$ is a 0-cell and a 2-cell connected by the Hopf map η; this let's you do some cofiber sequence thing and apparently you can show $\langle K\rangle = \langle KO\rangle$ once you know that η is nilpotent (apparently, $\eta^4 = 0$). ○

There was more that was said, but I didn't catch it well enough to write coherent things down...

3.23 Junyao: Homotopy limits, completions and localizations, Bousfield and Kan

3.23.1 Talk Notes

Main results

These are not my best notes...

- Construction of R-tower $\{R_s X\}$ and R-completion $R_\infty X$
  - $\cdots \to R_s X \to R_{s-1}X \to \dots$ is a tower of fibrations
  - $\varprojlim R_s X = R_\infty X$
  - $f_* : \widetilde{\mathrm{H}}_*(X; R) \xrightarrow{\sim} \widetilde{\mathrm{H}}_*(Y; R) \iff R_\infty \simeq R_\infty Y$

    Not sure if homotopy equivalence or weak homotopy equivalence
  - For "R-good" spaces,
  $$\widetilde{\mathrm{H}}_*(X; R) \xrightarrow{\sim} \widetilde{\mathrm{H}}(R_\infty X; R),$$
    and $R_\infty X$ is R-complete (i.e. $R_\infty X \simeq R_\infty^2 X$).

  Remark 3.23.1. For an R-good space X, its HR-localization is exactly its R-completion. ○

- Bousfield-Kan spectral sequence
$$E_2^{s,t} = \pi^s \pi_t \underline{R}X \implies \pi_* R_\infty X.$$

  Remark 3.23.2. Same construction gives lots of spectral sequences ○

Outline

- Cosimplicial spaces and totalization
- Tot tower and spectral sequences
- R-compltion of spaces
- Nilpotent spaces

Conventions

- space = simplicial set
- $\mathcal{J}$ is the category of spaces, $\mathcal{J}_*$ is pointed spaces
- $c\mathcal{J}$ is cat of cosimplicial spaces
- $\underline{X}$ is a cosimplicial space
- rings R assumine **solid** (i.e. $R \otimes_{\mathbb{Z}} R \xrightarrow{\sim} R$)

Cosimplicial spaces and totalization We start with constuction of derived (or homotopy) pullback (geometric cobar construction)

$$\begin{array}{ccc} ? & \longrightarrow & X \\ \big\downarrow & & \big\downarrow \\ Y & \longrightarrow & B \end{array}.$$

Consider a sequence of spaces $X \times B^n \times Y$ forming a cosimplicial space with coface maps

$$d^i(x, b_1, \ldots, b_n, y) = \begin{cases} (x, f(x), b_1, \ldots, b_n, y) & \text{if } i = 0 \\ (x, b_1, \ldots, b_i, b_i, \ldots, b_n, y) & \text{if } 1 \le i \le n \\ (x, b_1, \ldots, b_n, g(y), y) & \text{if } i = n+1 \end{cases}$$

and codegeneracy maps

$$s^i(x, b_1, \ldots, b_n, y) = (x, b_1, \ldots, \widehat{b_i}, \ldots, b_n, y) \text{ for } 1 \le i \le n.$$

These satisfy the relevant compatibility relations ($s^i d^i = s^i d^{i+1} = \mathrm{id}, \ldots$). Thus they form the data of a cosimplicial space $X \in c\mathcal{J}$.

Definition 3.23.3. The **total space** of $\underline{X} \in c\mathcal{J}$ is $\operatorname{Tot} \underline{X} \in \mathcal{J}$ given by $\operatorname{Tot} \underline{X} = \operatorname{Hom}_{c\mathcal{J}}(\underline{\Delta}, \underline{X})$ where $\underline{\Delta}$ is the standard cosimplicial simplex ($\underline{\Delta}^n = \Delta[n]$ with expected coface/codegeneracy). One has $(\operatorname{Tot} \underline{X})_n = \operatorname{Hom}_{c\mathcal{J}}(\Delta[n] \times \underline{\Delta}, X)$. ◇

Example. $\operatorname{Tot} X \underline{\times}_B Y$ is our homotopy pullback. It's the space of maps $f^i : \Delta[i] \to X \times B^i \times Y$ satisfying compatibilities coming from the coface and codegeneracy maps. If you write down what this means and thing about it hard enough, you'll see that everything is determined by what's happening in degrees 0 and 1, and that

$$\operatorname{Tot} X \underline{\times}_B Y \simeq \{\text{paths } f(x) \sim g(y)\} \simeq X \times_B \operatorname{Hom}_{\mathcal{J}}(\Delta[1], B) \times_B Y.$$

△

Tot tower and spectral sequences The n-**skeleton** of a cosimplical space is obtained by taking the degreewise n-skeleta. For $\underline{X} \in c\mathcal{J}$, we define

$$\operatorname{Tot}^n \underline{X} = \operatorname{Hom}_{c\mathcal{J}}(\operatorname{sk}_n \underline{\Delta}, \underline{X})$$

Example. $\mathrm{Tot}^0 \underline{X} \simeq \underline{X}^0$

$\mathrm{Tot}^1 \underline{X} \simeq \{\text{paths } p : d^0 x \sim d^1 x \text{ in } \underline{X}^1 \text{ over } x \in \underline{X}^0\}$

In general, $\mathrm{Tot}^n \underline{X}$ depends only on $\underline{X}^0, \ldots, \underline{X}^n$. △

The inclusion $\mathrm{sk}_{n-1} \underline{\Delta} \to \mathrm{sk}_n \underline{\Delta}$ induces $\mathrm{Tot}^n \underline{X} \to \mathrm{Tot}^{n-1} \underline{X}$, giving a Tot tower whose inverse limit is $\varprojlim \mathrm{Tot}^n X \simeq \mathrm{Tot}\, \underline{X}$.

Proposition 3.23.4. *If $\underline{X}$ is fibrant in $c\mathcal{J}_*$, then $\{\mathrm{Tot}^n \underline{X}\}$ is a tower of fibraions (in fact, principal fibrations).*

Remark 3.23.5. The fiber $F_n \to \mathrm{Tot}^n \underline{X} \to \mathrm{Tot}^{n-1} \underline{X}$ is

$$F_n = \Omega^n (N^n \underline{X})$$

where $N^n \underline{X} = \underline{X}^n \cap \ker s^0 \cap \ker s^1 \cap \cdots \cap \ker s^{n-1}$ is the normalized complex. ○

Remark 3.23.6. If $\underline{G}$ is a cosimplicial abelian group, then $\underline{G}$ is also a cochain complex

$$\underline{G}^0 \xrightarrow{d} \underline{G}^1 \xrightarrow{\cdots}$$

with differential $= \sum_i (-1)^i d^i$ (d^i the ith coface map).

N^* satisfies $\mathrm{H}^s(N^* \underline{G}, d) \cong \mathrm{H}^s(\underline{G}, d)$. ○

The LESs in homotopy of a fibration fit into an exact couple

$$\begin{tikzcd} \pi_* \mathrm{Tot}^n X \arrow[rr, "i"] & & \pi_* \mathrm{Tot}^{n-1} X \arrow[dl, "j"] \\ & \pi_* F_n \arrow[ul, "k"] & \end{tikzcd}$$

The gives a spectral sequence

$$E^1_{s,t} = \pi_{t-s}(F_s) \implies \pi_{t-s}(\mathrm{Tot}\, X)$$

Note that we have $\pi_{t-s}(\Omega^s N^s X) = \pi_t(N^s X) = N^s \pi_t \underline{X}$ above, a cosimplicial abelian group. Hence the E^2-page is

$$E^2_{s,t} = \mathrm{H}^s(N^s \pi_t \underline{X}, d = \sum (-1)^i d^i) = \mathrm{H}^2(\pi_t \underline{X}, d) = \pi^s \pi_t \underline{X}.$$

Application. Consider

$$\begin{tikzcd} X \times_B Y \arrow[r] \arrow[d] & X \arrow[d] \\ Y \arrow[r] & B \end{tikzcd}$$

with $X \times_B Y \simeq \mathrm{Tot}(X \underline{\times}_B Y)$ since $f : X \to B$ is a fibration. Then,

$$\mathrm{H}_*(X \times_B Y; k) = \mathrm{H}_*(\mathrm{Tot}; k) = \pi_*(k \otimes \mathrm{Tot}) = \pi_* \mathrm{Tot}(k \otimes (X \underline{\times}_B Y))$$

where conditions are needed for last equality (since we're commuting a left adjoint with a right adjoint). Can compute $E^2_{s,t} = \mathrm{Cotor}^{\mathrm{H}_* B}_{s,t}(\mathrm{H}_* Y, \mathrm{H}_* X)$.

R-completion of spaces Assume R commutative and $R \otimes_{\mathbb{Z}} R \xrightarrow{\sim} R$ (e.g. $R = \mathbb{F}_p, \mathbb{Q}$).

We want $X \to R_\infty X$ satisfying

(1) $\widetilde{\mathrm{H}}_*(X; R) \xrightarrow{\sim} \widetilde{\mathrm{H}}_*(Y; R) \iff R_\infty \simeq R_\infty Y$

(2) $\widetilde{\mathrm{H}}_*(X; R) \xrightarrow{\sim} \widetilde{\mathrm{H}}_*(R_\infty X; R)$

(3) $R_\infty X$ is R-complete

Remark 3.23.7. There's the Bousfield localization at HR which already does all of this. However, this more complicated seeming R-completion is also more concretely constructed, and so "easier" to work with (get spectral sequences). ○

Let $X \in \mathrm{SSet}$ and let $R \otimes X$ denote the free simplicial R-module

$$(R \otimes X)_n = R^{\oplus X_n}$$

Define $RX \subset R \otimes X$ the subspace with simplices $\sum_i x_i$ where $r_i \in R$ s.t. $\sum r_i = 1$ $(x_i \in X_n)$. (If X pointed, then $RX \cong R \otimes X / R \otimes *$ is a simplicial R-module) This R functor satisfies

- It has a monad structure $\varphi : \mathrm{id} \to R$ and $\psi : R^2 \to R$ (need $R \otimes_{\mathbb{Z}} R \cong R$ here).
- Fix $* \in X$. There is a canonical isomorphism

$$\pi_* RX \cong \widetilde{\mathrm{H}}_*(X; R)$$

  s.t. $\pi_* X \xrightarrow{\pi_* \varphi} \pi_* RX \to \widetilde{\mathrm{H}}_*(X; R)$ is the Hurewicz map.

Remember: A monad is a monoid in the category of endofunctors

Unclear why it's not enough to know you always have $R \otimes_{\mathbb{Z}} R \to R$, i.e. unclear why this needs to be an iso. Maybe something to do with this $\sum r_i = 1$ condition? Who knows?

Definition 3.23.8. The R**-cosimplicial resolution** of a space X is $\underline{R}X \in c\mathcal{J}$ with $(\underline{R}X)^n = R^n X$ and coface/codegen maps

$$d^i : R^n X \xrightarrow{R^i \varphi R^{n-1}} R^{n+1} X \text{ and } s^i R^{n+2} X \xrightarrow{R^i \psi R^{n-i}} R^{n+1} X.$$

◇

Remark 3.23.9. Every monad gives rise to a cosimplicial structure ○

Definition 3.23.10. The R**-completion** of a space X is $R_\infty X := \mathrm{Tot}(\underline{R}X)$ and its R**-tower** is $R_s X = \mathrm{Tot}^s(\underline{R}X)$. ◇

Remark 3.23.11. If $\underline{R}X$ is fibration, $\{R_s X\}$ is a tower of fibrations, so induces spectral sequences

$$E^2_{s,t} = \pi^s \pi_t \underline{R}_X \implies \pi_* R_\infty X$$

modulo convergence being tricky. ○

Definition 3.23.12. A space X is called

- R**-complete** if $X \xrightarrow{\sim} R_\infty X$
- R**-good** if $\widetilde{\mathrm{H}}_*(X; R) \xrightarrow{\sim} \widetilde{\mathrm{H}}_*(R_\infty X; R)$

- R-**bad** if not R-good

$\diamond$

Proposition 3.23.13. *TFAE*

- X *is* R*-good*
- $R_\infty X$ *is* R*-complete*
- $R_\infty X$ *is* R*-good*

Remark 3.23.14. The first two things being equivalent here shows that the last two things we wanted R-completions to satisfy are equivalent. $\circ$

Remark 3.23.15. If X is bad, then it is "very bad" since $R_\infty^n X \to R_\infty^{n+1} X$ is never a (weak) homotopy equivalence. $\circ$

Nilpotent spaces

Definition 3.23.16. A connected (pointed) space X is **nilpotent** if $\pi_1 X$ acts nilpotently on $\pi_n X$. $\diamond$

Example. $S^1 \vee S^2$ is not nilpotent (not $\mathbb{F}_p$-good) $\triangle$

Example. simply connected spaces are nilpotent. $\triangle$

Proposition 3.23.17. *For* $R \subset \mathbb{Q}$ *or* $R = \mathbb{F}_p$*,* X *nilpotent*

- X *is* R*-good,* $R_\infty X$ *is* R*-complete*
- $X \to R_\infty X$ *is the* HR*-localization*
- *If* $R \subset \mathbb{Q}$*,*
$$R \otimes \pi_* X \cong \pi_* R_\infty X \text{ and } R \otimes \widetilde{\mathrm{H}}_*(X;\mathbb{Z}) \cong \widetilde{\mathrm{H}}_*(R_\infty X;\mathbb{Z}).$$
- *If* $R = \mathbb{F}_p$*,* q *prime,*
$$\widetilde{\mathrm{H}}_*(R_\infty;\mathbb{F}_q) \cong \begin{cases} \widetilde{\mathrm{H}}_*(X;\mathbb{F}_q) & \text{if } q = p \\ 0 & \text{otherwise.} \end{cases}$$
If $\pi_n X$ *are f.g. abelian, then* $\pi_n R_\infty X \cong \mathbb{Z}_p \otimes \pi_n X$.

There's some subtltly with defining $R \otimes \pi_1 X$ with $\pi_1 X$ is a non-abelian nilpotent group

Example. The p-completion of S^n is $S^n_{H\mathbb{F}_p}$, the $H\mathbb{F}_p$-localization. Furthermore, $\pi_* S^n_{H\mathbb{F}_p} \cong \mathbb{Z}_p \otimes \pi_* S^n$ and so $S^n_{H\mathbb{F}_p}$ is $(n-1)$-connected. Furthermore, $\widetilde{\mathrm{H}}_*(S^n_{H\mathbb{F}_p};\mathbb{F}_q) = \mathbb{F}_p$ if $* = n, q = p$, but is 0 otherwise.

What about rational homology? It's more complicated. For example,

$$\mathrm{H}_3(S^3_{H\mathbb{F}_p};\mathbb{Q}) \cong \pi_3 S^3_{H\mathbb{F}_p} \otimes \mathbb{Q} \cong \mathbb{Z}_p \otimes \mathbb{Q} = \mathbb{Q}_p.$$

Also, $S^3_{H\mathbb{F}_p}$ is an H-space, so its homology is a Hopf algebra, so expect things to get worse in larger degrees. $\triangle$

3.24 Niven: Forms of K-Theory, Morava

3.24.1 Paper Notes

Like last time, I typed up some notes on the paper.

3.24.2 Talk Notes

For the talk itself, this is what I wrote down.

3.25 David: $\mathbb{A}^1$-homotopy theory of schemes, Morel and Voevodsky

3.25.1 Talk Notes

Fix some finite-dimensional noetherian scheme (can take $S = \operatorname{Spec} k$ if you want).

Goal. Construct a model category Spc which contains all smooth S-schemes (S-smooth schemes?) and $X \times \mathbb{A}^1_S \to X$ will be a weak equivalence.

Notation 3.25.1. We'll write A^1 or $\mathbb{A}^1$ for $\mathbb{A}^1_S$.

Why do this? There are many "cohomology theories" with $\mathbb{A}^1$-invariance, e.g.

$$K_*(X) \simeq K_*(X \times \mathbb{A}^1) \text{ and } CH^*(X) \simeq CH^*(X \times \mathbb{A}^1)$$

for smooth X.

Conjecture 3.25.2. $\operatorname{Vect}_r(X) \simeq \operatorname{Vect}_r(X \times \mathbb{A}^1)$ *for regular affine* X.

We write Sm/S for the category of smooth schemes over S. For us a **model category** will satisfy

- complete and cocomplete (i.e. all small (co)limits)
- 2/3 for weak equiv
- weak equiv, cofib, fib preserved under retracts
- lifting
- functorial factorizations

The first of this is already unsatisfied by Sm/S, so we first enlarge to the category $\operatorname{Psh}(\operatorname{Sm}/S)$ of presheaves of sets. We have $y : \operatorname{Sm}/S \hookrightarrow \operatorname{Psh}(\operatorname{Sm}/S)$ via Yoneda.

Remark 3.25.3. $\operatorname{Psh}(\operatorname{Sm}/S)$ is (co)complete, and y commutes with limits (but not with colimits). ○

Example. Say $X \in \operatorname{Sm}/S$ with open covering $X = U \cup V$. It is plausible to require that

$$\begin{tikzcd} U \cap V \arrow[r] \arrow[d] & V \arrow[d] \\ U \arrow[r] & X \end{tikzcd}$$

is a pushout. It is in the category Sm/S, but not necessarily so in $\operatorname{Psh}(\operatorname{Sm}/S)$ since the Yoneda embedding does not commute with colimits.

For this to be a pushout in $\mathrm{Psh}(\mathrm{Sm}/S)$, we would need to have that for any $F \in \mathrm{Psh}(\mathrm{Sm}/S)$ applying $\mathrm{Mor}(-, F)$ gives a pullback square

$$\begin{tikzcd} F(X) \arrow[r] \arrow[d] & F(U) \arrow[d] \\ F(V) \arrow[r] & F(U \cap V) \end{tikzcd}.$$

This is a sheaf condition, so certainly does not hold for arbitrary presheaves. $\triangle$

Nisnevich sheaves

Definition 3.25.4. An **elementary distinguished square** is a diagram in Sm/S:

$$\begin{tikzcd} U \times_X V \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & V \arrow[d, "p"] \\ U \arrow[r, "j"] & X \end{tikzcd}$$

such that

- J is an open immersion
- p is étale
- $p^{-1}(X \setminus U) \to X \setminus U$ is an isomorphism.

$\diamond$

Definition 3.25.5. A presheaf $F \in \mathrm{Psh}(\mathrm{Sm}/S)$ is called a **Nisnevich sheaf** (or just *sheaf*) if

- $F(\emptyset) = *$
- F takes elementary distinguished squares to pullback squares

$\diamond$

Example. Let $S = \operatorname{Spec} k$ with $\operatorname{char} k \neq 2$. Consider

$$\begin{tikzcd} \mathbb{A}^1 \setminus \{0, \alpha, -\alpha\} \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & \mathbb{A}^1 \setminus \{0, \alpha\} \arrow[d, "x \mapsto x^2"] \\ \mathbb{A}^1 \setminus \{\alpha^2\} \arrow[r, "j"] & \mathbb{A}^1 \end{tikzcd}$$

This is an elementary distinguished square. Note, in partticular that $X \setminus U = \{\alpha^2\}$ here and the fiber above it is the singleton $\{-\alpha\}$. $\triangle$

Let $\mathrm{Sh}(\mathrm{Sm}/S)$ denote the category of sheaves.

Lemma 3.25.6. *Any representable presheaf is a sheaf. In particular, the Yoneda embedding factors through the category of sheaves.*

Definition 3.25.7. The category Spc of spaces will be the category of simplicial objects in $\mathrm{Sh}(\mathrm{Sm}/S)$ (i.e. sheaves of simplicial sets). There is also Spc_*, the category of sheaves of pointed simplicial sets. $\diamond$

Everything we say about Spc will equally apply to Spc_*.

Example. For $X \in \mathrm{Sm}/S$, then X can be considered as an object of Spc as a discrete simplicial sheaf.

If $K \in \mathrm{SSet}$, then K is an object of Spc, considered as a constant sheaf. △

Definition 3.25.8. A **point** is a functor

$$x^* : \mathrm{Sh}(\mathrm{Sm}/S) \to \mathrm{Set}$$

which commutes with small colimits and finite limits. Note that this induces a functor $\mathrm{Spc} \to \mathrm{SSet}$. ◇

Example. The functor taking the stalk at a scheme-theoretic point of some $X \to S$ will be a 'point' in this sense. △

Model Category Structure

Theorem 3.25.9. *There exists a proper (can ignore this word) simplicial (i.e. enriched over* SSet*) model category structure on* Spc *such that $f : X \to Y$ is a*

- *weak equivalence if*
$$x^* f : x^* X \to x^* Y$$
is a weak equivalence in SSet *for every point of x^*.*
- *cofibration if monic*
- *fibration if it has right lifting property w.r.t acyclic cofibrations.*

*We call this the **Simplicial model category structure on*** Spc.

We will define another model category structure in a bit.

Notation 3.25.10. We write Ex for the (functorial) fibrant replacement in the above model category.

We let $\mathrm{Ho}_s(\mathrm{Sm}/S)$ denote its homotopy category, and $[-,-]_s$ denote the morphism set in $\mathrm{Ho}_s(\mathrm{Sm}/S)$.

Definition 3.25.11. A $Z \in \mathrm{Spc}$ is $\mathbb{A}^1$**-local** if

$$[X, Z]_s \to [X \times \mathbb{A}^1, Z]_s$$

is a bijection for every $X \in \mathrm{Spc}$. ◇

Definition 3.25.12. We call $f : X \to Y$ in Spc an $\mathbb{A}^1$**-equivalence** if

$$[Y, Z]_s \to [X, Z]_s$$

is a bijection for any $\mathbb{A}^1$-local Z. ◇

Note that any simplicial weak equivalence is an $\mathbb{A}^1$-equivalence.

Theorem 3.25.13. *There exists a proper simplicial model category structure on* Spc *s.t. $f : X \to Y$ is a*

- *weak equiv if $\mathbb{A}^1$-equiv*
- *cofibration if monic*
- *fibration if it has the right lifting property wrt acyclic cofibrations*

*We call this the $\mathbb{A}^1$**-model category structure on** Spc.*

Notation 3.25.14. We write $\mathrm{Ho}(\mathrm{Sm}/S)$ for the $\mathbb{A}^1$-homotopy category, and $[-,-]$ for its morphism sets.

Proposition 3.25.15. *Let X be a simplicially fibration object of* Spc*. Then, TFAE*

- *X is $\mathbb{A}^1$-fibrant*
- *X is $\mathbb{A}^1$-local*
- *X is $\mathbb{A}^1$**-invariant**, i.e.*
$$X(U) \xrightarrow{\sim} X(U \times \mathbb{A}^1)$$
is a weak equiv for every $U \in \mathrm{Sm}/S$.

Examples

Remark 3.25.16. We have (co)limits so can form quotients, smash products, etc. as (co)limits of suitable diagrams. ◦

There are two natural candidates for a "circle". There is the **simplicial circle**

$$S^1_s := \Delta^1/\partial\Delta^1$$

as well as the **Tate circle**

$$S^1_t := \mathbb{A}^1 \setminus 0.$$

We can higher dimension spheres by setting

$$S^{p,q} := S^{p-q}_s \wedge S^a_t \text{ when } p \geq q \geq 0.$$

We will also emphasize

$$T := S^{2,1} = S^1_s \wedge S^1_t.$$

Proposition 3.25.17. *$T \simeq \mathbb{A}^1/(\mathbb{A}^1 \setminus 0) \simeq \mathbb{P}^1$ where $\simeq$ means $\mathbb{A}^1$-equivalent.*

Proof. Consider the homotopy pushout

$$\begin{tikzcd} S^1_t \arrow[r] \arrow[d] & \mathbb{A}^1 \arrow[d] \\ \Delta^1 \wedge S^1_t \arrow[r] & X \end{tikzcd}$$

The usual pushout is a homotopy pushout since $S_t^1 \hookrightarrow \mathbb{A}^1$ is an inclusion (cofibration?). Can check that $\Delta^1 \wedge S_t^1$ is the cone on S_t^1, so this is contractible, which gives

$$X \simeq \mathbb{A}^1/S_t^1 = \mathbb{A}^1/\mathbb{A}^1 \setminus 0.$$

At the same time, $\mathbb{A}^1$ is $\mathbb{A}^1$-contractible, so we also have

$$X \simeq \Delta^1 \wedge S_t^1/S_t^1 = S_s^1 \wedge S_t^1 = T.$$

For the second equivalence, the diagram

$$\begin{tikzcd} \mathbb{A}^1 \setminus 0 \arrow[r] \arrow[d] & \mathbb{A}^1 \arrow[d] \\ \mathbb{A}^1 \arrow[r] & \mathbb{P}^1 \end{tikzcd}$$

is a homotopy pushout, and $\mathbb{A}^1 \simeq *$, so $\mathbb{P}^1 \simeq \mathbb{A}^1/\mathbb{A}^1 \setminus 0$. ■

Remark 3.25.18. Can show in general that $\mathbb{A}^n \setminus 0 \simeq S^{2n-1,n}$. ○

We can even make a stable homotopy theory in the present context. We do this by inverting Σ_s, Σ_t (or T). We can then say things like T-spectra and so on... "cohomology theories" represented in this stable homotopy theory will be bi-graded (since two types of suspensions).

On to the next example. Suppose S is a regular scheme. Let $K \in \Delta^{\mathrm{op}} \operatorname{Psh}(\mathrm{Sm}/S)$ (a simplicial presheaf) be the **K-theory space**

$$X \mapsto \Omega BQPX$$

whose homotopy groups are K-groups. It is a theorem that K sends elementary distinguished square to homotopy pullback squares (due to Thomason-Trobogh). Morevl-Voedosky call this the **BG property**. We also have that K is $\mathbb{A}^1$-invariant in the sends that $K(X) \to K(X \times \mathbb{A}^1)$ is a weak-eqiv.

Theorem 3.25.19. *Let a denote sheafification. The BG property implies that*

$$K(U) \simeq ((\mathrm{Ex} \circ a)K)(U)$$

for all $U \in \mathrm{Sm}/S$.

Now, $(\mathrm{Ex} \circ a)K$ is simplicially fibration and $\mathbb{A}^1$-invariant, so $\mathbb{A}^1$-fibrant. From this, can show that

$$[\Sigma_s^n U_+, (\mathrm{Ex} \circ a)K] \simeq K_n(U),$$

so K-theory is representable in the $\mathbb{A}^1$-homotopy category by $(\mathrm{Ex} \circ a)K$.

A final example. For a group object $G \in \mathrm{Spc}$, we can construct BG as the sheaf

$$U \mapsto B(G(U)).$$

Can prove that BG classifies G-principal bundles in the $\mathbb{A}^1$-homotopy category. Can also prove something like

$$(\mathrm{Ex} \circ a)K \simeq BGL^{+} \times \mathbb{Z} \simeq BGL \times \mathbb{Z} \simeq \mathrm{Gr}(\infty, \infty) \times \mathbb{Z}$$

so get a "$Q = +$-theorem" (first equivalence above). Above, $\mathrm{Gr}(\infty, \infty)$ is a colimit of schemes, so a geometric object.

4 Math 273X (Distributions of Class Groups of Global Fields) – Harvard

Instructor: Melanie Wood

Homeworks: Found here

4.1 Lecture 1 (9/4)

I was 5 minutes late

4.1.1 Administrative and Class Stuff

I forgot to type most of this down.

Um, homeworks on Wednesdays if you require a grade. Also some sort of final project.

4.1.2 Start of material

Every number field K has a class group Cl_K.

Question 4.1.1. *So what? Why do we care?*

Answer.

- measures failure of unique factorization of $\mathscr{O}_K$
- Is iso to $\mathrm{Gal}(H_K/K)$ where H_K maximal abelian unramified extension of K
- Tells us about isomorphism types of finitely generated modules over $\mathscr{O}_K$.
- Knowledge that Cl_K is (multiplicatively) small (e.g. $p \nmid |\mathscr{O}_K|$) often helps us solve diophantine problems, even over $\mathbb{Q}$.
- etc.

⋆

Question 4.1.2. *What are some class groups?*

Answer. $\mathrm{Cl}_{\mathbb{Q}} = 1$, $\mathrm{Cl}_{\mathbb{Q}(i)} = 1$, $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-163})} = 1$.

$\mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} = \mathbb{Z}/3\mathbb{Z}$

$\mathrm{Cl}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}/2\mathbb{Z}$

$\mathrm{Cl}_{\mathbb{Q}(\sqrt{-84})} = (\mathbb{Z}/2\mathbb{Z})^2$ (wrote 84 instead of 21 since it's the discriminat)

$\mathrm{Cl}_{\mathbb{Q}[x]/(x^3-x^2+1)} = 1$ ⋆

Example. See the LMFDB. △

Looking at the LMFDB, seems like imaginary quadratic class groups seems to grow in size, but the real imaginary ones don't. Gauss conjectured (more-or-less) this in 1798.

Theorem 4.1.3 (Heilbronn 1934)**.** *For imaginary quadratic fields K, as* $\operatorname{disc} K \to \infty$, $|\mathrm{Cl}_K| \to \infty$.

Theorem 4.1.4 (Heegner, Baker, Stark 1952-67)**.** *If $d < 0$, then $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})} = 1$ iff*

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Watkins (using Golfeld-Gross-Zagier) has computed, for example, all d such that $\left|\mathrm{Cl}_{\mathbb{Q}(\sqrt{-d})}\right| \leq 100$.

Theorem 4.1.5 (Littlewood 1928)**.** *Assuming GRH, then there exists some $c > 0$ such that for K imaginary quadratic,*

$$|\mathrm{Cl}_K| \geq c\,|\mathrm{Disc}\,K|^{1/2} \,/\, \log\log|\mathrm{Disc}\,K|\,.$$

The above result is not known unconditionally, but it tells us what to expect.

Question 4.1.6. *What upper bound do we have?*

Answer. We know $|\mathrm{Cl}_K| = O_{\deg K}(|\mathrm{Disc}\,K|^{1/2})$ from Minkowski bound. Hence, not a lot of wiggle room for imaginary quadratic fields. ⋆

Conjecture 4.1.7 (Gauss)**.** *There are infinitely many real quadratic fields with class number* 1*.*

This empirically looks to be the case, but it is very open.

This is getting to the kinds of question this class will be focused on, those of arithmetic statistics (of class groups). As we vary K, how is Cl_K distributed?

Ideally, we would put a measure on the set of K and do measure theorem. However, because we care about ∞ families of K, there is no good measure. To get around this, we usually put some ordering on the K (e.g. order "by discriminant"), take uniform measure on first N fields. Now we have a sequence of measures, so we can study them as $N \to \infty$.

For a sequence of measures, one can ask many questions, and there are several notions of convergence of measures. However, typically in this situation (countable things ordered with uniform measure at finite level), if the sequence converges, then it does so to the zero measure, which isn't super helpful... This is sometimes called *escape of mass*.[38]

Remark 4.1.8*.* By Fatou's lemma, can't "add mass" in limit. E.g. given a sequence of probability measures converging (in any sane sense) to μ, the total mass of μ will be at most 1. ∘

We'll have to deal with this escape of mass thing often.

Let $\mathcal{F}$ be a family of number fields. We'll order by discriminant for now. Let A be a finite abelian group. Can ask for the following limit (does it exist? If so, what's the value?)

$$\lim_{X\to\infty} \frac{\#\{K \in \mathcal{F} \mid \mathrm{Cl}_K \simeq A, |\mathrm{Disc}_K| \leq X\}}{\#\{K \in \mathcal{F} \mid |\mathrm{Disc}_K| \leq X\}},$$

i.e. "What proportion of class groups are isomorphic to A?" In general, even existence of such a limit is totally open.

Let's describe the above a little more measure-theoretically. Let μ_X be the uniform measure of fields K with $|\mathrm{Disc}_K| \leq X$. We took these μ_X and push them forward to measures on finite abelian groups using $K \to \mathrm{Cl}_K$.

Question 4.1.9. *When $\mathcal{F}$ is the set of imaginary quadratic fields, what happens with the above limit?*

[38] Have a sequence of probability measures which converges to the zero measure

Proof. The limit goes to 0. Eventually, there are no fields with a particular class group (i.e. since sizes go to infinity), and there are infinitely many such fields. ■

Question 4.1.10. *What about if we take $\mathcal{F}$ to be real quadratic fields?*

Answer (Audience)**.** Not sure, but there are known results about averages where you weight by the size of the regulartor. Maybe this is useful? ⋆

Response (Melanie)**.** In general, $|\mathrm{Cl}_K|\,\mathrm{Reg}_K$ is more accessible than $|\mathrm{Cl}_K|$ (e.g. see analytic class number formula). Some people might say that a lot of what we want to do is hard because we're trying to break the class group away from the regulator.

Answer (Audience)**.** From Cohen-Lenstra heuristics, I guess that this limit exists. However, this is different from the Cohen-Lenstra setup, so technically I am not sure. ⋆

Response (Melanie)**.** You are right that this exists. One thing we're doing here than Cohen and Lenstra didn't do is ask that the entire class group Cl_K be isomorphic to a particular group. They only asked about the odd part since we know something about the 2-torsion part (she said something like this).

Answer (Melanie)**.** There's a thing called genus theory, and it tells us, roughly, that

$$\mathrm{Cl}_K[2] = (\mathbb{Z}/2\mathbb{Z})^{\#\text{ramified primes, maybe minus 1}}.$$

This will tell us that the limit exists and is 0 in the real since the 2-torsion is getting too big. ⋆

To get nonzero answers, we ask more refined questions. For example, what is

$$\lim_{X\to\infty} \frac{\sum_{K\in\mathcal{F}} f(\mathrm{Cl}_K)}{\#\left\{K\in\mathcal{F} \mid |\mathrm{disc}_K| \le X\right\}} = \lim_{X\to\infty} \int_K f(\mathrm{Cl}_K)\mathrm{d}\mu_X = \lim_{X\to\infty} \mathbb{E}_{\mu_X}[f(\mathrm{Cl}_K)]$$

where, remember, μ_X denotes the uniform measure on fields in $\mathcal{F}$ "up to X" in our ordering (e.g. by Disc).

Before, we talking about $f = \mathbf{1}_A$, the indicator function of a particular group. This was not so good. Here are some better choices for f.

- $\mathbf{1}_{B^{\mathrm{odd}}\simeq A}(B)$, when is the odd-part of the class group isomorphic to A (fixes "genus theory issue"). We expect these averages to exist and be nonzero for any odd finite abelian group.
- $\mathbf{1}_{B/B[2]\simeq A}(B)$.
- $\mathbf{1}_{B[p^\infty]\simeq A}(B)$, when is the Sylow-$p$ subgroup isomorphic to A?
- $\mathbf{1}_{\mathrm{rank}_p B\simeq r}(B)$, when is the p-rank equal to r.
- $f(B) = \#\,\mathrm{Hom}(B, A)$ for some fixed A.
- $f(B) = \#\{\varphi : B \to A \mid \varphi \text{ surjective}\} = \#\,\mathrm{Sur}(B, A)$ with A fixed.

Remark 4.1.11. $\mathbb{E}[\#\,\mathrm{Sur}(B, A)]$ gives "moments of distribution", and play the role of $\mathbb{E}(X^k)$. Here A is fixed, so we will it the Ath moment of random B. ○

These are the kinds of questions of arithmetic statistics. Note that these only see phenomena that happen a positive percentage of the time, so e.g., they don't necessarily see if something happens infinitely often or not. However, it can be used to answer some "infinitely often" type questions. For example, in certain families of real quadratics, we expect a positive percent of them to have trivial class group; showing this would answer Gauss's question.

Question 4.1.12 (Audience)**.** *Is there a similar theory for global function fields?*

Answer. Yes, and we will talk about it at some point. Many analogous questions/results with some subtleties in setting up these analogies. If I understood Melanie correctly, we can say a little more in the function field case than in the global field case. $\star$

Question 4.1.13 (Audience)**.** *Do people consider families $\mathcal{F}$ not of fixed degree?*

Answer. Yes, but much less studied than those of fixed degree. Sometimes people ask interesting questions which can be related to statistics of families not of fixed degree, but we often don't even know what to conjecture in these cases. $\star$

Question 4.1.14 (Audience)**.** *Does every finite abelian group appear as the class group of some number field?*

Answer. I think this is open, but it will some times come up in this course. $\star$

Question 4.1.15 (Audience)**.** *Do we know the answer to the previous question is no if we just restrict to quadratic fields? That is, do we know of a group that does not appear as the class group of an imaginary quadratic?*

Answer. Not that I know of. We can predict that this is the case though (at least for imaginary quadratic fields). $\star$

Question 4.1.16 (Audience)**.** *Do we know of any class group which appears infinitely often for number fields?*

Answer. I don't think so. $\star$

Question 4.1.17 (Audience)**.** *Can we answer any of these questions for function fields?*

Answer. This a good question, but one I haven't thought about.

Melanie said more than this, but I was too busy listening to type. $\star$

4.2 Lecture 2 (9/9): Cohen and Lenstra's conjectures on Cl_K for K quadratic

Last time, we gave an overview of the kind of questions that we will be talking about. Today, let's focus on a specific conjecture. In particular, on Cohen-Lenstra for quadratic class fields.

Statement in imaginary quadratic case Let $\mathscr{I}_X := \{\text{iso classes of imag quad } K/\mathbb{Q} : |DiskK| \leq X\}$. Also, we'll let $\mathrm{Cl}_K^{\mathrm{odd}} := \mathrm{Cl}_K / \mathrm{Cl}_K[2^\infty]$ denote the **odd part** of the class group, the quotient by the 2-Sylow subgroup.

Conjecture 4.2.1 (**Cohen-Lenstra**, '84)**.** *For a "reasonable" function f,*

$$\lim_{X\to\infty}\frac{1}{|\mathscr{I}_X|}\sum_{K\in\mathscr{I}_X} f(\mathrm{Cl}_K^{\mathrm{odd}})=\lim_{Y\to\infty}\frac{\sum_{|G|\le Y}\frac{f(G)}{|\mathrm{Aut}\,G|}}{\sum_{|G|\le Y}\frac{1}{|\mathrm{Aut}\,G|}}$$

with sums over (iso classes of) odd, finite abelian groups.

"This didn't specify a precise definition for reasonable. This is a very smart thing to do when making a conjecture, because if you don't define all your terms, it can't be proven false." (paraphrase)

Remark 4.2.2. They thought at the time that every non-negative f would work, but we now think this is likely not the case. Last time, we gave examples of f's which should be reasonable. $\circ$

Example. Could take $f=\mathbf{1}_{\mathrm{cyclic}}$ or $f=\mathbf{1}_{\mathrm{square-freeorder}}$. This are believed to be reasonable. $\triangle$

Let's rewrite more probability theoretically. Let μ_X be the uniform measure on $\mathscr{I}_X$, and let ν_Y be the probability measure which is proportional to $\frac{1}{|\mathrm{Aut}\,G|}$ on $\{G\mid G\text{ odd fin ab },|G|\le Y\}$. Hence, the conjecture states that

$$\lim_{X\to\infty}\mathbb{E}_{\mu_x}(f(\mathrm{Cl}_K^{\mathrm{odd}}))=\lim_{Y\to\infty}\mathbb{E}_{\nu_Y}(f(G)).$$

Note that

$$\sum_{\substack{G\\ \text{odd, fin, ab group}}}\frac{1}{|\mathrm{Aut}\,G|}=\infty$$

e.g. because $|\mathrm{Aut}\,\mathbb{Z}/p\mathbb{Z}|=p-1$. Cohen-Lenstra had wanted to put a probability measure on all these groups, weighted by size of $\mathrm{Aut}\,G$, but they couldn't do that because of the above fact. This is similar to the issue we ran into last lecture. In both cases, what one does is consider finitary versions of the desired measure, and then takes limits.

4.2.1 Why the $1/\mathrm{Aut}\,G$ weighting?

Slogan. Objects appear with frequency proportional to $\frac{1}{\mathrm{Aut}\,G}$.

Example. Degree 3 (iso classes) of number fields. There are the cyclic fields which appear once in $\overline{\mathbb{Q}}$ ($\mathrm{Aut}=3$). There are the non-Galois ones which appear 3 times in $\overline{\mathbb{Q}}$ ($\mathrm{Aut}=1$). $\triangle$

Example. Suppose you wanted to make a group of order n. Do this by making an $n\times n$ grid (the multiplication table), fill it in uniformly randomly (with numbers 1 to n), and then ask, "does this give me a group?" The answer will be no most of the times, but sometimes it will be yes. Can ask, if we have a group G of order n, how many multiplication tables give a group isomorphic to G? Get a table for each ordering of the elements of G, so maybe answer is $n!$. This is not quite right because the table can already have some symmetries (i.e. the group can have some non-trivial automorphism). Applying these automorphisms does not change the table, so you really get $n!/|\mathrm{Aut}\,G|$.

Slightly more formally, there's an S_n-action on the multiplication tables by permuting the elements, and the stabilizer of a table is exactly the automorphism group. $\triangle$

More examples on homework.

This is a recurring phenomenon. When you pass from objects to iso classes, you often acquire $1/\mathrm{Aut}\,G$ factors.

Example (Audience)**.** See this type of phenomenon in the Siegel mass formula, in looking at random graphs, in counting points on varieties over finite fields, in looking at "stacky points" on moduli stacks, etc. △

Cohen and Lenstra's main motivation was that $\frac{1}{\mathrm{Aut}}$ was the most natural measure on odd, finite, abelian groups. The second piece of their philosophy was that $\mathrm{Cl}_K^{\mathrm{odd}}$ is so random/predictable that it should be distributed in the most natural way.

Remark 4.2.3. Secretly, there should be a $1/\mathrm{Aut}$ factor in the class group side of things too.

If you look at cubic fields, you want $\sum_{K \in blah} \frac{1}{\mathrm{Aut}\, K} f(\mathrm{Cl}_K)$. When ordering by discriminant, 100% of cubic fields are non-Galois ($\mathrm{Aut}\, K = 1$). Also, if K is Galois, then Cl_K is a finite $\mathbb{Z}[C_3]$-module, not just a finite abelian group so it kinda lives in a different world. We secretly shouldn't combine the Galois and non-Galois cases since one outputs abelian groups and one outputs $\mathbb{Z}[C_3]$-modules.

In the quadratic case, Cl_K is a $\mathbb{Z}[C_2]$-module. The number of $\mathbb{Z}[C_2]$-automorphisms can differ from the number of $\mathbb{Z}$-automorphisms. Note that if $K/\mathbb{Q}$ is quadratic, then an ideal multiplied by its conjugate is principal (e.g. $\mathfrak{p}\overline{\mathfrak{p}} = (p)$), so $C_2 = \mathrm{Gal}(K/\mathbb{Q})$ acts on Cl_K by multiplication by -1. Observe that a $\mathbb{Z}[C_2]$-module where action is always multiplication by -1 is the same thing as a $\mathbb{Z}$-module (same data, equiv of cats, however you wanna think about it). So we won't really need to take care of the $\mathbb{Z}[C_2]$-structure in the quadratic case. ○

Remark 4.2.4 (Why the odd part?)*.* We talked about this a bit last time. From genus theory, we know that $\mathrm{Cl}_K[2] \cong (\mathbb{Z}/2\mathbb{Z})^{\#\{p \mid \mathrm{Disc}\, K\}}$, so the 2-part is not so random/unpredictable. ○

4.2.2 Additional motivation for the conjecture

Other parts of C-L's motivation are empirical data (possible to efficiently compute class groups of quadratic fields, so many examples were available), and that the result was already a theorem for $f(A) = \#\,\mathrm{Sur}(A, \mathbb{Z}/3\mathbb{Z}) = |A[3]| - 1$ due to Davenport-Heilbronn. They found that the class group average is 1. Cohen and Lenstra developed machinery for computing RHS of their conjecture, and in particular showed that this case agrees with what they expect.

These days there are even more reasons to believe these conjectures.

Case of functions of Sylow-p subgrouops Considering just Sylow p-subgroups, the RHS of CL conjecture simplifies since

$$\sum_{G \text{ fin ab } p\text{-groups}} \frac{1}{|\mathrm{Aut}\, G|} < \infty.$$

Since this converges, you get an actual probability measure on the set of finite, abelian p-groups where $\nu(A) = c/|\mathrm{Aut}\, A|$. This means that if $f(A)$ depends only on $A[p^\infty]$, then RHS of the conjecture becomes $\mathbb{E}_\nu(f)$ with no tricky limiting business.

Friedman and Washington made a computation. For $M \in M_{n\times n}(\mathbb{Z}_p)$ a random p-adic matrix (using additive haar measure), its cokernel $\mathrm{coker}\, M = \mathbb{Z}_p^n / M(\mathbb{Z}_p^n)$ is a finite abelian group. They showed that

$$\lim_{n\to\infty} \Pr\left(\mathrm{coker}\, M \simeq A\right) = \nu(A) = \frac{c}{|\mathrm{Aut}\, A|}.$$

(Should think of this as happening integrally. We're doing it p-adically for technical reasons, e.g. access to haar measure and an actual measure ν). This gives more reason to believe this $1/\operatorname{Aut}$ measure ν is natural.

Observe that if S is a "large" set of primes of S, then $\mathrm{Cl}_K = I^S/\mathscr{O}_S^\times$ where I^S is the ideals with valuation 0 outside S, and similarly for $\mathscr{O}_S^\times$. This says $\mathrm{Cl}_K = \operatorname{coker}\left(\mathscr{O}_S^\times/\mu(\mathscr{O}_K) \to I^S\right)$ (where $\mu(\mathscr{O}_K) =$ roots of unity), so large enough means I^S generates class group. Think about this, not for a single S, but for many large S. Note that $I \simeq \mathbb{Z}^{|S|}$ and also (by Dirichlet unit), $\mathscr{O}_S^\times/\mu(\mathscr{O}_K) = \mathbb{Z}^{|S|}$. Hence, we see

$$\mathrm{Cl} \otimes \mathbb{Z}_p = \mathrm{Cl}_K[p^\infty] = \operatorname{coker}(\mathbb{Z}_p^{|S|} \to \mathbb{Z}_p^{|S|}).$$

This says that the (Sylow-p subgroup of the) class group arises, in a natural way as the cokernel of a map between free $\mathbb{Z}_p$-modules of the same rank. This motivates the Friedman-Washington model for predicting statistics of the class group, and that model agrees with what Cohen-Lenstra predicts.

4.3 Lecture 3 (9/11)

Homework up on website. Office hours Monday and Thursday.

Last time we were talking about the Freedman-Washington calculation of cokernels of random matrices, and were thinking about how this relates to class groups. We had a map $\mathscr{O}_S^\times/\mu_K \to I^S$. Since these are free abelian, this corresponds to a map $\mathbb{Z}^n \to \mathbb{Z}^n$. Focusing on the Sylow-$p$ subgroup, we can tensor with $\mathbb{Z}_p$ to get

$$\mathscr{O}_S^\times/\mu_k \otimes \mathbb{Z}_p \to I^S \otimes \mathbb{Z}_p \rightsquigarrow \mathbb{Z}_p^n \to \mathbb{Z}_p^n.$$

Starting with the Haar measure on elements of $M_{n\times n}(\mathbb{Z}_p)$ and taking cokernels gives the $\frac{1}{\operatorname{Aut}}$ measure.

One may worry that this does not answer "Why should class group be $1/\operatorname{Aut}$?" but just pushes it to "Why should these matrices be equidistributed over the Haar measure?".

4.3.1 Universality

Let $X \in N(0,1)$ be a random real number normally distributed with mean 0 and variance 1. If X_i are independent copies of X, one can compute that

$$\frac{X_1 + X_2 + \cdots + X_n}{\sqrt{n}} = N(0,1),$$

i.e. this scaled sum is distributed as a mean 0 variance 1 normal variable.

Now imagine that Y is a mystery random variable, and we want to understand its distribution. Let Y_i be independent copies of Y. Suppose we observe that

$$\frac{Y_1 + Y_2 + \cdots + Y_n}{\sqrt{n}} \approx N(0,1)$$

when n is very large.

Question 4.3.1. *Should we conjecture that $Y \approx N(0,1)$?*

Answer. No. The **Central Limit Theorem** says that if Y has mean 0 and variance 1, then we have "weak convergence in distribution" of

$$\frac{Y_1 + Y_2 + \cdots + Y_n}{\sqrt{n}} \to N(0,1).$$

Can think of this as saying that this weighted averaging process is a way of taking (nearly) any starting distribution and outputs a normal distribution. ⋆

Remark 4.3.2. The **Law of large numbers** says that

$$\frac{Y_1 + Y_2 + \cdots + Y_n}{n} \to 0.$$

when Y has mean 0. ○

The theme is that we have some process which takes in many random inputs, but then outputs something universal, independent of the inputs.

What does this have to do with anything? We want to think about universality for, say, random integral matrices.

Theorem 4.3.3 (Wood)**.** *Let $B^{(n)} \in M_{n\times n}(\mathbb{Z}_p)$ be random with independent entries. Assume that there exists an $\varepsilon > 0$ such that for all a, n, i, j,*

Can let ε depend on n (with some conditions) and still get the same conclusion.

$$\Pr\left(B_{ij}^{(n)} \equiv a \pmod{p}\right) \le 1 - \varepsilon.$$

Then, for any finite abelian p-group A,

$$\lim_{n\to\infty} \Pr\left(\operatorname{coker} B^{(n)} \simeq A\right) = \frac{\prod_{i\ge 1}(1-p^{-i})}{|\operatorname{Aut} A|}.$$

Freedman-Washington had look at Haar-random matrices. In the above theorem, we only require that the elements are independent. We are much more lenient about the individual distributions.

Slogan. As long as there is no conspiracy against you, your random $n \times n$ matrix (as $n \to \infty$) has $c/\,|\operatorname{Aut} A|$ cokernels.

There are two types of conspiracies. One is having something like that all 0 matrix (point distribution); the other is inter-dependent entries.

Remark 4.3.4. A symmetric matrix with otherwise independent entries (other than the top left being the bottom right) has a different cokernel distribution. The cokernel of a symmetric matrix has a symmetric pairing, so you end up with a formula involving Aut of groups of symmetric pairings. ○

Melanie does not think that the matrices arising from class group computations are Haar-random, but that is OK. The above result says they do not need to be for their cokernels to have this $1/\operatorname{Aut}$ distribution. We just need to believe that there is no vast conspiracy in them.

Remark 4.3.5. If you are interested in this random matrix aspect and are looking for a project/paper for this class, there are potential ideas here. Talk to Melanie in office hours. ○

4.3.2 Analytic/measure-theoretic issues

Recall 4.3.6.

$$\sum_{G \text{ fin ab}} \frac{1}{|\operatorname{Aut} G|} = \infty$$

Cohen-Lenstra fixed this via limits of finite distributions. ⊙

We want to talk about another way to fix this issue.

In some sense, the "class group of an imaginary quadratic field" under the distribution given by letting the discriminant go to ∞ is an infinite group (since class group sizes of imaginary quadratics grow with discriminants).

Notation 4.3.7. Let $\mathcal{A}$ be the set of isomorphism classes of profinite abelian groups G with Sylow-p subgroup all finite (when $p \geq 2$). Think of the Sylow-p subgroup as the inverse limit of p-group quotients.

Remark 4.3.8. This set $\mathcal{A}$ is isomorphic to $\prod_{p\geq 2}\{\text{finite ab } p\text{-groups}\}$ via the map $G \mapsto (G_p)_p$ (with inverse $(G_p)_p \mapsto \prod_p G_p$). So we're really just looking at collections of p-groups. ○

Recall 4.3.9. The set {finite ab p-groups} does have a natural $1/\operatorname{Aut}$ measure, for fixed p. ⊙

Let ν_P be the $1/\operatorname{Aut}$ (really, c/Aut) measure on {finite ab p-groups}, and let ν be the corresponding product measure on $\mathcal{A}$.

Conjecture 4.3.10 (**Cohen-Lenstra**, Take II)**.** *For "reasonable" f*

$$\lim_{X\to\infty} \mathbb{E}_{\mu_X}\left(f(\mathrm{Cl}_K^{\mathrm{odd}})\right) = \mathbb{E}_\nu(f(G)).$$

Remark 4.3.11. For all f we have discussed, the RHS of the above is the same as the RHS of original Cohen-Lenstra. However, they disagree for some "unreasonable" f. Consider $f = \mathbf{1}_{finite}$. Then,

$$\lim_{X\to\infty} \mathbb{P}_{\mu_x}(|\mathrm{Cl}_K| < \infty) = 1 \text{ but } \mathbb{P}_\nu(G \text{ finite}) = 0.$$

For some fixed (finite) A, $\mathbb{P}_\nu(G \simeq A) = q_2q_3q_5q_7\dots$. However, there's some p_0 such that A has trivial Sylow p-subgroup for $p \geq p_0$, so

$$q_p = \frac{\prod_{i\geq 1}(1-p^{-i})}{\#\operatorname{Aut}(1)} = \prod_{i\geq 1}(1-p^{-i}) \leq (1-p^{-1})$$

for all $p \geq p_0$. The product $(1-p^{-1})$ as p ranges over all (but finitely many) primes is 0, so we see $\mathbb{P}_\nu(G \simeq A) = 0$ (this is what we expect on LHS for fixed A). As ν is a measure (and countably many finite abelian groups), we then get $\mathbb{P}_\nu(G \text{ finite}) = 0$. ○

Above kinda makes rigorous earlier observation that "class group of a random quadratic imaginary is infinite."

Test functions There are lots of notions for convergence of measures. Many of them involve test functions, like the f is Cohen-Lenstra. Different notions may allow different f's. One may want to be able to have all test functions, but this is an unreasonable ask.

Here's a cute result

Theorem 4.3.12 (Poonen, in Bartel-Lenstra)**.** *If π is a (discrete) probability measure on $\{$finite odd abelian groups$\}$ (i.e. countable set), and $Y_1, Y_2, \dots$ are independent random finite abelian groups drawn from π, then*

$$\mathbb{P}\left(\exists f : E_\pi(f(A)) < \infty \text{ but } \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} f(Y_i) \text{ does not exist}\right) = 1.$$

where A drawn from π.

Above, the probability/randomness is coming from the choice of Y_i's. The law of large numbers tells us that for every test function f,

$$E_\pi(f(A)) = \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} f(Y_i)$$

with probability 1. Hence, any individual test function is fine with probability 1, but Poonen is telling us that there are too many test functions to ask for them all to work.

The moral is that you should not expect to use all test functions f, so which ones should we use? Well, we still don't know exactly. One popular choice is "weak-(*)" convergence: allow f bounded, continuous, i.e. **weak-* convergence** is when

$$\lim_{X\to\infty} \mathbb{E}_{\mu_X}(f(Y)) = \mathbb{E}_\mu(f(Y))$$

for all f bounded, continuous.

Note that $\mathbf{1}_{finite}$ is not continuous (we were secretly using a product topology, so questions of continuity make sense).

Next time we'll talk about genus theory in more detail, and what it tells us about 2-torsion. After that, we'll get to real quadratic fields.

Question 4.3.13 (Audience)**.** *What about $\mathbf{1}_{cyclic}$?*

Answer. $\mathbf{1}_{cyclic}$ and $\mathbf{1}_{\text{sq-free order}}$ are not continuous (wrt the product topology). Melanie recommends taking a finer topology where these are continuous. $\star$

Question 4.3.14 (Audience)**.** *In Bjorn's result, what is the π in our setting?*

Answer. There isn't one. It might help to look at the Cramer model.

This is an old way of modelling the primes. Consider a random variable

$$P_n = \begin{cases} 1 & \text{with prob } 1/\log n \\ 0 & \text{with prob } 1 - 1/\log n \end{cases}$$

One can look at the statistical behavior of P_n's, and maybe suspect that things which are true with probability 1 for P_n should be true for the primes. The moral idea is that our universe is drawn from the P_n's, so things true for 100% of universes are probably true for ours as well. It's more philosophical than mathematically rigorous.

The situation here is the same. Bjorn's result gives us intuition/predictions. Like, even in a nice, imagined setting where we have a literal measure, we don't get all test functions, so we don't expect to get them all in our world either. $\star$

4.4 Lecture 4 (9/16): Genus theory

Recall 4.4.1. Office hours Monday and Thursday 10 – 11am ⊙

Let's explore in more detail why Cohen and Lenstra took $\mathrm{Cl}^{\mathrm{odd}}$. In what sense, is the even part of Cl_K not random?

Recall 4.4.2. There's a thing called genus theory, and it tells us, roughly, that

$$\mathrm{Cl}_K[2] = (\mathbb{Z}/2\mathbb{Z})^{\#\text{ramified primes, maybe minus 1}}.$$

⊙

We'll talk about genus theory from a class field theory perspective. Start with a prime $p \equiv 1 \pmod 4$, and consider the imaginary quadratic $K = \mathbb{Q}(\sqrt{-4p})$ (put $-4p$ since this is the discriminant). Since there are two primes $2, p$ dividing the discriminant of K, its class group should have 2-rank 1, so there should be some unramified quadratic extension of K.

$$\begin{tikzcd}[arrows=dash]
 & K(\sqrt{p}) \arrow[dl] \arrow[dr] & \\
K = \mathbb{Q}(\sqrt{-4p}) \arrow[d] & & \mathbb{Q}(\sqrt{p}) \arrow[dll] \\
\mathbb{Q} & &
\end{tikzcd}$$

$\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is only ramified at p, so $K(\sqrt{p})/K$ is unramified outside $\{p\}$. To see if it is ramified by p, look at Galois diagram (The one's in the diagram are the trivial group. These are different from $1 \in \mathbb{Z}/2\mathbb{Z}$)

$$\begin{tikzcd}[arrows=dash]
 & 1 \arrow[dl] \arrow[dr] & \\
\mathbb{Z}/2\mathbb{Z} \times 1 \arrow[dr] & & 1 \times \mathbb{Z}/2\mathbb{Z} \arrow[dl] \\
 & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

Look at inertia groups in this diagram. Note that since p is odd, all ramification here is tame (so in particular, ramification groups are cyclic). One can stare at things and see that inertia at p in the bottom group, $\mathrm{Gal}(K(\sqrt{p})/\mathbb{Q})$, is $\langle(1,1)\rangle$.[39] Since the intersection of this with $(\mathbb{Z}/2\mathbb{Z} \times 1)$ is trivial, this means that $K(\sqrt{p})/K$ is unramified at p.[40]

[39] Use that p is ramified in both bottom extensions and that inertia cyclic. Also, that in a tower $F''/F'/F$, one has $I(F''/F, p) \twoheadrightarrow I(F'/F, p)$

[40] Let $L = \mathbb{Q}(\sqrt{p})$. We have $\mathrm{Gal}(KL/K) \hookrightarrow \mathrm{Gal}(KL/\mathbb{Q})$ sending $I(KL/K, p) \hookrightarrow I(KL/\mathbb{Q}, p)$. This realizes $I(KL/K, p) = \mathrm{Gal}(KL/K) \cap I(KL/\mathbb{Q}, p)$.

Can we do this trick more generally?

$$\begin{tikzcd}[column sep=small]
 & KL = L(\sqrt{-4p}) \arrow[dl, dash] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{-4p}) \arrow[d, dash] & & L \arrow[dll, dash] \\
\mathbb{Q} & &
\end{tikzcd}$$

Say $L/\mathbb{Q}$ now cyclic cubic with ramification only at p. Galois diagram now looks like

$$\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}/2\mathbb{Z} \times 1 \arrow[dr, dash] & & 1 \times \mathbb{Z}/3\mathbb{Z} \arrow[dl, dash] \\
 & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &
\end{tikzcd}$$

inertia is a cyclic subgroup with non-trivial projections in both coordinates as before, so inertia is $\langle(1,1)\rangle$, but $\langle(1,1)\rangle \cap (1 \times \mathbb{Z}/3\mathbb{Z}) \neq 1$ (it contains $(0,2)$).

Remark 4.4.3. When we talking about inertia at p, we really mean a conjugacy class of subgroups. These groups, in even non-abelian extensions, are cyclic when tame. i.e. the inertia groups in $\mathrm{Gal}(K^{\text{tame at } p}/K)$ is (pro-)cyclic. $\circ$

Fact. For a local field K, we know the structure of $\mathrm{Gal}(K^{\text{tame}}/K)$.

Question 4.4.4. *How far can we take this trick?*

Proposition 4.4.5. *Let $K/\mathbb{Q}$ be a degree 2 extension, and $L/\mathbb{Q}$ abelian (with $K \not\subset L$). If LK/K is unramified, then $\mathrm{Gal}(L/\mathbb{Q})$ is 2-torsion and*

$$\{\textit{places ramified in } L/\mathbb{Q}\} \subset \{\textit{places ramified in } K/\mathbb{Q}\}\,.$$

This trick only works to help build the 2-part of your class group.

Cl_K is the Galois group of the maximal unramified (abelian) extension H/K

Proof. Have diagrams

$$\begin{tikzcd}[column sep=small]
 & KL \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash, "A"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}/2\mathbb{Z} \times 1 \arrow[dr, dash] & & 1 \times A \arrow[dl, dash] \\
 & \mathbb{Z}/2\mathbb{Z} \times A &
\end{tikzcd}$$

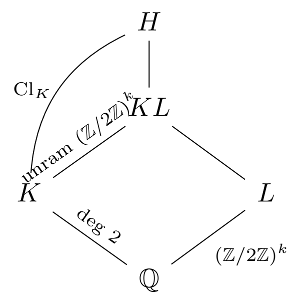
Let $A = \mathrm{Gal}(L/\mathbb{Q})$. What can element in inertia groups of $KL/\mathbb{Q}$ look like? Can't have elements $(0,a)$ with $a \neq 0$ since LK/K unramified. So all inertia elements are $(0,0)$ or $(1,a)$. If $(1,a)$ is in inertia, then so is $(0,2a)$, so $2a = 0$ by previous remark. Thus, the inertial of $KL/\mathbb{Q}$ is contained in $\mathbb{Z}/2\mathbb{Z} \times A[2]$.

We know that the Galois group is generated by inertia (otherwise, quotient would be Galois group of a nontrivial unramified extension of $\mathbb{Q}$), so $A = A[2]$. This gives first part of the claim.

For second part, choose a place v ramified in $L/\mathbb{Q}$. Starting at diagram, this implies that inertia has non-zero A coordinate. Above implies that it has a non-zero $\mathbb{Z}/2\mathbb{Z}$ coordinate, so it is ramified in $K/\mathbb{Q}$ as well. ■

This is almost an iff, except at 2. If nothing was ramified at 2, this argument could run backwards, but wild ramification or something gets in the way. Figuring out the condition you need at 2 is one of the homework problems.

The above proposition should already give the upper bound on genus theory that we have mentioned before. Consider a diagram



This gives $\mathrm{Cl} \to (\mathbb{Z}/2\mathbb{Z})^k$, so it tells us about $\mathrm{Cl}/2\,\mathrm{Cl}$ (which happens to have same rank as $\mathrm{Cl}[2]$).

Remark 4.4.6. Technically, we are only talking about the Galois coinvariants of the class group. However, we said before that $\mathrm{Gal}(K/\mathbb{Q})$ acts by -1 on the class group. Since $\mathrm{Cl}/2\,\mathrm{Cl}$ is 2-torsion, $\mathrm{Gal}(K/\mathbb{Q})$ acts on it by identity, so everything in there is invariant. ○

I think the point is that $\mathrm{Gal}(K/\mathbb{Q})$ acts trivially on $\mathrm{Gal}(KL/K)$ since it comes from $\mathrm{Gal}(L/\mathbb{Q})$ and $K \cap L = \mathbb{Q}$

If we want all of $\mathrm{Cl}/2\,\mathrm{Cl}$, since it is Galois invariant, it will come from an abelian extension of $\mathbb{Q}$. Thus, if we find all abelian extensions of $\mathbb{Q}$ giving unramified extensions of K, we will find everything.

Let's do the trick now.

Proposition 4.4.7. *Let K be imaginary quadratic. Then,*

$$\left|\frac{\mathrm{Cl}_K}{2\,\mathrm{Cl}_K}\right| = 2^{\omega(\operatorname{disc} K)-1}$$

where $\omega(\operatorname{disc} K) = \#$ of distinct prime divisors of $\operatorname{disc} K$.

Note that since K is imaginary quadratic any extension of it will be unramified at its infinite place, so only need to worry about finite ramification

Proof. It remains, from what was done above, to find the largest $(\mathbb{Z}/2\mathbb{Z})^k$ extension $L/\mathbb{Q}$ such that KL/K is unramified. How do we find abelian extensions of $\mathbb{Q}$ (or of any number field)? Use class field theory.

Recall, for a number field K (this will be $\mathbb{Q}$ later) with **idèle class group**

$$C_K = \prod_v{}' K_v^\times / K^\times,$$

the Artin map gives an isomorphism $\widehat{C}_K \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$ where $\widehat{C}_K$ is the profinite completion, which turns out to be

$$\widehat{C}_K = C_K/C_K^\circ \text{ where } C_K^\circ = \text{connected component of identity}.$$

We have an exact sequence (below,[41] $\mathscr{O}_v^\times := \{\pm 1\}$ if $v \mid \infty$)

$$1 \longrightarrow \mathscr{O}_K^\times \longrightarrow \prod_v \mathscr{O}_v^\times \longrightarrow \widehat{C}_K \longrightarrow \mathrm{Cl}_K \longrightarrow 0$$

with the right map being $(\alpha_v) \mapsto \prod_{v\nmid\infty} v^{\mathrm{ord}_v(\alpha_v)}$ with product taken as ideals.

The point of above is that the class group is finite, and units are finitely generated, so there's only a "finite obstruction" middle map being an isomorphism. In particular,

$$\prod_p \mathbb{Z}_p^\times \xrightarrow{\sim} \widehat{C}_{\mathbb{Q}}$$

with $\mathbb{Z}_p^\times$ being the inertia group at p.

Example. Melanie earlier said there was a cyclic degree 3 extension of $\mathbb{Q}$ ramified only at p. Let's see why. Note that any map

$$\prod_p \mathbb{Z}_p^\times \to \mathbb{Z}/3\mathbb{Z}$$

is trivial on $\mathbb{Z}_p^\times$ for any $p \equiv 2 \pmod 3$. However, you can make it trivial or not on $\mathbb{Z}_p^\times$ when $p \equiv 1 \pmod 3$. This product structure let's you make choices independently at primes, so (if $p \equiv 1 \pmod 3$) you can find a cyclic cubic ramified only at p. △

Back to the proof, the quadratic extension $K/\mathbb{Q}$ corresponds to a surjection $\widehat{C}_{\mathbb{Q}} = \prod_p \mathbb{Z}_p^\times \xrightarrow{\varphi_K} \mathbb{Z}/2\mathbb{Z}$. This factors as (the second map is sum of coordinates)[42]

$$\prod_p \mathbb{Z}_p^\times \to \prod_{p \text{ ram in } K} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}.$$

Let k be the number of such p. Then, there is a map

$$\prod_{p \text{ ram in } K} \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^{k-1}$$

given by projection onto first $k-1$ coordinates. The composition

$$\varphi_L : \prod_p \mathbb{Z}_p^\times \to \prod_{p \text{ ram in } K} \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^{k-1}$$

is that map that will give us L. We did not take all the coordinates so that φ_K does not factor through φ_L (i.e. so $K \not\subset L$).

We now claim that KL/K is unramified. Stare at the diagram

TODO: Make the ending of this proof better

[41] Local inertia at ∞ or something. What you get after looking connected component of identity

[42] This is just because $\mathbb{Z}_p^\times$ is the inertia at p, so map only nontrivial on factors where p ramifies

$$\begin{tikzcd}
& \widehat{C}_{\mathbb{Q}} \arrow[dl, "\varphi_L"'] \arrow[d, "\varphi_{KL}"] \arrow[dr, "\varphi_K"] & \\
(\mathbb{Z}/2\mathbb{Z})^{k-1} & \displaystyle\prod_{p \text{ ram in } K} \mathbb{Z}/2\mathbb{Z} \arrow[l] \arrow[r] & \mathbb{Z}/2\mathbb{Z}
\end{tikzcd}$$

By construction, φ_K and φ_L both factor through the product in the bottom middle above, so $K/\mathbb{Q}$ is ramified at every prime that $L/\mathbb{Q}$ is (Furthermore, still by construction, for any prime p ramified in L, the ramification degrees $e(L/\mathbb{Q}, p = e(K/\mathbb{Q}, p)$ are both equal to 2). Since KL/K is unramified at any prime in which $L/\mathbb{Q}$ is unramified, this let's us conclude that KL/K is unramified. In more detail, staring at the diagram

$$\begin{tikzcd}[column sep=small]
& 1 \arrow[dl, dash] \arrow[dr, dash] & \\
\mathrm{Gal}(KL/K) = (\mathbb{Z}/2\mathbb{Z})^{k-1} \times 1 \arrow[dr, dash] & & 1^{k-1} \times \mathbb{Z}/2\mathbb{Z} = \mathrm{Gal}(KL/L) \arrow[dl, dash] \\
& (\mathbb{Z}/2\mathbb{Z})^{k-1} \times \mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

of Galois groups, we see that any element of $I(KL/\mathbb{Q}, p) \subset \mathrm{Gal}(KL/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{k-1} \times \mathbb{Z}/2\mathbb{Z}$ (where p a prime ramified in L) must be nontrivial in the last factor since p is ramified in K as well as in L, so

$$I(KL/K, p) = \mathrm{Gal}(KL/K) \cap I(KL/\mathbb{Q}, p) = \big((\mathbb{Z}/2\mathbb{Z})^{k-1} \times 1\big) \cap I(KL/\mathbb{Q}, p) = 1^k \simeq 1$$

is trivial. ■

Remark 4.4.8. Genus theory telling us that $\mathrm{Cl}/2\,\mathrm{Cl}$ is not random. We have an exact sequence

$$1 \to 2\,\mathrm{Cl} \to \mathrm{Cl} \to \mathrm{Cl}/2\,\mathrm{Cl} \to 1$$

so can ask if other part $2\,\mathrm{Cl}$ is random? Gerth generalized C-L to remove "odd" to give predictions for $2\,\mathrm{Cl}$. ○

Next time we'll talk about real quadratic fields. We saw earlier, when looking at LMFDB, that real quadratic fields behave differently than imaginary quadratics, so we'll see what Cohen-Lenstra predict in this case. There will be 3 descriptions.

(1) Take $c/\operatorname{Aut} G$ group and take quotient by a (uniform/Haar) random element.

(2) Take G with prob $\sim \frac{c}{\#\operatorname{Aut} G \# G}$.

(3) Take $\operatorname{coker}(\widehat{\mathbb{Z}}^{n+1} \to \widehat{\mathbb{Z}}^n)$ for Haar random matrix as $n \to \infty$.

Question 4.4.9 (Audience)**.** *Is there an analogue of genus theory if you take degree n extensions and look at n-torsion in the class group?*

Answer. Yes. Everything we did was very generalizable. This setup can generally allow one to sometimes product unramified abelian extensions by pushing up the maximal abelian extension. For general $K/\mathbb{Q}$, we call L the **genus field** if it is the maximal abelian extension of $\mathbb{Q}$ such that KL/K is unramified. This always exists, but what you expect it to look like depends a lot on K. The extent to which you can understand L depends on $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ (Galois closure), the ramified primes, and the residues of the ramified primes mod N for some N depending on $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. ⋆

Question 4.4.10 (Audience)**.** *Why is this called "genus theory"?*

Answer. Gauss used things called "genera" to understand binary quadratic forms. This is ultimately the root. He used them to be able to understand 2-torsion of classes of binary quadratic forms under his composition law for them. ⋆

4.5 Lecture 5 (9/18): Real Quadratic Fields

Today we talk about real quadratic fields and how they are different and whatnot.

We've spent so much time talking about imaginary quadratic fields. What about the real ones? Cohen and Lenstra made different predictions about their distributions. Even going back to Gauss, it's been known/believed that their class fields should behave differently.

Here are some motivations.

- C-L said that Gross had observed that: taking a fixed prime $p \in \mathbb{Q}$ and imaginary quadratic fields K where p splits, then tables of $\mathrm{Cl}_K/[\mathfrak{p}]$, where $p = \mathfrak{p}\overline{\mathfrak{p}}$, empirically look like tables of real quadratic class groups.

  If you think $[\mathfrak{p}]$ looks like a random element of Cl_K, then maybe real quadratic class groups look like imaginary quadratic class groups quotiented out by a uniformly random element. This leads to the idea that you should take the $c/\#\mathrm{Aut}$ distribution, and then quotient out by a uniformly random element.

- Davenport-Heilbronn had shown

  $$\lim_{X\to\infty} \mathbb{E}_{\mu(X)}(\#\mathrm{Sur}(\mathrm{Cl}_K, \mathbb{Z}/3\mathbb{Z})) = \frac{1}{3}$$

  when μ_X uniform distribution on real quadratics with discriminants in $[-X, X]$. Cohen-Lenstra showed that this is what is predicted by the $c/\#\mathrm{Aut}$ quotiented by a uniformly random element distribution.

- Note that $h = hR/R$ where h = class number and R = regulator. You can Wave Your Hands A Lot™, and then imagine that hR is like a c/Aut random group and R is (the size of) a subgroup generated by a random element. This doesn't formally make sense, e.g. there's no finite abelian group of order hR since R is usually irrational.[43]

In imaginary quadratic case, the regulator is $R = 1$

Remark 4.5.1. In the first motivation, can ask whether it's right to mod out by a uniformly random *element* or by a uniformly random *cyclic subgroup*. These are different (bigger subgroups picked more often in the first case). It turns out that element is the right choice. ○

[43]Melanie didn't want to say too much about this because it's so non-precise, but she did have a quick, throw-away comment about connecting this idea to Arakelov class groups

Remark 4.5.2. Can ask, for imaginary quadratic K split at p, how is the pair $(\mathrm{Cl}_K, [\mathfrak{p}])$ distributed. You them expect it to be proportional to $1/\operatorname{Aut}_{\mathrm{Ab}_*}$ where you're taken Aut as a pointed abelian group. One can show[44] that this gives the same distribution as taking a $1/\operatorname{Aut}$ groups and then quotienting by a uniformly random element. ○

Recall that we earlier showed

$$\mathrm{Cl}_K[p^\infty] \xrightarrow{\sim} \operatorname{coker}\left(\mathscr{O}_S^\times \otimes \mathbb{Z}_p \longrightarrow I^S \otimes \mathbb{Z}_p\right)$$

where S is a large enough set of primes of K. In the real quadratic case, this looks like a map

$$\mathbb{Z}_p^{n+1} \longrightarrow \mathbb{Z}_p^n.$$

Maybe this motivates that $\mathrm{Cl}_K[p^\infty]$ is like cokernel of a Haar random matrix in $M_{n\times(n+1)}(\mathbb{Z}_p)$. Can ask why it should be a Haar random matrix instead of some other matrix distribution. Just as before, Melanie's universality result (Theorem 4.3.3) on p-adic cokernels (or, really, an analogue of it for non-square matrices) applies to say that the limiting distribution should look like $1/\operatorname{Aut}$ unless there's a conspiracy against you.

4.5.1 Analyzing cokernel of a Haar-random matrix

Melanie claims this is not too hard to do. There are several common steps. We want to figure out

$$\mathbb{P}(\operatorname{coker}(\mathbb{Z}_p^{n+1} \xrightarrow{M} \mathbb{Z}_p^n) \simeq A)$$

with M Haar random.

Remark 4.5.3. You get a finite abelian group with probability 1. Basically, even for one minor to vanish is some polynomial condition and so has measure 0 in the p-adic Haar measure ○

Note that[45]

$$\mathbb{P}(\operatorname{coker}(\mathbb{Z}_p^{n+1} \xrightarrow{M} \mathbb{Z}_p^n) \simeq A) = \mathbb{E}\left(\#\operatorname{Isom}(\operatorname{coker} M, A)\right) \cdot \frac{1}{\#\operatorname{Aut} A}$$

Such an isomorphism is a map $\mathbb{Z}_p^n/M\mathbb{Z}_p^{n+1} \to A$, so it comes from a map

$$\mathbb{Z}_p^n \to A$$

which we then ask if it factors through the above quotient and if it is surjective. This gives

$$\mathbb{E}\left(\#\operatorname{Isom}(\operatorname{coker} M, A)\right) = \sum_{f\in\operatorname{Sur}(\mathbb{Z}_p^n, A)} \mathbb{P}(\ker f = M\mathbb{Z}_p^{n+1}).$$

Fix a particular f, and pick a basis $e_1, \dots, e_n$ of $\mathbb{Z}_p^n$ such that $A = \mathbb{Z}/p^{\lambda_1} \times \mathbb{Z}/p^{\lambda_2} \times \dots$

$$A = \left\langle f(e_1), \dots, f(e_n) \mid p^{\lambda_1} f(e_1) = \cdots = p^{\lambda_n} f(e_n) = 0 \right\rangle.$$

[44] "orbit-stabilizer thing"

[45] This gives another perspective on $1/\operatorname{Aut}$ distributions. It's like asking for distributions where the average number of isomorphisms to a fixed object does not depend on the object, or something like this

As $n \to \infty$, since A fixed, eventually $\lambda_i = 0$. One we have this nice basis,

$$\ker f = \left\{ \begin{pmatrix} p^{\lambda_1}\mathbb{Z}_p \\ \vdots \\ p^{\lambda_n}\mathbb{Z}_p \end{pmatrix} \right\} \subset \mathbb{Z}_p^n.$$

This makes it easy to check if you are in $\ker f$. For $M \in M_{n\times(n+1)}(\mathbb{Z}_p)$ coming from a Haar measure, the probability that the top row is divisible by p^{λ_1} is $p^{-\lambda_1(n+1)}$. Thus,

$$\mathbb{P}(M\mathbb{Z}_p^{n+1} \subset \ker f) = p^{-\lambda_1(n+1)-\lambda_2(n+1)-\cdots} = |A|^{-(n+1)}.$$

Given that $M\mathbb{Z}_p^{n+1} \subset \ker f$ (so i row all divisble by p^{λ_i}), we have $M\mathbb{Z}_p^{n+1} = \ker f \iff$ when you divide each row i by p^{λ_i}, you get a matrix that has rank n mod p. This is with probability[46]

$$(1-p^{-n-1})(1-p^{-n})\cdots(1-p^{-2}).$$

Let's put this all together now.

$$\mathbb{P}(\operatorname{coker} M \simeq A) = \frac{\#\operatorname{Sur}(\mathbb{Z}_p^n, A)}{\#\operatorname{Aut} A(\#A)^{n+1}} \prod_{i=2}^{n+1}(1-p^{-i})$$

What happens as $n \to \infty$? More and more maps $\mathbb{Z}_p^n \to A$ become surjections. There are basically $|A|^n$ maps $\mathbb{Z}_p^n \to A$ so we get some cancellation, and end up with

$$\frac{1}{\#\operatorname{Aut} A}\frac{1}{\#A}\prod_{i\geq 2}(1-p^{-i}).$$

This brings us to the second description from the end of last class. This whole $\frac{1}{\#\operatorname{Aut}\#A}$ distribution idea.

4.5.2 Causes of worry

We've just observed that these limits exist, but we may still worry about "escape of mass." We wonder

Question 4.5.4. *Is*

$$\sum_A \frac{\prod_{i\geq 2}(1-p^i)}{(\#\operatorname{Aut} A)(\#A)} = 1?$$

We also want to connected this to the models of imaginary quadratics and this whole $\mathrm{Cl}_K/[\mathfrak{p}]$ idea.

Let $X_n = \operatorname{coker}(\mathbb{Z}_p^n \to \mathbb{Z}_p^n)$ and $Y_n = \operatorname{coker}(\mathbb{Z}_p^{n_1} \to \mathbb{Z}_p)$ both matrices Haar-random. Note that you can get from X_n to Y_n by taking the quotient by a uniformly random element (the image of the $(n+1)$st basis vector of $\mathbb{Z}_p^{n+1}$).

We still worry about whether limits commute with this whole uniformly random element process.

[46]To be full rank, every row needs to contribute to the rank. No row can be in the span of the previous ones

Question 4.5.5.

$$\left(\lim_{n\to\infty} X_n\right)/\textit{uniform random elt} \overset{?}{=} \lim_{n\to\infty}\left(X_n/\textit{uniform random elt}\right)$$

The LHS is a $1/\#\operatorname{Aut}$ *group (by same argument/calculation we did above).*

In this case, we get lucky. Let's give the argument for the first question (in the case of X_n, not Y_n. Both arguments are similar but this one is slightly simpler).

$$\sum_{G_1}\lim_{n\to\infty}\mathbb{P}(X_n\simeq G_1)\overset{?}{=}\lim_{n\to\infty}\sum_{G_1}\mathbb{P}(X_n\simeq G_1)=1.$$

Look at the finite level

$$\mathbb{P}(X_n\simeq A)=\frac{\#\operatorname{Sur}(\mathbb{Z}_p^n,A)}{\#\operatorname{Aut}A(\#A)^n}\prod_{i=1}^n(1-p^{-i})$$

The

$$\frac{\#\operatorname{Sur}(\mathbb{Z}_p^n,A)}{(\#A)^n}$$

factor is increasing to 1 (which is good for monotone convergence). However, the

$$\prod_{i=1}^n(1-p^{-i})$$

factor is decreasing with n, so we have an increasing part and a decreasing part, which is bad for MCT. However, this second part has no dependence on A. Thus, we can look at the factors separately. That is,

$$\frac{1}{\prod_{i\ge1}(1-p^{-i})}\sum_{G_1}\lim_{n\to\infty}\mathbb{P}(X_n\simeq G_1)=\sum_{G_1}\lim_{n\to\infty}\frac{\mathbb{P}(X_n\simeq G_1)}{\prod_{i=1}^n(1-p^{-i})}\overset{\text{MCT}}{=}\lim_{n\to\infty}\sum_{G_1}\frac{\mathbb{P}(X_n\simeq G_1)}{\prod_{i=1}^n(1-p^{-i})}=\prod_{i\ge1}(1-p^{-i})^{-1},$$

so

$$\sum_{G_1}\lim_{n\to\infty}\mathbb{P}(X_n\simeq G_1)=1$$

as hoped for. The same argument works for Y_n in place of X_n.

This actually also resolves the other worry.

$$\begin{aligned}
\mathbb{P}(Y\simeq G_2)\prod_{i\ge1}(1-p^{-i})^{-1}&=\sum_{G_1}\lim_{n\to\infty}\frac{\mathbb{P}(X_n\simeq G_1)}{\prod_{i=1}^n(1-p^{-i})}\mathbb{P}(G_1/\langle g\rangle\simeq G_2)\\
&=\lim_{n\to\infty}\sum_{G_1}\frac{\mathbb{P}(X_n\simeq G_1)}{\prod_{i=1}^n(1-p^{-i})}\mathbb{P}(G_1/\langle g\rangle\simeq G_2)\\
&=\lim_{n\to\infty}\frac{\mathbb{P}(Y_n\simeq G_2)}{\prod_{i=1}^n(1-p^{-i})}\\
&=\lim_{n\to\infty}\mathbb{P}(Y_n\simeq g_2)\prod_{i\ge1}(1-p^{-i})^{-1}
\end{aligned}$$

(above, g a uniformly random element, so Y is a $1/\operatorname{Aut}$ random group quotiented by a random element).

The upshot is that this shows that taking a $1/\operatorname{Aut}$ random group quotiented by a random element is the distribution proportional to $\frac{1}{(\#\operatorname{Aut}G_2)(\#G_2)}$.

Above, we saw that $\lim_{n\to\infty}\mathbb{P}(X_n\simeq G_1)=c/\#\operatorname{Aut}(G_1)$ for some constant c.

Question 4.5.6 (Audience, paraphrased)**.** *A new point of worry. Let's go back to the whose S-unit thing.*

$$\mathrm{Cl}_K[p^\infty]\xrightarrow{\sim}\operatorname{coker}\left(\mathscr{O}_S^\times\otimes\mathbb{Z}_p\longrightarrow I^S\otimes\mathbb{Z}_p\right)$$

Why don't we consider the map

$$\mathscr{O}_S^\times/\mathscr{O}_K^\times\to I^S$$

since the first map factors through this one? Now, the spaces have the same rank and so this would give different predictions.

Answer. It's a little tricky. Any map $\mathbb{Z}_p^{n+1}\to\mathbb{Z}_p^n$ will always factor through some map $\mathbb{Z}_p^n\to\mathbb{Z}_p^n$ (essentially by rank reasons). That is, the cokernel of a map $\mathbb{Z}_p^{n+1}\to\mathbb{Z}_p^n$ is always the cokernel of some map $\mathbb{Z}_p^n\to\mathbb{Z}_p^n$, so why ever consider the former? Well, precisely because this gives a different distribution.

In the particular case under consideration, one can legitimately wonder which model is correct (with or without the quotient by $\mathscr{O}_K^\times$). We prefer the model without the quotient since it agrees with other motivations, and because the idea of thinking of these things as matrices is like imagining these spaces had bases. But the don't. In particular, there's no natural splitting map $\mathscr{O}_S^\times/\mathscr{O}_K^\times\to\mathscr{O}_S^\times$. ⋆

Next time, we'll look at the function field analogues and curves over $\mathbb{F}_q$ and all that jazz.

4.6 Lecture 6 (9/23)

Remark 4.6.1. Yesterday was national register to vote day, so remember to vote. ○

Remark 4.6.2. Last time, we were looking at Haar-random matrices over $\mathbb{Z}_p$, and we saw

I think this comes from us seeing that there's no "escape of mass" in the Haar-random limit distribution we were looking at like time

$$\sum_{G\text{ fin ab }p\text{-groups}}\frac{1}{|G|\,|\operatorname{Aut}G|}=\prod_{i\geq 2}\left(1-p^{-i}\right)^{-1}.$$

This tells us that

$$\sum_{G\text{ fin ab groups}}\frac{1}{|G|\,|\operatorname{Aut}G|}=\prod_p\prod_{i\geq 2}(1-p^{-i})^{-1}$$

(can only look at odd groups if you want). When there was no $|G|$ in the denominator, the products started at $i=1$, so we had a factor of $\zeta(1)$ in their and we knew the expression diverged. How might we now understand if this expression converges or diverges?

Note that the $i=2$ term is $\prod_p(1-p^{-2})^{-1}=\zeta(2)$. So the question is does the product $\zeta(2)\zeta(3)\zeta(5)\dots$ converge? There are a few things one could do. Might, for example estimate $\zeta(k)$ using integral comparison to get something like $\zeta(k)\leq 1+\frac{1}{2^k}+\frac{1}{(k-1)2^{k-1}}$. This will give that this infinite product does indeed converge.

Question: Is it obvious we can commute these infinite products?

Here's another way to say this. Recall we have $\mathcal{A}=\prod_p\{\text{fin ab }p\text{-groups}\}$. On each product we can take the $1/|A|\,|\operatorname{Aut}A|$ distribution on each p. The product measure of these is indeed supported on finite abelian groups. ○

Answer: If one was being careful, they'd start with this ζ

Remark 4.6.3. Last time talked about matrices $M_{n\times(n+u)}(\mathbb{Z}_p)$ (we've talked about $u \in \{0,1\}$) from Haar measure. If you want to consider all primes at once, can replace $\mathbb{Z}_p$ with $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ whose Haar measure is the product of those in $\mathbb{Z}_p$. ◦

4.6.1 Function Field Analogs

Question 4.6.4 (Philosophy)**.** *Is number theory about $\mathbb{Q}$ or is it about $\mathbb{Z}$?*

If it is about $\mathbb{Q}$, but study $\mathbb{Z}$ and not $\mathbb{Z}[\frac{1}{2}]$? One way to think about this is to think about the geometric space $\operatorname{Spec}\mathbb{Z}$ and $\operatorname{Spec}\mathbb{Z}[1/2] = \operatorname{Spec} Z \setminus \{(2)\}$. From this, we see that studying $\mathbb{Z}[1/2]$ is like studying $\mathbb{Z}$ but we've forgotten about the prime 2. When you get a larger ring (localizing), you get a smaller geometric space. This maybe motivates $\mathbb{Z}$ over e.g. $\mathbb{Z}[\frac{1}{2}]$ since it sees all the primes. Basically, what has happened here is that $\mathbb{Z} \subset$ any subring of $\mathbb{Q}$, so it is special in this context.

What about in the function field setting? Well, we have $\mathbb{F}_q(t)$ with $\mathbb{F}_q[t]$ sitting inside there. However, $\mathbb{F}_q[t] \subset \mathbb{F}_q(t)$ is not as special as $\mathbb{Z} \subset \mathbb{Q}$. There are *many* subrings $R \subset \mathbb{F}_q(t)$ which *do not* contain $\mathbb{F}_q[t]$.

Example. Can take $R = \mathbb{F}_q, \mathbb{F}_p$, or $\mathbb{F}_q[t^k]$ $(k > 1)$ for example. One might complain that these have different fraction fields and so tell you about some field other than $\mathbb{F}_q(t)$.

One can also take $R = \mathbb{F}_q[t^2, t^3]$ which now has $\mathbb{F}_q(t)$ as its fraction field, but is not even integrally closed, e.g. $x^2 - t^2 = 0$ has solutions in $\mathbb{F}_q(t)$ but not in this R. △

Fact (Possibly homework)**.** $\mathbb{F}_q[t]$ is minimal in the sense that it has no proper subring that is integrally closed with fraction field $\mathbb{F}_q(t)$. This is a weaker notion of minimality than $\mathbb{Z}$ enjoys.

Example. $R = \mathbb{F}_q[1/t], \mathbb{F}_q[1/(t-a)]$, or $\mathbb{F}_q[1/p(t)]$ ($p(t)$ irreducible) are all integrally closed with fraction field $\mathbb{F}_q(t)$. None of these contain $\mathbb{F}_q[t]$. △

The upshot is that the thing associated to $\mathbb{F}_q(t)$, with a relationship analogous to $\mathbb{Z}$'s relation to $\mathbb{Q}$, is not $\mathbb{F}_q[t]$ (i.e is not $\operatorname{Spec}\mathbb{F}_q[t] = \mathbb{A}^1_{\mathbb{F}_q}$). It is $\mathbb{P}^1_{\mathbb{F}_q}$ the projective line.

Each $\mathbb{F}_q[t], \mathbb{F}_q[1/t], \mathbb{F}_q[1/(t-a)]$ is a different copy of the affine line sitting in the projective line, i.e. each of these are of the form $\mathbb{P}^1_{\mathbb{F}_q} \setminus p$ for some point $p \in \mathbb{P}^1_{\mathbb{F}_q}$ (in these three examples, they are $p = \infty$, $p = 0$, and $p = a$).

Note that the (finite) places of $\mathbb{Z}$ correspond to primes of $\mathbb{Z}$ (i.e. points of $\operatorname{Spec}\mathbb{Z}$). The places of $\mathbb{F}_q(t)$ correspond to the points of $\mathbb{P}^1_{\mathbb{F}_q}$, so to the primes of any of these above rings (+ for each ring, one place that it is missing). More about this in the homework.

This will all result in some subtly when talking about class groups in the function field setting. Let's look at quadratic extensions for example. Compare

$$\begin{tikzcd}[arrows=dash]
 & K \arrow[d] & & & k \arrow[d] \\
\mathbb{Q} \arrow[ur, "2"] \arrow[dd] & \mathscr{O}_K & & \mathbb{F}_q(t) \arrow[ur, "2"] \arrow[dd] & \mathscr{O}_k \\
 & & & & \\
\mathbb{Z} \arrow[uur] & & & \mathbb{F}_q[t] \arrow[uur] &
\end{tikzcd}$$

In number field setting, we have $\mathrm{Cl}\,\mathscr{O}_K$ which is a finite abelian group and we study this. In the function field setting, if we look at $\mathscr{O}_k$, then we are missing some information. Just like $\mathbb{F}_q(t)$ is the field of rational functions of $\mathbb{P}^1_{\mathbb{F}_q}$, k is also the field of rational functions of some smooth, projective curve $C/\mathbb{F}_q$ and the given map $\mathbb{F}_q(t) \hookrightarrow K$, corresponds to a map $\pi : C \to \mathbb{P}^1_{\mathbb{F}_q}$. This projection is degree 2 since $k/\mathbb{F}_q(t)$ is, so C is a hyperelliptic curve in this case. What's the right analogy of the class group?

In the number field setting, we usually define $\mathrm{Cl}\,\mathscr{O}_K :=$ fraction ideals / prime ideals. This works, but this is also $\mathrm{Cl}\,\mathscr{O}_K = \mathrm{Pic}\,\mathscr{O}_K$, the group of (isomorphism classes of) locally free rank 1 $\mathscr{O}_K$-modules. Hence, in the function field setting, we look at $\mathrm{Pic}\,C$, the group of isom classes of line bundles (locally free rank one $\mathscr{O}_C$-modules). This definition let's us see all of C (instead of just the part about some choice of affine line).

So, in the function field setting, we have $\mathrm{Cl}\,\mathscr{O}_k$ and on $\mathrm{Pic}\,C$. In general, these objects are different. For example, $\mathrm{Cl}\,\mathbb{F}_q[t] = 0$ while $\mathrm{Pic}\,\mathbb{P}^1_{\mathbb{F}_q} = \mathbb{Z}$. More generally, $\mathrm{Cl}\,\mathscr{O}_k$ is always a finite abelian group, but $\mathrm{Pic}\,C$ is never finite, e.g. because the degree map $\deg : \mathrm{Pic}\,C \to \mathbb{Z}$ is nonzero. Look at the exact sequence

Not surjective always over arbitrary fields, but it is over finite fields.

$$1 \longrightarrow \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}\,C \xrightarrow{\deg} \mathbb{Z}$$

Fact. $\mathrm{Pic}(\mathrm{Spec}\,\mathscr{O}_k) = \mathrm{Pic}\,C/\left\{\mathscr{L}(p)\right\}_{p \text{ over } \infty}$ where $\infty \in \mathbb{P}^1 \setminus \mathbb{A}^1$ is the missing point.

What is the analogue of imaginary quadratic in the function field setting. This should be "ramified at ∞" so there's a unique point $\infty_1 \in C$ (of degree 1) above $\infty \in \mathbb{P}^1$. Then, the above fact is saying that

$$\mathrm{Cl}\,\mathscr{O}_k \simeq \mathrm{Pic}(C)/\mathscr{L}(\infty_1) \simeq \mathrm{Pic}^0(C).$$

On the other hand, "real quadratic" should now mean "split at ∞" so there are two points $\infty_1, \infty_2 \in C$ over $\infty \in \mathbb{P}^1$. We still have $\mathrm{Pic}^0(C) \simeq \mathrm{Pic}(C)/\mathscr{L}(\infty_1)$ (e.g. by degree exact sequence) but now

$$\mathrm{Cl}(\mathscr{O}_k) \simeq \mathrm{Pic}^0(C)/(\mathscr{L}(\infty_1 - \infty_2)$$

since we need to get rid of both points above infinity.

One could also consider the case where the cover is "inert at ∞" so there is one point $\infty_1 \in C$ above $\infty \in \mathbb{P}^1$, but now ∞_1 is a degree 2 point, not a degree 1 point. There's no analogue of this in the number field case since ∞ there is actually different from the other places.

For $\mathbb{F}_q(t)$, there is nothing special about ∞. Hence, one might think it is more natural to study $\mathrm{Pic}\,C$ or $\mathrm{Pic}^0(C)$ instead of $\mathrm{Cl}\,\mathscr{O}_k$ (keep in mind $\mathrm{Pic}\,C \simeq \mathrm{Pic}^0(C) \times \mathbb{Z}$ as a group). It is natural to guess to that $\mathrm{Pic}^0(C)$ is distributed like a $1/\#\,\mathrm{Aut}\,A$ random group and that for C split @ ∞ into ∞_1, ∞_2, $\mathscr{L}(\infty_1 - \infty_2)$ is distributed like a uniform random element of $\mathrm{Pic}^0(C)$. These guesses then imply that for K "real quadratic," $\mathrm{Cl}(\mathscr{O}_k) = \mathrm{Pic}^0(C)/\mathscr{L}(\infty_1 - \infty_2)$ should be distributed like a $\frac{1}{|A||\mathrm{Aut}\,A|}$ random group. This potentially gives another motivation for the predicted distributions of class groups of real and imag quadratic number fields.

It is not natural to literally guess this because of genus theory, so take odd parts or kill 2-torsion or whatever

Remark 4.6.5. Recall the observation that the tables of real quadratic fields' class groups "look like" tables of "imaginary quadratic $\mathrm{Cl}/\mathfrak{p}$ for fields split at $p = \mathfrak{p}\overline{\mathfrak{p}}$." ∘

Remark 4.6.6. In $\mathbb{F}_q(t)$, ∞ is not special. So if you make a guess like the one above for ∞, you'd also want to make the same guess for any other point of $\mathbb{P}^1_{\mathbb{F}_q}$. A reference for making all of this precise is Melanie's paper "C-L + local conditions" (or something like this). ∘

Next time we'll look at another perspective in the function field case: $\mathrm{Pic}^0(C)$ is the Frobenius fixed points of $\mathrm{Jac}(\overline{\mathbb{F}}_q)$.

Question 4.6.7. *Why is degree map surjective over finite fields?*

Answer. Can have a curve $C/\mathbb{F}_q$ with $C(\mathbb{F}_q) = \emptyset$. However, as you extend fields (consider $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$), the number of $\mathbb{F}_{q^m}$ points on C is at least $q^m - 2gq^{m/2} + 1$ (by Riemann hypothesis or Lang-Weil). For $m \gg 0$, $\#C(\mathbb{F}_{q^m}) > 0$, but a point in $C(\mathbb{F}_{q^m})$ corresponds to a degree d (where $d \mid m$) scheme theoretic point of C. This gives the degree 1 divisor $\mathscr{L}(-(m/d_m)p_m + ((m+1)/d_{m+1})p_{m+1})$ where $d_m = \deg p_m$ and $p_m \in C(\mathbb{F}_{q^m})$. ⋆

4.7 Lecture 7 (9/25)

We'll be working over a field like $\mathbb{F}_q(t)$. Let $p = \operatorname{char} \mathbb{F}_q$ and let $\ell \neq p$ be a different prime. Let $K/\mathbb{F}_q(t)$ be quadratic extension, so concretely,

$$K = \mathbb{F}_q(t)[y]/(y^2 = a(t)y + f(t)) \text{ with } a(t), f(t) \in \mathbb{F}_q[t].$$

K will be the function field of a smooth projective curve $C/\mathbb{F}_q$. The above equation gives an (affine, possibly singular) module of C. If $p \neq 2$, can do a change of variables to assume $a(t) = 0$ and then we're just looking at the canonical way of writing down a hyperelliptic curve $y^2 = f(t)$. We have a projection map $C \xrightarrow{\pi} \mathbb{P}^1$ given by the t coordinate, and we're interested in the group $\mathrm{Pic}^0(C)$ of degree 0 line bundles.

Let $J := \mathrm{Jac}(C)$, a (principally polarized) abelian variety over $\mathbb{F}_q$.

Remark 4.7.1. From the point of view of ordering fields, the genus g is sort of like the discriminant of this extension. So, taking function fields as discriminant goes to ∞ is like taking hyperelliptic curves as the genus goes to ∞. ○

Fact. $J(\mathbb{F}_q) = \mathrm{Pic}^0(C)$ as groups.

People often like to look at the torsion of the geometric points of the Jacobian. When $p \nmid m$, we have $J(\overline{\mathbb{F}}_q)[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$. Note that $J(\mathbb{F}_q)[m] = \mathrm{Pic}^0(C)[m]$ are the Frob ($= \mathrm{Frob}_q$) fixed points of $J(\overline{\mathbb{F}}_q)[m]$. We have an action $\mathrm{Frob} \curvearrowright (\mathbb{Z}/m\mathbb{Z})^{2g}$ but writing down what this action is (e.g. as an element of $\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$) is subtle; it actually depends on the arithmetic of C.

We can package all the ℓ-power torsion together to get

$$\mathrm{Jac}(\overline{\mathbb{F}}_q)[\ell^\infty] = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$$

with Frobenius acting on this. However, people tend to not like divisible groups here, and so usually put together the ℓ-power torsion in a different way.

Definition 4.7.2. Let D be a divisible group such that $D[\ell^k]$ is finite for all $k \geq 0$. Its **Tate module** is

$$T_\ell D := \varprojlim D[\ell^k]$$

where the limit is taken under the multiplication by ℓ map $D[\ell^{k+1}] \xrightarrow{\ell} D[\ell^k]$. ◇

Remark 4.7.3. $D[\ell^k] = T_\ell(D)/\ell^k$, so morally, we still have the same information, just repackaged. ○

Applying this to $\mathrm{Jac}(\overline{\mathbb{F}}_q)[\ell^\infty]$ gives us $T_\ell J := T_\ell(J(\overline{\mathbb{F}}_q)) \simeq \mathbb{Z}_\ell^{2g}$.

Recall that $\mathrm{Pic}^0(C)[\ell^\infty]$ is $\ker(\mathrm{Frob}-\mathrm{Id})$ acting on $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$. We need to translate this to a statement about the Tate module.

Lemma 4.7.4 (Friedman-Washington '89)**.** *With D as above and $\varphi : D \to D$ a surjective homomorphism, then we get an associated map $T_\ell\varphi : T_\ell D \to T_\ell D$. If $\ker\varphi$ is a finite ℓ-group, then*

$$\ker\varphi \simeq \operatorname{coker} T_\ell\varphi.$$

Proof. We'll just say what the map is:

$$\begin{array}{ccc} \ker\varphi & \longrightarrow & \operatorname{coker} T_\ell\varphi \\ \alpha & \longmapsto & \left\{\varphi(\ell^{-n}\alpha) \in D[\ell^n]\right\}_n \end{array}.$$

The kernel being finite let's you check that it's injective. For surjectivity, use that inverse limits of finite sets in compact. ■

Remark 4.7.5. $\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell$, so when we write down $\mathrm{Frob} \curvearrowright J(\overline{\mathbb{F}}_q)[\ell^\infty] = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$, we are writing an element of $\mathrm{Hom}((\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}) = M_{2g\times 2g}(\mathbb{Z}_\ell)$. When we view Frob as acting on $\mathbb{Z}_\ell^{2g}$, this is also represented by some matrix in $M_{2g\times 2g}(\mathbb{Z}_\ell)$. These two matrices are on in the same! However, their actions on $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)$ vs. on $\mathbb{Z}_\ell^{2g}$ are slighly different in a way that turns the kernel of one to the cokernel of the other. ○

Anyways, the upshot is that

$$\mathrm{Pic}^0(C)[\ell^\infty] = \operatorname{coker}(\mathrm{Frob} - \mathrm{Id})|_{\mathbb{Z}_\ell^{2g}}.$$

Question 4.7.6 (Audience)**.** *How do we know that* $\mathrm{Frob} - \mathrm{Id}$ *is surjective?*

Answer. If it weren't surjective, it would have a large kernel, i.e. you would get infinitely many $\mathbb{F}_q$ points on the Jacobian (there's a notion of rank for these $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ maps). There are probably other ways to see surjectivity. ⋆

4.7.1 Next model

We have $\mathrm{Frob} \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. Friedman-Washington conjectured that Frob is equidistributed with respect to the Haar measure on $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.

Remark 4.7.7. You have to be careful since $g \to \infty$. F-W made things precise. ○

Question 4.7.8. *If $M \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ is a random matrix from the Haar measure on $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$, what is the distribution of* $\operatorname{coker}(M - \mathrm{Id})$*?*

Remark 4.7.9. Equidistribution does not mean that everything has to arise, just that the things that do arise are spread out enough that averages of (certain) test functions are close to averages of these test functions for the whole group. ○

Theorem 4.7.10 (Friedman-Washington)**.** *Let A be a finite abelian ℓ-group. Then,*

$$\lim_{n\to\infty} \mathbb{P}\left(\operatorname{coker} F - \mathrm{Id} \simeq A\right) = \frac{c}{\#\operatorname{Aut} A}$$

where F is a random matrix from the Haar measure on $\mathrm{GL}_n(\mathbb{Z}_\ell)$.

We will not give their proof, but we'll later talk about moments and then give a different, much easier proof of this fact. This will serve as motivation to believe that momemnts are nice.

Remark 4.7.11. This is another kind of universality. Note that $F - 1 \in M_{n\times n}(\mathbb{Z}_l)$ with F Haar from $\mathrm{GL}_n(\mathbb{Z}_\ell)$ gives a distribution on $M_{n\times n}$. Its entries are not independent (e.g. since $(F-1)+1 \in \mathrm{GL}_n(\mathbb{Z}_\ell) \subset M_{n\times n}(\mathbb{Z}_\ell))$, so our earlier universality result does not apply. However, we still have the cokernel distribution approaching the $1/\operatorname{Aut}$ distribution.

However, always remember not every random matrix has this same cokernel distribution. e.g. $F \in M_{n\times n}(\mathbb{Z}_\ell)$ where F Haar from $\mathrm{GL}_n(\mathbb{Z}_\ell)$ has cokernel distribution being the point mass on the trivial group. $\circ$

There is a problem with this model.

Question 4.7.12. *Why is* Frob *not general in* $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.

Answer. We have the Weil pairing: perfect, alternating pairing

$$J(\overline{\mathbb{F}}_q)[\ell^k] \times J(\overline{\mathbb{F}}_q)[\ell^k] \to \mu_{\ell^k}(\overline{\mathbb{F}}_q).$$

Between k, these are compatible exactly so as to give a perfect, alternating pairing

$$T_\ell J(\overline{\mathbb{F}}_q) \times T_\ell J(\overline{\mathbb{F}}_q) \xrightarrow{w} \mathbb{Z}_\ell(1).$$

Choose a basis so that

$$W = \begin{pmatrix} & I \\ -I & \end{pmatrix}.$$

How does Frobenius interact? Well,

$$w(\mathrm{Frob}x, \mathrm{Frob}y) = qw(x,y).$$

At the finite level, things are defined over $\mathbb{F}_q$, so you end up raising the result to the qth power. Written additively, this means multiplying by q. This, by definition, says that

$$\mathrm{Frob} \in \mathrm{GSp}^{(q)}(W).$$

$\star$

4.7.2 Next Model

Maybe Frob is like a Haar random matrix from $\mathrm{GSp}^{(q)}_{2g}(\mathbb{Z}_\ell)$.

Question 4.7.13. *What is the cokernel distribution of $F - \mathrm{Id}$ for F Haar random from $\mathrm{GSp}^{(q)}_{2g}(\mathbb{Z}_\ell)$?*

Friedman-Washington did not answer this, but Garton later computed the moments. This with some of Melanie's work determines the distribution. One finds that when $\ell \nmid (q-1)$, as $g \to \infty$

$$\mathbb{P}(\operatorname{coker}(F - I) \simeq A) \to \frac{c}{|\operatorname{Aut} A|}.$$

This is yet another manifestation of universality. Note that you don't get the $1/\operatorname{Aut}$ distribution at an particular size of matrix; it is only in the limit that they agree.

When $\ell \mid (q-1)$, you get a different cokernel distribution (Achter). Achter noticed this before Garton's work. Garton found the moments in this case. A recent paper has found formulas for the probabilities of each group[47].

What's going on here? When $\ell \mid (q-1)$, then $\mathbb{F}_q(t)$ has ℓth roots of unity. This represents a breakdown of the function field/number field analogy. When ℓ is odd, $\mathbb{Q}$ has no ℓth roots of unity, so in this way, if $\ell \mid (q-1)$, then $\mathbb{F}_q(t)$ is not like $\mathbb{Q}$ for current purposes. We expect different $\operatorname{Pic}^0(C)[\ell^\infty]$ distributions when $\ell \mid q-1$, and similarly when $\mathbb{Q}$ is replaced by a number field K with $\mu_\ell(K) \neq 1$. However, what exactly we expect and why is at the edge of current research.

Remark 4.7.14. To be clear, when $\ell \mid q-1$ the moments themselves are already different. ○

4.7.3 Coming up...

What are things we'll talk about, hopefully before too long?

- Moments and how they are more accessible. Also, when they determine the distribution.
- Function field theorems

4.8 Lecture 8 (9/30)

Remark 4.8.1 (From second homework). There was a question about counting $\#\operatorname{Sur}(\mathbb{Z}_p^n, A)$. Many people started with $\#\operatorname{Hom}(\mathbb{Z}_p^n, A) = |A|^n$ and it's clear that as $n \to \infty$, "all" of these become surjections. Some suggested doing an inclusion-exclusion thing to count the number of these that are surjective (but no one carried this out).

Here's an observation. If $\varphi \in \operatorname{Hom}(\mathbb{Z}_p^n, A)$, then φ is surjective iff it is mod p, by Nakyama's lemma. This reduces to question of what proportion of $\operatorname{Hom}((\mathbb{Z}/p\mathbb{Z})^n, A/p)$ are surjective, i.e. if $r = \operatorname{rank}_p A$, then which portion of $r \times n$ matrices over $\mathbb{F}_p$ have rank r? Need the rows to be linearly independent (each not in the span of the previous) so get $(1-p^{-n})(1-p^{-(n-1)})\dots(1-p^{-(n-r+1)})$. Hence, the answer is

$$\#\operatorname{Sur}(\mathbb{Z}_p^n, A) = |A|^n \prod_{i=0}^{r-1}(1-p^{-(n-i)}).$$

○

Homework 4 is currently up.

4.8.1 Moments of Class Groups & Counting Number fields

Let $\mathscr{F}$ be some set of number fields, and let $I : \mathscr{F} \to \mathbb{R}_{>0}$ be some invariant you are counting by. We can define

$$N_{\mathscr{F},I}(X) = \#\{K \in \mathscr{F} \mid I(K) < X\}$$

which is an interesting thing to study when this set is (always) finite. In that case, people like to study the asymptotic in X of $N_{\mathscr{F},I}(X)$?

[47] Assuming I heard Melanie correctly.

What kinds of $\mathscr{F}$ do people usually consider? Usually people will fix a degree and even a Galois structure[48].

There are other kinds of conditions one might be interested in when counting number fields.

- local conditions (splitting types, ramification, ...), even local conditions everywhere (e.g. square-free discriminant)
- w/ a fixed class group
- 'shape' conditions (think of lattice of ring of integers)
- number fields admitting elliptic curves with certain properties

What about the invariants people consider? These include...

- $I = \mathrm{Disc}$
- $I = \mathrm{rad}(\mathrm{Disc})$, the product of the ramified primes
- other products of local invariants (e.g. in abelian case, have the conductor)

Malle's Conjecture, Malle-Bhargava Principle gives "baseline" conjecture for many (but not all) of these questions; note that it is sometimes false. There's a lot one can say here, but we won't say more. See Melanie's AWS notes for more info

Let's relate counting number fields to moments in the quadratic case.

$$\begin{tikzcd}
& H \arrow[d, dash] \arrow[ddl, dash, "\mathrm{Cl}_K"'] \\
& L \arrow[dl, dash, "A"] \\
K \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

Note that, by Galois theory, $\mathrm{Sur}(\mathrm{Cl}_K, A)$ is in bijection with unramified A**-extensions** of K, i.e. pairs (L, φ) where L/K is Galois (+ unramified in this case) and $\varphi : \mathrm{Gal}(L/K) \xrightarrow{\sim} A$ (i.e. it comes with a fixed choice of isomorphism).

Question 4.8.2. *Is $L/\mathbb{Q}$ Galois?*

Answer. Well, $H/\mathbb{Q}$ is Galois, so we're asking if $\mathrm{Gal}(H/L)$ is normal in $\mathrm{Gal}(H/\mathbb{Q})$ (which is *not* necessarily abelian). We have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(H/K) \longrightarrow \mathrm{Gal}(H/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1$$

so to know if $\mathrm{Gal}(H/L) \subset \mathrm{Gal}(H/K)$ is normal in $\mathrm{Gal}(H/\mathbb{Q})$, we need to know about conjugation. Since $\mathrm{Gal}(H/K)$ is abelian, we only care if the usual "lift and conjugate" action of $\mathrm{Gal}(K/\mathbb{Q}) \curvearrowright \mathrm{Gal}(H/K)$ fixes $\mathrm{Gal}(H/L)$ (as a set, not pointwise).

[48] i.e. if $\widetilde{K}$ is the Galois closure, then $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ permutes the embeddings $K \to \widetilde{K}$ so acts by some permutation group. By Galois structure, we mean $\mathrm{Gal}(\overline{K}/\mathbb{Q})$ as a permutation group

Luckily for us, class field theory tells us more. The Artin map gives an iso $\mathrm{Gal}(H/K) \xrightarrow{\sim} \mathrm{Cl}(K)$ and this map is equivariant with respect to their $\mathrm{Gal}(K/\mathbb{Q})$-actions (because CFT says so). Recall that (the nontrivial element of) $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Cl}(K)$ by multiplication by -1. Thus, $\mathrm{Gal}(H/L)$ is indeed fixed by this action, so $\mathrm{Gal}(H/L)$ is normal in $\mathrm{Gal}(H/\mathbb{Q})$ and so $L/\mathbb{Q}$ is Galois. ⋆

Remark 4.8.3. This was special. We used critically that $K/\mathbb{Q}$ is quadratic and that L/K is unramified. In general, A-extensions of K do not need to be Galois over $\mathbb{Q}$. You can have more complicated Galois-actions on the relevant ray class group. ◦

Question 4.8.4. *What is* $\mathrm{Gal}(L/\mathbb{Q})$*?*

Answer. It sits in an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(L/K) \arrow[r] \arrow[d, "\wr"] & \mathrm{Gal}(L/\mathbb{Q}) \arrow[r] & \mathrm{Gal}(K/\mathbb{Q}) \arrow[r] \arrow[d, "\wr"] & 1 \\ & A & & \mathbb{Z}/2\mathbb{Z} & \end{tikzcd}$$

We now want to ask which kinds of groups fit in such an extension with the given action of $\mathbb{Z}/2\mathbb{Z} \curvearrowright A$. Since $|A|$ is odd (i.e. coprime to $2 = |\mathbb{Z}/2\mathbb{Z}|$), Schur-Zassenhaus tells us that this sequence splits[49] so $\mathrm{Gal}(L/\mathbb{Q}) \simeq A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. Note that choosing such an iso corresponds to choosing a splitting. ⋆

This was assumed at some point, but I missed it

We have now given a bijection

There are other ways to see this is split. For example, $\mathrm{Gal}(L/\mathbb{Q})$ has a Sylow-2 subgroup which must be $\mathbb{Z}/2\mathbb{Z}$

$$\left\{(K,\psi,L,\varphi)\;\middle|\; \begin{matrix} \varphi : \mathrm{Gal}(L/K) \xrightarrow{\sim} A, L/K \text{ unram} \\ \text{choice of splitting } \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \end{matrix}\right\} \leftrightarrow \left\{(L,\Theta)\;\middle|\; \begin{matrix} \Theta : \mathrm{Gal}(L/\mathbb{Q}) \simeq A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} \\ \mathrm{Gal}(L/L^A) \text{ is unram} \end{matrix}\right\}$$

In the left, morally should include choice of $\psi : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$, but there's only one such thing so technically can omit it

This reduces the question of determining[50]

$$\sum_K \#\,\mathrm{Sur}(\mathrm{Cl}_K, A)$$

to counting certain $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ fields.

Remark 4.8.5. If I heard correctly, even in the non-quadratic case, all such known moment calculations were determined by counting fields like this. ◦

Question 4.8.6. *When can we count* $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ *extensions?*

For $K/\mathbb{Q}$ quadratic, only so far for $A = \mathbb{Z}/3\mathbb{Z}$ where $\mathbb{Z}/3\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} \simeq S_3$. Counting S_3 extensions is roughly the same as counting non-Galois cubics. Keep in mind that the moment is just a literal number, so our count for this needs to pretty accurate (i.e. we want the exact constant in front of the asymptotic).

Theorem 4.8.7 (Davenport-Heilbronn)**.** *Let* $N_3(X) = \#\{K/\mathbb{Q} \text{ cubic} \mid |\mathrm{Disc}| \le X\}$. *Then,* $N_3(X) \sim c_3 X$ *where* c_3 *is some explicit constant. For* S *a finite set of places*

Before this, Cohn had counted cyclic cu-

$$N_{3,(\Sigma_p)_{p\in S}}(X) \sim \prod_{p\in S} \delta(\Sigma_p) c_3 X$$

[49]When A abelian, can think of this as the vanishing of some cohomology group, but Schur-Zassenhaus works even when A is non-abelian

[50]This divided by the number of quadratic fields will tell us the average number of surjections from $\mathrm{Cl}_K \twoheadrightarrow A$

where Σ_p gives some "local conditions at p."

Remark 4.8.8. For class group moment, we need cubic fields which are nowhere totally ramified.[51] ◦

Davenport-Heilbronn let's us impose conditions on finite sets of primes, but we'd like to do so for all p. It is formal from the above, that we at least get a bound

$$\limsup_{X\to\infty} \frac{N_{3,(\Sigma_p)_p}(X)}{X} \le c_3 \prod_p \delta(\Sigma_p).$$

What is *not* formal is the other inequality.

Example. Let $N(X)$ count positive integers m up to X. Let's impose local conditions

$$\Sigma_p : p^2 \nmid m \text{ and } m > p.$$

Given a finite set S of primes, we have[52]

$$N_{(\Sigma_p)_{p\in S}}(X) \sim \prod_{p\in S}\left(1-p^{-2}\right) X.$$

On the other hand,

$$N_{(\Sigma_p)_{p\in S}} = 0 \not\sim \prod_p (1-p^{-2})X = X/\zeta(2).$$

We do have the inequality $0 \le \prod_p (1-p^{-2})$ though. △

This example shows that we actually have to make some argument/give further input in order to conclude what we would like.

In this case, some further input sufficient to get the other inequality (what D-H used) is ($\overline{\Sigma}_p$ is the complement)

$$N_{\overline{\Sigma}_p}(X)/X \le c_p \text{ with } \sum_p c_p < \infty.$$

Given above input, one then formally gets

$$N_{(\Sigma_p)_p}(X) \sim c\prod_p \delta(p)X.$$

This is kind of like a dominated convergence condition which we are using to exchange two limits (one in X and one in p).

D-H in above case proved we have this for $c_p = c/p^2$ where c is some absolute constant. Next time, we'll say more about how one could prove this. We won't give D-H's proof, but will give a nicer one due to Datskovsky-Wright (one can argue about whether the two proofs are morally the same or not. We won't).

Question 4.8.9 (Audience). *What happens with this condition in our toy example?*

[51] Need $\mathrm{Gal}(L/L^A)$ unramified so inertia at every prime relegated to $\mathbb{Z}/2\mathbb{Z} \subset S_3$ if I'm understanding things correctly

[52] Via Chinese remainder theorem, this is some condition congruence condition and the fact that $m > p$ only gets rid of finitely many numbers so doesn't affect asymptotics

Answer. In our toy example, $N_{\overline{\Sigma}_p(X)}$ counts integers $m \le X$ such that $m \le p$ or $p^2 \mid m$. If we didn't have the $m \le p$ condition, we could just use $c_p = p^{-2}$. However, with this condition there, we can't really choose a uniform bound better than 1 (e.g. take $X = p$), but $\sum_p 1 \not< \infty$. ⋆

4.9 Lecture 9 (10/2)

Goal. $N_{3,\overline{\Sigma}_p}(X) = O\left(\frac{X}{p^2}\right)$ (constant independent of p), the number of cubic fields totally ramified at p to up $|\mathrm{Disc}| \le X$ is bounded above by something like $1/p^2$. We need this to use a sieve.

We also want to further explore connection between counting number fields and moments of class groups.

Recall 4.9.1. We have reduced $\mathbb{E}[\#\operatorname{Sur}(\operatorname{Cl} K, \mathbb{Z}/3\mathbb{Z})]$ to counting nowhere totally ramified cubic fields. Note that, concretely $\#\operatorname{Sur}(\operatorname{Cl} K, \mathbb{Z}/3\mathbb{Z}) = |\operatorname{Cl} K[3]| - 1 = 3^{\operatorname{rank}_3 \operatorname{Cl} K} - 1$ so we're also essentially finding the average of the size of the 3-torsion. ⊙

Remark 4.9.2 (Tangent). We've blackboxed how D-H counted cubic fields. They did some geometry of numbers thing. Why can't we use CFT to count cubic fields? The cyclic ones are easy, so what about the non-cyclic ones. These all fit in

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash, "2"'] \arrow[dr, dash, "C_3"] & \\ K \arrow[dr, dash, "3"'] & & F \arrow[dl, dash, "2"] \\ & \mathbb{Q} & \end{tikzcd}$$

i.e. they all come from a C_3-extension of a quadratic. For any F, we can count C_3-extensions of F. However, we can't sum over F. Recall the exact sequence

$$1 \longrightarrow \mathscr{O}_F^\times \longrightarrow \prod_v \mathscr{O}_v^\times \longrightarrow \widehat{C}_F \longrightarrow \operatorname{Cl}_F \longrightarrow 1$$

we're trying to count (surjective) homomorphisms $\widehat{C}_F \to \mathbb{Z}/3\mathbb{Z}$ (cyclic extensions of F). However, $\widehat{C}_F$ is pretty close to $\prod_v \mathscr{O}_v^\times$ and we can count $\prod_v \mathscr{O}_v^\times \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}$. Consider the exact sequence

$$0 \longrightarrow \operatorname{Hom}(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \operatorname{Hom}(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \operatorname{Hom}(\prod_v \mathscr{O}_v^\times/\mathscr{O}_F^\times, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \operatorname{Ext}^1(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \cdots$$

Hence, the things we want to count are close to $\operatorname{Hom}(\prod_v \mathscr{O}_v^\times/\mathscr{O}_F^\times, \mathbb{Z}/3\mathbb{Z})$, which is easy to count, but we're off by two places: $\operatorname{Ext}^1(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z}) \simeq \operatorname{Cl}_F[3]$ and $\operatorname{Hom}(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z}) \simeq \operatorname{Cl}_F[3]$. One of $\operatorname{Cl}_F[3]$'s is "overcounting" while the other is "undercounting", so one can hope that they cancel, but you don't know that.

The main obstruction to adding over F is not knowing the average behavior of $\operatorname{Cl}_F[3]$ over F. This is precisely the thing that motivated us counting cubic fields, so we've gone full circle.

If you have one particular F, the ambiguity just gets absorbed in the constant. However, if you average over F, you need to add up all these constants, so need better control. ∘

Recall 4.9.3. D-H had counted cubic fields, so we have an upper bound on $\Sigma_{D_F \le X} |\operatorname{Cl}_F[3]| = O(X)$. ⊙

Let's go back to the diagram

$$\begin{tikzcd}
 & L \arrow[dl, dash, "2"'] \arrow[dr, dash, "C_3"] & \\
K \arrow[dr, dash, "3"'] & & F \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Write $D_K = |\operatorname{Disc} K|$ and $D_F = |\operatorname{Disc} F|$. Let $H \subset \widehat{C}_F$ corresponding to L/F (the kernel of $\widehat{C_F} \twoheadrightarrow \operatorname{Gal}(L/F)$).

Recall 4.9.4. Let L/K be a finite abelian extension of non-archimedean local fields. The **conductor** of L/K, denoted $\mathfrak{f}(L/K)$, is the smallest non-negative integer n such that (note that $U^{(0)} = \mathscr{O}^\times$)

$$U^{(n)} = 1 + \mathfrak{m}^n = \left\{u \in \mathscr{O}^\times : u \equiv 1 \pmod{\mathfrak{m}_K^n}\right\}$$

is contained in $\operatorname{Nm}_{L/K}(L^\times)$. Equivalently, $\mathfrak{f}(L/K)$ is the smallest integer such that the local Artin map is trivial on $U_K^{(n)}$.

The **conductor** of a finite abelian extension L/K of number fields (or rather, its finite part) is the product

$$\mathfrak{f}(L/K) := \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{f}(L_\mathfrak{p}/K_\mathfrak{p})}$$

of local conductors. An infinite prime v occurs in the conductor iff v is real and becomes complex in L (i.e. v ramifies).

Example. For $K/\mathbb{Q}$, let n be minimal such that $K \subset \mathbb{Q}(\zeta_n)$. Then, the conductor of $K/\mathbb{Q}$ is n if K is fixed by complex conjugation and is $n\infty$ otherwise. △

Example. Let d be squarefree. Then,

$$\mathfrak{f}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \begin{cases} \left|\operatorname{Disc}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})\right| & \text{if } d > 0 \\ \infty\left|\operatorname{Disc}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})\right| & \text{otherwise.} \end{cases}$$

△

⊙

Fact (Some of these will be homework)**.**

- $D_K = f^2 D_F$ where $f \in \mathbb{Z}_{>0}$ is the conductor of L/F (in the sense of class field theory).
- In fact, f is the product of rational primes where $K/\mathbb{Q}$ is totally ramified (Note that D_F is squarefree except at 2).

I think Melanie said that primes which are totally ramified appear in the discriminant as

Notation 4.9.5. Let $\omega(f)$ be the number of rational prime divisors of f.

Lemma 4.9.6. *$\#H \subset \widehat{C}_F$ which are index 3 (and closed?) of conductor f is $O\left(9^{\omega(f)}\#\operatorname{Cl}_f[3]\right)$.*

Proof. Recall

$$0 \longrightarrow \operatorname{Hom}(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \operatorname{Hom}(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \operatorname{Hom}(\prod_v \mathscr{O}_v^\times/\mathscr{O}_F^\times, \mathbb{Z}/3\mathbb{Z}) \longrightarrow \operatorname{Ext}^1(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z})$$

Note that we can see the conductor even after passing to $\operatorname{Hom}(\prod_v \mathscr{O}_v^\times/\mathscr{O}_F^\times)$. Since we just want an upper bound, we can ignore the Ext^1 term as[53]

$$\#\operatorname{Hom}(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z})^f \le |\operatorname{Hom}(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z})|\cdot\left|\operatorname{Hom}(\prod_v \mathscr{O}_v^\times/\mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z})^f\right| \le |\operatorname{Hom}(\operatorname{Cl}_F, \mathbb{Z}/3\mathbb{Z})|\cdot\left|\operatorname{Hom}(\prod_v \mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z})^f\right|$$

(we're only considering homomorphisms *of conductor f*. This is what the superscript denotes). Each $p \mid f$ has at most 2 places v above it in F, so the number of places of F at which L/F ramifies is at most $2\omega(f)$. Note that $\#\operatorname{Hom}(\mathscr{O}_v^\times, \mathbb{Z}/3\mathbb{Z}) \le 3$, except for $v \mid 3$, but there are only finitely many $v \mid 3$ (with a uniform bound[54] on how many maps they have to $\mathbb{Z}/3\mathbb{Z}$). Hence,

$$\#\operatorname{Hom}(\widehat{C}_F, \mathbb{Z}/3\mathbb{Z})^f = O\left(3^{2\omega(f)}\,|\operatorname{Cl}_F[3]|\right).$$

∎

Remark 4.9.7. Being more careful, one can replace that 9 with a 4, but it won't matter for our purposes. ○

Let's now use this lemma to prove our goal. Recall that $N_{e,\overline{\Sigma}_p}(X)$ counts cubic fields of $|\mathrm{Disc}| \le X$ which are totally ramified at p. We have

$$N_{3,\overline{\Sigma}_p}(X) = O\left(\sum_{f>0, p\mid f}\ \sum_{\substack{F \text{ quad} \\ D_F \le X/f^2}} 9^{\omega(f)}\#\operatorname{Cl}_F[3]\right)$$

where we've used $D_K = f^2 D_F$. Note that

$$\sum_{\substack{F \text{ quad} \\ D_F \le X/f^2}} |Cl_F[3]| = O(X/f^2)$$

because we already had an upper bound from yesterday. Hence, (note $p \mid f \iff f = mp$)

$$N_{3,\overline{\Sigma}_p}(X) = O\left(\sum_m 9^{\omega(m)}\frac{X}{p^2m^2}\right) = O\left(\frac{X}{p^2}\sum_{m\ge1}\frac{9^{\omega(m)}}{m^2}\right) = O\left(\frac{X}{p^2}\right)$$

[53] Note that rank $\mathscr{O}_F^\times \le 1$, so ignore this quotient only changes our count by a factor of ≤ 3

[54] At $v \mid 3$, $\mathscr{O}_v^\times$ lives in a degree 2 extension of $\mathbb{Q}_3$ and there are only finitely many such things, so get a uniform bound by just taking a max. Less lazily, the structure of these units of completions (at odd primes) is known, so you could look it up and get a more concrete answer.

where, in the last equality, we have used that

$$\sum_{m\geq 1}\frac{9^{\omega(m)}}{m^2}=\prod_{\ell}\left(1+\frac{9}{\ell^2}+\frac{9}{\ell^4}+\cdots\right)\leq\prod_{\ell}\left(1-\frac{9}{\ell^2}\right)^{-1}$$

is convergent, since $\pi_\ell(1-9/\ell^2)\neq 0$ since $\sum 9/\ell^2<\infty$.

This proves the goal.

Moral. Determining $\sum_F \#\operatorname{Cl}_F[3]$ or $\sum_F \#\operatorname{Sur}(\operatorname{Cl}_F,\mathbb{Z}/3\mathbb{Z})$ is hard, but the difference between Cl_F and $\widehat{C}_F$ is much easier (exact sequence).

We saw that $\mathbb{E}\left[\#\operatorname{Sur}(\operatorname{Cl}_K,A)\right]$ is related to counting $A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z}$ extensions.

Example. When $A=\mathbb{Z}/\ell\mathbb{Z}$, $\mathbb{E}(\#\operatorname{Sur}(\operatorname{Cl}_K,\mathbb{Z}/\ell\mathbb{Z}))$ is related to D_l-extensions (only known how to do this when $\ell=3$). We did this when $\ell=3$ by taking advantage of the close relationship between these two things. △

Theorem 4.9.8 (Klüners)**.**

- *C-L conjecture for $\mathbb{E}(\#\operatorname{Sur}(\operatorname{Cl}_K,\mathbb{Z}/\ell\mathbb{Z}))\implies$ conjectured upper bound for D_ℓ extensions (Malle, up to constants).*

Note that this is the opposite direction from the way we went today. Think, can count fields using CFT if you know $\mathbb{E}(\operatorname{Cl}_F[\ell])$.

- *Proves the conjectured lower bound for D_ℓ extensions.*[55]

In some sense, the second half of this is saying that the lower bound for D_ℓ extensions is not so closely tied to class group moments. They key for Klüners' proof is that you need only one D_ℓ extension per quadratic to get this lower bound. The clover observation is that if $\operatorname{Cl}_F[\ell]\neq 1$, then there is an unramified degree ℓ extension over F, so you get a D_ℓ extension which is unramified over F. If $\operatorname{Cl}_F[\ell]=1$, then our exact sequence simplifies and one can actually use is to count.

The next thing we'll do is talk more generally about the theory of moments of distributions of random groups.

4.10 Lecture 10 (10/07)

Today we talk more about moments of random groups. We begin by recalling the classical theory.

4.10.1 Moments, classically

Say X is a random real number.

Definition 4.10.1. The **kth moment** ($k\in\mathbb{N}$) of X is $\mathbb{E}(X^k)$, the average/expected value of X^k. ⋄

Remark 4.10.2. If X takes countably many values (as is often the case when dealing with random finite groups), then

$$\mathbb{E}(X^k)=\sum_{\lambda}\mathbb{P}(X=\lambda)\lambda^k$$

where λ ranges over possible values of X. ∘

[55] The conjectured lower bound is the same as the conjectured upper bound

Remark 4.10.3. If X comes from a probability distribution μ on $\mathbb{R}$, then

$$\mathbb{E}(X^k) = \int_{\mathbb{R}} X^k \mathrm{d}\mu.$$

$\circ$

Remark 4.10.4. If X and Y have the same distribution, then $\mathbb{E}(X^k) = \mathbb{E}(Y^k)$, they have the same moments. $\circ$

This last remark leads to the following problem.

Question 4.10.5 (Moment problem). *Do these moments determine a unique distribution, i.e. given $m_1, m_2, \dots \in \mathbb{R}$, does there exist a unique X (up to having the same distribution) such that $\mathbb{E}(X^k) = m_k$ for all k?*

There are two questions above: existence and uniqueness.

We'll focus on uniqueness since, in this class at least, we usually have some distribution (e.g. the Cohen-Lenstra one) and we're interested if another distribution agrees with it. The existence problem can also be relevant to arithmetic statistics, but it is beyond the scope of this class.[56]

Theorem 4.10.6 (Carleman's condition)**.** *If $\sum_{n\geq 1} m_{2n}^{-1/2n} = \infty$, then we get uniqueness above (i.e. at most* 1 *distribution).*

Note that m_{2n} is positive since we're looking at distributions on the reals

Remark 4.10.7. The above sum is a sum of reciprocals of things. So, morally, it's telling us that to get uniqueness, we want our moments (or rather $m_{2n}^{1/2n}$) to be small. $\circ$

Example. Say $m_{2n} = c$ are constant. Then we get

$$\sum_n \frac{1}{c^{1/2n}} = \infty$$

e.g. since terms above approach $1 \neq 0$ as $n \to \infty$. $\triangle$

Example. Say $m_{2n} = c^{2n}$. Then,

$$\sum_n \frac{1}{c} = \infty.$$

$\triangle$

Example. Say $m_{2n} = c^{2n^2}$. Then,

$$\sum_n \frac{1}{c^n} < \infty$$

so we fail Carleman's condition. $\triangle$

Remark 4.10.8. In general, moments are given by integrals so they don't even have to be finite, e.g. you can have $m_8 = \infty$. $\circ$

There are examples of moments belonging to inequivalent distributions.

Example. The moments $m_n = e^{n^2}$ are moments of more than 1 distribution. $\triangle$

[56]Melanie mentioned she's currently working on a problem where they have the moments of a distribution, but do not yet know the underlying distribution.

Remark 4.10.9. There are conditions other than Carleman's for uniqueness. However, there is no nice iff type result for knowing exactly when a set of moments fails the moment problem. ○

Note 12. By determining a distribution, we really mean determining a measure on $\mathbb{R}$.

Other kinds of moments Let's briefly mention other "moments" people consider on the real line.

Definition 4.10.10. The **factorial moments** (or **falling moments**), indexed by $r \in \mathbb{N}$, are

$$\mathbb{E}((X)_r) = \mathbb{E}(X(X-1)\dots(X-r+1)).$$

◇

Example.

$$\begin{aligned} \mathbb{E}((X)_1) = \mathbb{E}(X) &= \mathbb{E}(X^1) \\ \mathbb{E}((X)_2) = \mathbb{E}(X(X-1)) &= \mathbb{E}(X^2) - \mathbb{E}(X^1) \end{aligned}$$

In general $\mathbb{E}((X)_r)$ is some precise linear combination of $\mathbb{E}(X^1), \dots, \mathbb{E}(X^r)$ and vice versa, so these falling moments contain the same information as the regular moments. △

Why use factorial moments sometimes and regular moments other times? Well, sometimes one is easier to work with than the other.

Example. If you have a Poisson distribution with parameter λ, then $\mathbb{E}((X)_r) = \lambda^r$ while $\mathbb{E}(X^r) = \lambda^r + blah$ is some more complicated polynomial in λ. △

The factorial moments are also nicer for binomial distributions. However, the regular moments are nicer for Gaussian distributions.

If you have a nice 1-1 function f, then you might also want to use $\mathbb{E}(f(X)^k)$ as your moments. These are a different type of thing as what is going on above, but the point is just that moments are meant to be nice, accessible invariants you can attach to your distribution (and maybe you hope they determine your distribution.

Here's yet another type of moment.

Definition 4.10.11. Say $X = (X_1, \dots, X_n) \in \mathbb{R}^n$ is some random value. Then one gets **mixed moments** indexed by $k_1, k_2, \dots, k_n \in \mathbb{N}^n$ and given by

$$\mathbb{E}(X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}).$$

◇

These have a similar theory surrounding the moment problem, e.g. if these are not too big then they satisfy uniqueness.

4.10.2 Our moments

Say X is a random group (e.g. finite abelian (ℓ-)group).

Definition 4.10.12. Given a (non-random) group A, the **Ath moment** of X is $\mathbb{E}(\#\operatorname{Sur}(X,A))$. $\diamond$

Of course, if you working with finite abelian ℓ-groups, then you probably want A to also be a finite abelian ℓ-group so that the moment is nonzero. However, this isn't too big a deal since if you throw in extra A's, then you just get some extra zero moments.

Example. If X is a random elementary ℓ-group (e.g. $\mathrm{Cl}_K[\ell]$), i.e. $X = (\mathbb{Z}/\ell\mathbb{Z})^m$ where $m \in \mathbb{N}$ random, then the moments are indexed by $(\mathbb{Z}/\ell\mathbb{Z})^k$ (equiv, indexed by $k \in \mathbb{N}$) and they are

$$\mathbb{E}\left(\#\operatorname{Sur}\left(X, \left(\frac{\mathbb{Z}}{\ell\mathbb{Z}}\right)^k\right)\right).$$

$\triangle$

One sometimes calls these the **Sur-moments**.

One can also consider the **Hom-moments** given by $\mathbb{E}(\#\operatorname{Hom}(X,B))$. The relationship between these and the sur moments is much like the relationship between the regular moments and the factorial moments in the classical setting (e.g. see last problem of HW1). This is because

$$\#\operatorname{Hom}(X,B) = \sum_{A\subset B} \#\operatorname{Sur}(X,A).$$

and so

$$\#\operatorname{Sur}(X,A) = \sum_{B\subset A} \mu(A,B)\#\operatorname{Hom}(X,B)$$

for some coefficients $\mu(A,B)$. Just like in the classical case, in practice, one uses whichever of the two of these gives less ugly looking results.

One can reasonably ask why we uses these functions for our moments. Consider again the finite abelian elementary ℓ-group case. Then,

$$\#\operatorname{Hom}\left((\mathbb{Z}/\ell\mathbb{Z})^m, (\mathbb{Z}/\ell\mathbb{Z})^k\right) = (\ell^m)^k$$

so if $X = (\mathbb{Z}/\ell\mathbb{Z})^k$, we have

$$\#\operatorname{Hom}(X, (\mathbb{Z}/\ell\mathbb{Z})^k) = |X|^k,$$

so this Hom-moment is literally the kth moment of the size of this group.

$$\mathbb{E}(\#\operatorname{Hom}(X, (\mathbb{Z}/\ell\mathbb{Z})^k)) = \mathbb{E}(|X|^k).$$

More generally, consider all finite abelian ℓ-groups. Pick a partition

$$\lambda : \lambda_1 \geq \lambda_2 \geq \cdots \geq 0 \text{ with } \lambda_i \in \mathbb{Z}_{\geq 0}.$$

Let λ' be the transpose (draw a Young tableau or whatever for λ and then λ' counts boxes in the columns). For such a partition, define

$$G_\lambda = \bigoplus_i \frac{\mathbb{Z}}{\ell^{\lambda_i}\mathbb{Z}}.$$

This gives a parameterization of all finite abelian ℓ-groups, and one finds that

$$\#\operatorname{Hom}(G_\lambda, G_\mu) = \ell^{\sum \lambda_i' \mu_i'}.$$

If we consider an alternate partition where $F_\lambda = G_{\lambda'}$, then we get

$$\#\operatorname{Hom}(F_\lambda, G_\mu) = (\ell^{\lambda_1})^{\mu_1}(\ell^{\lambda_2})^{\mu_2}\dots$$

and so the averages of these recover the classical mixed moments of $(\ell^{\lambda_1}, \ell^{\lambda_2}, \dots)$.

Question 4.10.13 (Audience)**.** *This formula is symmetric in λ and μ and so maybe equally motivates looking at $\#\operatorname{Hom}(A, X)$ and Inj-moments. Do people do this?*

Answer. Let's first contemplate why this formula is symmetric. Given A (finite abelian group) it has a (Cartier?) dual $A^\vee := \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(A, \mathbb{C}^\times)$. This is nice (e.g. $(A^\vee)^\vee \simeq A$ naturally), and

$$\operatorname{Hom}(A, B) \simeq \operatorname{Hom}(B^\vee, A^\vee)$$

as one would expect. Unnaturally, $A \cong A^\vee$ so $\operatorname{Hom}(B^\vee, A^\vee) \cong \operatorname{Hom}(B, A)$. From this point of view, you can always switch things with their duals, e.g.

$\#\operatorname{Sur}(X, B) = \#\operatorname{Inj}(B, X)$. That's weird

$$\operatorname{Sur}(X, B) \simeq \operatorname{Inj}(B^\vee, X^\vee).$$

So, formally, asking for Sur moments of a group is the same as asking for Inj-moments of dual group. $\star$

Let's continue with "why these moments?". The motivation we've given so far is dependent on encoding abelian groups in particular ways (e.g. encode $(\mathbb{Z}/\ell\mathbb{Z})^k$ as k vs. as ℓ^k). Other motivations include

- Our only actual theorem on class groups so far is on $\mathbb{E}(\#\operatorname{Sur}(\operatorname{Cl}_K, \mathbb{Z}/3\mathbb{Z}))$ (or $\mathbb{E}(\#\operatorname{Hom}(\operatorname{Cl}_K, \mathbb{Z}/3\mathbb{Z}))$ or $\mathbb{E}(\#\operatorname{Cl}_K[3])$). We don't, for example, have a result about $\mathbb{E}(\operatorname{rank}_3 \operatorname{Cl}_K)$.
- We'll see later that in the function field setting (over $\mathbb{F}_q[t]$), there are many theorems in the "large q limit" (as $q \to \infty$) about $\mathbb{E}(\#\operatorname{Sur}(\operatorname{Cl}_K, A))$ for all A.
- Empirically, $\mathbb{E}(\#\operatorname{Sur}(\operatorname{Cl}_K, A))$ converge (in X, the $\operatorname{Disc} K$ bound) faster than $\mathbb{P}(X \simeq A)$.

On the random group side, these moments are also nice (e.g. see HW3).

Example. Say $X = \operatorname{coker} M$ where $M \in M_{n\times n}(\mathbb{Z}_\ell)$ Haar random. Then, one has

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \sum_{f \in \operatorname{Sur}(\mathbb{Z}_\ell^n, A)} \mathbb{P}(f(M\mathbb{Z}_\ell^n) = 0).$$

Above, we're asking that each column of M vanishes under f. The columns e_i are from Haar measure on $\mathbb{Z}_\ell^n$ which pushes forward to the Haar measure on A (i.e. the uniform measure since A finite), so $f(e_i)$ uniform on A (i.e. is 0 with prob $1/\#A$). Hence,

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \frac{\#\operatorname{Sur}(\mathbb{Z}_\ell^n, A)}{|A|^n} \xrightarrow{n\to\infty} 1.$$

Using monotone convergence theorem, one then shows that if X is C-L, i.e. $\mathbb{P}(X \simeq A) = c/\#\operatorname{Aut} A$, then (take $u = 0$ on problem 2 on HW3)

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = 1.$$

This really tells you that you have picked the right moments for this problem since they're as simple as possible. △

Question 4.10.14 (Audience)**.** *In cases when you have uniqueness, do you use all the moments or can you throw out some of them?*

Answer. In general, you need to use all of them. There are some particular problems where you may only need a subset, but usually you want them all. We'll talk later about C-L moments determining the distribution, and there we'll need all of them. ⋆

Question 4.10.15 (Audience)**.** *We have a C-L distribution for imaginary quadratics and a separate C-L distribution for real quadratics. You could put these together by looking at quadratics with* $|\mathrm{Disc}| \leq X$*. Is the resulting distribution determined by its moments?*

Answer. Yes, as are the individual imaginary and real cases. We will see this later. ⋆

4.11 Lecture 11 (10/9)

5 minutes late

More moments stuff.

Example. Consider X with $\mathbb{P}(X \simeq A) = \frac{c}{|A|^u |\operatorname{Aut} A|}$ for $u \geq 0$ some integer. Then,

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \frac{1}{|A|^u}.$$

△

Example. Let X_n be the cokernel of a Haar random matrix from $\operatorname{Sym}_{n\times n}(\mathbb{Z}_\ell)$, symmetric $n \times n$ matrices.

$$\lim_{n\to\infty} \mathbb{E}(\#\operatorname{Sur}(X_n, A)) = \left|\bigwedge^2 A\right|$$

where $\bigwedge^2 A = A \otimes A / \langle a \otimes a \rangle$. These X_n have a limiting distribution X and the moments of this distribution are precisely this limit.

If $A = (\mathbb{Z}/\ell\mathbb{Z})^k$, for example, then $\left|\bigwedge^2 A\right| = \ell^{\binom{k}{2}}$. △

Example. X_n Haar random from $\operatorname{Alt}_{n\times n}(\mathbb{Z}_\ell)$, alternating matrices. Then,

$$\lim_{n\to\infty} (\#\operatorname{Sur}(X - n, A)) = \left|\operatorname{Sym}^2 A\right|.$$

If $A = (\mathbb{Z}/\ell\mathbb{Z})^k$, for example, then $\left|\operatorname{Sym}^2 A\right| = \ell^{k(k+1)/2}$. △

4.11.1 Another model

Consider $F \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ "Haar" random matrix.

Recall 4.11.1. In the function field case, with respect to the Weil pairing, we have $\mathrm{Frob} \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$. $\odot$

Recall 4.11.2. If W is an alternating perfect pairing, we say $\varphi \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ if $W(\varphi x, \varphi y) = qW(x, y)$. $\odot$

Sp is invariant. GSp is scales by some constant. $\mathrm{GSp}^{(q)}$ is scales by q

Remark 4.11.3. We had "Haar" if parentheses before. This is because $\mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ is not a group, but is a coset of $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$, so we really use the Haar measure on $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$. Note that Haar measures on profinite groups are very concrete; this is just the uniform measure mod ℓ^k for each k. $\circ$

Should this say GSp instead of Sp?

In this setup, we want to consider $X = \operatorname{coker}(1 - F)$. This was our model in the function field case. What are its moments? It will take us a while in class to do this, but in the grand scheme of things, this is not so bad.

We start with linearity of expectation:

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \sum_{f \in \operatorname{Sur}(\mathbb{Z}_\ell^{2n}, A)} \mathbb{P}\left(f((1-F)\mathbb{Z}_\ell^{2n}) = 0\right)$$

We want $f \circ (1 - F) = 0 \iff f = fF$, so here's another perspective. $\mathrm{GSp}_{2n}(\mathbb{Z}_\ell)$ acts on $\operatorname{Sur}(\mathbb{Z}_\ell^{2n}, A)$ by composition, and so we're summing over F-fixed points of this action.

Let's explore a general fact about fixed points of random permutations.

Slogan.

$$\mathbb{E}(\#\text{fixed points}) = \#\text{orbits}$$

Let G be a group with Haar *probability* measure acting on a finite set S. Let $g \in G$ be a random element from this Haar measure, and let $s \in S$. Then,

$$\mathbb{P}(gs = s) = \mathbb{P}(g \in \operatorname{Stab} s) = |G : \operatorname{Stab} s|^{-1} = \frac{1}{|Gs|}$$

where we've used that G partitions into cosets of $\operatorname{Stab} s$. Hence,

$$\mathbb{E}(\# s \in S \text{ fixed by } g) = \sum_s \frac{1}{\# Gs} = \#\text{orbits of } G \text{ on } S.$$

In our current application, we need to be a little more careful since we don't have an actual Haar random measure, but this coset measure instead.

So consider G, S as above, $H \subset G$ a subgroup and a fixed $g_0 \in G$. Let μ_0 be the "Haar probability measure" on the coset $g_0 H$, and let μ be the actual Haar measure on H. We want to know

$$\mu_0(\operatorname{Stab} s \cap g_0 H) := \mu(g_0^{-1} \operatorname{Stab} s \cap H).$$

Let $s' = g_0^{-1} s_0$ so $g_0^{-1} \operatorname{Stab} s$ is the set of elements taking $s \mapsto s'$. We want to know the measure of these elements in H. There are two things that could happen.

(1) If there exists $h \in H$ such that $hs = s'$, then $g_0^{-1} \operatorname{Stab} s = h \operatorname{Stab} s$, and so translation invariance would tell us that
$$\mu(h \operatorname{Stab} s \cap H) = \mu(\operatorname{Stab} s \cap H) = \frac{1}{\# Hs}.$$

(2) If there is no $h \in H$ such that $hs = s'$, then $g_0^{-1} \operatorname{Stab} s \cap H = \emptyset$, and so has measure 0.

In conclusion, summing these up, we see that

$$\mathbb{E}(\#\text{fixed points of } g_0 h \text{ in } S) = \#\text{orbits of } H \text{ on } S \text{ that are fixed (setwise) by } g_0.$$

where h is Haar random from H.

Back to the problem at hand. From the aside, we see that

$$\mathbb{E}(\# \operatorname{Sur}(\operatorname{coker}(1-F), A)) = \mathbb{E}(\# F \text{ fixed } \operatorname{Sur}(\mathbb{Z}_\ell^{2n}, A)) = \#\text{orbits of } \operatorname{Sp}_{2n}(\mathbb{Z}_\ell) \text{ on } \operatorname{Sur}(\mathbb{Z}_\ell^{2n}, A) \text{ fixed by } g_0 \in \operatorname{GSp}^{(q)}$$

The first equality is because a surjection $\operatorname{coker}(1-F) \twoheadrightarrow A$ is the same thing as a surjection $\varphi : \mathbb{Z}_\ell^{2n} \twoheadrightarrow A$ with $\varphi = \varphi F$. Hence, we are reduced to a linear algebra question.

Question 4.11.4. *What are the orbits of* $\operatorname{Sp}_{2n}(\mathbb{Z}_\ell)$ *on* $\operatorname{Sur}(\mathbb{Z}_\ell^{2n}, A)$*?*

Recall that Friedman-Washington had considered a different model where $F \in \operatorname{GL}_n(\mathbb{Z}_\ell)$ instead, so one might also be interested in the simpler question

Question 4.11.5. *What are the orbits of* $\operatorname{GL}_n(\mathbb{Z}_\ell)$ *on* $\operatorname{Sur}(\mathbb{Z}_\ell^{n}, A)$*?*

Answer. There is only 1 orbit (when $n \geq \operatorname{rank}_\ell A$).[57] $\star$

Corollary 4.11.6. $\mathbb{E}(\# \operatorname{Sur}(\operatorname{coker}(1-G), A)) = 1$ *if G Haar random from* $\operatorname{GL}_n(\mathbb{Z}_\ell)$ *(when $n \geq \operatorname{rank}_\ell A$), so this is another matrix model giving the C-L distribution in the limit.*

That was a nice short tangent, but let's finish up what we started. Write $V = \mathbb{Z}_\ell^{2n}$ so we can think of W as an alternating element of $V \otimes V$,[58] and the symplectic group is matrices preserving this element. Given $f : V \to A$, we can consider $(f \otimes f)(W) \in A \otimes A$ to get a map $\operatorname{Sur}(V, A) \to A \otimes A$ landing in the subgroup of alternating elements, generated by $x \otimes y - y \otimes x$. If $\varphi \in \operatorname{Sp}(V)$, then $\varphi \otimes \varphi(W) = W$, so the map $\operatorname{Sur}(V, A) \to \bigwedge_2 A \subset A \otimes A$ is constant on $\operatorname{Sp}(V)$-orbits (where $\bigwedge_2 A \simeq \bigwedge^2 A$ is the subgroup generated by $x \otimes y - y \otimes x$).

Proposition 4.11.7. *This map is a bijection from* $\operatorname{Sp}(V)$*-orbits to* $\bigwedge_2 A$*.*

Corollary 4.11.8. $\mathbb{E}(\# \operatorname{Sur}(\operatorname{coker}(1-G), A)) = \left|\bigwedge^2 A\right|$ *if G Haar random from* $\operatorname{Sp}_{2n}(\mathbb{Z}_\ell)$ *(when $2n \geq \operatorname{rank}_\ell A$).*

We wanted to know not about the orbits of $\operatorname{Sp}(V)$, but about the orbits of $\operatorname{Sp}(V)$ that are fixed by an element $g_0 \in \operatorname{GSp}^{(q)}$. By definition, $g_0 \otimes g_0(W) = qW$, so the orbits of Sp fixed by g_0 correspond exactly to the elements of $\bigwedge^2 A$ fixed by q, i.e. we want $b \in \bigwedge^2 A$ such that $b \in \left(\bigwedge^2 A\right)[q-1]$.

[57] I think I may have really overcomplicated that homework problem

[58] Technically, more natural to think of it as an element of $(V \otimes V)^\vee$. However, W was a perfect pairing so it gives an iso $V \xrightarrow{\sim} V^\vee$ and hence we can also think of it as an element of $V \otimes V$

Proposition 4.11.9. $\mathbb{E}(\#\operatorname{Sur}(\operatorname{coker}(1-G),A)) = \left|\bigwedge^2 A[q-1]\right|$ *if G Haar random from* $\mathrm{GSp}_{2n}^{(q)}$ *(when $2n \ge \operatorname{rank}_\ell A$). In particular, if $\ell \nmid (q-1)$, then there is no $(q-1)$-torsion, so this is 1, and we recover the C-L distribution in the limit.*

Question 4.11.10 (Audience)**.** *Is there any intuition for why these moments depend on n in the arithmetic case, but not in the geometric case (up to needing n to be big enough)?*

Answer. Ultimately, in the geometric case, this is coming from the connection to the number of orbits which is always an integer. Like, in the arithmetic-inspired setting we got sequences like

$$\frac{\#\operatorname{Sur}(\mathbb{Z}_\ell^n, A)}{|A|^n} \xrightarrow{n\to\infty} 1,$$

but in this geometric-inspired setting, we have integer valued distributions. Hence, in order to have limiting behavior they need to look something like

$$\begin{cases} 1 & \text{if } \operatorname{rank}_\ell A \le n \\ 0 & \text{otherwise.} \end{cases} \xrightarrow{n\to\infty} 1.$$

⋆

4.12 Lecture 12 (10/14)

4.12.1 Uniqueness of C-L Moments

Much of last time was spent analyzing the moments of one particular matrix model. So far in this class, we have seen at least 3 random matrix models with

$$\lim_{n\to\infty} \mathbb{E}(\#\operatorname{Sur}(\operatorname{coker} M_n, A)) = 1$$

for all finite abelian ℓ-groups A.

- $M_n \in M_{n\times n}(\mathbb{Z}_\ell)$ Haar-random
- $M_n \in I - \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ "Haar"-random (when $\ell \nmid (q-1)$)
- $M_n \in M_{n\times n}(\mathbb{Z}_\ell)$ with independent entries not too concentrated (the universality result)
- $M_n \in I - \mathrm{GL}_n(\mathbb{Z}_\ell)$ "Haar"-random

These are different distribution, but their cokernels all have the same limiting moments.

This returns us to the moment problem. Do their cokernels necessarily have the same limiting distributions?

For now, let's ignore the analytic issues with letting $n \to \infty$. Our main question this lecture is the following.

Question 4.12.1. *If X is a random finite abelian ℓ-group with*

$$\mathbb{E}(\#\operatorname{Sur}(X,A)) = 1$$

for all A a finite abelian ℓ-group, is

$$\mathbb{P}(X \simeq A) = \frac{c}{\#\operatorname{Aut} A}?$$

For simplicity, let's stick with elementary ℓ-groups (i.e. ℓ-torsion groups).

Remark 4.12.2. If X is any finite abelian ℓ-groups, then $X/\ell X$ is an elementary ℓ-group and

$$\#\operatorname{Sur}(X, (\mathbb{Z}/\ell\mathbb{Z})^k) = \#\operatorname{Sur}(X/\ell X, (\mathbb{Z}/\ell\mathbb{Z})^k),$$

so by focussing on elementary ℓ-groups we're just considering one class of Sur-moments (or just considering $X/\ell X$). ○

Recall that for a random elementary ℓ-group X, we have

$$\mathbb{E}(\#\operatorname{Hom}(X, (\mathbb{Z}/\ell\mathbb{Z})^k)) = \mathbb{E}(|X|^k).$$

Note that since X is a random elementary ℓ-group, it is determined by its size, so we can think of X has a random number and these are just usual moments. This will let us use what we already know about uniqueness of ordinary moments.

Note that if $\mathbb{E}(\#\operatorname{Sur}(X, A)) = 1$ for all A, then $\mathbb{E}(\#\operatorname{Hom}(X, A))$ is equal to the number of subgroups of A (since every homomorphism is a surjection onto a subgroup + linearity of expectation). In particular,

$$\mathbb{E}(|X|^k) = \#\text{subspaces of } \left(\frac{\mathbb{Z}}{\ell\mathbb{Z}}\right)^k.$$

Example. How many dim $k/2$ subspaces are there? Count full rank $k/2 \times k$ matrices. There are $\ell^{k^2/2}$ matrices, so the number of which that are full rank is

Can't remember if it is a plus or a minus

$$\ell^{k^2/2}(1 - q^{-k})(1 - \ell^{-(k\pm 1)})\dots.$$

We're overcounting so need to divide by $\#\operatorname{GL}_{k/2}(\mathbb{Z}/\ell\mathbb{Z})$ to account for the number of bases of a subspace. You end up with something like $\ell^{k^2/4}$. Recall our moment problem results from before, this is (precisely) too big to guarantee uniqueness. △

It is a genuinely true fact that there are random $Y \in \mathbb{R}$ from *different distributions* with $\mathbb{E}(Y^k) = \#$ subspaces of $(\mathbb{Z}/\ell\mathbb{Z})^k$.

However, we do not care about random real numbers. We care about distributions of (sizes of) elementary abelian ℓ-groups (i.e. powers of ℓ). Now, we basically just have a linear algebra problem.

Consider some random $n \in \mathbb{Z}_{\geq 0}$ such that $\mathbb{E}(\#\operatorname{Sur}(\mathbb{F}_\ell^n, \mathbb{F}_\ell^k)) = 1$, i.e.

$$\sum_{a \geq 0} \mathbb{P}(n = a) \cdot \#\operatorname{Sur}(\mathbb{F}_\ell^a, \mathbb{F}_\ell^k) = 1.$$

The values 1 and $\#\operatorname{Sur}(\mathbb{F}_\ell^a, \mathbb{F}_\ell^k)$ are given/fixed, so we are just attempting to solve a linear equation in the countably many variables $\mathbb{P}(n = a)$ (for $a \geq 0$). We know one solution already. Are there more?

4.12.2 Linear Algebra

Consider a matrix $M = (m_{ij})_{i,j=0}^{\infty} \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}}$ and a vector $b = (b_i)_{i=0}^{\infty} \in \mathbb{R}^{\mathbb{N}}$.

Question 4.12.3. *Given M, b, is there a unique x such that $Mx = b$?*

There are some things we need to worry about when trying to answer these questions.

Warning 4.12.4. We can't multiply arbitrary matrices (even when dimensions match up). That is, Mx or MN (with $x \in \mathbb{R}^{\mathbb{N}}$ and $N \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}}$) might not exist. They involve infinite sums which just may not converge. •

Warning 4.12.5. Even when $M(NP)$ and $(MN)P$ both exist, they may not be equal. The difference between these two involves changing an order of summation in infinite sums which is not always allowed. •

This is why people doing infinite-dimensional linear algebra usually study Hilbert spaces or Banach space or whatever and only consider bounded linear operators and then, you know, things are nice. Sadly for us, our problem appeared in the guise of purely algebraic infinite-dimensional linear algebra.

Suppose that M is invertible, i.e. exists $N \in \mathbb{R}^{\mathbb{N}\times\mathbb{N}}$ such that $NM = MN = \mathrm{Id}$. If

- Nb exists, and
- $M(Nb)$ exists, and
- $(MN)b = M(Nb)$

then $x = Nb$ is a solution to $Mx = b$ (so we get existence). What about uniqueness? If $Mx = b$ is a solution and

- Nb exists, and
- $(NM)x = N(Mx)$

then $x = Nb$ (since $x = \mathrm{Id}\, x = (NM)x = N(Mx) = Nb$), so we get uniqueness in this case.

In summary, for invertible M, small enough $b \implies \exists$ a solution where "small enough" means e.g. that

$$\sum_k |N_{jk}|\,|b_k|\,, \sum_{j,k} |M_{ij}|\,|N_{jk}|\,|b_k| < \infty$$

the relevant sums converge absolutely (this is not necessary, but it suffices). In general, there is no uniqueness.

However, one may still ask for uniqueness of small solutions where "small" may mean, for example, that

$$\sum_{j,k} |M_{ij}|\,|N_{jk}|\,|b_k| < \infty.$$

Under this particular definition of small, one indeed gets $(NM)x = N(Mx)$, and so we would have a unique small solution.

4.12.3 Back to the Moments Problem

The upshot of the previous section is that for invertible M, one gets uniqueness of small solutions. So, is our M invertible?

Recall 4.12.6. We want to solve $\sum_{a\geq 0}\mathbb{P}(n=a)\cdot \#\operatorname{Sur}(\mathbb{F}_\ell^a,\mathbb{F}_\ell^k)=1$ for all k, so $x_a=\mathbb{P}(n=a)$, $m_{ka}=\#\operatorname{Sur}(\mathbb{F}_\ell^a,\mathbb{F}_\ell^k)$ and $b_k=1$. ⊙

Well, it is at least upper triangular since $\#\operatorname{Sur}(\mathbb{F}_\ell^n,\mathbb{F}_\ell^k)=0$ if $n<k$. Hence, our equations look like

$$\begin{array}{ccccccccc} m_{00}x_0 & + & m_{01}x_1 & + & m_{02}x_2 & + & \dots & = & b_0 \\ & & m_{11}x_1 & + & m_{12}x_2 & + & \dots & = & b_1 \end{array}$$

Note that in the infinite case, upper/lower triangular are different. A lower triangular system looks like

$$\begin{array}{ccccc} m_{00}x_0 & & & = & b_0 \\ m_{10}x_0 & + & m_{11}x_1 & = & b_1 \end{array}$$

and so on, which is easy to solve.

Let's assume that $m_{ii}\neq 0$.[59] By analogy with the finite dimensional case, we hope this will suffice for our matrix to be invertible. For simplicity, we can scale each row (equation) to assume that $m_{ii}=1$.

Proposition 4.12.7. *For M upper triangular with $m_{ii}=1$ for all i, there exists an N such that $NM=MN=1$.*

Proof. Consider $N=1+(1-M)+(1-M)^2+(1-M)^3+\dots$ " $=$ " $\frac{1}{1-(1-M)}$. We need to show this exists. Note that AT always exist for any matrix A and any upper triangular matrix T since all the sums involved are finite; in particular, $1-M$ is (strictly) upper triangular, so the powers $(1-M)^n$ all exist. In fact, $(1-M)^n$ is *n-strictly upper triangular*, i.e. the i,j entry is 0 if $j\leq i+n$ (up to typos), so each entry of N only sees contributions from finitely many of the summands. Thus, N exists.

One can multiply NM,MN and telescope to see that $NM=\mathrm{Id}=MN$. Keep in mind that every entry only involves finitely many summands. ■

For our M with
$$M_{ij}=\frac{\#\operatorname{Sur}(\mathbb{F}_\ell^j,\mathbb{F}_\ell^i)}{\#\operatorname{Sur}(\mathbb{F}_\ell^i,\mathbb{F}_\ell^i)},$$
we have invertibility and so uniqueness of small solutions. Actually, we wanted uniqueness of non-negative solutions x, i.e. $x_k\geq 0$. Since our M_{ij} are positive, (b small and all $x_k\geq 0$) $\implies$ x small, e.g. since $|x_k|\leq b_k$ (recall we have 1's on the diagonal and $M_{ij}\geq 0$ always).

Thus, when M is invertible with non-negative entries, for small enough b, we have uniqueness of non-negative solutions x.

Question 4.12.8 (Audience)**.** *Our uniqueness criteria were associativity conditions. Our matrix M and desired solutions x all have non-negative entries and infinite sums of non-negative numbers are always associative. Could we have used this to get uniqueness without needing to talk about this notion of smallness?*

[59] In our case $m_{ii}=\#\operatorname{Sur}(\mathbb{F}_\ell^i,\mathbb{F}_\ell^i)=\#\operatorname{GL}_i(\mathbb{F}_\ell)\neq 0$

Answer. Almost, but not quite. You have to remember that N is involved as well, and this matrix has negative entries. ⋆

Question 4.12.9 (Audience)**.** *Can we say anything about uniqueness of N?*

Answer. *I missed most of the answer to this one, but I think the takeaway was that this is similar to asking about uniqueness of solutions (think $MN = \mathrm{Id}$ as a system of equations) and we should not expect unique inverses in general* ⋆

So we have unique non-negative solutions when our desired "moments" b are small.

Remark 4.12.10. This is maybe reminiscent of the fact that we expect uniqueness of moments when they are small, but not when they are big. ○

What exactly is small enough? This depends on M (in upper Δ case; in general, would depend on N too). A sufficient condition will be of the form $\sum_k c_k |b_k| < \infty$ where $c_k \geq 0$ are given as functions of M.

Here's one version of a uniqueness-type result:

Theorem 4.12.11 (Wood)**.** *There is at most one distribution on random elementary ℓ-groups such that $\mathbb{E}(\#\operatorname{Sur}(X, A)) = b_A$ for $|b_A| = O(\# \bigwedge^2 A)$, i.e. when $A = \mathbb{F}_\ell^k$ we have $b_A = O\left(\ell^{\frac{k(k-1)}{2}}\right)$.*

For example, $b_k = 1$ satisfies this

This answers our original question since it gives uniqueness of distributions with Cohen-Lenstra moments. This means that we expect our M_n matrices from the beginning to have the same limiting distributions. However, before we can conclude this, we would have to deal with some analytic issues. The problem is that we simply wrote down sequences of distributions, so we'd need to make sure their "limits" make sense.

Next time we'll talk about the extent to which this is optimal.

4.13 Lecture 13 (10/21)

5 minutes late

4.13.1 Moment Problem

Theorem 4.13.1. *If X and Y are random finite abelian groups such that for all A,*

$$\mathbb{E}(\#\operatorname{Sur}(X, A)) = \mathbb{E}(\#\operatorname{Sur}(Y, A)) \leq \left|\bigwedge^2 A\right|,$$

then X and Y have same distribution.

Can extend this to profinite abelian groups with finite Sylow-p subgroups, i.e to $\prod_p G_p$ with G_p the set of finite abelian p-groups.

Example.

- $X \sim$ "$\frac{c}{\#\operatorname{Aut} A}$" distribution $\mathbb{E}(\#\operatorname{Sur}(X, A)) = 1$
- $X \sim \frac{c}{|A|\#\operatorname{Aut} A}$ distribution $\mathbb{E}(\#\operatorname{Sur}(X, A)) = |A|^{-1}$
- $X_n = \operatorname{coker} S_n$ with $S_n \in \operatorname{Sym}_{n\times n}(\mathbb{Z}_\ell)$ Haar. Then, $\lim\limits_{n\to\infty} X_n$ has moments $\left|\Lambda^2 A\right|$.

- $X_n = \operatorname{coker}(1 - G_n)$ with $G_n \in \mathrm{GSp}_{2n}^{(q)}(\mathbb{Z}_\ell)$ Haar random. Then, the Ath moment $\to \left|\Lambda^2 A[q-1]\right|$ so if $q = 1$, then $G_n \in \mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$ and the Ath moment approaches $\left|\Lambda^2 A\right|$.

△

Note that, while the last two examples have the same "limiting distributions" by this theorem, they are not the same at an particular distributions. Recall that in the symmetric case, we have

$$\mathbb{E}(\#\operatorname{Sur}(\operatorname{coker} S_n, A)) = \frac{\#\operatorname{Sur}(\mathbb{Z}_\ell^n, A)}{|A|^n}\left|\Lambda^2 A\right|$$

whereas in the 1-symplectic case, we have

$$\mathbb{E}(\#\operatorname{Sur}(\operatorname{coker}(1 - G_n), A)) = \left|\Lambda^2 A\right| \quad \text{when } \; n \gg 0,$$

so these differ for any finite n, but agree in the limit.

What happens when we go past this bound? Let $A_n \in \mathrm{Alt}_{n\times n}(\mathbb{Z}_\ell)$ be a Haar random skew-symmetric matrix (so 0's on the diagonal among other things).

Remark 4.13.2. The notion of skew-symmetric does not depend on a choice of basis. Think of the matrix as a map

$$\mathbb{Z}_\ell^n \otimes \mathbb{Z}_\ell^n \longrightarrow \mathbb{Z}_\ell$$

with skew-symmetric meaninig $x \otimes x \mapsto 0$. ○

What are the moments of $\operatorname{coker} A_n$?

- $\sum_{f\in \operatorname{Sur}(\mathbb{Z}_\ell^n, A)} \mathbb{P}(f(A_n) = 0)$
- Choose basis so

$$\ker f = \begin{pmatrix} \ell^{a_1} \\ \vdots \\ \ell^{a_n} \end{pmatrix} \subset \mathbb{Z}_\ell^n$$

  with $a_1 \geq a_2 \geq \ldots$.
- Note that Haar measure is the same as picking (strictly) upper triangular entries independently Haar in $\mathbb{Z}_\ell$ (this is translation invariant)
- $\mathbb{P}(f(A_n) = 0)$ is the probability that the i row is divisible by ℓ^{a_i}. By previous bullet point this is

In ith row, only $n-i$ entries left you care about

$$(\ell^{-a_1})^{(n-1)}(\ell^{-a_2})^{n-2}\cdots = \ell^{a_1}\ell^{2a_2}\ell^{3a_3}\cdots = \frac{\left|\operatorname{Sym}^2 A\right|}{|A|^n}.$$

-
$$\mathbb{E}(\#\operatorname{Sur}(\operatorname{coker} A_n), A) = \frac{\#\operatorname{Sur}(\mathbb{Z}_\ell^n, A)}{|A|^n}\left|\operatorname{Sym}^2 A\right|.$$

  This is bigger than $\left|\bigwedge^2 A\right|$ (in the limit)

Example. If $A = \mathbb{F}_\ell^k$, then $\left|\bigwedge^2 A\right| = \ell^{\binom{k}{2}}$ while $\left|\operatorname{Sym}^2 A\right| = \ell^{\frac{k(k+1)}{2}} = \ell^{\binom{k}{2}+k}$. △

Here's a fact that will soon be useful.

Fact. The rank of a skew-symmetric (really, alternating) matrix is always even. Can put an alternating form in the standard form

$$\begin{pmatrix} 0 & I_{n,m} \\ -I_{n,m} & 0 \end{pmatrix}$$

I'm not 100% both of these n, m's should be the same

with $I_{n,m} = \operatorname{diag}(1, \ldots, 1, 0, \ldots, 0)$ via change of basis.

Note that $\operatorname{rank}_\ell \operatorname{coker} A_n = n - \operatorname{rank} A_n$, so $n - \operatorname{rank}_\ell \operatorname{coker} A_n$ is always even. That is, when n is even, this construction gives us all even rank groups, and when n is odd, it gives us all odd rank groups. In fact, these A_n are all singular over $\mathbb{Q}_\ell$ for n odd (i.e. $\det A_n = 0$), so $\operatorname{coker} A_n = \mathbb{Z}_\ell \times \text{torsion}$. This is not too bad; we can take $(\operatorname{coker} A_n) \otimes \mathbb{Z}/\ell^5\mathbb{Z}$ or whatever to deal with this. As $n \to \infty$,

$$\lim_{n\to\infty} \mathbb{E}(\# \operatorname{Sur}(\operatorname{coker} A_n, A)) = \begin{cases} \left|\operatorname{Sym}^2 A\right| & \text{if } \ell^5 A = 0 \\ 0 & \text{otherwise.} \end{cases}$$

However, we have this weird phenomenon. $\operatorname{coker} A_{2n}$ gives even rank groups while $\operatorname{coker} A_{2n+1}$ gives odd rank groups. These have the same moments in the limit, but they cannot give the same limiting distribution! In particular, the $\lim\limits_{n\to\infty} \operatorname{coker} A_n$ does not exist; there is no limiting distribution here since we're flipping between all odd-rank groups and all even-rank groups.

One can show that the limit distributions

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{coker} A_{2n} \simeq A) \text{ and } \lim_{n\to\infty} \mathbb{P}(\operatorname{coker} A_{2n+1} \simeq A)$$

both exist. You just write down explicit formulas for these probabilities.

These are not random distributions. They are the predicted distributions for $\operatorname{Sel}_{\ell^\infty}$ of elliptic curves $/\mathbb{Q}$ for rank 0 and rank 1 curves, respectively (conjecture of Poonen-Rains and extended by Bhargava-Kane-Lenstra). This is an area of arithmetic statistics we have not talked about. The idea is to write down elliptic curves

$$E_{A,B} : y^2 = x^3 + Ax + B$$

and then one has $\operatorname{rank}_\ell \operatorname{Sel} = \operatorname{rank}_\ell E + \operatorname{rank}_\ell Ш$ (and $\operatorname{rank}_\ell Ш$ is even or expected to be even). Hence, the parity of $\operatorname{rank}_\ell \operatorname{Sel}$ depends on that of $\operatorname{rank}_\ell E$, so one wants distributions that either always give odd-rank groups or even-rank groups depending on $\operatorname{rank}_\ell E$. These two $\operatorname{coker} A_n$ distributions turn out to be good candidates.

Remark 4.13.3. Can prove uniqueness right up to $\left|\operatorname{Sym}^2 A\right|$ boundary, e.g. for elementary ℓ-groups one has uniqueness when

$$\left(\frac{\mathbb{Z}}{\ell\mathbb{Z}}\right)^k \text{ moment} \le \ell^{k^2/2 + \frac{(1-\varepsilon)k}{2}}$$

for some $\varepsilon > 0$, one still gets uniqueness. ○

Question 4.13.4. *If we have a sequence X_n with*

$$\lim_{n\to\infty} \mathbb{E}(\# \operatorname{Sur}(X_n, A))$$

known (e.g. these limiting moments always 1), does that imply that $\lim_{n\to\infty} X_n$ *(i.e.* $\lim_{n\to\infty} \mathbb{P}(X_n \simeq A)$*) exist and is the distribution with these moments?*

Answer. We saw above that the answer is no in general. We saw the coker A_n example. In fact, whenever there are ≥ 1 distributions with the same moments, then of course limit moments $\not\Rightarrow$ limit distribution, e.g. take

$$X_n = \begin{cases} Y_0 & \text{if } n \text{ even} \\ Y_1 & \text{otherwise.} \end{cases}.$$

If Y_0, Y_1 have the same moments, then the limit moments of X_n exist, but there is no limit distribution. $\star$

Remark 4.13.5. In arithmetic statistics, we can interested in

$$X_Z = \mathrm{Cl}_{\text{uniform random } K \text{ w/ } |\mathrm{Disc}\, K| \leq Z} \quad \text{as} \quad Z \to \infty,$$

so we are really interested in (existence of) limits of distributions. $\circ$

Since we really want to guarantee limiting distributions, let's restrict ourselves to the $\left|\bigwedge^2 A\right|$ bound on moments, and now ask this same question.

Example. Take X real quadratic C-L group, so

$$\mathbb{P}(X \simeq A) = \frac{c}{|A|\,|\mathrm{Aut}\, A|} \quad \text{and} \quad \mathbb{E}(\#\,\mathrm{Sur}(X, A)) = \frac{1}{|A|}.$$

Consider the random groups $X_n = X \times \mathbb{Z}/p_n\mathbb{Z}$ where p_n is the nth prime. Then, (A a finite abelian group)

$$\lim_{n\to\infty} \mathbb{E}(\#\,\mathrm{Sur}(X_n, A)) = \frac{1}{|A|}$$

Once, $p_n > |A|$ (of even just larger than any prime dividing size of A), we have $\mathrm{Sur}(X, A) = \mathrm{Sur}(X_n, A)$. Unfortunately though,

$$\lim_{n\to\infty} \mathbb{P}(X_n \simeq B) = 0$$

by the same reasoning. We have total escape of mass. Could have done this $X \times \mathbb{Z}/p_n\mathbb{Z}$ trick only with probability δ in order to have δ escape of mass instead. $\triangle$

This shows that uniqueness in the moment problem + limit moments $\not\Rightarrow$ limit distribution is as expected.

Question 4.13.6. *What if one also requires that the limit distribution exists and is a probability distribution (i.e. total measure* 1*)?*

This is a natural, interesting analytic question without an immediate answer, but it is not super relevant to arithmetic statistics. In practice in arithmetic statistics, we do not know the hypothesis of this question to be the case, so this question does not often come up.

Theorem 4.13.7. *For* X, Y_n *random finite abelian* ℓ*-groups. If for all* A

$$\mathbb{E}(\#\,\mathrm{Sur}(X, A)) = \lim_{n\to\infty} \mathbb{E}(\#\,\mathrm{Sur}(Y_n, A)) \leq \left|\bigwedge^2 A\right|,$$

then $\lim_{n\to\infty} \mathbb{P}(Y_n = B) = \mathbb{P}(X \simeq B)$ *for all* B.

Corollary 4.13.8. *If*

$$\lim_{n\to\infty} \mathbb{E}(\#\operatorname{Sur}(Y_n, A)) = 1,$$

then

$$\lim_{n\to\infty} \mathbb{P}(Y_n \simeq B) = \frac{c}{\#\operatorname{Aut} B}.$$

Remark 4.13.9. In the world of finite abelian ℓ-groups we can't do this same trick of attaching on bigger and bigger groups without surjections. In fact, you can't play any trick at all since we have the above theorem. ∘

This kind of result has been used a lot in arithmetic statistics.

This will close our section on moments. What were the main takeaways?

- Can conveniently access distributions via their moments.
- Moments are number theoretically meaningful, e.g.

$$\operatorname{Sur}(\mathrm{Cl}_K, A) \leftrightarrow \text{unramified } A\text{-extensions of } K.$$

- $$\begin{tikzcd} L \arrow[d, dash, "A"', "\text{unram}"] \\ K \arrow[d, dash, "2"'] \\ \mathbb{Q} \end{tikzcd}$$

  gives correspondence

$$(K, \varphi \in \operatorname{Sur}(\mathrm{Cl}_K, A)) \leftrightarrow (A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z})\text{-extensions } L/\mathbb{Q} \text{ unramified above } L^A$$

  so understanding these surjections related to counting these extensions.

I missed what she said we are going to start talking about from now on.

Question 4.13.10. *Are all unramified extensions abelian?*

Answer. No. Really should have said A abelian up above. In fact, these days, Melanie is intrested in statistics of $G = \mathrm{Gal}(K^{\mathrm{ur}}/K)$ (so $G^{\mathrm{ab}} = \mathrm{Cl}_K$). ⋆

4.14 Lecture 14 (10/23): More function field stuff

Recall 4.14.1. $\mathrm{Pic}^0(C) \otimes \mathbb{Z}_\ell = \operatorname{coker}(1 - \mathrm{Frob}|_{T_\ell \operatorname{Jac}})$ with $\mathrm{Frob} \in \mathrm{GSp}^{(q)}(\mathbb{Z}_\ell)$. See Lemma 4.7.4. ⊙

Let $K/\mathbb{F}_q(t)$ be a finite extension, so K is the function field of a smooth, projective irreducible curve (dim 1 variety) over $\mathbb{F}_q$. Note that

$$\left\{\begin{matrix}\text{smooth, projective irred} \\ \text{curve over } \mathbb{F}_q\end{matrix}\right\} \xrightarrow{\sim} \left\{\begin{matrix} K/\mathbb{F}_q \text{ finitely generated} \\ \text{of transcendence degree } 1\end{matrix}\right\}$$

(via taking function fields) gives an equivalence of categories. Hence, $K/\mathbb{F}_q(t)$ finite is the same thing as a map $C_K \to \mathbb{P}^1_{\mathbb{F}_q}$ of curves.

4.14.1 Abelian extensions of K

$K/\mathbb{F}_q(t)$ finite as before. This is a global field, so one can still do class field theory. We have

J_K instead of C_K for adele class group since C_K is already the curve associated to K

$$\prod_v K_v^\times/K =: J_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

via the Artin map. Taking profinite completions induces

$$\widehat{J}_K \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

We can also think of this adele class group geometrically. Recall that the places of K correspond exactly to the closed points of the curve C_K (or to the $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ orbits of $\overline{\mathbb{F}}_q$ points of C_K).

Each place v has a **degree**

$$\deg v = \text{degree of reisude field over } \mathbb{F}_q = \text{size of } \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \text{ orbit}.$$

Abelian unramified extensions A finite abelian extension looks something like this

$$\prod_v K_v^\times/K^\times \longrightarrow A.$$

It its unramified, it kills inertia, so it factors through

$$\prod_v (K_v^\times/\mathscr{O}_v^\times)/K^\times \longrightarrow A.$$

Killing units in a local field just leaves you with powers of the uniformizer so the domain above is exactly

$$\prod_v \langle \pi_v \rangle /K^\times \simeq \mathrm{Pic}(C_K),$$

the **divisor class group**.

Hence, abelian unramified extensions of K correspond exactly to maps $\mathrm{Pic}(C) \to A$.

Recall 4.14.2. We have a degree map $\deg : \mathrm{Pic}(C) \to \mathbb{Z}$ sending $\pi_v \mapsto \deg v$ (so $\mathrm{Pic}(C)$ is infinite). ⊙

What are these degree extensions coming from $\mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$? We got them for free, so they should be simple.

Consider a field $K \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r} = K[x]/(f(s))$ with $f(s)$ the minimal polynomial of some element of $\mathbb{F}_{q^r}/\mathbb{F}_q$ (in particular, f has coefficients in $\mathbb{F}_q$). All finite extensions of K look like this, but not all of them come from a polynomial if $\mathbb{F}_q[t]$. Geometrically, this is performing the base change $C \rightsquigarrow C_{\mathbb{F}_q^r}$.

Melanie drew a picture, and at one point remarked, "It's crazy to draw pictures over $\mathbb{F}_q$, but it's also crazy to not draw pictures when you're doing algebraic geometry." (paraphrase) Of note, the curve $C_{\mathbb{F}_{q^r}}$ is not geometrically irreducible (even if it is irreducible) which can be annoying.

The upshot is that these free, degree extensions correspond to changing your base field. This sort of phenomenon is something you usually want to ignore/sweep under the rug.

If you recall, we decided way back when that the right analog of the class group is not the whole Picard group. We should instead study $\mathrm{Pic}^0(C) = \ker\left(\mathrm{Pic}(C) \xrightarrow{\deg} \mathbb{Z}\right)$. Even more specifically, in the imaginary quadratic case[60], we may want to look at $\mathrm{Pic}(C)/\infty \simeq \mathrm{Pic}^0(C)$, and in the real quadratic case[61], we may want to look at $\mathrm{Pic}(C)/(\infty_1, \infty_2) \simeq \mathrm{Pic}^0(C)/(\infty_1 - \infty_2)$. In either case, this is the affine class group $\mathrm{Cl}\,\mathscr{O}_K$.

Using class field theory, quotients of $\mathrm{Pic}(C)$ are more natural since their moments correspond to certain abelian unramified extensions.

Example. Looking at $\mathrm{Pic}(C)/v_0 \to A$ says that the uniformizer at v_0 (i.e. Frobenius there) must be 0, so these are abelian unramified extension with $\mathrm{Frob}(v_0) \mapsto 0$, i.e. v_0 is split completely. △

Question: Why does frob going to 0 mean it's split completely?

This is telling us that studying surjections from Pic/∞ or $\mathrm{Pic}/(\infty_1, \infty_2)$ is like looking at abelian unramified extensions split completely at places above $\infty \in \mathbb{P}^1$.

Now consider $\mathrm{Pic}(C)/\infty$ or $\mathrm{Pic}(C)/(\infty_1, \infty_2)$ for C hyperelliptic.

- These are finite groups
- Extensions split completely at ∞ (∞_1, ∞_2) have $\mathbb{F}_q$ points (since these ∞'s are $\mathbb{F}_q$-points themselves)[62], so these don't include the basechange examples we wanted to avoid.

Question 4.14.3. *How can one study* Pic/∞ *using geometry over* $\mathbb{F}_q$*?*

This is a tool not available in the number field case. We will talk about multiple ways to do this, but all of them are built on étale cohomology. We will use étale cohomology as a black box in this class; on Wednesday we'll give a quick intro to main features of étale cohomology.

4.14.2 Using Geometry over $\mathbb{F}_q$

The two main approaches to discuss are

- Deligne-Katz equidistribution
- Grothendieck-Lefschetz trace formula

Recall 4.14.4. Given a curve $C/\mathbb{F}_q$, we have $\mathrm{Frob} \curvearrowright T_\ell(\mathrm{Jac}(C)) \simeq \mathbb{Z}_\ell^{2g}$ allowing us to consider it as a matrix in $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$. We saw that "if Frob were Haar random in $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$ (and $\ell \nmid q-1$), then we get C-L distribution." This is a big "if" since Frob isn't really even random to begin with. ⊙

Instead of asking for Haar-randomness, we can ask for some concrete notion of equidistribution.

Definition 4.14.5. Given $F_1, F_2, \dots \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}_\ell)$, for each k look at

$$\overline{F}_1, \overline{F}_2, \dots \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/\ell^k\mathbb{Z}) \longleftarrow \text{finite.}$$

[60] $C \to \mathbb{P}^1$ of degree 2, ramified at ∞

[61] $C \to \mathbb{P}^1$ of degree 2, split at infinity

[62] There's another case: when $\infty \in \mathbb{P}^1$ is inert. In this case, the $\infty \in C$ is not an $\mathbb{F}_q$ point

We may define condition (*) to be that for all $h \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/\ell^k\mathbb{Z})$, we have

$$\lim_{X\to\infty} \frac{\#\{i \le X \mid \overline{F}_i = h\}}{X} = \frac{1}{\#\,\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/\ell^k\mathbb{Z})}.$$

$\diamond$

Remark 4.14.6. Having condition (*) for all k implies that $\operatorname{coker}(1-F_n)$ have C-L limit distribution, e.g. look at moments. $\circ$

Deligne-Katz equidistribution will give us $(*)$ for F_i's Frobenius of $T_\ell(\mathrm{Jac}(C_i))$ for C_i's in certain families over $\mathbb{F}_q$ with $q \to \infty$.

We'd want something like C_i all hyperelliptic curves over $\mathbb{F}_q$ (with q fixed), say ordered by genus. Instead, what we get is C_i all genus g (with fixed g) hyperelliptic over $\mathbb{F}_q$ (all q with $q \nmid \ell-1$, or arbitrarily large q).

We will talk more about the equidistribution theorem next Friday after getting some étale cohomology/fundamental groups tool on Wednesday. It sounds like it was work of Achtar which showed that the actual equidistribution theorem gives a result like what we claimed we get above.

Question 4.14.7 (Audience)**.** *What would equidistribution mean in the case he want with g varying since the underlying group changes?*

Answer. This is a good question. Hadn't thought about this since we don't have anything like that. It's not immediately clear what it should be. We do have q varying in the result we do get, but this is less problematic. You can relate $\mathrm{GSp}_{2g}^{(q)}$ and $\mathrm{GSp}_{2g}^{(q')}$ with $u \in \mathbb{Z}_\ell^\times$ and $1-q-u(1-q')$. $\star$

What about this Grothendieck-Lefschetz trace formula? What's it good for?

It let's us count $\mathbb{F}_q$ points on X by knowing enough about the étale cohomology of X. This approach to arithmetic statistics was pioneered by work of [Ellenberg-Venkatesh-Westerland]. The connection is that moments are related to certain $A \times_{-1} \mathbb{Z}/2\mathbb{Z}$ extensions, i.e. covers of $\mathbb{P}^1$, but these are $\mathbb{F}_q$ points on a moduli space of such covers, so now one can use étale cohomology to try to count points on this moduli space.

4.15 Lecture 15 (10/28)

We'll tell the story of étale fundamental groups and étale cohomology. We won't be that detailed, but it should help you feel more oriented if you ever decide to learn it more carefully.

4.15.1 Étale fundamental groups

Let X be a nice topological space, so it has a universal cover U, and $\pi_1(X) = \mathrm{Aut}(U/X)$, the group of covering automorphisms of $U \to X$. If one is being precise, X should be given a fixed basepoint, but meh.

path-connected, locally path-connected, and semilocally simply connected

U is universal in the sense that all connected covering spaces $Y \to X$ factor as $U \to Y \to X$. Just like in Galois theory, we can draw a diagram like

$$\begin{array}{ccc} U & & 1 \\ | & & | \\ Y & & \pi_1(Y) = \mathrm{Aut}(U/Y) \\ | & & | \\ X & & \pi_1(X) = \mathrm{Aut}(U/X) \end{array}$$

and the subgroups of $\pi_1(X)$ are in order-reversing correspondence with connected covering spaces. The normal subgroups correspond to quotients.

If G is a group, then normal G-covers correspond to surjections $\pi_1(X) \twoheadrightarrow G$.

There's an equivalence of categories underlying this

This is a quick rundown of the topological situation. In algebraic geometry, it is hard to deal with infinite covers, so we only consider the finite ones. We basically take the above as the definition of $\pi_1^{\text{ét}}(X)$.

Let X be a scheme (technically, it needs a geometric basepoint). Our "covers" will be étale morphisms. These are maps which

- are smooth of relative dimension 0
- satisfy an (infinitesimal) lifting property ("formally étale" + finite presentation)

From the category of étale morphisms to X, one defines $\pi_1^{\text{ét}}(X)$ so that its finite quotients are equivalent to finite, normal étale covers of X.

Example. Consider the map

$$\begin{array}{ccc} \mathbb{A}^1 & & x \\ \downarrow & & \downarrow \\ \mathbb{A}^1 & & x^2 \end{array}$$

This is étale when restricted to $\mathbb{A}^1 \setminus \{0\}$. This gives an étale map whose automorphism groups is $\mathbb{Z}/2\mathbb{Z}$. You can replace 2 with n to get a cover with automorphism group $\mathbb{Z}/n\mathbb{Z}$. In fact, $\pi_1(\mathbb{A}^1_{\mathbb{C}} \setminus \{0\}) = \widehat{\mathbb{Z}}$ (and possibly also over other algebraically closed fields) △

Example. When K is a perfect field, and finite extension is étale, so in this case $\pi_1(\operatorname{Spec} K) = \mathrm{Gal}(\overline{K}/K)$. △

Warning 4.15.1. étale morphisms are unramified, which maybe seems counter to the last example, e.g. since it's claiming "$\mathbb{Q}(i)/\mathbb{Q}$ is étale" even though one may say that "$\mathbb{Q}(i)/\mathbb{Q}$ is ramified at 2." There's no contradiction since when we say "ramified at 2" we really mean the extension $\operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$ of number fields is ramified at $(2) \in \operatorname{Spec} \mathbb{Z}$. •

Example. $\pi_1(\operatorname{Spec} \mathscr{O}_K) = \mathrm{Gal}(K^{\text{un}}/K)$ where K^{un} is the maximal unramified extension of the number field K. In other words, étale $Y \to \operatorname{Spec} \mathscr{O}_K$ corresponds to rings of integers in "unramified" extensions L/K. △

This gives algebraic geometry a notion of fundamental group.

4.15.2 Étale Cohomology

Say X is a nice scheme over $\mathbb{C}$. Then, $X(\mathbb{C})^{\text{an}}$ is a good topological space, so one can do things like consider its cohomology $\mathrm{H}^*(X(\mathbb{C})^{\text{an}};\mathbb{Z})$.

Example. If $X = \mathbb{P}^1$, then $\mathbb{P}^1(\mathbb{C})^{\text{an}} = \mathbb{CP}^1$ and

$$\mathrm{H}^n(\mathbb{CP}^1;\mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if } n = 0, 2 \\ 0 & \text{otherwise.} \end{cases}$$

△

We had to leave the world of schemes to get these (singular) cohomology groups. We'd like to be able to define them purely algebraically, so that we get analogous cohomology groups over $\mathbb{Q}, \mathbb{F}_q, \dots$. Furthermore, if we have a k-scheme X, then we want $\mathrm{Gal}(\overline{k}/k)$ to act on $X_{\overline{k}}$'s cohomology.

Étale cohomology does this. When X is a nice scheme over k, one usually takes coefficients in finite ℓ-groups where $\ell \neq \operatorname{char} k$. You don't take $\mathbb{Z}$-coefficients, but things like $\mathbb{Z}/\ell^n\mathbb{Z}$-coefficients work well, so one can use some shenanigans to define étale cohomology with $\mathbb{Z}_\ell$ coefficients or $\mathbb{Q}_\ell$-coefficients. So we have groups

$$\mathrm{H}^*_{\text{ét}}(X, \mathbb{Z}/\ell^n\mathbb{Z}) \rightsquigarrow \mathrm{H}^*_{\text{ét}}(X; \mathbb{Z}_\ell \text{ or } \mathbb{Q}_\ell)$$

which are functorial in X as expected and which vanish for $* > 2\dim(X)$. This factor of 2 essentially comes from the difference between $\mathbb{R}$ and $\mathbb{C}$, e.g. $\mathbb{P}^1/\mathbb{C}$ is a 1-dimensional scheme, but $\mathbb{P}^1(\mathbb{C})^{\text{an}}$ is a 2-dimensional real manifold. There's also a compactly supported version of étale cohomology.

How does one construct these groups? Recall that one property of covering spaces is that they are locally disjoint unions of copies of the base. Like, if $Y \xrightarrow{\pi} X$ is a covering space, there around any $x \in X$, there's some open $U \ni x$ such that $\pi^{-1}(U) \cong U \times \Sigma$ for some finite set Σ.

This property is very much not the case for étale maps of schemes. Zariski open sets are just too big. E.g. consider $\mathbb{A}^1_{\mathbb{C}} \setminus \{0\} \to \mathbb{A}^1_{\mathbb{C}} \setminus \{0\}$ via $z \mapsto z^2$. Every nonempty open of $\mathbb{A}^1_{\mathbb{C}}$ is all but finitely many points (they're all so big that they twist all the way around the origin).

Picture $\mathbb{A}^1_{\mathbb{C}}$ as a punctured disk

This would make one think that they need "smaller" neighborhoods to get this property. In the end, though, one uses "larger" neighborhoods, ones so "large" they don't even fit in the space. Instead of considering the usual topology where opens are subsets of your space, one uses a *Grothendieck topology* where now opens are spaces mapping to your space (e.g. they don't have to inject anymore). In particular, one considers the *Étale topology* where étale morphisms are declared to be open. With this topology, one has this locally disjoint union property.

Stopped paying attention for 5 minutes

One defines $\mathrm{H}^*_{\text{ét},(c)}(X, \mathbb{Z}/\ell^n\mathbb{Z})$ (the (c) there since it could be compactly supported or not) with this idea and then an analog of a "classical" definition of cohomology groups. One even has a version of Poincaré duality. If X is smooth and connected, then there is a perfect pairing via cup products

$$\mathrm{H}^i(X) \times \mathrm{H}^{2r-i}_c(X) \longrightarrow \mathrm{H}^{2r}_c(X)$$

with $r = \dim X$ and $\dim \mathrm{H}^{2r}_c(X) = 1$. If X is proper, then $\mathrm{H}^i_c = \mathrm{H}^i$. Furthermore, there's the

Grothendieck-Lefschetz Trace Formula. Over $k = \mathbb{F}_q$, this gives

$$\#X(\mathbb{F}_q) = \sum_i (-1)^i \operatorname{Tr}\left(\operatorname{Frob}|\operatorname{H}^i_c(X_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell)\right).$$

This is analogous to Lefschetz fixed point since $\#X(\mathbb{F}_q)$ is the number of fixed points of Frobenius.

Remark 4.15.2 (Smooth and proper base change). Say $X \to \operatorname{Spec}\mathbb{Z}$ nice (proper, smooth, ...). Then, we can relate the étale cohomology of the fibers of this map. In particular,

$$\operatorname{H}^i_c(X_{\mathbb{C}}, \overline{\mathbb{Q}}_\ell) = \operatorname{H}^i_c(X_{\overline{\mathbb{F}}_q}, \overline{\mathbb{Q}}_\ell).$$

$\circ$

Remark 4.15.3 (Artin Comparison Theorem).

$$\operatorname{H}^i_c(X_{\mathbb{C}}, \overline{\mathbb{Q}}_\ell) \simeq \operatorname{H}^i_{\mathrm{sing},c}(X(\mathbb{C})^{\mathrm{an}}, \overline{\mathbb{Q}}_\ell)$$

$\circ$

Remark 4.15.4 (Riemann Hypothesis). For X smooth, proper over $\mathbb{F}_q$, the eigenvalues of Frob on H^i_c are $\alpha \in \overline{\mathbb{Q}}$ (i.e. algebraic over $\mathbb{Q}$) with all their conjugates, and all their conjugates have absolute value $|\cdot| = q^{i/2}$. $\circ$

One can drop the proper, smooth hypotheses and still have some facts, but things get more complicated.

The point is that these combined with Grothendieck-Lefschetz can allow us to uses cohomology over $\mathbb{C}$ to answer questions about geometry over $\mathbb{F}_q$.

Example. Let's count $\#\mathbb{P}^1(\mathbb{F}_q)$. This is

$$\operatorname{Tr}\operatorname{Frob}\operatorname{H}^0(\mathbb{P}^1) - \operatorname{Tr}\operatorname{Frob}\operatorname{H}^1(\mathbb{P}^1) + \operatorname{Tr}\operatorname{Frob}\operatorname{H}^2(\mathbb{P}^1).$$

We know from Artin that $\operatorname{H}^0(\mathbb{P}^1), \operatorname{H}^2(\mathbb{P}^1)$ are 1-dimensional and Frob on them acts with eigenvalues of absolute value $1, q$, respectively. We also know that $\operatorname{H}^1(\mathbb{P}^1) = 0$, so $\#\mathbb{P}^1(\mathbb{F}_q) = \pm 1 \pm q$ and it is not too hard to figure out which are $+$'s and which are $-$'s. $\triangle$

Question 4.15.5 (Audience)**.** *How do we make sense of compactly-supported?*

Answer. Roughly, just replace the role of compactness with properness. $\star$

4.16 Lecture 16 (10/30): Using AG in the function field case

Let's see how to use alg geom over $\mathbb{F}_q$ to get results on the statistics of class groups over function fields. We're gonna need a bunch of primes...

We're working over $\mathbb{F}_q(t)$, so let $K/\mathbb{F}_q(t)$ be some Γ-extension; we'll be interested in $\operatorname{Cl}_{\mathscr{O}_K}$ or $\operatorname{Pic}^0(C_K)$. We'll also need some prime $p \neq \operatorname{char}\mathbb{F}_q$; we'll be thinking about $\operatorname{Cl}_{\mathscr{O}_K}[p]$ or $\#\operatorname{Sur}(\operatorname{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})$. When making use of étale cohomology and friends, we'll need one other prime which we'll call ℓ. In summary, we have a prime power q, a prime $p \neq \operatorname{char}\mathbb{F}_q$, and we'll later introduce another prime ℓ.

We want to calculate something roughly of the form[63]

$$\frac{(\#\operatorname{Cl}_{\mathscr{O}_K}[p] \text{ or } \#\operatorname{Sur}(\operatorname{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})) \text{ of some } \Gamma\text{-extension } K/\mathbb{F}_q(t)}{\#\Gamma\text{-extensions}} \tag{4.1}$$

The point is that we can view both the numerator and the denominator (of (4.1) as counts of $\mathbb{F}_q$-points on some moduli space, i.e. variety over $\mathbb{F}_q$. AG tools then tell us about the number of $\mathbb{F}_q$ points on these varieties.

There is more than one way to turn the numerators/denominators into counts of $\mathbb{F}_q$ points on suitable moduli spaces. We will pick one way which is more attached to the $\#\operatorname{Sur}(\operatorname{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})$ perspective.

Note that Γ-extensions correspond to Galois covers (the data is both (C, π))

$$\begin{tikzcd} C \arrow[d, "\pi"', "\Gamma"] \\ \mathbb{P}^1 \end{tikzcd}$$

Example. When $\Gamma = \mathbb{Z}/2\mathbb{Z}$, one is looking at hyper elliptic curves. △

There is a Γ-**Hurwitz space** H_Γ which is a variety[64] over $\mathbb{F}_q$ whose points correspond to this data. These come up from the big AG machinery of producing moduli space; we don't e.g. have equations for them or something like that.

Recall 4.16.1. $\#\operatorname{Sur}(\operatorname{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})$ correspond to unramified $\mathbb{Z}/p\mathbb{Z}$-extensions of K, split completely at ∞.

For $K/\mathbb{F}_q(t)$ quadratic, $(K, \varphi \in \operatorname{Sur}(\operatorname{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z}))$ corresponds to a $\mathbb{Z}/p\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$-extension L of $\mathbb{F}_q(t)$ with $L/L^{\mathbb{Z}/p\mathbb{Z}}$ unramified everywhere and split completely over ∞. Note that $\mathbb{Z}/p\mathbb{Z} \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} = D_p$, the dihedral group of order $2p$. ⊙

We (4.1) is almost $\#H_{D_p}(\mathbb{F}_q)/\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)$, but the numerator is off since we have these extra conditions about $L/L^{\mathbb{Z}/p\mathbb{Z}}$ being unramified everywhere and split completely over ∞. Luckily for us, these conditions can be incorporated into a moduli space using the usual machinery, so we let H'_{D_p} with a prime denote the moduli space with these conditions baked in. Hence,

$$(4.1) \approx \frac{\#H'_{D_p}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}.$$

Now, if one was being careful, they'd keep in mind that we really only want to calculate the above fraction up to some bound. These moduli spaces split into components for each genus g (we'll denote this by H^g_Γ), so really we should be considering something like

$$\lim_{g\to\infty} \frac{\#(H'_{D_p})^g(\mathbb{F}_q)}{\#H^g_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}.$$

One last minor point. Really we should be looking at expressions like $\sum_{h=0}^g \#H^h_\Gamma(\mathbb{F}_q)$ in the numerator/-

[63] When you put in a bound and then take the limit as the bound goes to infinity, this is exactly $\mathbb{E}\left(\#\operatorname{Sur}(\operatorname{Cl}_{\mathscr{O}_K}, \mathbb{Z}/p\mathbb{Z})\right)$, the moments of our distribution on class groups

[64] The data (C, π) has automorphisms, so this is to quite true. Secretly, it is a stack or one has added extra data to get rid of automorphisms.

denominator, but one can show that the ratio of such things has the same limit as what we've written about; the point is that H^g has so many more points than H^h for $h < g$ that it just dwarfs it in the limit.

So now our goal is to understand the number of $\mathbb{F}_q$-points on the varieties $(H'_{D_p})^g$ and $H^g_{\mathbb{Z}/2\mathbb{Z}}$. Let's switch gears and talk more generally about points on varieties over $\mathbb{F}_q$.

Notation 4.16.2. Writing $(H'_{D_p})^g$ is annoying, so I'm just gonna write $H'^g_{D_p}$ instead.

In the end, this was simplified to H' instead

4.16.1 Points on varieties over $\mathbb{F}_q$

Question 4.16.3. *How many points "should" a variety X over $\mathbb{F}_q$ have?*

Answer (Level 0)**.** $\approx q^{\dim X}$ ⋆

Let's give a more refined answer.

Theorem 4.16.4 (**Riemann Hypothesis for Curves**, '40)**.** *Let X be a smooth projective, geometrically integral curve over $\mathbb{F}_q$. Then,*

$$|\#X(\mathbb{F}_q) - q - 1| \le 2g\sqrt{q}.$$

This shows that the level 0 answer is more-or-less right for curves. Note that the error term depends on the geometry of X (includes the genus).

Theorem 4.16.5 (**Lang-Weil**, '55)**.** *Let $X \subset \mathbb{P}^n$ be a projective, geometrically integral variety of degree d and dimension r. Then,*

$$|\#X(\mathbb{F}_q) - q^r| \le \delta q^{r-\frac{1}{2}} + A_{n,d,r}q^{r-1}$$

where $\delta = \delta_d = (d-1)(d-2)$ and $A_{n,d,r}$ is some explicit function of n, d, r.

Again, the level 0 is actually not so bad.

Proof Sketch. Start w/ RH for curves, and then induct on the dimension of X. We have $X \hookrightarrow \mathbb{P}^n$, so we can slice it with hyperplanes $H \subset \mathbb{P}^n$. Most of the time, $X \cap H$ will be 1 dimension smaller, so we can now imply the inductive hypothesis on $X \cap H$. The idea is to do this for all hyperplanes, so consider[65]

$$\mathbb{P}^{n-1}(\mathbb{F}_q)\cdot X(\mathbb{F}_q) = \sum_{\substack{H\subset\mathbb{P}^n \\ \text{hyperplane}}} (X\cap H)(\mathbb{F}_q) = \sum_{\substack{X\cap H \\ \text{satisfies hypothesis and has codim 1}}} (X\cap H)(\mathbb{F}_q) + \sum_{\text{bad } H} (X\cap H)(\mathbb{F}_q).$$

Use inductive hypothesis on LHS and use a cruder bound on RHS (+ show not too many such H). ■

Why is the level 0 answer only a level 0 answer?

Example. Consider $X = \mathbb{P}^1 \cup_* \mathbb{P}^1$, two linear intersecting at a point (which is connected), and $Y = \mathbb{P}^1 \sqcup \mathbb{P}^1$ (which is not connected). Then,

$$\#X(\mathbb{F}_q) = 2q+1 \text{ and } \#Y(\mathbb{F}_q) = 2q+2,$$

so neither X nor Y have $\sim q$ points. In either case, the issue is having multiple components. △

[65] The space of hyperplanes though a point of X is, by considering the dual projective space, $\mathbb{P}^{n-1}$ or something (don't quote me)

Example. Let $f(x)$ be an irreducible cubic over $\mathbb{F}_q$, and consider $X = V(f(x) = 0) \subset \mathbb{P}^2$. This is a smooth, connected variety over $\mathbb{F}_q$, but $X(\mathbb{F}_q) = 0$ which is certainly not like $q^{\dim X}$. △

These show that we really do need geometrically integral.

More generally, given X, consider the number of geometric components of X defined over $\mathbb{F}_q$, i.e. components of $X_{\overline{\mathbb{F}}_q} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ that are fixed by Frobenius (raising coordinates to qth power).

Question: Is this relative Frobenius $\mathrm{Fr}_X \times 1$?

Answer (Level 1)**.** $\#X(\mathbb{F}_q) \approx q^{\dim X} \cdot \#$geom components of X defined over $\mathbb{F}_q$. ⋆

This gives the write answer in our earlier examples. Note that one can extend Lang-Weil by applying it to each geometrically integral piece of your variety.

Answer (Level 1.5)**.** The error is $q^{\dim X - 1/2}$ with constant depending on "coarse" geometric invariants of X. Note that this "error" can be larger than the "main term" when X has no geometric components defined over $\mathbb{F}_q$. ⋆

Say X is smooth and projective or otherwise sufficiently nice. Remember that

$$\#X(\mathbb{F}_q) = \sum_{i \geq 0} (-1)^i \operatorname{Tr} \mathrm{Frob} | \mathrm{H}^{2i} = \operatorname{Tr} \mathrm{Frob} | \mathrm{H}^{2r} - \operatorname{Tr} \mathrm{Frob} | \mathrm{H}^{2r-1} + \dots$$

where the eigenvalues of Frobenius on H^k have absolute value $q^{k/2}$. Note that $\mathrm{H}^{2r} \sim \mathrm{H}^0$ via Poincare duality (technically, there's some twisting which gives rise to a q^r factor), and H^0 captures info on the components of X which are being permuted. The trace of a permutation representation is equal to the number of fixed points. Taking twisting into account, this gives another way of seeing that you get something like cq^r where c is the number of components fixed by Frobenius. The exact statement you get is (probably) neither strictly stronger nor weaker than Lang-Weil since the error here is now in terms of cohomological information. In practice, one might have better access to cohomological information or coarse geometric information (degree, dimension, etc.).

Recall our favorite fraction (4.1) which we rewrote in terms of $\mathbb{F}_q$-points on suitable moduli spaces. We'll write this here as

$$\frac{\#H'(\mathbb{F}_q)}{\#H(\mathbb{F}_q)},$$

simplifying notation. Luckily for us, both of these spaces turn out to have the same dimension r, so our approximation tells us that this fraction is roughly (assuming the numerator has a single geometric component defined over $\mathbb{F}_q$) $q^r/q^r = 1$ which is good (1 is precisely the Cohen-Lenstra moment we hope for). How good is our approximation? We'll, it's only good as q gets large.

Our original problem was for q fixed and g getting large, but the machinery we have is better suited for varying q. Next time we'll get a theorem as $q \to \infty$ instead of one for the original problem.

4.17 Lecture 17 (11/4)

Last time, at least as $q \to \infty$, the "main term" of $\#X(\mathbb{F}_q)$ is given by the (# of Frobenius fixed components of $X_{\overline{\mathbb{F}}_q}$) $\cdot\, q^{\dim X}$. Also, we saw that our moments can be written as

$$\mathbb{E}(\# \operatorname{Sur}(\operatorname{Cl} \mathscr{O}_K, A)) \text{``}=\text{''} \frac{\#H'_{A \rtimes \mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}$$

(a limit of) a quotient of counts of $\mathbb{F}_q$-points on certain moduli spaces. To make this literal, we need to be careful about what it is going to infinity, and where.

Recall that in the original problem, we have $\mathbb{Q}$ (number field case) and we were looking at $\mathbb{E}(\#\operatorname{Sur}(...))$ for $|\operatorname{Disc} K| \le X$ as $X \to \infty$. In the number field/function field analogy, $\mathbb{Q}$ is like $\mathbb{F}_q(t)$ and instead of ordering by discriminant, we usually order by the genus of associated curve C_K (here $K/\mathbb{F}_q(t)$ finite). In fact, these genii come in big chunks, so big that one gets the same asymptotics by considering either $g(C_K) \le g$ or $g(C_K) = g$ as $g \to \infty$.

In the function field case, there are two types of limits we could take. We can fix q and let $g \to \infty$, or we can fix g and let $q \to \infty$. The former is more analogous to the number field case, but the latter is more easily accessible. Note that, without further information, in general, these two limits do not need to give the result. A simple picture/counterexample to keep in mind is the following:[66]

$$\begin{array}{c|cccc}
g & & & & \\
 & 2 & 2 & 2 & \\
 & 2 & 2 & 1 & \\
 & 2 & 1 & 1 & \\
 & 1 & 1 & 1 & \\
\hline
 & & & & q
\end{array}$$

Still, it is heuristically useful to consider the "large q" case. It is also a perfectly fine question about the distribution of class groups (or of Pic^0) of curves over finite fields to ask about what happens as $q \to \infty$, even if it is not completely analogous to the original question. In fact, one can also consider question where $g, q \to \infty$ together. Somehow, fixed g is "easiest," fixed q is "hardest", it "gets harder" as you "interpolate" from fixed g to fixed q.

Question 4.17.1 (Audience)**.** *Is there a relationship between the discriminant in the function field case and the genus?*

Answer. Yes. For $K/\mathbb{F}_q(t)$ a finite extension, one has

$$\operatorname{Nm}(\operatorname{Disc} K/\mathbb{F}_q(t)) = \prod_{\text{ram places}} \mathfrak{q}_i^{\text{some power depending on ramification}}.$$

The Riemann-Hurwitz formula shows that the genus is involved in a similar equation (involving ramification indices), and one can play these off each other to show that $\operatorname{Nm}\operatorname{Disc} = q^{ag+b}$ for some a, b. An example of this (for quadratic K) was on one of the homeworks. $\star$

The idea of looking at the q limit was introduced by J.-K. Yu. The first $q \to \infty$ type result is due to Achter. This is what we'll talk about today. The next really important work along these lines is due to Ellenberg, Venkatesh, and Westerland; they're breakthrough came from looking not just at components but also at the higher cohomology groups. We will follow their perspective even as we talk about Achter's work.

I think this is what she said. I may have misheard; I was slightly distracted

Recall we are looking at
$$\frac{\#H'_{A \rtimes \mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}{\#H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}$$

[66]The limit with fixed g is 1, but the limit with fixed q is 2

where the $'$ just means we want certain ramification properties. Keep in mind the one case where we already have results; that is $A = \mathbb{Z}/3\mathbb{Z}$ so S_3-covers. We'll assume $2 \nmid q$. In the denominator, we have the moduli space of (smooth) hyperelliptic curves $y^2 = f(x)$. This is the space of 2 variable homogeneous polynomials w/o repeated roots.

What does this space look like over $\mathbb{C}$? Well, a polynomial $f(x)$ is determined by its roots (so an element of this space looks like 2 points in $\mathbb{C}$), and since we're looking at smooth curves, we require its roots to be distinct, so we basically get $\mathrm{Conf}_2(\mathbb{C})$, the configuration space of 2 points in $\mathbb{C}$ (don't worry about different polys giving isomorphic curves). For asymptotics, we care about the number of connected components. It is pretty easy to see that this space is connected.

This paragraph should not be taken literally. We're ignoring some subtleties; we just want to highlight the main ideas.

If $H_{\mathbb{Z}/2\mathbb{Z}}$ was smooth and proper, then it would be well-known that connected over $\mathbb{C} \implies$ connected over $\overline{\mathbb{F}}_q$. However, it is definitely not proper (two roots coming together let's us easily see that this space is not proper). Luckily for us, in this case, one can still use geometry to show that connected $/\mathbb{C} \implies$ connected $/\overline{\mathbb{F}}_q$. The moduli space $M_{0,n}$ of smooth genus 0 curves with n (ordered) marked points is a degree $n!$ étale cover of $H_{\mathbb{Z}/2\mathbb{Z}}$. We understand the relationship of $M_{0,n}$ to its compactification $\overline{M}_{0,n}$; in particular, the *boundary divisor* $\overline{M}_{0,n} \setminus M_{0,n}$ is well understood enough to use the compactification and knowledge of the boundary and $H_{\mathbb{Z}/2\mathbb{Z}}$ connected over $\mathbb{C}$ to get that $H_{\mathbb{Z}/2\mathbb{Z}}$ is connected over $\overline{\mathbb{F}}_q$. This is *not* the best way to see that $H_{\mathbb{Z}/2\mathbb{Z}}$ is connected over $\overline{\mathbb{F}}_q$, but this method generalizes.

Question 4.17.2 (Audience). *What is meant by compactification here?*

Answer. Let's fit things into a bigger context. $M_{g,n}$ is the moduli space of smooth genus g curves with n ordered, distinct marked points (this is known to be a variety; actually, a stack). Now, $\overline{M}_{g,n}$ is the same thing with smooth replaced by stable, and this space is proper with $M_{g,n} \hookrightarrow \overline{M}_{g,n}$ as an open, dense subset. This is why we call it a "compactification." It is not the only one though, so we really should have spoken of "a compactification" instead of "the compactification." There's modern work in trying to relate the different compactifications of $\overline{M}_{g,n}$ and how they fit into the minimal model program.

As a general theme, one can try to understand a non-proper space X by understanding some proper space $\overline{X}$ into which X includes and also understanding the boundary $\overline{X} \setminus X$. ⋆

Question 4.17.3 (Audience). *Do you form $\overline{M}_{g,n}$ by letting points come together (on the boundary)?*

Answer. Not actually. In $\overline{M}_{g,n}$, what you do when points are coming together is attach a $\mathbb{P}^1$ (where they would join) and then move the points away from each other on this $\mathbb{P}^1$. There may be other compactifications where one does allow the points to come together in some way; there are many compactifications these days. ⋆

Now let's look at the numerator. What is the fiber of $H'_{A \times \mathbb{Z}/2\mathbb{Z}} \to H_{\mathbb{Z}/2\mathbb{Z}}$? Recall that we're looking at fields $L/K/\mathbb{F}_q(t)$ with $\mathrm{Gal}(L/K) = A$ and $[K : \mathbb{F}_q(t)] = 2$; the prime $'$ denotes that we also require L/A to be unramified. Fix a point $*$ of $H_{\mathbb{Z}/2\mathbb{Z}}$; A point in $H'_{A \times \mathbb{Z}/2\mathbb{Z}}$ in the fiber above $*$ corresponds to a curve $\pi : D \to \mathbb{P}^1$ that is ramified only at $*$. That is, $D \setminus \pi^{-1}(x\text{'s in } *) \to \mathbb{P}^1 \setminus (x\text{'s in } *)$ is an unramified map, i.e. a map

$$\pi_1(\mathbb{P}^1 \setminus (x\text{'s in } *)) \to A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}.$$

We're thinking of $*$ as being a collection of roots, i.e. points in $\mathbb{A}^1_{\mathbb{F}_q}$

Question: What does this mean?

Answer: See

This is π_1 of a punctured $\mathbb{P}^1$, so it is a (profinite) free group on $n-1$ generators where n is the number of x's. Above, we should require that $\gcd(q, |A|) = 1$.

Let's think about the S_3 case (so $A = \mathbb{Z}/3\mathbb{Z}$). We're looking at maps fom some free (profinite) group on $x_1, x_2, \ldots, x_{n-1}$ to S_3. The data of a map from a free group is simply the images of its generators, so the fiber is

$$\left\{(g_1, g_2, \ldots, g_{n-1}) \,\middle|\, \begin{array}{c} g_i \in S_3 \text{ such that } S_3 = \langle g_i \rangle \\ g_i \neq (1) \text{ and } g_i \text{ a transposition} \end{array}\right\}$$

(the conditions other than $g_i \in S_3$ are there to ensure that it is an S_3-cover and that we have our ramification conditions). Generating S_3 makes it an S_3-cover; not being the identity makes $D \setminus \pi^{-1}(x\text{'s in } *) \to \mathbb{P}^1 \setminus (x\text{'s in } *)$ unramified, and being transpositions makes L/K unramified. One can form analogous conditions in the general case.

Now that we know the fibers, we ask ourselves, "are all these points in the fiber in the same connected component or not?" Remember that the map $H'_{A\times\mathbb{Z}/2\mathbb{Z}} \to H_{\mathbb{Z}/2\mathbb{Z}}$ is an étale cover. Connected components upstairs correspond to orbits of $\pi_1(H_{\mathbb{Z}/2\mathbb{Z}})$ on fiber. So far, everything we have said would be fine over $\mathbb{C}$ or over $\overline{\mathbb{F}}_q$ (modulo the fact that we only know the fundamental group over $\overline{\mathbb{F}}_q$ by comparison with it over $\mathbb{Z}$). However, we now use something that really corresponds to thinking over $\mathbb{C}$.

Over $\mathbb{C}$, one can draw pictures to see how $\pi_1(H_{\mathbb{Z}/2\mathbb{Z}})$ acts on the fiber. A loop in $H_{\mathbb{Z}/2\mathbb{Z}}$ is basically a "movie" with the first frame being n points in $\mathbb{C}$ in some position and the last frame being those points in the same position. If I'm understanding what Melanie is saying, then basically $\pi_1(H_{\mathbb{Z}/2\mathbb{Z}})$ is the (profinite completion of?) the "infinite braid group" (or maybe a quotient of this?); like take a colimit of all the n-strand braid groups as $n \to \infty$. Maybe not actually this; I didn't really follow well...

To be precise, one needs to take care of things like

- choices of automorphisms of $\mathrm{Gal}(L/\mathbb{F}_q(t))$ with $A \rtimes \mathbb{Z}/2\mathbb{Z}$
- what's going on at ∞ (technically, we said we want extensions split completely at ∞, so need to incorporate this into moduli space)
- distinguish maps $\pi_1 \to A \rtimes \mathbb{Z}/2\mathbb{Z}$ or conjugacy classes of such map. Need to pick one and stick with it.

One finds that $|\bigwedge^s A|$ components of this space. When $A = \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$, $\bigwedge^2 A = 1$ so we have 1 component over $\mathbb{C}$. One uses this to show that there's also 1 component over $\overline{\mathbb{F}}_q$, which is necessarily fixed by Frobenius, so we have our asymptotics (looks like $q^{\dim}$), and we get that the Moment is 1 as desired.

Next time, we'll look at cases with more components (e.g. $A = \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ which has 3 components). In this case, it is not obvious how Frobenius acts, so more work needs to be down to analyze higher moments.

4.18 Lecture 18 (11/6)

Recall we have

$$\mathbb{E}(\#\,\mathrm{Sur}(\mathrm{Cl}\,\mathscr{O}_K, A)) = \lim \frac{\# H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}{\# H_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{F}_q)}$$

where we're basically counting $L/K/\mathbb{F}_q(t)$ with L an unramified A-extension and $K/\mathbb{F}_q(t)$ quadratic. We saw last time that $H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z}}/\overline{\mathbb{F}}_q$ has $\left|\bigwedge^2 A\right|$ components (for sufficiently large genus/discriminant/#ram geom pts).

Today we'll focus on the case when $\left|\bigwedge^2 A\right| > 1$, and how to get an idea for hos Frobenius acts on these $\overline{\mathbb{F}}_q$ components.

To get the components over $\mathbb{C}$, one "draws pictures" and uses the path interpretation of π_1^{top}. This is something you cannot do over $\overline{\mathbb{F}}_q$. Note that you never see Frob/$\mathbb{C}$, so you need to see these components over $\overline{\mathbb{F}}_q$, i.e. they need an algebraic definition.

Often, you can define some algebraic invariant (e.g. of curves) that must be constant in families (i.e. on components of moduli spaces of curves). A simple example is the genus. This gives a lower bound on the number of components. On the other hand, the component count over $\mathbb{C}$ gives an upper bound.[67]

Consider a curve $C \to \mathbb{P}^1$ with Galois group $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. Let $D \subset \mathbb{P}^1$ be the divisor where $C/\mathbb{P}^1$ is ramified, and let $U = \mathbb{P}^1 \setminus D$. Since C is unramified over U, it corresponds to some map $\varphi : \pi_1(U) \to A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. By comparing étale and topological fundamental groups, we conclude that $\pi_1(U)$ is the (profinite) free group of $n-1$ generators. Topologically, these generators are loops γ_i around each of the n points in D; these satisfy exactly one relation:

$n =$ deg D_{red}?

$$\gamma_1\gamma_2 \ldots \gamma_n = 1.$$

We get $(g_1, g_2, g_3, \ldots, g_n)$ with $g_i = \varphi(\gamma_i)$ up to relations

$$\ldots g_i, g_{i+1}, \cdots \to \ldots, g_{i+1}, g_{i+1}^{-1} g_i g_{i+1}, \ldots.$$

This is what we did topologically. How do we do this algebraically?

What, algebraically, are these loops around each point? These loops correspond to automorphisms of the cover $C \to \mathbb{P}^1$, i.e to elements of the Galois group $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$, but which ones? Given a particular point, the "loops around it" we'll be related to a certain inertia subgroup of $G = A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$. Let's make things more precise.

We work over $\overline{\mathbb{F}}_q$ and we require $\gcd(q, |A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}|) = 1$. We have extensions

$$\begin{tikzcd}
 & L \\
K \arrow[ur, dash, "A"] & \\
\overline{\mathbb{F}}_q(t) \arrow[u, dash] \arrow[uur, dash, "A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}"'] &
\end{tikzcd}$$

Can take $\gamma_1, \gamma_2, \cdots \in \pi_1(U^{\mathrm{tame}}_{\overline{\mathbb{F}}_q})$, generators of tame inertia. Then consider

Remember: Tame inertia is cyclic. This is kinda like the fact that the punctured neighborhood of a point has cyclic fundamental group

$$(\varphi(\gamma_1), \ldots, \varphi(\gamma_n)) \in (A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z})^n.$$

Question 4.18.1. *Is this object well-defined? ... How does it depend on choices? Is it constant in families?*

We really only need to answer the second question because the first is asking "is it constant in the

[67]If I understand, by "upper bound" we really mean the "true number of components." We do know that there are $\left|\bigwedge^2 A\right|$ components in our example; we want an algebraic invariant in order to characterize them in a way that let's us understand what Frobenius does to them.

For each ramified

one-point family?". There were 3 kinds of choices made in the definition

- The order of the points $1, \ldots, n$
- The conjugacy class of the inertia subgroup
- Choice of generator

This sounds like a lot of choices, but actually it's not so bad.

Let's first think about the local inertia group so there's no conjugacy class worry. We have

$$\mathbb{F}_q((t))^{\text{prime-to-q}} / \overline{\mathbb{F}}_q((t)) / \mathbb{F}_q((t))$$

with the lower extension the maximal unramified extension, and the upper extension having Galois group equal to inertia. The inertia in $\mathrm{Gal}(\mathbb{F}_q((t))^{\text{prime-to-q}} / \mathbb{F}_q((t)))$ is a canonical subgroup, and is canonically identified with roots of unity $\mu_\infty(\overline{\mathbb{F}}_q) = \varprojlim_{q \nmid m} \mu_m(\overline{\mathbb{F}}_q)$. This comes from the fact that

$$\mathbb{F}_q((t))^{\text{prime-to-q}} = \overline{\mathbb{F}}_q((t^{1/m} : (m, q) = 1)).$$

So for $\sigma \in \mathrm{Gal}$ fixing $\overline{\mathbb{F}}_q$ (i.e. σ in inertia), we have $\frac{\sigma(t^{1/m})}{t^{1/m}} \in \mu_m(\overline{\mathbb{F}}_q)$, and taking the limit as m ranges gives a canonical element of $\mu_\infty(\overline{\mathbb{F}}_q)$.

Let's think about the choices we made over $\mathbb{C}$. We did not just choose γ_1, γ_2,etc. so that they generate inertia over each point. We chose them so that also the product $\gamma_1 \gamma_2 \ldots \gamma_n = 1$ is trivial. Hence, we should also require this in our choice of inertia generators $\gamma_i / \overline{\mathbb{F}}_q$. This turns out to imply that all γ_i are associated to the same generator of $\mu_\infty(\overline{\mathbb{F}}_q)$ (exercise: use étale cohomology or class field theory).

Now, we can say things in a way that's a little more canonical.

- Pick a topological generator ζ of $\mu_\infty(\overline{\mathbb{F}}_q)$
- Pick an ordering of $\overline{\mathbb{F}}_q$ pts on D
- Pick $\gamma_1, \ldots, \gamma_n$ generators of inertia @ ith pt, corresponding to ζ, s.t. $\gamma_1 \gamma_2 \ldots \gamma_n = 1$.

The next step is to pass from these orders of tuples to something more algebraic. Define

Note that the formal symbol $[e]$ is not the identity in this group, it just commutes with everything. In particular, out tuples are not all length n and the formal symbol $[g]$ corresponds to a size 1 tu-

$$\mathscr{G} = \langle [g] : g \in A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z} \rangle \,/\, \left([g_i][g_{i+1}] = [g_{i+1}][g_{i+1}^{-1} g_i g_{i+1}] \right).$$

The semigroup on these generators with these relations is exactly the orbits of tuples we saw topologically. Thus, we have a well-defined map

$$\text{orbits of tuples} \longrightarrow \mathscr{G}.$$

Now take

$$[\varphi(\gamma_1)] \ldots [\varphi(\gamma_n)] \in \mathscr{G}$$

as our invariant.

Theorem 4.18.2 (Group Theory)**.** *The above element of $\mathscr{G}$ is independent of choices does not depend on the ordering or choice of inertia generator. It does depend on ζ though.*

The above "independence result" is not true at the level of orbits of tuples.

This tells us that the semigroup of tuple-orbits does not have the cancellation property (e.g. $ab = cb \not\Rightarrow a = c$). In particular, padding a tuple could potentially change its orbit type

We have one final input. When $n \gg 0$ (length of tuple/degree of ramification divisor), one shows (using group theory) that orbits of tuples of length n *do inject* into $\mathscr{G}$ (this is not true in general).

For $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ covers $C \to \mathbb{P}^1$ over $\overline{\mathbb{F}}_q$, we have (almost, up to choice of generator of $\mu_\infty(\overline{\mathbb{F}}_q)$) an element of $\mathscr{G}$. Then, one can show that this element of $\mathscr{G}$ is constant in families. This has two kinds of uses: can look at this invariant in a family over $\operatorname{Spec}\mathbb{Z}$, going from the geometric point over $\mathbb{C}$ to a geometric point over $\overline{\mathbb{F}}_q$. Can also use this to see that it is constant on $\overline{\mathbb{F}}_q$-components of $H'_{A\times\mathbb{Z}/2\mathbb{Z}}$. The key to showing constancy in families is specialization maps of π_1: given a nice family $Y \to S$ with two geometric points $x \in S(\overline{k})$ and $X \in S(\overline{K})$ such that $x \in \overline{X}$ (the closure of $\overline{X} \subset S$), have good maps

$$\pi_1(X_{\overline{K}}) \to \pi_1(X_{\overline{k}}).$$

All this γ_i business is compatible with these specialization maps. Can choose $\gamma_i \in \pi_1(X_{\overline{K}})$ first and then use their image in $\pi_1(X_{\overline{k}})$ to compute the element, and then our independence of choices results means everything works out nicely.

One can see these $\left|\bigwedge^2 A\right|$ worth of components algebraically now, and work out that Frobenius acts by multiplication by q on $\mathscr{G}$ (who woulda thunk it?). Thus, the Frobenius fixed components correspond to $\bigwedge^2 A[q-1]$. When A is an ℓ-group and $\ell \nmid q-1$, then there is 1 Frobenius fixed component over $\overline{\mathbb{F}}_q$. This is enough to give $\mathbb{E}(\#\operatorname{Sur}(\operatorname{Cl}\mathscr{O}_K, A)) = 1$ in a $q \to \infty$ limit. Thus, as $q \to \infty$, there is a C-L distribution of $\operatorname{Cl}\mathscr{O}_K$ (this was originally due to Achter).

Question 4.18.3 (Audience)**.** *The n for which the group theory result holds, does it depend on anything?*

Answer. It depends on the group A, but inexplicitly so. It's just an existence result. $\star$

Question 4.18.4 (Audience)**.** *In the case when $\ell \nmid q-1$ so there's one frobenius fixed component, can we write down what it is as an element of $\bigwedge^2 A$?*

Answer. We can't since the components are not canonically identified with $\bigwedge^2 A$, they're simply a $\bigwedge^2 A$-torsor. $\star$

Question 4.18.5 (Audience)**.** *Is $\mathscr{G} \simeq \bigwedge^2 A$ or does it just contain $\bigwedge^2 A$ as a subgroup?*

Answer. It has many $\bigwedge^2 A$'s in it. For example, we have this map $\mathscr{G} \to \mathbb{Z}$ sending $[g] \mapsto 1$, e.g. the length of the tuple. Once n is sufficiently large, all the fibers of this map are isomorphic to $\bigwedge^2 A$. $\star$

Question 4.18.6 (Audience)**.** *The n that we talk about, is it the degree of the ramification divisor or the degree of the reduction of the ramification divisor?*

Answer. In our case, there isn't really a distinction. We're looking a tower like

$$\begin{tikzcd} L \arrow[d, dash, "A"', "\text{unram}"] \\ K \arrow[d, dash, "2"'] \\ \mathbb{F}_q(t) \end{tikzcd}$$

so all the ramification is happening the bottom, quadratic extension and the ramification divisor will already be reduced (e.g. $e_i - 1 \le 1$). In a more general, where you could have varying degrees of ramification, you would then probably want to reduce it first. $\star$

4.19 Lecture 19 (11/11)

Where were we? For large q, $\#X(\mathbb{F}_q)$ is controlled by the number of Frob fixed components over $\overline{\mathbb{F}}_q$ (note this is not the same as the number of components over $\mathbb{F}_q$.[68]). For moments of $\mathrm{Cl}\,\mathscr{O}_K$, we discussed Hurwitz spaces whose $\mathbb{F}_q$ points give moments and their components. As $q \to \infty$, when $\ell \nmid (q-1)$, we see the Cohen-Lenstra moments. This $q-1$ arose as $\#\mu(\mathbb{F}_q(t))$.[69]

Today, the plan is to talk about going beyond components. What happens if we look further at the topology of these moduli spaces? In particular, we'll need to use Grothendieck-Lefschetz and not just Lang-Weil. We'll gives our Hurwitz spaces names that look like X; before they had names that look like H, but we'll need H for cohomology.

Say we have $X_n/\mathbb{F}_q$ of dimension n. Then,

$$\#X_n(\mathbb{F}_q) = \operatorname{tr} F|_{\mathrm{H}_c^{2n}} - \operatorname{tr} F|_{\mathrm{H}_c^{2n-1}} + \dots$$

with the first term $\operatorname{tr} F|_{\mathrm{H}_c^{2n}}$ comes from components.[70] Since X_n is smooth, we know that the eigenvalues of $F|_{\mathrm{H}_c^{2n-1}}$ have absolute value at most $q^{n-1/2}$. How many eigenvalues are there o this space?

$$\dim \mathrm{H}_c^{2n-i} = \dim \mathrm{H}^i =: h_i(n)$$

(X_n smooth + Poincaré duality).

If we want to put $\operatorname{tr} F|_{\mathrm{H}_c^{2n-1}}$ into error term (using dimension and bound on eigenvalues), we need

$$\frac{h_1(n)q^{n-1/2}}{q^n} = \frac{h_1(n)}{q^{1/2}} \to 0.$$

How can we be in a situation where this expression goes to 0 (note that $h_1(n) \in \mathbb{Z}$)? Unless $h_1(n) = 0$, this forces us to take $q \to \infty$. This is what we did/talked about before.

Two ways to do this:

- Fix n, let $q \to \infty$, then let $n \to \infty$, i.e. take $\lim_{n\to\infty} \lim_{q\to\infty} (blah)$.
- Formally, let $n \to \infty$ slowly enough, i.e. take $\lim_{(n,q)\to\infty} (blah)$ with n growing "slowly enough" compared to q.

These two are formally equivalent. If you have convergence in one case, then you get convergence in the other case (where "slowly enough" depends on the particular application). Either of these formally equivalent approaches use absolutely nothing about $h_1(n)$.

[68] e.g. you may have a component over $\mathbb{F}_q$ made up of two $\overline{\mathbb{F}}_q$ components which are switched by Frobenius

[69] The point is that we say that $\mathbb{F}_q(t)$ is like $\mathbb{Q}$, but if $\mathbb{F}_q(t)$ has extra roots of unity and these play a role in the question under consideration, then $\mathbb{F}_q(t)$ isn't really like $\mathbb{Q}$ for your purposes.

[70] Remember this is cohomology of the space base-changed to $\overline{\mathbb{F}}_q$. Frobenius permutes these, and the trace of a permutation is the number of fixed points. Technically components have to do with H^0, but then one has Poincaré duality (with twists involved)

Surely, we know something about $h_1(n)$, so what if instead of using nothing about it, we use something about it? Our next input will be a basic upper bound on $h_1(n)$. This is

$$\dim \mathrm{H}^i(X(n)) \leq D^n$$

for some constant $D > 0$. This uses a topological CW complex with D^n cells. Recall that we need $h_1(n)/q^{1/2} \to 0$. This basic upper bound gives us an explicit expression for how quickly q can grow vs n, e.g. $q \geq (D+1)^{2n} \implies h_1(n)/q^{1/2} \to 0$. Note that the better upper bound we have on $h^i(n)$, the less restrictive the growth rate of q can be. Note that we are ultimately interested in the case where q is fixed; for this have tighter upper bounds alone won't get us all the way there.

Question: Is this the étale homotopy type stuff?

4.19.1 Homological Stability

There are often natural sequences of spaces $X_1, X_2, X_3, \ldots$ which are getting "larger" or "more complicated" in some sense(s) where nevertheless, it can happen that for fixed i, the groups $\mathrm{H}_i(X_n, \mathbb{Z})$ stabilize as $n \to \infty$.

Example (Harer stability)**.** Take $X_g = \mathcal{M}_g$, the moduli space of genus g curves. These spaces have homological stability △

Example (Borel Arithmetic Groups)**.** For $\mathrm{H}^i(\mathrm{SL}_n(\mathbb{Z}); \mathbb{Q})$ or $\mathrm{Sp}_{2n}(\mathbb{Z})$ or other examples. △

Example (McDuff Configuration Spaces)**.** $X_n = \mathrm{Conf}^n M$ where M an open manifold (not compact). X_n is the moduli space of n distinct, unordered points of M. △

Often one expects there to be maps $X_n \to X_{n+1}$ realizing the isomorphisms in the stable range. These do not always exist.

One can worry about coefficients. Do you get stability integrally or only rationally or mapping with mod p coefficients?

There is also a notion of representation stability.

Question 4.19.1 (Audience)**.** *Are these three examples proven in similar ways?*

Answer. Originally, there were different proofs in each case. Nowadays, there are multiple ways for getting these type of results, so some ways work for multiple examples. There is not one unified framework for proving stability, but there are common proof strategies which each work for many examples. ⋆

Recall 4.19.2. $\mathrm{Conf}^n \mathbb{P}^1 = \mathrm{H}_{\mathbb{Z}/2\mathbb{Z}}$ is the Hurwitz space of hyperelliptic curves. This was like the denominator in our problem. ⊙

This maybe suggests that Hurwitz spaces are homologically stable.

Theorem 4.19.3 (Eilenberg-Venkatesh-Westerland)**.** *$H'_{A \rtimes_{-a} \mathbb{Z}/2\mathbb{Z}}(n)$ have homological stability*[71] *with $\mathbb{Q}$-coeffs. Here, n is the # of (geom) branch points.*

They did not prove general Hurwitz spaces have homological stability, but they did prove it for exactly the spaces which are relevant for Cohen-Lenstra.

The style of their proof is maybe closest to the style of proof for $\mathcal{M}_g$.

[71] Fix i. There exists k s.t. for n large enough, $\mathrm{H}_i(X_n, \mathbb{Q}) \simeq \mathrm{H}_i(X_{n+k}, \mathbb{Q})$. In fact, they show you only need $n \geq ai + b$ bigger than some linear function of i.

4.19.2 Back to Statistics

What does the Eilenberg-Venkatesh-Westerland result tell us about $h_1(n)/q^{1/2} \to 0$? We now have an absolute bound for $h_1(n)$, so we can let $q \to \infty$ at *any* rate at all, even very small compared to n. Unfortunately, we still have to let $q \to \infty$, but this is still an improvement.

We'll ignore the issue about k-steps pointed out in a footnote. One can just pass to a subsequence to assume $k = 1$ anyways.

We have $\dim \mathrm{H}_i(X_n, \mathbb{Q}) \le \dim \mathrm{H}_i(X_{ai+b}, \mathbb{Q}) \le D^{ai+b} \le E^i$ for some constant $E > 0$.[72] This tells us that

$$\left|\mathrm{Tr}\, F|_{\mathrm{H}_c^{2n-i}}\right| \le q^{n-i/2} E^i = \left(\frac{E}{\sqrt{q}}\right)^i q^n.$$

The main term is order q^n. It is also the order of our denominator. We divide through by q^n and sum over i. To sum over i, we need $E/\sqrt{q} < 1$ (i.e. $q > E^2$), and then we can sum

$$\frac{\#X_n(\mathbb{F}_q)}{q^n} = \#\{\text{Frob-fixed } \overline{\mathbb{F}}_q\text{-components}\} + (|\cdot| \le E/\sqrt{q}) + \left(|\cdot| \le (E/\sqrt{q})^2\right) + \dots.$$

For fixed $q > E^2$, the above sequence is certainly summable with

$$\limsup_{n\to\infty} \frac{\#X_n(\mathbb{F}_q)}{q^n} \le \frac{1}{1 - E/\sqrt{q}} \quad \text{and} \quad \liminf_{n\to\infty} \ge 1 - \frac{E/\sqrt{q}}{1 - E/\sqrt{q}}.$$

Note that, as $q \to \infty$, the $\liminf, \limsup$ both go to 1. This is the main consequence of EVW homological stability. Can take $\liminf, \limsup$ for a fixed q, and then as $q \to \infty$, they both to q (the desired moments).

Given that we would like q to stay fixed, this is really the best possible $q \to \infty$ result. This is because $q \to \infty$ last, or equivalently, we have $(q, n) \to \infty$ w/ q going arbitrarily slowly compared to n.

To get from above to a better fixed q result, must *know* $\mathrm{Tr}\, F|_{\mathrm{H}_c^{2n-i}}$. This involves knowing the group H_c^{2n-1} and knowing the Frobenius eigenvalues. One might hope to understand these by first finding $\dim \mathrm{H}^i$ over $\mathbb{C}$ using topology, and then identifying the cohomology coming from "something algebraic" (i.e. pulled back from known classes on other spaces, especially from a top dimensional class on some space) so as to be able to understand the action of Frobenius.

EVW conjecture that

$$\mathrm{H}^i\left(H'_{A\rtimes_{-1}\mathbb{Z}/2\mathbb{Z}}(n); \mathbb{Q}\right) \xrightarrow{n\to\infty} \begin{cases} \mathbb{Q} & \text{if } i = 0, 1 \\ 0 & \text{otherwise.} \end{cases}.$$

Note that its not even currently known that these groups stabilize (there may be some oscillation. See k in a footnote). If one shows this, understanding the Frobenius action would be easy. This would imply C-L for fixed $q \gg_A 1$.

Question 4.19.4 (Audience)**.** *Does this EVW conjecture sort of say that Weil-Lang captures everything? Like you just have the main term and one other term*

Answer. It's somehow saying something more than that. It's saying these spaces are super special in that most of their cohomology vanishes. I should also mention that the eigenvalue in degree 1 has abs.

[72] these constants only depend on the group A, but are quite inexplicit

val. q^{n-1} instead of $q^{n-1/2}$. ⋆

Question 4.19.5 (Audience)**.** *What motivates this conjecture on the stable homology? Is it just because it's about the simplest thing that would give C-L?*

Answer. Historically/empirically, they thought they had proven it, but it turned out there was a subtle error in their proof. Philosophically, one cannot find any other cohomological algebraically if they look (this is not a formal/proven statement), but this would be the simplest explanation why. ⋆

Question 4.19.6 (Audience)**.** *Does this conjecture mean that the limit, for fixed q, is like* $1 + 1/q$*?*

Answer. Yeah, but that's in the numerator and the denominator. They both look like $q^n - q^{n-1}$, so the moment itself is 1. ⋆

4.20 Lecture 20 (11/13): Conjectures for Cl_K in Galois extensions

5 minutes late

4 class meeting left or something.

- Cl Galois extensions
- Cl non-Galois extensions
- $\mathrm{Gal}(K^{\mathrm{un}}/K)$ distributions
- $q \to \infty$ function field theorems for all of the above

Today, conjectures for distributions of Cl_K for Galois extensions. Original Conjecture are from a paper of Cohen-Martinet. People often talk about "Cohen-Lenstra-Martinet conjectures" but the three of them never wrote a paper together; it was one paper by Cohen-Lenstra and another by Cohen-Martinet. We'll talk about Melanie's perspective on these conjectures.

What's the data we start with? We have a Galois extension $K/\mathbb{Q}$ with Galois group Γ. We also fix some "signature data". What is signature data? Some times in number theory "signature" refers to the number of real/complex places, i.e. $K \otimes \mathbb{R}$ as an $\mathbb{R}$-algebra. However, here we have Γ-action, so we can consider $K \otimes \mathbb{R}$ furthermore as a Γ-module. Our "signature data" or "**Γ-signature**" will be a fixed decomposition group $\Gamma_\infty \subset \Gamma$ at ∞, i.e. the subgroup generated by complex conjugation (so Γ_∞ is 1 or C_2). Cyclic of order 2

Recall that Cl_K is not just an abelian group, it is a $\mathbb{Z}[\Gamma]$-module. Two perspectives:

- This is a Γ-module so I want to understand its distribution as a Γ-module
- Who cares? I only care that it is an abelian group, so I only care about its distribution as an abelian group

In either case, you actually need to understand its structure as a Γ-module to understand the distribution.

Warning 4.20.1. If we don't have a choice of iso $\Gamma \simeq \mathrm{Gal}(K/\mathbb{Q})$, then Cl_K is not a Γ-module. So for us, when we say a "**Γ-field**" we mean both K *and* a choice of iso $\Gamma \simeq \mathrm{Gal}(K/\mathbb{Q})$.[73] It is convenient to take $K \subset \overline{\mathbb{Q}}$ with a fixed embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$, so "complex conjugation" is an element and not an "elment up to conjugacy." •

[73]So each field K appears $\mathrm{Aut}(\mathrm{Gal}(K/\mathbb{Q}))$-times

Remark 4.20.2. Recall from the (first?) homework that actually Cl_K is a (finite) module over the smaller ring

$$R := \frac{\mathbb{Z}[\Gamma]}{\left(\sum_{\gamma\in\Gamma}\gamma\right)}.$$

$\circ$

If we want a distribution on R-modules, we should first understand what R-modules are.[74] The first step is to separate by primes. Map of finite order $\mathbb{Z}$-modules $M \to N$ take M_p to N_p (Sylow p-subgroups). In fancy terminology

$$\text{Cat. of finite } R\text{-modules} = \prod_p \text{Cat. of finite } p\text{-group } R\text{-modules}.$$

This let's us reduce to p-group modules. We abuse notation by taking $R = \mathbb{Z}_p[\Gamma]/\sum_{\gamma\in\Gamma}\gamma$.

Note that the question of "What are the R-modules?" has a nice answer only when $p \nmid |\Gamma|$. Hence, Cohen-Martinet (and so us) decided to only consider the case when $p \nmid |\Gamma|$.

Then, $\mathbb{Q}_p[\Gamma]$ is a semisimple algebra over $\mathbb{Q}_p$, and $\mathbb{Z}_p[\Gamma]$ is a maximal order (relative to $\mathbb{Z}_p$). Here, **maximal order** means it is a maximal f.g. $\mathbb{Z}_p$-module subring.

Remark 4.20.3. Sounds like, in general, semisimple algebras are always products of matrix algebras of division algebras. Also, maximal orders may not be unique in general, but *they are unique* in the local setting. $\circ$

When Γ is abelian, we have $\mathbb{Q}_p[\Gamma] = E_1 \times \ldots \times E_r$, a product of field extensions $E_i/\mathbb{Q}_p$, and then $\mathbb{Z}_p[\Gamma] = \mathscr{O}_{E_1} \times \ldots \times \mathscr{O}_{E_r}$, the product of the corresponding maximal orders.

When Γ is non-abelian, have instead

$$\mathbb{Z}_p[\Gamma] \simeq M_{n_1}(\Delta_1) \times \ldots,$$

a product of matrices over maximal orders in division algebras over $\mathbb{Q}_p$. This is in general what a maximal order of $\mathbb{Q}_p[\Gamma]$ for any p (even, $p \mid \#\Gamma$) looks like. Saying that $\mathbb{Z}_p[\Gamma]$ is a maximal order is what uses $p \nmid \#\Gamma$. Further, when $p \nmid \#\Gamma$ then all the division algebras Δ_i involved are commutative[75] (i.e. fields).

Say Γ is abelian, so we're interested in the category of $\mathscr{O}_{E_1} \times \mathscr{O}_{E_2} \times \ldots \times \mathscr{O}_{E_r}$-modules. It is not hard to see (use idempotents) that this is equivalent to

$$\prod_i \left(\text{Categoy of } \mathscr{O}_{E_i}\text{-modules}\right).$$

Thus, we are reduced to understanding the category of $\mathscr{O}_{E_i}$-modules of finite order, for some fixed i. This is classification of (f.g. or even finite here) modules over a Dedekind domain (or even dvr). These are all of the form

$$\frac{\mathscr{O}_{E_i}}{\mathfrak{m}_i^{a_1}} \times \frac{\mathscr{O}_{E_i}}{\mathfrak{m}_i^{a_2}} \times \ldots \times \frac{\mathscr{O}_{E_i}}{\mathfrak{m}_i^{a_s}}.$$

for $a_1 \geq a_2 \geq \cdots \geq a_s$.

[74] When working with abelian groups, we knew all the (finite) abelian groups

[75] Intuitively, this is the case working over $\mathbb{F}_p$, and $p \nmid \#\Gamma$ means that working over $\mathbb{F}_p$ should be "the same" as working over $\mathbb{Z}_p$, so we get the same result over $\mathbb{Z}_p$

Recall that we're actually working over $\mathbb{Z}_p[\Gamma]/\sum_{\gamma\in\Gamma}\gamma$. Note that the thing we're quotient out by is $|\Gamma|\cdot e_1$ with e_1 an idempotent (corresponding to the trivial representation?). Hence, saying it acts trivially really just amounts to killing on of the $\mathscr{O}_{E_i}$ factors, say killing $\mathscr{O}_{E_1}$ or something.

Now say Γ non-abelian. The **Morita theorem** says that the category of $M_n(\mathscr{O}_E)$-modules is equivalent to the category of $\mathscr{O}_E$-modules themselves. We'll construct the functor in the reverse direction here. Let A be an $\mathscr{O}_E$-module A. Then, we get an $M_n(\mathscr{O}_E)$-module

$$A^n = \begin{pmatrix} A \\ \vdots \\ A \end{pmatrix}.$$

The upshot is that we know all finite $\mathbb{Z}_p[\Gamma]/\sum\gamma$-modules. In terms of data, they are given by a partition for each nontrivial (since we killed $\sum_{\gamma\in\Gamma}\gamma$) representation V of Γ over $\mathbb{F}_p$ (or $\mathbb{Q}_p$).[76]

Question: And irreducible?

Remark 4.20.4. Let k be a field. Modules for $k[\Gamma]$ are exactly the same things as Γ-reps over k. Above, knowing that $p\nmid\#\Gamma$ is tells us that rep theory of Γ over $\mathbb{F}_p, \mathbb{Z}_p, \mathbb{Q}_p$ are all the same. ∘

The moral is that we understand R-modules and they're not much more complicated than finite abelian groups.

Cohen-Lenstra use this fact. For example, the show that

$$\sum_{\text{finite } R\text{-modules } A}\frac{1}{\#\operatorname{Aut}_R A} < \infty.$$

4.20.1 Cohen-Martinet Distribution

(1) Take a $1/\operatorname{Aut}_R$ random group, i.e. X with $\mathbb{P}(X\simeq A) = c/\#\operatorname{Aut}_R A$. This wasn't even enough in the (real) quadratic case, so there has to be a second step.

(2) Take a "certain" random quotient of X.

Example. Recall that when $\Gamma = \mathbb{Z}/2\mathbb{Z}$, the real quadratic distribution is the imaginary quadratic distribution mod a uniformly random element. △

Interpretation of the second step This is forthcoming work of Melanie's with Yuan Liu.

Maybe it's come out by the time you read this

Recall 4.20.5. There was a heuristic for the quadratic distributions coming from an expression of the form

$$I^S/\mathscr{O}_S^\times\otimes\mathbb{Z}_p$$

with numerator of rank $|S|$ and denominator of rank $|S|$ or $|S|+1$ depending on whether we were in the imaginary or real quadratic case. ⊙

Fix R-modules V, W (fin dimensional, free as $\mathbb{Z}_p$-modules). Then, $\operatorname{Hom}_R(V,W)\simeq\mathbb{Z}_p^N$ is a free $\mathbb{Z}_p$-module; in particular, it is a compact abelian group so has a Haar measure. Can think about $V/_RW$, a random R-module given as $V/\varphi(W)$ for Haar random $\varphi\in\operatorname{Hom}_R(V,W)$.

[76] Reps over $\mathbb{F}_p$ and over $\mathbb{Q}_p$ are same here since $p\nmid\#\Gamma$

Example. When $R = \mathbb{Z}_p$ (e.g. $\Gamma = \mathbb{Z}/2\mathbb{Z}$), then V, W are $\mathbb{Z}_p^n, \mathbb{Z}_p^{n+u}$ and this random quotient $V/_R W$ is the cokernel of a Haar random matrix in $M_{n\times(n+u)}(\mathbb{Z}_p)$. This gave the imaginary quad C-L distribution as $n \to \infty$ when $u = 0$ and the real quad C-L distribution as $n \to \infty$ when $u = 1$. △

Notation 4.20.6. Melanie wrote $\underset{\text{Rand}}{/}$ instead of $/_R$, but that takes longer to type.

The idea now is to combine these things. First question: how to choose S? At least, we should pick S to be Γ-closed, so $\Gamma \curvearrowright I^S, \mathscr{O}_S^\times$. Note that I^S, as a Γ-module, depends on the splitting type of primes in S.

Example. Let p be a rational prime which is totally inert: $p\mathscr{O} = \mathfrak{p}$ is prime. Then, $\mathfrak{p}$ is fixed by Γ, so get a trivial rep $I^{\{p\}}$. However, if $p\mathscr{O} = \mathfrak{p}_1 \dots \mathfrak{p}_{\#\Gamma}$ is split completely, then $I^{\{\mathfrak{p}_1,\dots,\mathfrak{p}_{\#\Gamma}\}}$ gives a regular representation of Γ. △

Thus, $I^S \simeq V_{(n_1,n_2,\dots)}$, a fixed $\mathbb{Z}_p[\Gamma]$-module (not depending on any field) with indices n_i giving the # of primes in S of each splitting type.

Also, $\mathscr{O}_S^\times \otimes \mathbb{Z}_p \cong (I^S \times \mathscr{O}^\times) \otimes \mathbb{Z}_p$ as $\mathbb{Z}_p[\Gamma]$-modules.[77] This is not hard to see and uses that $p \nmid \#\Gamma$. We just discussed what the first of these two pieces look like. The second piece $\mathscr{O}^\times \otimes \mathbb{Z}_p$ only depends on Γ_∞; it is $\operatorname{Ind}_{\Gamma_\infty}^{\Gamma} \mathbb{Z}_p/\mathbb{Z}_p$.

I think anyways, I lost zoom connection as she was saying this so I may have missed something. Presumably Γ acts trivially on the piece getting killed.

Theorem 4.20.7 (Liu-Wood)**.** *For a fixed R-module Y,*

$$\lim_{\text{all } n_i\to\infty} V_{(n_1,n_2,\dots)} \big/_R V_{(n_1,n_2,\dots)} \times Y$$

exists (gives an actual probability distribution in the limit). Furthermore, when $Y = 1$ is trivial, you get the $1/\operatorname{Aut}_R$ group (i.e. the step **(1)** *Cohen-Martinet group). When $Y = \operatorname{Ind}_{\Gamma_\infty}^{\Gamma} \mathbb{Z}_p/\mathbb{Z}_p$, the limit is the C-M conjectured final distribution.*

This is saying something like take step **(1)** of C-M and then quotient out by a random map from the unit group $\mathscr{O}^\times \otimes \mathbb{Z}_p$.

Remark 4.20.8. If you want to read more about this, the paper the above theorem is from is still forthcoming, but can check out Melanie's paper with Weitong. ○

Harvard has no classes Wednesday–Friday of Thanksgiving week, and the last day of class is the Thursday after Thanksgiving. So we have two classes next week and then one more the day before the last day.

Question 4.20.9 (Audience)**.** *How do you show $\mathscr{O}^\times \otimes \mathbb{Z}_p \simeq \operatorname{Ind}_{\Gamma_\infty}^{\Gamma} \mathbb{Z}_p/\mathbb{Z}_p$?*

Answer. I was distracted when she was answering this, but sounds like you want to use Minkowski map with $\mathbb{Q}_p$ (or $\mathbb{Z}_p$?) in place of $\mathbb{R}$, and then do something akin to the proof of finite generation of the unit group or something? I don't know; I clearly wasn't listening well enough. ⋆

[77] There's not a natural isomophism between them. They are structurally/abstractly isomorphic as $\mathbb{Z}_p[\Gamma]$-modules. The natural map $\mathscr{O}_S^\times/\mathscr{O} \to I^S$ is injective, but not surjective. If you think about it, what's going on is like the fact that $2\mathbb{Z} \hookrightarrow \mathbb{Z}$ but the two are isomorphic $\mathbb{Z}$-modules.

4.21 Lecture 21 (11/18): Class groups of non-Galois fields

Last 3 classes will be

- (Today) Class groups of non-Galois fields.
- (Next time) $\mathrm{Gal}(K^{\mathrm{un}}/K)$, "non-abelian class groups"
- (Last class) function field $q \to \infty$ proofs of above

Say $K/\mathbb{Q}$ is a non-Galois number field. Cohen-Martinet did not directly address the non-Galois case in their conjectures, but gave the following reason for not needing to: If $L = \widetilde{K}$ is the Galois closure of K with Galois group $\Gamma = \mathrm{Gal}(L/\mathbb{Q})$ and $p \nmid |\Gamma|$, then we have the map $i : \mathrm{Cl}_K[p^\infty] \to \mathrm{Cl}_L[p^\infty], [I] \mapsto [I\mathscr{O}_L]$.

Question 4.21.1. *Is i injective?*

Answer. The composition $\mathrm{Cl}_K \xrightarrow{i} \mathrm{Cl}_L \xrightarrow{\mathrm{Nm}_{L/K}} \mathrm{Cl}_K$ is multiplication by the degree $[L/K]$, i.e. it sends $[I] \mapsto [I]^{[L:K]}$. Since $p \nmid [L:K]$, this composition is injective, so i is injective. ⋆

Question 4.21.2. *Is i surjective?*

Answer. Let $\Gamma' = \mathrm{Gal}(L/K)$ so $i(\mathrm{Cl}_K) \subset \mathrm{Cl}_L^{\Gamma'}$. So i is probably not surjective. ⋆

Question 4.21.3. *Is $i(\mathrm{Cl}_K[p^\infty]) = \mathrm{Cl}_L^{\Gamma'}[p^\infty]$?*

Answer. It feels like they should be equal since $K = L^{\Gamma'}$. However, there are two obstructions to this happening. First, elements of $\mathrm{Cl}_L^{\Gamma'}$ don't need to come from Γ'-fixed ideals. We have

$$0 \longrightarrow P_L \longrightarrow I_L \longrightarrow \mathrm{Cl}_L \longrightarrow 0$$

which induces

$$0 \longrightarrow P_L^{\Gamma'} \longrightarrow I_L^{\Gamma'} \longrightarrow \mathrm{Cl}_L^{\Gamma'} \longrightarrow \mathrm{H}^1(\Gamma', P_L) \longrightarrow \dots.$$

However, the H^1 above is annihilated by $|\Gamma'|$; since $p \nmid |\Gamma|$, we see that we do indeed have $I_L^{\Gamma'} \otimes \mathbb{Z}_p \twoheadrightarrow \mathrm{Cl}_L^{\gamma'}$.

Now, do Γ'-fixed ideals have to come from K? We have the composition

$$I_L^{\Gamma'} \xrightarrow{\mathrm{Nm}} I_K \to I_L.$$

This sends $\mathfrak{a} \mapsto \mathfrak{a}^{|\Gamma'|} \mapsto \mathfrak{a}^{|\Gamma'|}$ (the equality since $\mathfrak{a}$ is Γ'-fixed). Since $p \nmid |\Gamma'|$, this composition is surjective, so $I_K \twoheadrightarrow I_L^{\Gamma'}$ surjectively. That is, every Γ'-fixed ideal does come from K.

The above is the argument C-M gave. However, seems we could just consider

$$\mathrm{Cl}_L^{\Gamma'} \xrightarrow{\mathrm{Nm}} \mathrm{Cl}_K \xrightarrow{i} \mathrm{Cl}_L^{\Gamma'}$$

from the start to see that $i(\mathrm{Cl}_K[p^\infty]) = \mathrm{Cl}_L^{\Gamma'}[p^\infty]$. ⋆

We conclude that for $p \nmid |\Gamma'|$, we indeed have

$$i : \mathrm{Cl}_K[p^\infty] \xrightarrow{\sim} \mathrm{Cl}_L[p^\infty]^{\Gamma'}.$$

C-M gave a conjectural distribution for $\mathbb{Z}_p[\Gamma]$-modules. Taking the Γ' fixed parts gives a distribution on $\mathbb{Z}_p$-modules.

In above, L didn't need to be the Galois closure; it just needed to be Galois and contain K. Furthermore, K did not have to be non-Galois.

This is potentially a cause of worry. It gives many "natural-seeming" distributions over K by considering distributions on larger fields and taking Galois-fixed points or whatever. It is not clear a priori that all these things should agree.

Slogan. $1/\operatorname{Aut}$ doesn't always push forward.

Example. Take $1/\operatorname{Aut}$ finite $\mathbb{Z}_p$-module, i.e. $\mathbb{P}(X \simeq A) = c/\#\operatorname{Aut} A$. Then, $X[p] \cong X/pX$ is not in $1/\operatorname{Aut}$ distribution for $\mathbb{F}_p$-vector spaces. △

Theorem 4.21.4 (Wang-W.)**.** *The C-M distributions pushed forward from 2 different larger Galois groups agree.*

Is that it? Do we know just know the (expected) distributions of class groups for all types of number fields?

Say A is a $\mathbb{Z}_p[\Gamma]$-module (e.g. $\mathrm{Cl}_L[p^\infty]$). We consider $A^{\Gamma'}$; does this have any structure (beyond being an abelian group)?

Remember that Γ' acts on the left

Example. If Γ' were normal, then $\mathbb{Z}_p[\Gamma/\Gamma'] \curvearrowright A^{\Gamma'}$, so the answer would be yes. △

What do we do in general (i.e. when Γ' not normal)? Define

$$e_{\Gamma'} = \frac{1}{\Gamma'} \sum_{\gamma \in \Gamma'} \gamma$$

(recall that $p \nmid |\Gamma|$). This is an idempotent (but not usually central if Γ' not normal), but intuitively it is the idempotent projecting to the Γ' fixed part. Note that $e_{\Gamma'}\mathbb{Z}_p[\Gamma]$ acts on $A^{\Gamma'}$, but $e_{\Gamma'}\mathbb{Z}_p[\Gamma]$ is not a ring. However, $e_{\Gamma'}\mathbb{Z}_p[\Gamma]e_{\Gamma'}$ is a ring and still acts on $A^{\Gamma'}$. In fact, $e_{\Gamma'}\mathbb{Z}_p[\Gamma]e_{\Gamma'} \simeq \mathbb{Z}_p[\Gamma' \backslash \Gamma / \Gamma']$ the "ring of functions on a double coset" or the "Hecke algebra of a finite group" or however you want to think of it. We adopt the notation

$$H_{\Gamma,\Gamma'} := e_{\Gamma'}\mathbb{Z}_p[\Gamma]e_{\Gamma'} \simeq \mathbb{Z}_p[\Gamma' \backslash \Gamma / \Gamma'].$$

Theorem 4.21.5 (Wang-W.)**.** *A $1/\operatorname{Aut}_{H_{\Gamma,\Gamma'}}$ distribution agrees with the Cohen-Martinet (pushed-forward) prediction.*

In particular, this is something to recognize about class groups of (non-Galois) fields: they have structure beyond that of an abelian group.

Example. Take $\Gamma = A_5$ and $\Gamma' = \{(123), (12)(45)\}$. Get

$$\begin{tikzcd} & L \arrow[dl, dash, "\Gamma'"'] \arrow[ddl, "A_5=\Gamma"] \\ K \arrow[d, dash, "10"'] & \\ \mathbb{Q} & \end{tikzcd}$$

Then, $K/\mathbb{Q}$ has no non-trivial automorphisms, but one can work out that $H_{\Gamma,\Gamma'} \simeq \mathbb{Z}_p[\sigma]/(\sigma^2-1)$, so the class group comes with an order 2 automorphism (which *does not* come from an automorphism of K).

This additional structure restricts the structure of class groups (e.g. their p-ranks may be constrained). $\triangle$

This whole time we've been working with the assumption that $p \nmid |\Gamma|$. What happens when this doesn't hold, i.e. when $p \mid |\Gamma|$?

Recall 4.21.6. When $K/\mathbb{Q}$ imaginary quadratic, genus theory told us that $\mathrm{Cl}_K[2]$ is not random, it is

$$\mathrm{Cl}_K[2] \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\omega(\mathrm{Disc}_K)-1}.$$

This is why C-L threw out 2 when making their conjectures. $\odot$

Gerth went a slightly different direction. Instead of killing the whole 2-Sylow subgroup, he asked about $2\,\mathrm{Cl} \simeq \mathrm{Cl}/\mathrm{Cl}[2]$. He conjectured that $\mathrm{Cl}/\mathrm{Cl}[2]$ follows the C-L distribution (e.g. predicted 2-Sylow of $\mathrm{Cl}/\mathrm{Cl}[2]$ is $1/\mathrm{Aut}$ distributed).

Theorem 4.21.7 (Fouvry-Klüners)**.** *Gerth's conjecture is correct for* 2 *ranks of* $\mathrm{Cl}/\mathrm{Cl}[2]$ *("4-rank").*

They showed this by finding moments and then using uniqueness of moments. One interesting thing is that genus theory was a big input into their arguments.

(Gerth actually had proven this but with a nonstandard ordering on K. First order by $\omega(D_K)$, the number of prime divisors of the discriminant. So something like $\lim\limits_{\#\text{prime divisors}} \lim\limits_{X\to\infty} (blah)$. After his work, it was unclear if this ordering was misleading. But F-K's work shows that this is a robust phenomenon since they got the same result when ordering by discriminant)

Ask about 4-torsion by asking which elements of $\mathrm{Cl}[2]$ are multiples of 2? Why stop there? Can get a handle on 2^n-torsion by looking at which elements of $\mathrm{Cl}[2^{n-1}]$ are multiples of 2, and genus theory maybe gives you some hope that this is possible (with extra inputs).

Theorem 4.21.8 (Smith)**.** *Proves Gerth conjecture for* $\mathrm{Cl}/\mathrm{Cl}[2][2^\infty]$ *(*$(2\,\mathrm{Cl})[2^\infty]$*) of quadratic fields.*

For $|\Gamma| > 2$, the $p \mid |\Gamma|$ regime is much murkier...

Recall 4.21.9. In the C-M setup, the first step in getting your random group is to build a $1/\mathrm{Aut}$ random $\mathbb{Z}_p[\Gamma]$-module. To do this, they used that this was a maximal order in $\mathbb{Q}_p[\Gamma]$ in order to understand its modules very well. $\odot$

When $p \mid \#\Gamma$, $\mathbb{Z}_p[\Gamma]$ is no longer maximal in $\mathbb{Q}_p[\Gamma]$ so their machinery for understanding things no longer applies so well in general. However, consider $e \in \mathbb{Q}_p[\Gamma]$ a central idempotent (irreducible central idempotents $\leftrightarrow$ irreps of Γ). If $e \in \mathbb{Z}_p[\Gamma]$ (no p's in denominator) and $e\mathbb{Z}_p[\Gamma]$ is a maximal order in $e\mathbb{Q}_p[\Gamma]$, then we're back in business. C-M say that (p,e) is **good**. If (p,e) is good, then (L a Γ-field)

$$e\,\mathrm{Cl}_L[p^\infty] \text{ is a } e\mathbb{Z}_p[\Gamma]\text{-module}$$

(action makes sense since $e \in \mathbb{Z}_p[\Gamma]$), and Cohen-Martinet conjecture that $e\,\mathrm{Cl}_L[p^\infty]$ is distributed with step 1 being to take a $1/\mathrm{Aut}_{e\mathbb{Z}_p[\Gamma]}$ group.

In Wang-W., for $(p, e_{\Gamma/\Gamma'})$ good in C-M sense ($e_{\Gamma/\Gamma'}$ is the idempotent you see from the induced rep $\mathrm{Ind}_{\Gamma'}^{\Gamma}$ Trivial, I think), one has
$$\mathrm{Cl}_K[p^\infty] \simeq \left(e_{\Gamma/\Gamma'}\,\mathrm{Cl}_L[p^\infty]\right)^{\Gamma'}.$$
The upshot is that *sometimes*, even when $p \mid |\Gamma|$, one can still prove $\mathrm{Cl}_K[p^\infty]$ is some particular function of $\mathrm{Cl}_L[p^\infty]$.

Example. $\Gamma = S_3$, $\Gamma' = \langle(23)\rangle$, and $p = 2$ (The 2-part of the class group of non-Galois cubic fields). Bhargava has determined that $\mathbb{Z}/2\mathbb{Z}$-moment in this case and shown it agrees with what is predicted. △

So we have at least one statistical data point.

There are still more issues where it is not 100% clear how to deal with thing. One source of problems is roots of unity. We say in the function field case that roots of unity can affect these distributions (e.g. when we were looking at moment expressions of the form $\bigwedge^2 A[q-1]$). The question of revised conjectures taking into account roots of unity are at the boundary of current work. It seems like there are some floating around, but it's still early?

4.22 Lecture 22 (11/20): Non-abelian class groups

Recall 4.22.1. $\mathrm{Cl}(K) = \mathrm{Gal}(K^{\mathrm{un,ab}}/K)$ is the Galois group of the maximal abelian, unramified extension of K. Thus, $\mathrm{Cl}(K)$ is naturally the abelianization of $\mathrm{Gal}(K^{\mathrm{un}}/K)$, the Galois group of the maximal unramified extension of K. ⊙

It's nonstandard but this gives reason to call $\mathrm{Gal}(K^{\mathrm{un}}/K)$ the "non-abelian class group" of K. This group actually has another name. Recalling that unramified extensions of K are basically just étale extensions of $\mathscr{O}_K$, one has
$$\mathrm{Gal}(K^{\mathrm{un}}/K) = \pi_1^{\text{ét}}(\mathrm{Spec}\,\mathscr{O}_K)$$
is the the étale fundamental group of $\mathscr{O}_K$ (compare with $\mathrm{Gal}(\overline{K}/K) = \pi_1^{\text{ét}}(\mathrm{Spec}\,K)$.

Question 4.22.2. *For K in some family of number fields, what is the distribution of* $\mathrm{Gal}(K^{\mathrm{un}}/K)$*?*

Remark 4.22.3. If you answer this question, to answer the corresponding question(s) on the distribution of class groups, since you get these by just pushing forward/taking abelianizations. ∘

What some motivation for this question?

- In some sense, the goal of number theory is to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ along with its inertia subgroups and Frobenius elements.
- Understand Cl_K.

  Recall 4.22.4. The p-torsion of the $1/\mathrm{Aut}$ distribution on finite abelian p-groups *does not* push forward to the $1/\mathrm{Aut}$ distribution on $\mathbb{F}_p$ vector spaces. The point is that $G[p]$ is not just an object in its own write, but naturally comes from this bigger thing (namely, G). ⊙

  Similarly, Cl_K naturally arises as the abelianization of $\mathrm{Gal}(K^{\mathrm{un}}/K)$, and this can pose otherwise unexpected constraints on Cl_K. You can find examples where certain class groups are impossible in Melanie's paper with Liu and Zureick-Brown; this is known because they are not the abelianization of a possible $\mathrm{Gal}(K^{\mathrm{un}}/K)$.

Another well studied object is $\text{Gal}(K^{\text{un,pro}-p}/K)$, the **$p$-class tower group** (this is the Sylow-p subgroup of $\text{Gal}(K^{\text{un}}/K)$). It's called the "class tower" group because you can get it from the sequence $K = H_0 \subset H_1 \subset H_2 \subset ...$ of class fields where H_{i+1} is the p-Hilbert class field of K.

The actual Hilbert class tower (as opposed to p-Hilbert class tower) gives $\text{Gal}(K^{\text{un,pro}-\text{sol}}/K)$. This is not so well studied.

Unlike $\text{Cl}_K = \prod_p \text{Cl}_K[p^\infty]$, $\text{Gal}(K^{\text{un}}/K)$ is not built up in this way, so there's something lost by only studying p-class tower (though maybe the pro-nilpotent group is). We will say that the p-class tower group is the most studied "piece" of $\text{Gal}(K^{\text{un}}/K)$. For example, Golo-Shafaevich have a theorem about finite p-groups and their (number of?) generators/relations. A corollary of their theorem is that, for p odd prime, if K imaginary quadratic with $\# \text{Cl}_K[p] \geq 4$, then $\text{Gal}(K^{\text{un,pro}-p}/K)$ is infinite.[78] This is one of the first ways we know that these p-class towers can be infinite.

In particular, $\text{Gal}(K^{\text{un}}/K)$ can be infinite whereas Cl_K is always finite.

Recall 4.22.5. For real quadratic fields, the conjectured distribution of Cl_K^{odd} was discrete. For imaginary quadratic fields, it was a product of discrete distributions on p-groups. $\odot$

For $\text{Gal}(K^{\text{un}}/K)$, the limiting distribution will not be discrete. That's ok though; there are plenty of non-discrete measures.

Example. The p-adic measure on $\mathbb{Z}_p$ is not discrete. Since $\mathbb{Z}_p$ is profinite, we often work with this by using the fact that it has compatible measures on $\mathbb{Z}/p^k\mathbb{Z}$ which are discrete (and even uniform). $\triangle$

The distribution on $\text{Gal}(K^{\text{un}}/K)$ will be a distribution on profinite groups. It will not be discrete, but we'll understand it by taking compatible discrete distributions.

Question 4.22.6. *There are only countably many K. How could the limiting distribution be non-discrete?*

Answer. This is not actually a problem. In general, countable sequences can have non-discrete limiting distribution. Imagine discrete distributions on $[0, 1]$ would get more and more "dense" in the limit, for example. $\star$

To have a non-discrete measure, we'll need a σ-algebra on $\{\text{profinite groups}\}$. Technically, in order to not run into set theoretic issues, we should say "small" profinite groups of something, but whatever; let's not worry about that. We'll take the Borel σ-algebra on the topology whose open sets are as follows.

For C a finite set of finite groups, we let $\overline{C}$ be the **variety**[79] generated by C.

Example. When $C = \{1\}$, $\overline{C} = \{1\}$.

When $C = \{\mathbb{Z}/2\mathbb{Z}\}$, $\overline{C} = \left\{ \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^k : k \geq 0 \right\}$ $\triangle$

For a variety $\overline{C}$ the **pro-$\overline{C}$ completion** of a topological group G is

$$G^{\overline{C}} := \varprojlim_{N \text{ open and } G/N \in \overline{C}} G/N$$

[78] Galois cohomology tell us something about the # of generators and relations of $\text{Gal}(K^{\text{un,pro}-p}/K)$, and then Golod-Shafarevich just show there's no finite p-group with that number of generators and relations

[79] Not an algebraic variety, but a group-theoretic notion. A set of groups closed under taking subgroups, quotients, and finite direct products

Example. If $\overline{C}$ is abelian groups, then $G^{\overline{C}}$ is the (pro-)abelianization.

If $\overline{C}$ is p-groups, then $G^{\overline{C}}$ is the pro-p completion.

$G^{\overline{\{\mathbb{Z}/2\mathbb{Z}\}}} = G^{\text{ab}}/2G^{\text{ab}}$, the maximal quotient of the form $(\mathbb{Z}/2\mathbb{Z})^k$. △

We never finished describing out topology on {profinite groups}. For every finite set C of finite groups and (pro)finite group H, we declare the set

Should usually let H be any profinite group, but in our case, taking H finite will suffice

$$\mathcal{U}_{H,\overline{C}} = \left\{G : G^{\overline{C}} \simeq H\right\}$$

is open. This give a basis for our topology. You can think of these opens are representing a "level of precision" for looking at your profinite groups.

Our $\mathrm{Gal}(K^{\text{un}}/K)$, for C finite, have $G^{\overline{C}}$ finite.

Exercise. Prove this. Has to do with things like only the number of number fields of a given discriminant.

For each C, we can ask what is the distribution on $\mathrm{Gal}(K^{\text{un}}/K)^{\overline{C}}$ which is now a distribution on the set of finite groups, which is countable. This will turn out to be discrete (at least, conjecturally).

How are we going to describe these distributions? Maybe now it's $1/\mathrm{Aut}$? (might hope this).

Example. If $C = \{\mathbb{Z}/p\mathbb{Z}\}$, then

$$\mathrm{Gal}(K^{\text{un}}/K)^{\overline{C}} = \mathrm{Cl}_K/p\,\mathrm{Cl}_K \cong \mathrm{Cl}_K[p]$$

which is not distributed like $1/\mathrm{Aut}$. △

So not $1/\mathrm{Aut}$? What about an analog of cokernels of matrices $M \in M_{n\times n}(\mathbb{Z})$? Note that $\operatorname{coker} M = \mathbb{Z}^n/(n \text{ relations})$ with (random) relations given by the columns of M. That is, we can get a random group by taking a fixed group (e.g. free abelian of rank n) and quotienting it by random relations.

Let F_n be the free group on n generators. We'll want to take something like F_n/n random relations. In a paper with Yuan Liu, Melanie studies $\widehat{F}_n/n$ independent relations from Haar measure (like a generic, random profinite (balanced) group).

However, $\mathrm{Gal}(K^{\text{un}}/K)$ is not generic. What we talk about next will be on Melanie's joint work with Liu and Zureick-Brown. Let $K/\mathbb{Q}$ be Galois with group Γ. We'll restrict to studying $G_K := \mathrm{Gal}(K\text{un},'/K)$ where we're looking at extensions of degree prime to $2|\Gamma|$ (the 2 since $\mu_2 \subset \mathbb{Q}$).

(1) G_K has a Γ-action. This is because it sits in an exact sequence

$$1 \longrightarrow G_K \longrightarrow \mathrm{Gal}(K^{\text{un},'}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1.$$

In general, such a situation only gives an outer action, but Schur-Zassenhaus tells us that this becomes a genuine action when restricted to the prime to $|\Gamma|$ piece.

Definition 4.22.7. For a group G, recall the exact sequence

$$1 \longrightarrow \mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1.$$

An **outer action** on G is a map $\Gamma \to \mathrm{Out}(G)$, so it's quite an action (i.e. a map $\Gamma \to \mathrm{Aut}(G)$). ⋄

Theorem 4.22.8 (**Schur-Zassenhaus**)**.** *When you have*

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

with $\gcd(\#N, \#H) = 1$*, then there exists a section which is unique up to conjugacy.*

This first thing generalizes the fact that Cl_K is a $\mathbb{Z}[\Gamma]$-module.

(2) This will generalize the fact that $\left(\sum_{\gamma\in\Gamma}\gamma\right) \cdot \mathrm{Cl}_K = 0$.

Theorem 4.22.9. $G_K = \mathrm{Gal}(K^{\mathrm{un},'}/K)$ *is generated by elements of the form* $x\gamma(x)^{-1}$ *for* $\gamma \in \Gamma$*,* $x \in G_K$*.*

Remark 4.22.10. In the abelianization, generated by $x - \gamma(x) \iff$ annihilated by $\sum_{\gamma\in\Gamma}\gamma$ (Exercise). ○

(3) There's one further fact, which we don't see in the abelian case. If

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$$

is a non-split central extension of Γ-groups, and there is a surjection $G_K \twoheadrightarrow H$, then there exists a lift $G_K \to \widetilde{H}$, i.e. if you have an unramified H-extension, then there is also an unramified $\widetilde{H}$-extension. The main input to this is the Hasse-Brauer-Noether theorem. This is the source of thing stated earlier where there were some 2-Sylow subgroups of class groups that could not appear.

We now want to give a random group model which has these properties. Start with the profinite free group $F_{n|\Gamma|}$ of generators γx_i for $i = 1, \ldots, n$ and $\gamma \in \Gamma$, with obvious γ action. Inside of there, take the subgroup $\mathcal{F} \subset F_{n|\Gamma|}$ generated by $y\gamma(y)^{-1}$.

Fact. $\mathcal{F}$ is generated by $z\gamma(z)^{-1}$ for $z \in \mathcal{F}$ and $\gamma \in \Gamma$. This is non-obvious.

Fact. **(3)** holds for a profinite group G iff group G is $\mathcal{F}/\left\langle r\gamma(r)^{-1}\right\rangle_{\in R, \gamma\in\Gamma}$

Now, the model is to take a group of the above form for r independent Haar random elements in $\mathcal{F}$ and then let $r \to \infty$.

Question 4.22.11 (Audience)**.** *How does property **(3)** obstruct the appearance of certain groups?*

Answer. For example, if H has a non-split central extension, then $G_k \not\simeq H$. ⋆

Question 4.22.12 (Audience)**.** *Does **(3)** hold also for* $\mathrm{Gal}(K^{\mathrm{un}}/K)$*?*

Answer. Almost. This is where the issue of roots of unity crops up. There are non-split central extensions of $\mathrm{Gal}(K^{\mathrm{un}}/K)$ which involve roots of unity. It does still satisfy **(3)** though, "up to roots of unity." ⋆

Question 4.22.13 (Audience)**.** *We said **(3)** does not hold for the class group, but when* $H, \widetilde{H}$ *are both abelian, these maps will factor through the class group. Do we really not have an analogue of **(3)** for something like "non-split abelian extensions away from roots of unity?"*

Answer. That's a good question. You really don't get a third condition on class groups for the following subtle reason. The extensions

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 0$$

under consideration are extensions of Γ-groups and $\mathbb{Z}/p\mathbb{Z}$ in particular has trivial Γ-action. If you have a surjection $\mathrm{Cl}_K \twoheadrightarrow H$, then H will have a non-trivial Γ-action (e.g. because $\sum_{\gamma\in\Gamma}\gamma$ will kill it), and you cannot have a non-split abelian extension of a non-trivial Γ-module by a trivial Γ-module. ⋆

Question 4.22.14 (Audience)**.** *We spent time setting up the topology, but then it quickly faded into the background. Where did we actually make use of it?*

Answer. We formally needed it to get a σ-algebra and so be able to talk about distributions/measures. Also, I guess when we wrote "let $n \to \infty$" in the end. We were looking at convergence in the weak topology. ⋆

Question 4.22.15 (Audience)**.** *What is the profinite free group?*

Answer. It is the profinite completion of the usual free group. It satisfies the expect universal property (it's left adjoint to the forgetful functor from profinite groups to sets). ⋆

No class next week. Last class a week from Wednesday.

4.23 Lecture 23 (12/2): Last Class

Fix Γ a finite group, and let Γ_∞ be a subgroup of order 1 or 2 (signature data). As K varies among Γ-fields over Q ($\mathbb{Q}$ or $\mathbb{F}_q(t)$), i.e. K/Q Galois with a choice of isomorphism $\mathrm{Gal}(K/Q) \simeq \Gamma$, with decomposition group @∞ isomorphic to Γ_∞. What is the distribution of $\mathrm{Gal}(K^{\mathrm{un}}/K)$?

Really, to have better understanding, we ask instead about $\mathrm{Gal}(K^{\mathrm{un},'}/K)$ where the $'$ means we are looking at the prime to $|\Gamma|\,|\mu_Q|$ part. Last time we described a random group from generators/random relations that was a conjectural answer. How to detect this distribution? As usual, via moments. These moments

$$\mathbb{E}(\#\,\mathrm{Sur}(\mathrm{Gal}(K^{un,'}/K), H))$$

give the average number of unramified H-extensions of K, so they are independently meaningful.

The moment problem has also been studied in the non-abelian case (e.g. recent work of Will Sawin[80]). There's now a choice of which moments. Recall that there is a Γ-action on $\mathrm{Gal}(K^{un,'}/K)$ (i.e. it is a Γ-group). Naturally then ask, for (possibly non-abelian) group M with Γ-action, about the "**equivariant moments**"

$$\mathbb{E}(\#\,\mathrm{Sur}_\Gamma(\mathrm{Gal}(K^{un,'}, M)).$$

Remark 4.23.1. Clearly, the non-equivariant moments cannot determine the distribution on Γ-groups, they could only (possibly) determine the distribution on groups. This is simple because the same group could have two non-isomorphic Γ-actions.

On the other hand, the equivariant moments can determine the distribution of Γ-groups which then determines the distribution on groups (just push-forward by forgetting Γ-action). ∘

[80] or Melanie's paper with Nigel Boston I think?

In particular, we should expect that the plain moments are a function of the equivariant moments. For G a Γ-group an H a group, one has

$$\operatorname{Hom}(G,H) = \operatorname{Hom}_\Gamma(G, \operatorname{Ind}_1^\Gamma H),$$

i.e. $\operatorname{Ind}_1^\Gamma$ is right adjoint to the forgetful functor. There is some special subset $\operatorname{Hom}_\Gamma^*(G, \operatorname{Ind}_1^\Gamma H)$ of the RHS corresponding to surjecting $\operatorname{Sur}(G,H)$ on the LHS. These are the Γ-maps $G \to \operatorname{Ind}_1^\Gamma H$ surjecting onto the first factor. Hence,

$$\#\operatorname{Sur}(G,H) = \sum_{\substack{S \subset \operatorname{Ind}_1^\Gamma H \\ \Gamma\text{-submod surj onto first factor}}} \#\operatorname{Sur}_\Gamma(G,S).$$

Remark 4.23.2. In general in situations like this, it is usually preferable to look at equivariant moments. You can recover plain moments from them, and they often have nicer, more recognizable expressions. $\circ$

Say we're looking at $\operatorname{Sur}_\Gamma(\operatorname{Gal}(K^{un,'}/K), M)$, so we're looking at

$$\begin{tikzcd} L \arrow[d, dash, "{M,\text{unram}}"] \arrow[dd, dash, bend right] \\ K \arrow[d, dash, "\Gamma"] \\ Q \end{tikzcd}$$

Then Γ-equivariance tells us precisely that L/Q is Galois. Recall that $\operatorname{Gal}(L/Q) = M \rtimes \Gamma$ since $(\#\Gamma, \#M) = 1$. We want to count $M \rtimes \Gamma$-extensions (where M part is unramified) and divide by the count of Γ-extensions.

Over $Q = \mathbb{F}_q(t)$ (always assume $(q, |\Gamma|\,|M|) = 1$), we again have these Hurwitz spaces, so we consider

$$\frac{\#H'_{M \rtimes \Gamma}(\mathbb{F}_q)}{\#H_\Gamma(\mathbb{F}_q)}$$

where the $'$ here indicated the inertia condition that the M part be unramified.

What are the components of these spaces? If r is a (non-trivial) conjugacy class of G ($M \rtimes \Gamma$ or Γ) and we have a G-cover $C \xrightarrow{G} \mathbb{P}^1$, we can define the **inertia degree of** $C/\mathbb{P}^1$ **of type** r to be

$$e_r := \sum_{\substack{x \in \mathbb{P}^1_{\mathbb{F}_q} \\ x \text{ inertia type } r}} \deg(x)$$

where we're summing over scheme-theoretic points. One needs to take care when making this definition, e.g. if r is the conjugacy class of an element g of order 3, then how do you need to be able to distinguish between inertia of type g and of type g^2. To not have to worry about this, one can consider r instead as a *conjugacy class of cyclic subgroups of* G.

For $G = \mathbb{Z}/2\mathbb{Z}$ or $A \rtimes_{-1} \mathbb{Z}/2\mathbb{Z}$ when inertia couldn't intersect A, there was only one inertia type. So before we only saw the total amount of ramification which was essentially encoded in the genus.

The tuple $(e_r)_r$ is a component invariant. Can picture this as a lattice of (groups of) components of these Hurwitz spaces. There are a few (like 3) natural questions at this point.

Question 4.23.3. *How will be project these components to one dimension? In the end, we want one invariant to count by which we can take up to X and then let $X \to \infty$.*

For example, genus is some linear combination of the e_r using Riemann-Hurwitz. One could also consider $\sum e_r$, the "total amount of ramification" or degree of ramification divisor on $\mathbb{P}^1$; arithmetically, this is like $\mathrm{Nm}\sqrt{\mathrm{Disc}}$ (over $\mathbb{Q}$, product of ramified primes).

Question 4.23.4. *Which $(e_r)_r$ have any components at all?*

Recall 4.23.5. In the quadratic case, one has a hyperelliptic curve $C \xrightarrow{2} \mathbb{P}^1$, and there are restrictions e.g. on the degree of its branch locus. We can put this curve in the form

$$C : y^2 = f(x)$$

with branch points corresponding to the roots of f. Furthermore, whether you have branching at ∞ depends on $\deg f$ being odd or even. The upshot is that when char $\neq 2$, the degree of the branch locus must be even. $\odot$

In some sense, the above fact is "the same" as the fact that discriminants over $\mathbb{Q}$ are $\equiv 0, 1 \pmod 4$. We'll give another explanation for the hyperelliptic branch locus condition that applies equally well to this discriminant/$\mathbb{Q}$ claim.

Proof that the degree of the branch locus of a hyperelliptic curve is even. Class field theory tells us that a quadratic extension of $\mathbb{F}_q(t)$ corresponds to a surjection

$$\Phi : J_{\mathbb{F}_q(t)} \twoheadrightarrow \frac{\mathbb{Z}}{2\mathbb{Z}}$$

from the idele class group. How do we see ramification from this map. The ramification at v is given by $\varphi_v := \Phi|_{\mathscr{O}_v^\times} : \mathscr{O}_v^\times \to \mathbb{Z}/2\mathbb{Z}$. We have $\varphi_v = 1$ if v unramified. In odd characteristic, there is only 1 nonzero map

$$\varphi_v : \mathscr{O}_v^\times \longrightarrow k(v)^\times \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

where $k(v)$ is the residue field whose units form a cyclic group of order $q^{\deg v} - 1$.

Let ε be a generator of $\mathbb{F}_q^\times$ (i.e. a primitive $(q-1)$st root of unit in $\mathbb{F}_q$); then $\Phi(\varepsilon) = 0$ by definition ($J_{\mathbb{F}_q(t)} = \mathbb{A}_{\mathbb{F}_q(t)}^\times / \mathbb{F}_q(t)^\times$). At the same time,

$$\Phi(\varepsilon) = \#\text{ramified } v \text{ s.t. } \varepsilon \text{ is not a square in } k(v)) \pmod 2.$$

Exercise. $\varepsilon \neq \square \in k(v) \iff \deg v$ is odd.

Thus,

$$\#\{\text{ram } v \text{ s.t. } \deg v \text{ is odd}\} \text{ is even}$$

so the degree of the branch locus is even. ■

Exercise. Use this to prove that all discriminants of number fields (over $\mathbb{Q}$) are $0, 1 \pmod 4$.

In general, this sort of consideration gives all obstructions to which $(e_r)_r$ are possible. This is in Melanie's paper with Liu, Zureick-Brown.

Given a Γ-extension $C \xrightarrow{\Gamma} \mathbb{P}^1$, can always factor this through an abelian extension

$$C \longrightarrow C^{\text{ab}} \xrightarrow{\Gamma^{\text{ab}}} \mathbb{P}^1,$$

so get $J_{\mathbb{F}_q(t)} \to \Gamma^{\text{ab}}$. The fact that $\Phi(\mathbb{F}_q^\times) = 0$ gives congruence conditions on certain linear combinations of the e_r.

Theorem 4.23.6. *There are no Hurwitz components when these conditions fail. When the conditions are satisfied (and also e_r sufficiently large), then there are Hurwitz components with these e_r.*

Example. You need inertia to generate the group, so when you have a big group, the e_r can't be so small you don't get something generating the groups. △

Question 4.23.7. *For the $(e_r)_r$ satisfying congruence conditions, how many Frob fixed components are there?*

The answer to this is kinda subtle and awkward and not nice to write down. However, the moments (which are a ratio of two numbers) you get in the end still look nice. For $(e_r)_r$ as above and all e_r sufficiently large,

$$\frac{\#\text{Frob-fixec components of } H'^{,(e_r)_r}_{M\rtimes\Gamma}(\mathbb{F}_q)}{\#\text{Frob-fixec components of } H_\Gamma(\mathbb{F}_q)} = \left|H_2(M,\mathbb{Z})^\Gamma\left[\left|\mu_{\mathbb{F}_q(t)}\right|\right]\right|.$$

Above, the H_2 is group homology (we take Γ-invariants of it) and $\#\mu_{\mathbb{F}_q(t)} = q-1$. In particular, when $(|M|, (q-1)|\Gamma|) = 1$, the above expression is simply 1. In the end, one obtains a $q \to \infty$ theorem getting the conjectured moments (which determine a unique distribution) for $\text{Gal}(K^{un,'}/K)$.

Question 4.23.8 (Audience)**.** *Is there any hope in the number field case to get results as good as this?*

Answer. Now, no. What's the cutting edge in the number field case?

- Today in the Harvard number theory seminar, there is talk about finding the average 2-torsion (i.e. $\mathbb{Z}/2\mathbb{Z}$-extensions) in certain families. See Shankar's talk today and his paper with Ho and Varma. In certain cases, they find a single moment.
- Alex Smith's work on $\text{Cl}_K[2^\infty]$ for quadratic fields gets entire distribution. Notice here that he's looking at the 2-part in degree 2 extensions (these are the same 2) which is a case we've largely ignored.

⋆

Question 4.23.9 (Audience)**.** *It seems a little weird that the thing that ends up being nice is the ratio. Really, we have a sum in the numerator and a sum in the denominator, and somehow their ratio is not a mess.*

Answer. In some sense, it had to be this way. Melanie said more than this. ⋆

Question 4.23.10 (Audience)**.** *Why was it important to order by the radical of the discriminant in this setting? There was more to this question I didn't get.*

Answer. You just had to order in some way; it was not necessary to order by this radical of the discriminant. You could use this approach, for example, when ordering by genus. The things that make square root of discriminant better are more subtle than the level of discussion we've had on this. These orderings could give different results (I think Melanie mentioned $\mathbb{Z}/3\mathbb{Z}$-moments in cubic fields), but won't in this case. $\star$

Question 4.23.11 (Audience)**.** *In the hyperelliptic example from earlier is there some restriction on the field being geometrically irreducible?*

Answer. There should not be. Class field theory will give you all abelian extensions, an you can determine from the map on the idele class group if the curve is geometrically irreducible or not. $\star$

There were a couple other questions, but I can only type so fast.

5 MAT 517 (Abelian and Shimura Varieties) – Princeton

5.1 Lecture 1 (9/1)

Instructure: Shou-Wu Zhang

5.1.1 Course/Administrative stuff

This will be a course on abelian and Shimura varieties. The first 2/3 will be "elementary." Think of this as a second course in algebraic geometry.

The first third will focus on elliptic curves and modular curves. The second third will focus on abelian varieties and the Siegal modular varieties. The last part will be about Shimura varieties.

We will spend a lot of time talking about arithmetic. The geometry parts can be found in references, but those tend to be more for algebraic geometers than for number theorists. We'll try to balance this by proving e.g. Mordell-Weil and Hasse bound when talking about elliptic curves. (Each third 8 lectures)

As for prereqs, good to know some AG, say chapters 1 – 4 of Hartshorne. The beginning will be "elementary" so have some time to read up on things if you don't know that material already.

References. For elliptic curves, Silverman. For modular curves, Katz-Mazur. For Abelian varieties, Mumford's book. For Shimura varieties, maybe Deligne's two papers. Other references that I missed...

The plan is pretty flexible since there is no particular goal to explain (just want to cover what all number theorists should know, roughly), so can email Shou-Wu with questions/suggestions. We will try to give an idea of what things people ask/can't answer in this material; we will see a lot of open questions. It's a huge package of arithmetic geometry, "typical Chinese meal. 8 dishes, not 3 dishes." (paraphrase)

5.1.2 Elliptic curves

Many ways to define. The typical AG way is...

Definition 5.1.1. Let k be a field. An **elliptic curve** E is a pair (E, O) where E is a complete, smooth, geometrically connected curve over k of genus 1, and $O \in E(k)$ is a rational point. $\diamond$

The first theorem is the following.

Theorem 5.1.2. *E has a unique algebraic group structure with identity O. More precisely, for any k-algebra A, the map*

$$\begin{array}{ccc} E(A) & \longrightarrow & \mathrm{Pic}^0(E_A) \\ x & \longmapsto & \mathscr{O}(x - O) \end{array}$$

is an isomorphism. Since the RHS has a group structure, this gives the (abelian) group structure on $E(A)$.

Corollary 5.1.3. *If E_1, E_2 are two elliptic curves, and $f : E_1 \to E_2$ is a morphism taking $f(O_1) = O_2$, then f is a group homomorphism.*

This corollary comes from the *uniqueness* in the theorem statement.

Proof idea of Theorem 5.1.2. Use Riemann-Roch ("For curves, you have only one theorem: Riemann-Roch" (paraphrase)). This says that for any complete, geometrically connected curve C/k with canonical divisor K, we have

$$h^0(D) - h^0(K-D) = \deg D + 1 - g$$

for any divisor $D \in \operatorname{Div}_k C$. ■

What are other basic, useful theorems?

Theorem 5.1.4. *Every elliptic curve E can be embedding into $\mathbb{P}^2$ by the linear system $|3O|$ with equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_3x + a_6 \text{ where } a_i \in k.$$

In above coordinates, $O \leftrightarrow \infty = (0:1:0)$. Conversely, any such equation defines an elliptic curve if it is smooth.

"The proof is also using Riemann-Roch; you don't have any other method."

Proof. Use

$$\mathrm{H}^0(\mathscr{O}_E) \hookrightarrow \mathrm{H}^0(\mathscr{O}_E(O)) \hookrightarrow \mathrm{H}^0(\mathscr{O}_E(2O)) \hookrightarrow \ldots \hookrightarrow \mathrm{H}^0(\mathscr{O}_E(5O))$$

where, by Riemann-Roch, $\dim \mathrm{H}^0(\mathscr{O}_E(nO)) = n$ if $n \geq 1$ and is 1 if $n = 0$. Pick generators $x \in \mathrm{H}^0(\mathscr{O}_E(2O))$ and $y \in \mathrm{H}^0(\mathscr{O}_E(3O))$. Note that $\operatorname{div}(x^3) = 6O + \ldots$ and $\operatorname{div}(y^2) = 6O + \ldots$, so $\operatorname{div}(x^3 - y^2) \in \mathrm{H}^0(\mathscr{O}_E(5O))$.

For the converse, just use genus formula $g = (d-1)(d-2)/2$ which is 1 if $d = 3$ (i.e. use adjunction). Another way to do it is say that $E \xrightarrow{2} \mathbb{P}^1$ is a double cover with ramification divisor of degree 4 (something like this), i.e. use Hurwitz. ■

How unique is the Weierstrass equation? Above proof shows that it depends on a choice of x and a choice of y. If (x, y) is one choice, then $(u^3x + v, u^2y + \alpha x + \beta)$ is another choice (with $u, v, \alpha, \beta \in k$) is another one. These are the only other choices.

Recall 5.1.5 (Adjunction formula). Say $f : X \hookrightarrow Y$ an embedding of smooth varieties. Get an exact sequence

$$0 \longrightarrow I_X/I_X^2 \longrightarrow f^*\Omega_Y \longrightarrow \Omega_X \longrightarrow 0$$

(where $\mathscr{O}_X = \mathscr{O}_Y/I_X$). Taking determinants gives

$$f^*\omega_Y = \omega_X \otimes \det(I_X/I_X^2).$$

⊙

Recall 5.1.6 (Hurwitz formula). Say $f : X \twoheadrightarrow Y$. This time get an exact sequence

$$0 \longrightarrow f^*\Omega_Y \longrightarrow \Omega_X \longrightarrow \Omega_{X/Y} \longrightarrow 0$$

where $\Omega_{X/Y}$ is actually a torsion sheaf, but can still define its determinant with some work. Get

I'm not sure why Shou-Wu included det in front of ω_X since that should already be a line bundle, but whatever

$$\det \omega_X = f^* \det \omega_Y \otimes \det \Omega_{X/Y}.$$

Define $\det \Omega_{X/Y}$ using projective resolutions or something like that? The normal Hurwitz formula drops out of taking degrees of the above equality. ⊙

Let's say something about the group law in Weierstrass form. The main take-away is that $\infty = (0 : 1 : 0)$ is the identity and

$$P + Q + R = 0 \iff P, Q, R \text{ colinear.}$$

Similarly,

$$P + Q = 0 \iff P, Q, \infty \text{ colinear} \iff P, Q \text{ are in a vertical line.}$$

(He said something about reading degrees of freedom off of the Weierstrass equation, but I missed it).

Remark 5.1.7. If $\operatorname{char} k \neq 2, 3$, we can simply the Weierstrass equation by completing the square/cube. Recall that we got

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_3x + a_6 \text{ where } a_i \in k.$$

before. Completing the square on the left makes $a_1 = 0 = a_3$ and completing the cube on the right makes $a_2 = 0$. Thus, we can get an equation

$$E_{a,b} : y^2 = x^3 + ax + b \text{ with } \Delta = 4a^3 + 27b^3 \neq 0.$$

These are not unique. We have

$$E_{a,b} \simeq E_{a',b'} \iff (a', b') = (au^4, bu^6)$$

for some $u \in k$. If $k = \overline{k}$, we can always make $a = 1$ or $b = 1$, but we can not do so in general. ○

This leads to the j-invariant.

5.1.3 j-invariants and classification

For any elliptic curve E defined by Weierstrass equation, get an invariant $k \ni j(E) =$ rational function of coefficients. If $\operatorname{char} k \neq 2, 3$, we get a simple formula

$$j(E_{a,b}) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

This only depends on the isomorphism type of E, so we get a map

$$\{\text{ellipic curves}/k\}/\simeq \xrightarrow{j} k.$$

Here are some facts.

- j is algebraic.
- j is surjective. We easily get $j = 0$ or $j = 1728$ by setting $a = 0$ or $b = 0$ (need $\operatorname{char} k \neq 2, 3$ for the $j = 1728$ case. Write down a different curve in those characteristics). For $j \neq 0, 1728$, can use

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}.$$

- If $k = \overline{k}$, then j is bijective. In general, this is not true when k is not algebraically closed.

This leads to a natural question. What are the fibers of the j-map? We call this fibers **twists**, i.e. E is a twist of E' if $j(E) = j(E')$.

We essentially always assume $\operatorname{char} k \neq 2, 3$. These characteristics are evil.

Fact. The twists of E are in bijection with $\mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(E_{\overline{k}}))$.

When $j(E) \neq 0, 1728$, all twists are **quadratic twists** (essentially because the Aut group above is small). Given $E : y^2 = x^3 + ax + b$, these twists are of the form $E^{(d)} : dy^2 = x^3 + ax + b$ or equivalently $E^{(d)} : y^2 = x^3 + ad^2x + bd^3$ for $d \in k^\times/(k^\times)^2$. If $j(E) = 0$, also get **cubic twists** $E_d : y^2 = x^3 + d$ where

$$E_{d_1} \simeq E_{d_2} \iff d_1/d_2 \in (k^\times)^6.$$

When $j(E) = 1728$, get $E'_d : y^2 = x^3 + dx$ where

$$E_{d_1} \simeq E_{d_2} \iff d_1/d_2 \in (k^\times)^4.$$

The upshot is that even when j-invariant is not bijective, its fibers are easily understood (usually just quadratic twists).

There is no family of elliptic curves defined over $\mathbb{A}^1$. This is the reason why we include level structures when talking about moduli spaces of elliptic curves.

He mentions what the issue is, but I didn't follow. Something about twists and/or negation.

5.1.4 Elliptic curves over $\mathbb{C}$

When $k = \mathbb{C}$, the complex points $E(\mathbb{C})$ for a complex Lie group of dimension 1 which is commutative and compact, so $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. This isomorphism is not canonical, but can make a canonical choice. Let $\widetilde{E(\mathbb{C})}$ be the universal cover, and then use $\widetilde{E(\mathbb{C})}/\pi_1 E(\mathbb{C})$. In alg geo, we prefer using differential forms, so let ω be a differential form. e.g. if $\omega = \mathrm{d}x/y$ when $E = E_{a,b}$. Then we get a map

$$\frac{\widetilde{E(\mathbb{C})}}{\pi_1(E(\mathbb{C}))} \xrightarrow{\int_0^P \omega} \mathbb{C}/\Lambda$$

with $\Lambda \subset \mathbb{C}$ a lattice.

This helps explain the name "elliptic curve". We just looked at something like $\int \frac{\mathrm{d}x}{\sqrt{x^3+ax+b}}$. This is an integral with no elementary anti-derivative, and is related to arc length of the ellipse $x^2/a^2 + y^2/b^2 = 1$.

Conversely, given $\mathbb{C}/\Lambda$, can get an algebraic elliptic curve, i.e. can write a Weierstrass equation in $\mathbb{P}^2(\mathbb{C})$. Recall that Weierstrass equation comes from finding two functions x, y with poles of order $2, 3$ at ∞. In this case, we can take

$$x = \wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right)$$

(summand above chosen so absolutely convergent when $z \notin \Lambda$) and

$$y = \wp'(z) = \frac{-2}{z^3} + \sum_{\lambda \in \Lambda} \frac{-2}{(z+\lambda)^3}$$

(our modification term has disappeared to derivative a little nicer). We can now try to match coefficients to find the polynomial relationship between these two. One gets

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$$

where

$$G_k(\Lambda) = \sum_{\substack{\lambda\in\Lambda \\ \lambda\neq 0}} \frac{1}{\lambda^k}.$$

Note that the above **Eisenstein series** is convergent only if $k \geq 3$ and is 0 is k is odd (pair λ^k with $-\lambda^k = (-\lambda)^k$).

Classification The j-invariant from before gives an algebraic classification of elliptic curves, but there is also an analytic method. Note that

$$\mathrm{Hom}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda'\}$$

(get this by lifting to universal cover $\mathbb{C}$) and the isomorphisms are exactly the α for which $\alpha\Lambda = \Lambda'$. Writing $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we can divide by $1/\omega_1$ to assume $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau = \omega_2/\omega_1 \in \mathbb{C} \setminus \mathbb{R}$. By negating τ if necessary, we can even require $\tau \in \mathfrak{H}$, the upper half-plane. Thus every complex elliptic curve is of the form $E_\tau := \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau$ with $\tau \in \mathfrak{H}$. We have $E_{\tau_1} \simeq E_{\tau_2}$ if and only if $\tau_2 = \gamma\tau_1$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. The action is

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \gamma\tau := \frac{a\tau + b}{c\tau + d}.$$

Could equivalently have used the lower half plane, but traditionally, people prefer the upper half plane.

The upshot is that we have bijections

$$\mathbb{C} \xleftarrow{\sim} \{\text{elliptic curves}/\mathbb{C}\} \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$$

From this we see that $j(\tau)$ is an analytic function on $\mathfrak{H}$ which is invariant under $\mathrm{SL}_2(\mathbb{Z})$. One can even write down an explicit formula for it.

Note that $\mathrm{SL}_2(\mathbb{Z})$ is generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1$ and $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : \tau \mapsto -\frac{1}{\tau}$. One can show that a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ is given by the usual picture. A few of the points

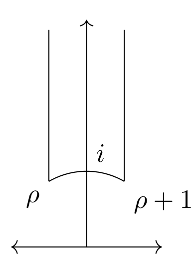


Figure 19: A fundamental domain for $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathfrak{H}$

in this domain have non-trivial stabilizers, so this gives you an orbifold. Note that $j(i) = 1728$ and $j(\rho) = 0$ where $\rho = \exp(2\pi i/3)$. These stabilizers help explain why you cannot have a universal family over $\mathbb{C} = \mathbb{A}^1(\mathbb{C})$.

Remark 5.1.8. Consider $\mathcal{E} = \mathbb{Z}^2 \backslash \mathfrak{H} \times \mathbb{C}$ where the action is

$$(m, n) \cdot (\tau, z) = (\tau, z + m + n\tau).$$

This is a universal elliptic curve over $\mathfrak{H}$. Can mod out by $\mathrm{SL}_2(\mathbb{Z})$ action to get a diagram

$$\begin{tikzcd} \mathcal{E} \arrow[r] \arrow[d] & \mathfrak{H} \arrow[d] \\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{E} \arrow[r] & \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \end{tikzcd}$$

but the bottom arrow is *not* a universal elliptic curve. In fact, it might be a ruled surface (?).

Something about $z \mapsto -z$ again

To construct a universal family of elliptic curves, we need to

- add a level structure to get rid of twists (from algebraic point of view)
- replace $\mathrm{SL}_2(\mathbb{Z})$ by a subgroup (from analytic point of view)

Next class, we'll say a little bit about level structures, and then talk about arithmetic of elliptic curves (Mordell-Weil, Selmer group, Shafervich group, etc.).

Question 5.1.9 (Audience)**.** *What's going on with the obstruction to the universal elliptic curve?*

Answer (At least, what I was able to understand of the answer)**.** We have $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ acting on $\mathfrak{H} \times \mathbb{C}$. What is this action?

Question: Why is this the action of the second coordinate (& did I write down the wrong thing)?

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\tau, z) = \left(\frac{a\tau + b}{c\tau + d}, \frac{z}{c\tau + d} \right).$$

If you take $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathrm{Id}$, then $\gamma(\tau, z) = (\tau, -z)$. The fibers are then (quotients of) $E/(x \sim -x)$ (and this is isomorphic to $\mathbb{P}^1$?[81]) or something like this. Ultimately, the issue is that we want to avoid fixed points of the $\mathrm{SL}_2(\mathbb{Z})$-action (especially those inducing non-trivial automorphisms on the associated fiber of $\mathcal{E} \to \mathfrak{H}$).

Something something points with stabilizers are 0 and ρ, so sif you have a subgroup without any points of order $2, 4, 6$ (or 3?), you can get a universal family.

This overflow post is potentially helpful. ⋆

5.2 Lecture 2 (9/3)

Last time We fixed an elliptic curve $(E, 0)$ over some field k (usually $\operatorname{char} k \neq 2, 3$). We gave it a Weierstrass equation, and then studied the set of elliptic curves over k up to isomorphism. We constructed

[81] Give E a Weierstrass equation $E : y^2 = f(x)$. Then there's a degree 2 map $E \to \mathbb{P}^1, (x, y) \mapsto x$ whose fibers are $\{P, -P\} = \{(x, y), (x, -y)\}$, so $E/(P \sim -P) = \mathbb{P}^1$. Alternatively, letting $C = E/(x \sim -x)$, Hurwitz formula gives

$$0 = 2g(E) - 2 = 2(2g(C) - 2) + \sum_{x \in E} (e_x - 1)$$

The ramification points of $E \to C$ are the 2-torsion points of E; there are 4 of these, each with ramification degree 2, so $0 = 2(2g(C) - 2) + 4 \implies g(C) = 0$

the j-invariant which is a map

$$\{\text{ellipic curves}/k\}/\simeq \xrightarrow{j} k$$

which is always surjective (even when $\operatorname{char} k = 2, 3$), but is not always injective. It is injective if $k = \overline{k}$, but in general there are non-trivial "twists."

Question 5.2.1. *How to build up a moduli?*

We looked at this question over $k = \mathbb{C}$, where elliptic curves are 1-dimensional complex tori. This connection was given, in one direction, by considering the integral $\int \frac{dx}{y}$, and in the other direction, by using the Weierstrass function $\wp$. The ability to study moduli, came from the connection between complex tori and lattices. The picture looks like

$$\begin{tikzcd}
& \left\{\substack{\text{elliptic curves}\\ y^2=x^3+ax+b}\right\}/\text{iso} \arrow[dl, "\sim"'] \arrow[rr, bend left, "\int \frac{dx}{y}"] & & \{\text{complex tori of dimension } 1\}/\text{iso} \arrow[ll, bend left, "(\wp,\ \wp')"] \arrow[dd] \\
\mathbb{C} & & & \\
& \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \arrow[ul, "\sim"] & & \{\text{lattices } \Lambda \subset \mathbb{C}\}/\text{homothety} \arrow[ll, "\sim"']
\end{tikzcd}$$

We see that this moduli space is $\mathbb{C}$. Can we get a universal family over it? The answer turns out to be no. Say we have some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ giving a map

$$\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau) \longrightarrow \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\gamma\tau).$$

Recall this sends

$$\gamma\tau = \frac{a\tau + b}{c\tau + d} \text{ and } z \mapsto \frac{1}{c\tau + d} z.$$

We get an issue when $\gamma = -\operatorname{Id}$ since this induces a non-trivial automorphism on $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$.

We can solve this problem by replacing $\mathrm{SL}_2(\mathbb{Z})$ with a subgroup which acts *freely* on the upper half plane $\mathfrak{H}$. This will get us modular curves.

5.2.1 Category of elliptic curves

In geometry, you typically don't study just one object. It is more profitable to study classes of objects together all at once.

Notation 5.2.2. We'll write E instead of (E, O) with the understanding that it comes with a choice of basepoint. Also, let $\operatorname{Hom}(E_1, E_2) = \{f : E_1 \to E_2 : f(0) = 0\}$.

Note that $\operatorname{Hom}(E_1, E_2)$ is an abelian group, so this category is an additive category.

Fact. Every $\varphi : E_1 \to E_2$ is a group homomorphism.

Hence, the additive structure on $\operatorname{Hom}(E_1, E_2)$ can come from the additive structure on E_1 or the one on E_2; they give the same result.

Fact. There is a natural bijection $\mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \mathrm{Hom}(E_2, E_1)$.

For the above fact, consider some $\varphi : E_1 \to E_2$. Recall that[82] $E_1 \cong \mathrm{Pic}^0(E_1)$ (degree 0 line bundles) and $E_2 \cong \mathrm{Pic}^0(E_2)$. The morphism φ induces a pullback morphism $\varphi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$. The composition

$$E_2 \xrightarrow{\sim} \mathrm{Pic}^0(E_2) \xrightarrow{\varphi^*} \mathrm{Pic}^0(E_1) \xleftarrow{\sim} E_1$$

is called $\varphi^\vee : E_2 \to E_1$. On line bundles, this looks like

$$\varphi^* : \mathscr{O}_{E_2}([P] - [O]) \mapsto \mathscr{O}_{E_1}\left(\sum_{\varphi(Q)=P} [Q] - \sum_{\varphi(R)=[O]} [R]\right)$$

so, on curves, looks like

$$\varphi^\vee(P) = \sum_{\varphi(Q)=P} Q - \sum_{\varphi(R)=O} R.$$

Fix $Q_0 \in E_1$ with $\varphi(Q_0) = P$. Then, $Q = Q_0 + R$ also maps to P (and this gives everything mapping to P), so $\varphi^\vee(P) = (\deg \varphi) Q_0$ if $\varphi(Q_0) = P$.

Notation 5.2.3. We also use $\widehat{\varphi}$ to denote $\varphi^\vee$.

Fact.

- φ is linear.
- $\widehat{\widehat{\varphi}} = \varphi$.
- $\widehat{\varphi_1 \circ \varphi_2} = \widehat{\varphi}_2 \circ \widehat{\varphi}_1$.
- $\varphi \circ \widehat{\varphi} : E_2 \to E_2$ and $\widehat{\varphi} \circ \varphi : E_1 \to E_2$ are both multiplication by $\deg \varphi$.

Note that E_1 is a kind of covering of E_2. Note that, over $\mathbb{C}$, when we encounter covers we can study them by appealing to a universal cover of our base space, but in algebraic geometry, we do not have universal covers.

Consider a sequence $\ker \varphi \to E_1 \xrightarrow{\varphi} E_2$, and assume that $\# \ker \varphi$ and $\mathrm{char}\, k$ are coprime. Then, φ is an étale map.

Temporarily assume $k = \overline{k}$. In above situation, looks like $E_2 = E_1/G$ (where $G = \ker \varphi$?). We also have the dual map $E_2 \xrightarrow{\widehat{\varphi}} E_1$, so we also get $\widehat{G} = \ker \widehat{\varphi}$.

Question 5.2.4. *What is the relation between G and $\widehat{G}$?*

Theorem 5.2.5. *There is a canonical pairing $G \times \widehat{G} \to k^\times$.*

This can be constructed abstractly or concretely. Let's do abstract first. Consider

$$\begin{tikzcd} \mathrm{Pic}^0(E_1) \arrow[r, equal] & E_1 \arrow[d, "\varphi"] \\ \mathrm{Pic}^0(E_2) \arrow[u, "\varphi^*"] \arrow[r, equal] & E_2 \end{tikzcd}$$

Note that $\ker \varphi^*$ are the line bundles $\mathscr{L}$ on E_2 such that $\varphi^* \mathscr{L}$ is trivial.

[82] This map is $E \ni p \mapsto \mathscr{O}(p - 0) \in \mathrm{Pic}^0(E)$ where $0 \in E$ is the chosen basepoint.

Discussion of a general result Say $\pi : X \to Y$ is a map of topological spaces. Assume there is a transformation group Γ such that $Y = X/\Gamma$ (and π is the natural projection). We get a pullback map $\pi^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$. Here's a general fact:

$$\ker(\mathrm{Pic}(Y) \to \mathrm{Pic}(X)) = \mathrm{H}^1(\Gamma, \mathscr{O}(X)^\times).$$

Proof sketch. Start with some $\mathscr{L} \in \mathrm{Pic}\, Y$ and suppose $\pi^*\mathscr{L} \simeq X \times \mathbb{A}^1$ is trivial. Note that, for $x \in X$, the fibers $(\pi^*\mathscr{L})(x) \simeq (\pi^*\mathscr{L})(\gamma x) \simeq \mathscr{L}(y)$ via the map π, by definition. For any γ, we get

$$\begin{tikzcd}
\mathbb{A}^1 \arrow[rr, "\sim"] \arrow[d, equal] & & \mathbb{A}^1 \arrow[d, equal] \\
\pi^*\mathscr{L}(x) \arrow[rr, "\sim"] \arrow[dr, "\sim"] & & \pi^*\mathscr{L}(\gamma x) \arrow[dl, "\sim"'] \\
& \mathscr{L}(y) &
\end{tikzcd}$$

The top map is a linear map between 1-d vector spaces, so given by multiplication by some $\sigma(\gamma)(x) \in k^\times$.

What have we defined so far? For any $x \in X$, and $\gamma \in \Gamma$, we have $\sigma(\gamma)(x) \in k^\times$. We have a diagram

$$\begin{tikzcd}
\mathbb{A}^1 \times X \arrow[r] \arrow[d] & \mathscr{L} \arrow[d] \\
X \arrow[r] & Y
\end{tikzcd}$$

where, remember, $\pi^*\mathscr{L} \simeq \mathbb{A}^1 \times X$. Furthermore, Γ acts on both $\mathbb{A}^1 \times X$ and on X. The first action given by $\gamma(t, x) = (\sigma(\gamma)(x)t, \gamma x)$.

Basically, for $\gamma \in \Gamma$, we have constructed $\sigma(\gamma) \in \mathscr{O}(X)^\times$. One can check that this construction defines a 1-cochain. However, it depends on our choice of trivialization $\pi^*\mathscr{L} \simeq \mathbb{A}^1 \times X$. Luckily though, changing the trivialization only modifies σ by a coboundary. Hence, we get a well-defined cohomology class in $\mathrm{H}^1(\Gamma, \mathscr{O}(X)^\times)$. ∎

Corollary 5.2.6. *When the action of Γ on $\mathscr{O}(X)^\times$ is trivial, we have*

$$\ker(\mathrm{Pic}(Y) \to \mathrm{Pic}(X)) = \mathrm{H}^1(\Gamma, \mathscr{O}(X)^\times) = \mathrm{H}^1(\Gamma, k^\times) = \mathrm{Hom}(\Gamma, k^\times).$$

Back to elliptic curves Note that $\ker \widehat{\varphi} = \ker(\mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)) = \ker(\mathrm{Pic}(E_2) \to \mathrm{Pic}(E_1))$, so we have shown that actually

$$\ker \widehat{\varphi} \simeq \mathrm{Hom}(\ker \varphi, k^\times).$$

Question: Why is the action trivial here?

Answer: $\ker \varphi \curvearrowright E_1$ by translation, and this does nothing to constant functions

This gives us our pairing

$$\ker \widehat{\varphi} \times \ker \varphi \xrightarrow{\sim} k^\times$$

which is called the **Weil pairing**.

We'll do something similar with modular forms later on, but I didn't get the details...

Another extreme situation is X simply connected so $\pi : X \to Y$ is the universal cover. Here, $\mathrm{Pic}(Y) = \mathrm{H}^1(\pi_1(Y), \mathscr{O}(X)^\times)$. This applies, for example, when $X = \mathbb{C}$ and $Y = \mathbb{C}/\Lambda$. Also when $X = \mathfrak{H}$

and $Y = \Gamma\backslash\mathfrak{H}$.

Can also consider the situation $\mathbb{C} \to \mathbb{C}^\times \to E = \mathbb{C}^\times/q^{\mathbb{Z}}$ where the first map is $z \mapsto \exp(2\pi i z)$. Note that $\operatorname{Pic}\mathbb{C}^\times = 0$ is trivial. I didn't get where he was going with this...

Let's now give a more concrete construction of the Weil pairing. Recall our favorite diagram

$$\begin{tikzcd} E_1 \arrow[r, "\varphi"] \arrow[d, equal] & E_2 \arrow[d, equal] \\ \operatorname{Pic}^0(E_1) & \operatorname{Pic}^0(E_2) \arrow[l, "\varphi^*=\widehat{\varphi}"'] \end{tikzcd}$$

We have $x \in \ker\widehat{\varphi} \iff \widehat{\varphi}x = 0$. This means there is some rational function $f \in k(E_1)$ such that

$$\operatorname{div} f = \sum_{\varphi(z)=x} [z] - \sum_{\varphi(z')=0} [z']$$

Note that $\operatorname{div}(f)$ is invariant under translation by the kernel. Given $y \in \ker\varphi$, consider $(T_y^* f)(z) = f(z+y)$. Note that $\operatorname{div}(T_y f) = \operatorname{div} f$ which means that $f/T_y^* f \in k^\times$ is a constant! This is the Weil pairing:

$$\langle x, y\rangle_{\text{weil}} = \frac{f(y+z)}{f(z)}$$

Question: Why does this not only depend on y?

Answer: Because f depends on $x \in \ker\widehat{\varphi}$

for any $z \in E_1$.

He wrote something like given $E_1 \xrightarrow{\varphi} E_2$, we have

$$\varphi_*\mathscr{O}_{E_1} \simeq \bigoplus_{x\in\ker\widehat{\varphi}} \mathscr{L}_x \simeq \bigoplus_{\psi:\ker\varphi\to k^\times} \mathscr{L}(\psi).$$

The Weil paring comes from having two ways to calculate push forward of structure sheaf. Since φ is étale, this push-forward is a rank n vector bundle, with the above two descriptions.

5.2.2 Applications of Weil pairing

Homology of elliptic curves Fix $n \in \mathbb{Z}$ coprime to $\operatorname{char} k$, and consider the multiplication by n map $n_E : E \to E$ on some elliptic curve E. We claim that

$$\ker(n_E) \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

One way to see this is to note that $\deg n_E = n_E^2$. This is because $\deg n_E = n_E \circ \widehat{n}_E$ and $\widehat{n}_E = n_E$. Hence, the kernel is a group of order n_E^2 and also contains subgroups of size m^2 for all $m \mid n_E$. This (or something close to this) uniquely determines it.

Note we have maps $E[\ell^n] \xrightarrow{\times\ell} E[\ell^{n-1}]$. Take inverse limits, we get the **Tate module** $T_\ell(E) = \varprojlim E[\ell^n]$. The Weil pairing gives a map

$$T_\ell(E) \times T_\ell(E) \to \mathbb{Z}_\ell(1)$$

where $\mathbb{Z}_\ell(1) = \varprojlim_m \mu_{\ell^m}$ where μ_{ℓ^m} is the group of roots of unity, so

$$\mu_{\ell^m}(k) = \left\{z \in k : z^{\ell^m} = 1\right\}.$$

Note that $T_\ell(E) = \mathrm{H}_1(E, \mathbb{Z}_\ell)$ (take this as a definition of the RHS for now). The Weil paring then looks like

$$\mathrm{H}_1(E, \mathbb{Z}_\ell) \times \mathrm{H}_1(E, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell(1)$$

which is reminiscent of Poincaré duality. The $\mathbb{Z}_\ell(1)$ more-or-less tells you "orientation"; abstractly, $\mathbb{Z}_\ell(1) \simeq \mathbb{Z}_p$ but $\mathbb{Z}_\ell(1)$ has a canonical choice of basis. The cohomology will be $\mathrm{H}_1(E, \mathbb{Z}_p)^\vee$ so you get something like $\mathrm{H}^1(E, \mathbb{Z}_\ell) = \mathrm{H}_1(E, \mathbb{Z}_\ell)(-1)$.

Level structure on elliptic curves An **elliptic curve E with a full level n-structure** is a triple (E, p, q) where E is an elliptic curve, and $\{p, q\}$ form a base for $E[n]$.

Theorem 5.2.7. *If $n \geq 3$ and $(n, \operatorname{char} k) = 1$, then the fine moduli space of $\{(E, p, q)\}$ does exist.*

This is easy over $\mathbb{C}$. Recall $E = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$. We can take $P = \frac{1}{n}$ and $Q = \frac{\tau}{n}$, so consider pairs $(E, \frac{1}{n}, \frac{\tau}{n})$. The moduli space is given by $Y(n) = \Gamma(n)\backslash\mathfrak{H}$ where $\Gamma(n) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))$.

Next time we'll talk about elliptic curves over finite fields, then elliptic curves over number fields, then come back to modular curves at some point.[83]

5.3 Lecture 3 (9/8)

Last time we studied the category of elliptic curves. Given E_1, E_2, get an abelian group $\mathrm{Hom}(E_1, E_2)$. We observed some nice properties

- (duality) Have a map
$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(E_2, E_1) \\ \varphi & \longmapsto & \widehat{\varphi} \end{array}.$$
satisfying $\widehat{\varphi_1 + \varphi_2} = \widehat{\varphi}_1 + \widehat{\varphi}_2$, $\widehat{\varphi_1 \circ \varphi_2} = \widehat{\varphi}_2 \circ \widehat{\varphi}_1$, and $\varphi \circ \widehat{\varphi} = \mathrm{id}$.

  Question: Isn't this multiplication by degree

- (Weil pairing) Start with $E_1 \xrightarrow{\varphi} E_2$ so get
$$\varphi^* : \mathrm{Pic}^0(E_2) \simeq E_2 \xrightarrow{\widehat{\varphi}} E_1 \simeq \mathrm{Pic}^0(E_1).$$
The Weil paring is perfect pairing $\ker \varphi \times \ker \widehat{\varphi} \to k^\times$. There are a couple ways to describe it
  - The sheaf $\varphi_* \mathscr{O}_{E_1}$ is a locally free sheaf of rank $\deg \varphi$, and it comes with an action of $\ker \varphi \curvearrowright \varphi_* \mathscr{O}_{E_1}$. If $(\# \ker \varphi, \operatorname{char} k) = 1$, then (like in the theory of finite group actions), we can decompose
$$\varphi_* \mathscr{O}_{E_1} = \bigoplus_{\chi : \ker \varphi \to k^\times} \mathscr{O}_{E_2}(\chi).$$

[83] Studying one modular curve is also boring, but studying morphisms between them reveals a rich structure

We can be a little more explicit. Given $U \subset E_2$ open, we have

$$\mathscr{O}_{E_2}(\chi)(U) = \left\{f \in \varphi^{-1}(u) \mid f(x+t) = \chi(t)f(x)\,\forall t \in \ker\varphi, x \in E_1\right\}$$

The Weil pairing is like an explicit way to write down the torsion sheaf and/or a kind of Fourier analysis. The actual pairing

$$\ker\varphi \times \ker\widehat{\varphi} \longrightarrow k^\times$$

comes from $\operatorname{Hom}(\ker\varphi, k^\times) \simeq \ker\widehat{\varphi}$ via $\chi \mapsto \mathscr{O}_{E_2}(\chi)$.

– Write $\mathscr{L} = \mathscr{O}_{E_2}(P-0)$ with $\varphi^*\mathscr{L}$ trivial, i.e. $\mathscr{O}_{E_2}(\varphi^*P - \varphi^*0) \simeq \mathscr{O}_{E_2}$. So there's some $f \in k(E_1)^\times$ such that

$$\operatorname{div} f = \varphi^*P - \varphi^*0 = \sum_{\varphi(Q)=P}[Q] - \sum_{\varphi(R)=0}[R].$$

For any $T \in \ker\varphi$, we can translate points in above divisor by T without changing anything, so $\operatorname{div} f(X+T) = \operatorname{div} f(X)$, i.e. $f(X+T)/f(X)$ is a constant. The map $T \mapsto f(X+T)/f(X)$, we'll call $\chi(T)$. This gives another description of the Weil pairing.

We saw 2 applications of the Weil pairing before.

5.3.1 Homology or something

The first was "singular" homology and cohomology of elliptic curves. Fix some ℓ with $(\ell, \operatorname{char} k) = 1$. Define $T_\ell(E) = \varprojlim_n E[\ell^n] = \mathrm{H}_1(E, \mathbb{Z}_\ell)$. The Weil pairing is like an intersection pairing

$$\mathrm{H}_1(E, \mathbb{Z}_\ell) \times \mathrm{H}_1(E, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}.$$

Can define $\mathrm{H}^1(E, \mathbb{Z}_\ell) = \operatorname{Hom}(\mathrm{H}_1(E, \mathbb{Z}_\ell), \mathbb{Z}_\ell)$. Recall that $\mathrm{H}_1(E, \mathbb{Z}_\ell)$ is a free $\mathbb{Z}_\ell$-module of rank 2. Why do we like cohomology? Think of H_1 as a functor from elliptic curves$/k$ to abelian groups. Consider

$$\operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \mapsto \operatorname{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

This map is injective since $\operatorname{rank}\operatorname{Hom}(E_1, E_2) \le 4$. Also, $\operatorname{End}(E) \otimes \mathbb{Q}$ is semi-seimple of dimension ≤ 4. There are a few cases $\operatorname{End}(E)\otimes\mathbb{Q}$ is $\mathbb{Q}$, K (and imaginary quadratic), or D (a definite quaternion algebra).

Definition 5.3.1. D being a **definite quaternion algebra** means $D = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ with $i^2 < 0$, $j^2 < 0$, and $ij = -ji$. ◇

If $D = \operatorname{End}(E) \otimes \mathbb{Q}$ comes from an elliptic curve E/k, then D is ramified at ∞ and $p = \operatorname{char} k$.

Note that $\operatorname{End}(E)$ has an involution $\varphi \mapsto \widehat{\varphi}$ satisfying $\varphi \circ \widehat{\varphi} = \deg\varphi > 0$. Hence, $\varphi \mapsto \deg\varphi$ is a positive quadratic form on $\operatorname{End}(E)$. When $\operatorname{End}(E) \otimes \mathbb{Q} = \mathbb{Q}$, we have $\widehat{\varphi} = \varphi$. When it is K, we have $\widehat{\varphi} = \overline{\varphi}$. When it is D, we have $\widehat{\varphi} = \overline{\varphi}$ where here

$$\varphi = a + bi + cj + dk \implies \overline{\varphi} = a - bi - cj - dk$$

so $\varphi\overline{\varphi} = a^2 + b^2(-i^2) + c^2(-j^2) + d^2(-k)^2$.

If $\operatorname{char} k = 0$, we have $\operatorname{End} E \otimes \mathbb{Q} = \mathbb{Q}$ (**non-CM curve**) or $\operatorname{End}(E) \otimes \mathbb{Q} = K$ (**CM curve**).

When $\operatorname{char} k = p$ ($k = \mathbb{F}_q$), then $\operatorname{End}(E) \ni \varphi$, the Frobenius map $(x, y) \mapsto (x^q, y^q)$. This map is purely inseparable. Hence,

$$\operatorname{End}(E) \otimes \mathbb{Q} = \begin{cases} K & \text{if } \textbf{ordinary or CM} \\ D & \text{if } \textbf{supersingular} \end{cases}.$$

We know $\varphi\widehat{\varphi} = q$ (φ=Frobenius still). E is ordinary when $\widehat{\varphi}$ is étale while E is supersingular when $\widehat{\varphi}$ is purely inseparable. Note that purely inseparable maps always factor through Frobenius, so in the supersingular case, $\widehat{\varphi}$ is basically (maybe literally?) φ.

In the ordinary case, we have $E[q] \simeq \mathbb{Z}/q\mathbb{Z}$ since $\deg_s \widehat{\varphi} = q$ and $\deg_s \varphi = 1$. When $\widehat{\varphi}$ is purely inseparable, turns out it actually has a model over $\mathbb{F}_{p^2}$. Hence, there are only finitely many supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ for a given p.

This all gives a decent homology theory for elliptic curves.

5.3.2 Modular curves

This is our second application of the Weil pairing. Recall that the j-invariant is nice, but we cannot have a universal family for elliptic curves, even in characteristic 0.

Definition 5.3.2. Fix a positive integer N. An **Elliptic curve with full level N-structure** is a triple (E, P, Q) with E/k an elliptic curve (can make definition for arbitrary base scheme) and two points $P, Q \in E(k)$ such that

$$\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^2 \xrightarrow{\sim} E[N] \text{ via } (a, b) \mapsto aP + bQ.$$

$\diamond$

Fact. If $N \geq 3$, then $\operatorname{Aut}(E, P, Q) = \{1\}$ is trivial (when $N = 2$, multiply by -1, I think). This gives the existence of universal family of elliptic curves with full level N structure.

The universal family will look like a scheme $\mathcal{E} \to \mathcal{M}$ with three sections $0, P, Q : \mathcal{M} \to \mathcal{E}$ and whose fibers are elliptic curves (and $0, P, Q$ satisfy the obvious properties). It also comes with a Weil pairing, landing in $\mu_N \subset \mathscr{O}(\mathcal{M})^\times$. Hence, $\mathcal{M}$ will be defined over $\mathbb{Z}[\zeta_N, \frac{1}{N}]$. We write $\mathcal{M} = X(N)$.

Over complex numbers Want $E/\mathbb{C}$ with points P, Q generating $E[N]$. The typical situation looks like $E_\tau = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ with $P_\tau = \frac{1}{N}$ and $Q_\tau = \frac{\tau}{N}$. What do the maps between these look like? Say we have

$$\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau \longrightarrow \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau'$$

This comes from some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ so $\tau' = \frac{a\tau+b}{c\tau+d}$ and $z \mapsto \frac{z}{c\tau+d}$ (since you are turning one latice into the other). We now also need

$$\frac{1}{N} \bmod \mathbb{Z} + \mathbb{Z}\tau \longmapsto \frac{1}{N} \bmod \mathbb{Z} + \mathbb{Z}\tau'$$

and same for τ/N. This forces

$$\gamma \in \Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

The quotient $X(N) = \Gamma(N)\backslash\mathfrak{H}$ is a modular curve.

Definition 5.3.3. A discrete group $\Gamma \hookrightarrow \mathrm{SL}_2(\mathbb{Q})$ is called a **congruence subgroup** if $\Gamma \supset \Gamma(N)$ for some N. $\diamond$

If Γ is a congruence subgroup, then $\Gamma\backslash\mathfrak{H}$ is a modular curve, so we get a whole system of modular curves. This system has an action by $\mathrm{GL}_2(\mathbb{Q})^+$ which gives us Hecke operators.

An interesting this is that $X(N) = \Gamma(N)\backslash\mathfrak{H}$ is a Riemann surface and so also an algebraic curve over $\mathbb{C}$. In fact, it can even be defined over $\mathbb{Q}(\zeta_N)$ where ζ_N is a primitive Nth root of unity.

If one likes, they can do something wild like take the projective limit of these modular curves. This will be something like an 'algebraic universal cover' of these modular curves. Analytically, $\mathfrak{H}$ is a cover of all of them, but this limit thing would be something more algebraic.

$$X(N) = \{(E, P, Q) \mid \langle P, Q\rangle = \zeta_N\}$$

Note that we have a ramified covering $X(N) \to X(1) = \mathbb{A}^1$. The function field of $X(1)$ is $\eta = \mathbb{Q}(j)$, so the function field $K = K(X(N))$ of $X(N)$ is a finite (Galois) extension of $\mathbb{Q}(j)$. One can show $\mathrm{Gal}(K/\eta) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. One has a diagram

$$\begin{tikzcd} X(N) \arrow[r] \arrow[d] & \operatorname{Spec}\mathbb{Q}(\zeta_N) \arrow[d] \\ X(1) \arrow[r] & \operatorname{Spec}\mathbb{Q} \end{tikzcd}.$$

Note that $X(N)$ is connected over $\mathbb{Q}(\zeta_N)$, but not over $\mathbb{Q}$ or something like that. I didn't really understand.

5.3.3 Arithmetic

Our first question is to count rational points $E(\mathbb{F}_q)$ when $E/\mathbb{F}_q$ is an elliptic curve.

Example. $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q$. Given x, one wonders whether $f(x) = x^3 + ax + b$ has $1, 2$ or 0 square roots. $\triangle$

Theorem 5.3.4 (Hasse)**.** *$\#E(\mathbb{F}_q) = q + 1 - a_E$ where $|a_E| \leq 2\sqrt{q}$.*

This is the first thing we want to prove. Let $\varphi : E \to E$ be Frobenius, so $\varphi(x, y) = (x^q, y^q)$. Note that

$$E(\mathbb{F}_q) = \left\{P \in E(\overline{\mathbb{F}}_q) \mid \varphi(P) = P\right\} = \ker\left(\varphi - 1 : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)\right).$$

The map $\varphi - 1$ is separable since $\mathrm{d}(\varphi - 1) = 0 - \mathrm{d}\,\mathrm{id} = -\,\mathrm{id}$ (the latter id is identity on tangent space). Thus, $\#E(\mathbb{F}_q) = \deg(\varphi - 1)$. This degree is

$$(\varphi - 1)(\widehat{\varphi} - 1) = \varphi\widehat{\varphi} - (\varphi + \widehat{\varphi}) + 1 = \deg\varphi + 1 - (\varphi + \widehat{\varphi}) = q + 1 - (\varphi + \widehat{\varphi}).$$

Thus, we have shown that $\varphi + \widehat{\varphi}$ is multiplication by $a =: \operatorname{tr}\varphi$. Thus, we need to show

$$|\operatorname{tr}\varphi| \le 2\sqrt{q}.$$

This feels very quadratic equation-y. We're basically saying something like $X^2 - aX + q$ has no real roots ($a^2 - 4q \le 0$). It suffices to show that $x^2 - ax + q \ge 0$ for all $x \in \mathbb{R}$; in fact, enough to show this for $x \in \mathbb{Q}$. Say $x = m/n$, so we want

$$\left(\frac{m}{n}\right)^2 - a\frac{m}{n} + q \ge 0.$$

This says that

$$m^2 - amn + qn^2 \ge 0.$$

We are in luck because (see below by remembering how we arrived at this quadratic)

$$m^2 - amn + qn^2 = (m - n\varphi)(m - n\widehat{\varphi}) = \deg(m - n\varphi) \ge 0,$$

so we are done.

Remark 5.3.5.

- There's a connection between deg and Hodge index theorem on $E \times E$.

  Recall 5.3.6 (**Hodge-Index Theorem**). Say X is a surface with an ample line bundle H. Write

  $$\operatorname{NS}(X)_{\mathbb{Q}} = \mathbb{Q}H \oplus (\mathbb{Q}H)^{\perp}.$$

  Then, $H^2 > 0$ and $D^2 < 0$ for any $D \in (\mathbb{Q}H)^{\perp}$. ⊙

  Since Hodge-Index works for any surface, can use it to generalize Hasse bound to all curves. Take $H = \mathscr{O}(* \times C + C \times *)$ on $C \times C$. Let $\Gamma(\varphi) \subset C \times C$ be the graph of Frobenius. Something like

  $$\Gamma(\varphi) = (0 \times E) + q(E \times 0) + \Gamma(\varphi)^0$$

  and we've basically shown this guy is positive.

- Can generalize to abelian varieties. Here, we have $\varphi \mapsto \widehat{\varphi}$ still but $\varphi \in \operatorname{End}(A)$ and $\widehat{\varphi} \in \operatorname{End}(\widehat{A})$ are in two groups. So assume we have a **polarization** $A \xrightarrow{\lambda} \widehat{A}$. Then get

  $$\begin{tikzcd} A \arrow[r, "\lambda"] \arrow[d, "\varphi"'] & \widehat{A} \arrow[d, "\widehat{\varphi}"] \\ A \arrow[r, "\lambda"] & \widehat{A} \end{tikzcd}$$

  Can show $\varphi \mapsto \widehat{\varphi}$ is a positive involution.

○

Shou-Wu claims Hodge index is a generalization of positivity of Neron-Tate heights.

Consider $E \times E \to E$, so $\Gamma(\varphi) : E \to E \times E$ is a section. Hence, can view it as a rational point $\Gamma(\varphi) \in E(\eta)$. We'll use this observation (+ more) to give a proof of Hodge-index without using Riemann-Roch next time.

He started saying more stuff, but I'm not sure where he's going. He mentioned that $\text{Hom}(E_1, E_2) = E_2(E_1)$ is like E_1-points on E_2. Also, if $X(N)$ is the modular curve, we will study $\text{Hom}(X(N), E)$.[84]

5.4 Lecture 4 (9/10): Mordell-Weil

Last time We've studied the basic geometry of elliptic curves, and a little of the arithmetic over finite fields.

5.4.1 Mordell-Weil

Today, we want to look at the arithmetic over global fields, so we'll be looking at E/K where K is either a number field $K/\mathbb{Q}$ or a function field (over a finite field) $K/\mathbb{F}_q(t)$. Our goal will be the following.

Theorem 5.4.1 (**Mordell-Weil Theorem**). *The group $E(K)$ of K-rational points is finitely generated, when K is a global field.*

We will focus on number fields. Modifying the argument for function fields is left as an exercise.

Remark 5.4.2. If $E/\mathbb{F}_q$ is defined over a finite field, can base change to a function field (e.g. $\mathbb{F}_q(t)$ or the function field of E) and then apply Mordell-Weil to recover some of the stuff from last time. ○

History. The study of cubic equations has a long history, going back to Diophantus. He did not have the group law, but he knew that if you drew a line could get a thrid point from two starting ones. It was first conjectured that the group should be finitely generated in 1900. In 1922, Mordell proved this for elliptic curves over $\mathbb{Q}$. Some years later (1928?) Andre Weil proved it for arbitrary abelian varieties (over any global field?) using the theory of heights.

The proof will have two parts.

Theorem 5.4.3 (**Weak Mordell-Weil**). *For any $m > 0$, $E(k)/mE(k)$ is finite.*

Theorem 5.4.4 (**Height Machinery**). *There is a positive definite quadratic form on $E(k) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that for any $H > 0$, the set*

$$\{x \in E(K) : \langle x, x\rangle < H\}$$

is finite.

Example. Suppose $E_0/\mathbb{F}_q$ elliptic and $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_p(E_0)$ is the basechange to the function field $K = \mathbb{F}_q(E_0)$ of E_0. Then, $E(K) = \text{Hom}(E, E)$. In this case, $\langle , \rangle$ is just the degree map. We'll have something like

$$\langle \varphi, \psi\rangle = \frac{1}{2}\left(\varphi\overline{\psi} + \psi\overline{\varphi}\right).$$

△

These two theorems will together give the full Mordell-Weil.

Proof that WMW + HM $\implies$ MW. Consider any $P_0 \in E(K)$. We know that $E(K)/mE(K)$ is finite set, say $Q_1, \dots, Q_N \in E(K)$ give a full list of (in-equivalent) representatives. Then, $P_0 = Q_i + mP_1$ for

[84] Modularity says that this is nontrivial for certain choices of N, E. This is non-obvious

some $1 \le i \le N$ and $P_1 \in E(K)$. Let $\| \cdot \| = \sqrt{\langle \cdot, \cdot \rangle}$ be a norm. Since $mP_1 = P_0 - Q_i$, we have

$$m\|P_1\| \le \|P_0\| + \|Q_i\| \implies \|P_1\| \le \frac{1}{m}\|P_0\| + \frac{1}{m}C$$

where $C = \max(\|Q_j\|)$. Can repeat this process to get some P_2 with

$$\|P_2\| \le \frac{1}{m}\|P_1\| + \frac{1}{m}C \le \frac{1}{m^2}\|P_0\| + \frac{1}{m^2}C + \frac{1}{m}C.$$

Eventually, get

$$\|P_n\| \le \frac{1}{m^n}\|P_0\| + \frac{C}{1 - \frac{1}{m}}.$$

When $n \gg 0$, we have $\|P_n\| \le 1 + \frac{C}{1-\frac{1}{m}} = H$. This implies that $E(K)$ is generated by elements with norm at most H (+ the finite set $\{Q_1, \dots, Q_N\}$). Since there are only finitely points of bounded height/norm, we win. ■

5.4.2 Weak Mordell-Weil

We now want to prove Weak Mordell-Weil. We will do something cohomological. We will eventually do some kind of pigeon-hole argument (using Hermite's theorem of number of number fields with bounded degree?).

Let $\overline{K}$ be the algebraic closure of K, so $E(\overline{K})$ is a divisible group. This means we have a short exact sequence

$$0 \longrightarrow E[m](\overline{K}) \longrightarrow E(\overline{K}) \xrightarrow{m} E(\overline{K}) \longrightarrow 0.$$

Note that these are modules over the Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$, so we can take Galois cohomology to get a long exact sequence

$$0 \to E[m](K) \to E(K) \xrightarrow{m} E(K) \to \mathrm{H}^1(G_K, E[m](\overline{K})) \to \mathrm{H}^1(G_K, E(\overline{K})) \xrightarrow{m} \mathrm{H}^1(G_K, E(\overline{K})).$$

This gives a short exact sequence

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\partial} \mathrm{H}^1(G_K, E[m](\overline{K})) \longrightarrow \mathrm{H}^1(G_K, E(\overline{K}))[m] \longrightarrow 0.$$

The partial/connecting map above takes $x \in E(K)/mE(K)$ to the crossed homomorphism $\partial(x) = \{g \mapsto g(y) - y\}$ where $my = x$.

Another perspective with fancy language. The covering $E \xrightarrow{m} E$ gives a "principal homogeneous space" for the group $E[m]$. For some $\operatorname{Spec} K = x \in E$, it's pullback under this map $m^{-1}(x)$ is a PHS over $\operatorname{Spec} k$, and so is related to (gives an element of?) $\mathrm{H}^1(\operatorname{Spec} k, E[m])$.

It suffices to show that $\mathrm{H}^1(G_K, E[m])$ is finite. However, this is not the case, so we'll need to refine the argument.

Say $E : y^2 = X^3 + ax + b$ is some elliptic curve over K. This can extend to a family of elliptic curves, but over what? Consider the discriminant $\Delta = 27a^2 + 4b^3$. Use $U = \operatorname{Spec} \mathscr{O}_K \setminus S$ where S is some finite set (e.g. numerators and/or denominators of your data). This scheme U is affine. Can take $U = \operatorname{Spec} \mathscr{O}_K[1/N]$ for some multiplicatively large N (at least, $m \mid N$). We choose S, N in such a way that $E_U \to U$ is a proper, smooth map and such that $E_U(U) = E(K)$.

Let $\overline{U}$ be the universal cover of U. What we mean is $\overline{U} = \operatorname{Spec} \mathscr{O}_{K_U}$ where K_U is the maximal subfield of $\overline{K}$ which is unramified over all primes of U. Hence, we have

$$\operatorname{Gal}(\overline{K}/K) \twoheadrightarrow \operatorname{Gal}(K_U/K) = \pi_1(U).$$

Since rational points of E extend to sections of E_U (i.e. $E_U(U) = E(K)$). The idea is to replace $\overline{K}$ by K_U and G_K by $\operatorname{Gal}(K_U/U) = \pi_1(U)$. We now get a new short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E(K)/mE(K)] \arrow[r] \arrow[d, equal] & \mathrm{H}^1(\pi_1(U), E[m]) \arrow[r] & \mathrm{H}^1(\pi_1(U), E(K_U))[m] \arrow[r] & 0 \\ & E(\mathscr{O}_U)/mE(\mathscr{O}_U) & & & \end{tikzcd}$$

The first group has not changed, but the other two are much smaller now. In fact.

Claim 5.4.5. $\mathrm{H}^1(\pi_1(U), E[m])$ *is finite.*

Intuition. $\mathrm{H}^1(\pi_1(U), E[m])$ is unramified coverings of U with Galois group $E[m]$. Topologically, it's like we've taken an open Riemann surface, and we are looking at (unramified) coverings with a fixed (finite!) Galois groups. This set will be finite. Question: Why?

Proof. Let $L = K(E[m])$. We have a picture like

$$\begin{tikzcd} \widetilde{U} \arrow[r, equal] \arrow[d] & \operatorname{Spec} K_U \\ E[m] \arrow[d] & \\ U & \end{tikzcd}$$

so we can compute cohomology in two steps. We have

$$0 \longrightarrow \mathrm{H}^1(\operatorname{Gal}(L/K), E[m]) \longrightarrow \mathrm{H}^1(\pi_1(U), E[m]) \longrightarrow \mathrm{H}^1(\operatorname{Gal}(K_U/L), E[m])$$

with the kernel finite since both $\operatorname{Gal}(L/K)$ and $E[m]$ are. The group of the right is (the group action is trivial by definition of L)

$$\mathrm{H}^1(K_U/L, E[m]) = \operatorname{Hom}(\operatorname{Gal}(K_U/L), E[m]) = \left\{ \begin{matrix} \text{extensions } F/L \text{ unramified over } U \\ \text{with Galois group a subgroup of } E[m] \end{matrix} \right\}.$$

This set is finite by CFT or by the fact below this proof. ■

Fact. For any integers Δ, d, there are only finitely many number fields F with $\deg F \leq d$ which are unramified outside of Δ.

This completes the proof of Weak Mordell-Weil.

5.4.3 Heights

We'll use simple heights. Consider the map $E \to \mathbb{P}^1$ given by modding out by ± 1. In coordinates $E : y^2 = x^3 + ax + b$, this map is $(x, y) \mapsto x$.

On $\mathbb{P}^1$, we can define the **Weil height**. First recall the p-adic absolute values $|\cdot|_p : \mathbb{Q} \to \mathbb{Z}$, say normalized so that $|p|_p = p^{-1}$. Let $|\cdot|_\infty$ denote the usual (archimedean) norm on $\mathbb{Q}$. Note that, for $x \in \mathbb{Q}$ if $x \neq 0$, then

$$\prod_{p \leq \infty} |x|_p = 1 \quad (\textbf{product formula})$$

(use multiplicative to reduce to x being a prime where this is obvious). For each $p \leq \infty$, we can embed $\mathbb{Q} \hookrightarrow \mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}_p$ where $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$ ($\mathbb{C}_p$ is complete and algebraically closed).

Example. When $P = \infty$, the above sequence is $\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} = \mathbb{C}$. When $p \neq \infty$, actually get 4 different spaces though. △

What about for a number field $K/\mathbb{Q}$? Two ways to define absolute values. For a prime $\mathfrak{p}$ of K lying above p, we can embed $\sigma : K \hookrightarrow \overline{\mathbb{Q}}_p$ and use the absolute value there. Still get a product formula

$$\prod_p \prod_{\sigma : K \hookrightarrow \overline{\mathbb{Q}}_p} |\sigma(x)|_p = 1$$

when $x \neq 0$ (since $\prod_{\sigma : K \hookrightarrow \overline{\mathbb{Q}}_p} |\sigma(x)|_p = \left|\mathrm{N}_{K/\mathbb{Q}}(x)\right|_p$). Another way is consider the set of places (i.e. primes or conjugate-pair of embeddings into $\mathbb{C}$) Σ_K on K. For each $v \in \Sigma_K$, get a natural absolute value $|\cdot|_v$ on K. When $v \nmid \infty$, $|x|_v = N(v)^{-\operatorname{ord}_v(x)}$ and if $v \mid \infty$ then

$$|x|_v = \begin{cases} |x| & \text{if } v \text{ real} \\ \|x\|^2 & \text{otherwise.} \end{cases}.$$

Either definition works. Shou-Wu prefers the first one.

Now that we know how to get absolute values on our fields, we can define heights on $\mathbb{P}^1(\overline{Q})$. We want a function $\mathbb{P}^1(\overline{Q}) \to \mathbb{R}$. Consider any $x \in \mathbb{P}^1(\overline{Q})$, and write $x = (x_1, x_2)$ with $x_i \in K$. Then, the **Weil height** is

$$h(x) = \frac{1}{[K : \mathbb{Q}]} \sum_{p \leq \infty} \sum_{\sigma : K \to \overline{\mathbb{Q}}_p} \log \max\left(|\sigma x_1|_p, |\sigma x_2|_p\right).$$

This does not depend on your choice of K or on your choice of homogeneous coordinates (by product formula). Question: Why?

Remark 5.4.6. When $x \in \mathbb{P}^1(\mathbb{Q})$ and $x = (a, b)$ for $a, b \in \mathbb{Z}$ coprime, we have

$$h(x) = \log \max(|a|, |b|).$$

∘

Remark 5.4.7. Say $x \in \overline{\mathbb{Q}} \hookrightarrow \mathbb{P}^1$ (thinking of it as $(x, 1) \in \mathbb{P}^1$). Let $P(T) \in \mathbb{Z}[T]$ be the minimal polynomial of x, and let x_i be the complex roots of P. Write

$$P(T) = a_0 x^d + a_1 x^{d-1} + \ldots$$

Then,
$$h(x) = \frac{1}{\deg x}\left[\log|a_0| + \int_0^1 \log\left|P(e^{2\pi i\theta})\right| \mathrm{d}\theta\right].$$
We also have
$$P(T) = \frac{1}{\deg x}\left[\log|a_0| + \sum_i \log\max(1,|x_i|)\right].$$

Question: I think this is what was written, but isn't it missing a T somewhere?

Remark 5.4.8 (Properties of heights).

(1) $h(x) \geq 0$ always, and $h(x) = 0 \iff x$ is a root of unity or 0. Also, $h(x^d) = dh(x)$.

(2) For any d, H, the set
$$\#\left\{x \in \overline{\mathbb{Q}} \mid \deg x < d \text{ and } h(x) < H\right\} < \infty.$$

We'll prove this next time.

Conjecture 5.4.9 (Lehmer)**.** *There is a constant $C > 0$ such that for any nonzero x which is not a root of unity,*
$$h(x) > C/\deg x.$$

5.5 Lecture 5 (9/15)

Last time Started studying Mordell-Weil theorem. Say E/K is an elliptic curve over a number field. We are in the midst of proving that $E(K)$ is finitely generated. This has a two-step proof. We use cohomology to prove weak MW – $E(K)/mE(K)$ is finite – last time. The second step is to use heights to construct a quadratic form
$$E(K) \times E(K) \to \mathbb{R}$$
which is "**discrete**", i.e. for any $H \in \mathbb{R}$ the set $\{x \in E(K) : \langle x, x\rangle < H\}$ is finite.

5.5.1 Heights

To get heights on E, we are using the composition
$$E \longrightarrow \mathbb{P}^1 \xrightarrow{h} \mathbb{R}$$
where h is the height of $\mathbb{P}^1$ defined last time. On $\mathbb{P}^1$, this height looks like
$$h(x) = \begin{cases} \log\max(|a|, |b|) & x = \frac{a}{b} \in \mathbb{Q} \\ \frac{1}{\deg K}\sum_{p\leq\infty}\sum_{\sigma: K\to\overline{\mathbb{Q}}_p} \log\max(|\sigma(x)|_p, 1) & x \in \overline{\mathbb{Q}}, K = \mathbb{Q}(x) \end{cases}$$

Recall that we have a **Product formula** – for K a number field and $x \in K^\times$, one has
$$\prod_{v\in\Sigma(K)} |x|_v = 1$$

where $\Sigma(K)$ is the set of places. There's another way to compute heights which is

$$h(x) = \frac{1}{\deg K} \int \dots$$

We can extend the definition of heights to $\mathbb{P}^n$. If $x = (x_0, \dots, x_n) \in \mathbb{P}^n(K)$, then can define

$$h(x) = \frac{1}{\deg K} \sum_{v \in \Sigma_K} \log \max(|x_1|_v, \dots, |x_n|_v).$$

We want to prove three properties.

(1) If $f : \mathbb{P}^n \to \mathbb{P}^m$ is degree d, then

$$h(f(p)) \le dh(p) + C(f)$$

where $C(f)$ is independent of K.

(2) If $f : \mathbb{P}^n \to \mathbb{P}^n$ is finite of degree d, then

$$h(f(p)) = dh(p) + O(1)$$

where "$O(1)$" means bounded function.

(3) (**Northcott property**) The set

$$\left\{p \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid \deg P < D \text{ and } h(p) < H\right\}$$

is finite for any $d, H > 0$.

Proof of 1. Say we have a morphism $\mathbb{P}^n \to \mathbb{P}^m$, $x = (x_0, \dots, x_n) \mapsto (f_0(x), \dots, f_m(x))$. Then,

$$h(f(x)) = \frac{1}{\deg K} \sum_{v \in \Sigma_K} \log \max \left(|f_0(x)|_v, \dots, |f_m(x)|_v\right).$$

Define an L^∞-norm $\| \cdot \|_{L^\infty} : \overline{\mathbb{Q}}_p^{n+1} \to \mathbb{R}$ given by

$$\|x\|_{L^\infty} = \max_{0 \le i \le n} |x_i|.$$

Since each f_i is homogeneous on $\overline{\mathbb{Q}}_p^{n+1}$ of degree d, the function

$$\frac{|f_i(x)|}{\|x\|^d}$$

is bounded, so we define

$$\|f_i\| = \max_x \frac{|f_i(x)|}{\|x\|^d} \text{ and } \|f\| := \max_i \|f_i\|.$$

Hence,

$$h(f(x)) = \sum_v \log \|f(x)\|_v = \sum_v \log \left(\|f\|_v \|x\|_v^d\right) = d \sum_v \log \|x\|_v + \sum_v \log \|f\|_v = dh(x) + h(f)$$

which gives 1. ∎

Proof of 2. Have $f : \mathbb{P}^n \to \mathbb{P}^n$ finite. This induces a pullback morphism $f^* : k[x_0, \dots, x_n] \to k[x_0, \dots, x_n]$ say with $f^*(x_i) = f_i(x)$. Since f is well defined,

$$f_0(x) = \cdots = f_n(x) = 0$$

has only solution $(0, \dots, 0)$. The ideal $f^*(x_0, \dots, x_n) \subset (x_0, \dots, x_n)$ has root $\sqrt{(f^*(x_0), \dots, f^*(x_n))} = (x_0, \dots, x_n)$ by Hilbert Nullstellsatz. Hence, there exists N such that

$$x_i^N = \sum_{j=0}^{n} f_j(x) g_{ij}(x)$$

for all i. Thus, (note g_{ij} degree $N - d$ since f_j degree d)

$$\|x\|^N \le (n+1) \max |f_j(x) g_{ij}(x)| \le (n+1) \max_j \|f_j(x)\| \cdot \max_{i,j} \|g_{ij}(x)\| \le (n+1) \|f(x)\| \max_{i,j} \|g_{ij}\| \|x\|^{N-d}.$$

Hence,

$$\|x\|^d \le C \|f(x)\|$$

for some constant $C > 0$. Thus,

$$d h(x) \le h(f(x)) + \log C.$$

∎

Proof of 3. For any D, H, we want to show that

$$\{x \in \mathbb{P}^n \mid \deg x < D \ \text{ and } \ h(x) < H\}$$

is finite. We first reduce to the case that $n = 1$. We want to define a map $(\mathbb{P}^1)^n \to \mathbb{P}^n$. This will fit in a diagram

$$\begin{tikzcd}
(\mathbb{A}^1)^n \arrow[r] \arrow[d] & \mathbb{A}^n \arrow[d] \\
(\mathbb{P}^1)^n \arrow[r] & \mathbb{P}^n
\end{tikzcd}$$

where the top map is $(x_1, \dots, x_n) \mapsto (\sigma_1, \dots, \sigma_n)$ with σ_i the ith elementary symmetric polynomials, i.e.

$$\prod_{i=1}^{n} (T - x_i) = \sum a_i T^i \in \overline{k}[T].$$

To write down the bottom map, use homogeneous coordinates $x_i = \frac{u_i}{v_i}$. Then,

$$a_j = \left(\prod_{i=1}^{n} u_i \right) \sigma_j \left(\frac{u_i}{v_i} \right).$$

This morphism is finite (even Galois with Galois group S_n). Hence, by property 2, points on $\mathbb{P}^n$ of bounded degree/height, come from points on $(\mathbb{P}^1)^n$ of bounded degree/height. Thus reduces to $n = 1$.

Say now we have $x \in \mathbb{P}^1(K)$ with $\deg x = d$. Recall the map $(\mathbb{P}^1)^d \to \mathbb{P}^d$. Let $\underline{x} = (x_1, \dots, x_d)$ be the conjugates of x. Then, $f(x) \in \mathbb{P}^d(\mathbb{Q})$. This let's us reduce Northcott for $\mathbb{P}^1(\overline{\mathbb{Q}})$ to Northcott for $\mathbb{P}^n(\mathbb{Q})$.

The case of $\mathbb{P}^n(\mathbb{Q})$, we can do by hand. Write $x = (x_0, \dots, x_n) \in \mathbb{P}^n(\mathbb{Q})$ with $x_i \in \mathbb{Z}$ and $\gcd(x_i) = 1$. Then, $h(x) = \log \max |x_i|$, so

$$\#\{h(x) < H\} \le (2H+1)^{n+1} < \infty.$$

■

5.5.2 Back to elliptic curves

Using the map $E \xrightarrow{x} \mathbb{P}^1$, we define $h_E(p) = h_{\mathbb{P}^1}(x(p))$. This has the Northcott property. We want to check that $h_E(p)$ is "almost" quadratic, i.e.

Claim 5.5.1.

$$h_E(p+q) + h_E(p-q) = 2h_E(p) + 2h_E(q) + O(1).$$

Proof. Consider the diagram

$$\begin{tikzcd} E \times E \arrow[r, "\varphi"] \arrow[d, "x\times x"'] & E \times E \arrow[d, "x \times x"] \\ \mathbb{P}^1 \times \mathbb{P}^1 \arrow[r, "\psi"] & \mathbb{P}^1 \times \mathbb{P}^1 \end{tikzcd}$$

where $\varphi(p,q) = (p+q, p-q)$. We claim that ψ is a morphism of degree $(2,2)$. Say we have some $(\alpha, \beta) \in \mathbb{P}^1 \times \mathbb{P}^1$. Pulling back to $E \times E$, we get $(A, B) \in E \times E$ with $\alpha = \pm A$ and $\beta = \pm B$. We want to find preimages, so we are trying to solve

$$p + q = \pm A \text{ and } p - q = \pm B.$$

This gives

$$p = \frac{1}{2}(A+B) \text{ and } q = \frac{1}{2}(A-B)$$

with some $\pm$'s thrown in. This shows that ψ has degree $(2,2)$. Thus,

$$h(\psi(p,q)) = 2h_E(p) + 2h_E(q) + O(1)$$

by property 2 of heights. ■

We have proved that $h_E(p)$ satisfies 2 properties: Northcott + almost quadratic. Using these, we can define the **Normalized height** (or **Néron height**)

$$\widetilde{h}(p) = \lim_{n\to\infty} \frac{h_E(2^n p)}{4^n}.$$

This function will be very nice.

(1) $\widehat{h}(p)$ is positive semi-definite, and satisfies Northcott

(2) $\widehat{h}(p)$ is actually quadratic

This is what he need to prove Mordell-Weil. We are running low on time, so we won't prove this now.

Effectiveness Mordell-Weil tells us that the group of rational points is finitely generated.

Question 5.5.2. *How do we find an actual set of generators?*

Before this, we may ask about numeric invariants, such as the rank of this group. This leads to BSD.

Conjecture 5.5.3 (**BSD Conjecture**). *This relates $E(K)$ to the L-function of E. There are 3 parts.*

(1) Tate-Shafervich group

(2) L-function

(3) Order of vanishing

We won't detail what all these parts actually say, but we'll at least say something.

The Tate-Shafervich group gives an obstruction for a genus 1 curve with local solutions to have global solutions. Note that for $g(C) = 1$, C/K, if $C(K) \neq \emptyset$ then C is an elliptic curve. Also, $C(K) \neq \emptyset$ gives $C(K_v) \neq \emptyset$, but the converse does not always hold.

Example. $C : 3x^3 + 4y^3 + 5z^3$ has local solutions but no global ones. △

What do we do then? Consider the jacobian $\mathrm{Jac}(C) = E$ which is an elliptic curve. Something about $E \times C \to C$ being a principal homogeneous space of E. Define

$$Ш(E) = \{C \mid g(C) = 1, \mathrm{Jac}(C) = E, C(K_v) \neq \emptyset \forall v\}.$$

This is the set of localy trivial principal homogeneous spaces over E, and so

$$Ш(E) = \ker \left(\mathrm{H}^1(K, E) \to \prod_v \mathrm{H}^1(K_v, E) \right).$$

This suggests arranging genus 1 curves by Jacobian, and then looking for local solutions before finding global ones.

Exercise. Prove Hasse for all curves of genus 1. If $g(C) = 1$ on a finite field $\mathbb{F}_q$, then

$$|C(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Remark 5.5.4. By the Hasse theorem, $C(\mathbb{F}_q) \neq \emptyset$, so $C(K_v) \neq \emptyset$ if C has good reduction at v. ◦

The upshot is that to check if C has local solution, we need only check that the bad places.

Now let's say some words about the L-function. For an elliptic curve E/K, we get a minimal model $\mathcal{E}/\mathscr{O}_K$. We define

$$L(E, s) = \prod_{v \text{ good}} \left(1 - a_v q_v^{-s} + q_v^{1-2s}\right)^{-1} \prod_{v \text{ bad}} \begin{cases} 1 & \text{additive} \\ \frac{1}{1-q_v^{-s}} & \text{split multiplicative} \\ \frac{1}{1+q_v^{-s}} & \text{non-split multiplicative} \end{cases}$$

This is absolutely convergent for $\mathrm{Re}(s) > 3/2$ (by hasse).

Conjecture 5.5.5. *$L(E,s)$ has a holomorphic continuous to whole complex plane. Also, it has a function equation*

$$L(E,s) = (blah)L(E,2-s).$$

Finally, $L(E,s) = L(\pi, s = \frac{1}{2})$ for π a cuspidal representation of $\mathrm{GL}_2(\mathbb{A}_K)$.

When $K = \mathbb{Q}$, this is known due to Wiles and Taylor-Wiles and Breuil-Conrad-Diamond-Taylor. Some other results are known on some special cases, but this is generally open.

Conjecture 5.5.6 (BSD Conjecture).

(1) *$\text{Ш}(E/K)$ is finite.*

(2) $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\, E(K) = r$

(3)

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = c(E)R(E)\#\text{Ш}(E)$$

where $c(E)$ some local constants and $R(E)$ the ***regulator****,*

$$R(E) = \det \langle P_i, P_j \rangle \in \mathbb{R} \ \textit{where} \ E(K)/E(K)_{\mathrm{tors}} = (P_1, \dots, P_r).$$

What is known?

- When $K = \mathbb{Q}$, $\mathrm{ord}_{s=1} L(E,s) \le 1$ BSD holds by Gross-Zagier and Kolyvagin.
- Functional field situation. Have E/K where $K/\mathbb{F}_p(t)$ finite. Tate showed that

$$\#\text{Ш}(E/K) < \infty \implies \text{whole BSD}.$$

(so finiteness of Ш is hard). Finiteness of Ш is known in the case $E = (E_0)_K$ with $E_0/\mathbb{F}_q$ (i.e. E a **constant elliptic curve**).

Conjecture 5.5.7 (Goldfeld Conjecture). *50% of elliptic curves over $\mathbb{Q}$ have* $\mathrm{rank} = 0$ *and 50% have* $\mathrm{rank} = 1$.

There's much work on this by Bhargava, Skinner, Zhang (maybe all 3 of them on the same paper?) and Alex Smith and others.

5.6 Lecture 6 (9/17)

The next set of topics will be modular curves, modular forms, and L-functions.

5.6.1 Modular Curves over $\mathbb{C}$

Example. The basic example is $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} = X(1) \simeq \mathbb{C}$ with isomorphism given by the j invariant. This is the "coarse moduli of elliptic curves over $\mathbb{C}$" △

Example. $X(N) = \Gamma(N)\backslash\mathfrak{H}$ is the "course moduli of elliptic curves over $\mathbb{C}$ with full level N structure." In fact, when $N \ge 3$, this is actually the fine moduli space. △

Note that the space $X(N)$ are not compact, so our first goal is to remedy this.

Compactification of $X(N)$ We will do this by replacing $\mathfrak{H}$ with $\mathfrak{H}^* = \mathfrak{H} \sqcup \mathbb{P}^1(\mathbb{Q})$ with $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{P}^1(\mathbb{Q})$ in the usual way.

Think of the the usual fundamental domain for $X(1)$. Note that, near ∞, $X(1)$ looks like the line

$$\left\{ z = x + iy : -\frac{1}{2} \leq x < \frac{1}{2}, y > T \right\}$$

Taking $q = e^{2\pi i z}$, we have $|q| \leq e^{-2\pi T}$. Near i, we have a reflection $z \leftrightarrow -z$, so we use $w = z^2$ as our coordinate instead. We get a compactification

$$\overline{X(1)} = X(1) \bigsqcup_{D'} D$$

where D is the unit disk and $D' = \{0 < |q| \leq e^{-2\pi T}\}$ is a punctured disk.

To form the compactification for $X(N)$, the idea is similar. Glue in a bunch of punctured disks D_i indexed by $\pm\Gamma(N)\backslash\mathbb{P}^1(\mathbb{Q})$. Note that $\mathbb{P}^1(\mathbb{Q}) = \{[a : b] \mid a, b \in \mathbb{Z} \text{ and } \gcd(a, b) = 1\}$. Since $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$, we get an embedding

$$\Gamma(N)\backslash\mathbb{P}^1(\mathbb{Z}) \hookrightarrow \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}).$$

These give the cusps of $\overline{X(N)}$.

Remark 5.6.1. $X(N)$ parameterize (E, P, Q) with Weil pairing $\langle P, Q\rangle = e^{2\pi i/N}$. ∘

When $E = \mathbb{C}/\Lambda$, we have $E[N] = \frac{1}{N}\Lambda/\Lambda$ and the Weil pairing $E[N] \times E[N] \to \mu_N$ is given concretely by

$$(P, Q) \mapsto \exp\left(2\pi i N \frac{\mathrm{Im}(x\overline{y})}{\mathrm{vol}(\Lambda)}\right)$$

where $x, y \in \mathbb{C}$ represent P, Q.

Example. $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $P = \frac{1}{N}$, $Q = \frac{1}{N}\tau$. Then, $\mathrm{vol}(\Lambda) = \mathrm{Im}\,\tau$ and

$$\langle P, Q\rangle = \exp\left(2\pi i N \frac{1}{N^2}\right) = \exp\left(\frac{2\pi i}{N}\right).$$

△

Remark 5.6.2. The universal family of curves E extends to $\overline{X(N)}$ by adding a nodal curve with N-gon (think Kodaira classification). In this way, get a universal family

$$\mathcal{E} \longrightarrow \overline{X}(N)$$

with $\mathcal{E}$ a smooth surface. ∘

Remark 5.6.3. There is a Hodge bundle (modular form bundle).

$$\begin{tikzcd} \mathcal{E} \arrow[d] \\ X(N) \arrow[u, bend left, "e"] \end{tikzcd}$$

Let $\omega = e^*\Omega^1_{\mathcal{E}/X(N)}$. This is a line bundle on $X(N)$ which even extends to one on $\overline{X(N)}$. By Kodaira-Spencer, there is a canonical isomorphism

$$\omega^{\otimes 2} \simeq \Omega^1_{\overline{X(N)}}(\text{cusps}).$$

We can explain this more precisely. Here's a picture

$$\begin{tikzcd} \mathfrak{H} \times \mathbb{C}/\Lambda \arrow[d] \\ \mathfrak{H} \end{tikzcd}$$

I'm not following what he's doing. He wrote a $\mathrm{d}z$ somewhere and said it is a trivialization of ω on $\mathfrak{H}$. We have a comm square

$$\begin{tikzcd} \mathbb{C} \arrow[r] \arrow[d] & \mathbb{C} \arrow[d] \\ E_\tau \arrow[r] & E_{\gamma\tau} \end{tikzcd}$$

with $E_\tau = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ as usual (and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$). Consider the pullback

$$\gamma^*\mathrm{d}z = \frac{1}{cz+d}\mathrm{d}z.$$

$\circ$

Question 5.6.4. *Why is $\omega^2 \simeq \Omega^1_X$?*

$\mathrm{d}\tau$ is a trivialization of Ω^1_X and

$$\gamma^*\mathrm{d}\tau = \mathrm{d}\gamma\tau = \mathrm{d}\frac{a\tau+b}{c\tau+d} = \frac{\mathrm{d}\tau}{(c\tau+d)^2}$$

For some reasons, he says this basically explains $\omega^{\otimes 2} \simeq \Omega^1$.

Remember that near cusps we use coordinate $q = e^{2\pi i\tau}$ so the trivialization there is $\mathrm{d}\tau = 2\pi i\frac{\mathrm{d}q}{q}$. Near cusp, have a "Tate uniformization" given by

$$\mathbb{C}[\![q, q^{-1}]\!]^\times / q^{\mathbb{Z}}.$$

This is maybe coming from

$$\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau) \xrightarrow{\exp} \mathbb{C}^\times/q^{\mathbb{Z}}$$

Let z be the coordinate on the source, and let $t = e^{2\pi iz}$, so $\mathrm{d}z = \frac{1}{2\pi i}\frac{\mathrm{d}t}{t}$. Then,

$$\left(\frac{\mathrm{d}t}{t}\right)^{\otimes 2} \leftrightarrow \frac{\mathrm{d}q}{q}$$

so we get $\omega^{\otimes 2} \simeq \Omega^1(\infty)$ (even near the cusp). The twist is because of the q in the denominator.

We use ω more often than we use Ω^1 (though we use Ω^1 for duality). I think he said something like ω descends to a bundle on $X(N)$ only if Γ has no fixed point.

Example. For $X(1)$ there is a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(i) = i$, and $\gamma^* \mathrm{d}z = i\mathrm{d}z$ (deg 4). Can also get $\gamma(\rho) = \rho$ and $\gamma^*\mathrm{d}z = \rho\mathrm{d}z$ (deg 6). In general $-I$ has $-I(\tau) = \tau$ and $(-I)^*\mathrm{d}z = -\mathrm{d}z$ (deg 2).

The conclusion is that $\omega^{\otimes 12}$ will descend to $X(1)$. In fact, we have a section Δ for $\omega^{\otimes 12}$ given by

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} (\mathrm{d}z)^{\otimes 12}.$$

△

Remark 5.6.5. ω is actually ample. One can calculate its degree.

$$\deg \omega = \frac{1}{12} \deg \Delta = \frac{1}{12}.$$

○

In other words, if $\overline{X(1)} = \mathbb{P}^1$, then $\omega^{\otimes 12} \simeq \mathscr{O}_{\mathbb{P}^1}(1)$. We can use the powers $\Gamma(\omega^{\otimes k})$ to construct maps $X(N) \hookrightarrow \mathbb{P}^N$.

In summary we constructed a projective family of modular curves $\overline{X(N)}$ with specified ample line bundle ω.

Remark 5.6.6. $\pi^*\omega = \omega$ for $\overline{X(N)} \xrightarrow{\pi} \overline{X(M)}$. ○

This family has an action by $\mathrm{GL}_2(\mathbb{Q})^+$.

Definition 5.6.7. A subgroup $\Gamma \subset \mathrm{GL}_2(\mathbb{Q})^+$ is called a **congruence subgroup** if there is some $N > 0$ such that $\Gamma \supset \Gamma(N)$ and $[\Gamma : \Gamma(N)] < \infty$. Can then define compact $X_\Gamma = \Gamma \backslash \mathfrak{H}$. ◇

This gives a bigger family of modular curves. For any $g \in \mathrm{GL}_2(\mathbb{Q})^+$, get a square

$$\begin{tikzcd}
\mathfrak{H} \arrow[r] \arrow[d] & \mathfrak{H} \arrow[d] \\
\Gamma\backslash\mathfrak{H} \arrow[r] & g\Gamma g^{-1}\backslash\mathfrak{H}
\end{tikzcd}$$

with the top map is $\tau \mapsto g\tau$ and the bottom map is $\Gamma\tau \mapsto g\Gamma\tau = (g\Gamma g^{-1})g\tau$. Thus, we have a map

$$g : X_\Gamma \to X_{g^{-1}\Gamma g}.$$

The nice thing about modular curves is that there are a lot of them. It's not just one Riemann surface, but many Riemann surfaces. One can imagine combining all of these into something like

$$\varprojlim_{\Gamma} X_\Gamma$$

This has an action of $\mathrm{GL}_2(\mathbb{Q})^+$, and something like "this action complete using compact topology" (?). The set $\{\Gamma(N)\}_N \subset \mathrm{GL}_2(\mathbb{Q})^+$ will be open, and we can complete to get $\mathrm{SL}_2(\widehat{\mathbb{Q}})^+ \cdot \mathbb{Q}_+^\times = \widehat{\mathrm{GL}_2(\mathbb{Q})}^+$. The $\mathbb{Q}_+^\times$ factor comes from insistence on Weil pairing (otherwise we'd get something disconnected).

Question: What?

Question: What?

Question: What?

Assumption. From now one, use X_Γ as compactified modular curve, i.e. just always assume modular curves are compactified.

Example. Take $\Gamma = \Gamma_0(N)$. This matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N.$$

It parameterizes (E, C) with $C \subset E[N]$ a cyclic subgroup of order N. The canonical example is $(E_\tau, \langle 1/N \rangle)$. Equivalently,

$$X_0(N) = \{\varphi : E \to E' \mid \ker \varphi \simeq \mathbb{Z}/N\mathbb{Z}\}$$

is the moduli of cyclid degree N isogeny.

The existence of dual isogenies means that we have an involution

$$w_N : X_0(N) \to X_0(N).$$

One can show that w_N is induced by the matrix $\begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$. At least, note that

$$w_N \Gamma_0(N) w_N^{-1} = \Gamma_0(N)$$

since

$$\begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix} \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \begin{pmatrix} 0 & -1/N \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -bN & a \end{pmatrix} \in \Gamma_0(N).$$

This shows that this matrix gives an involution of $X_0(N)$ (one still has to check that it comes from taking dual isogenies). △

Example. Also have

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

This parameterizes (E, p) with $p \in E[N]$ of order N. We have a natural map $X_1(N) \to X_0(N)$ sending $(E, p) \mapsto (E, \langle p \rangle)$. The "most typical" modular curve is $X(N)$ and it turns out that

$$X(N) \simeq X_1(N^2).$$

This is because

$$\Gamma(N) = \left\{ \begin{pmatrix} a & bN \\ cN & d \end{pmatrix} : a, d \equiv 1 \pmod N \right\} \longrightarrow \left\{ \begin{pmatrix} a & b \\ cN^2 & d \end{pmatrix} : a, d \equiv 1 \pmod N \right\} = \Gamma_1(N^2).$$

This map is realized by the conjugation

$$\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \begin{pmatrix} a & bN \\ cN & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & N^{-1} \end{pmatrix} = \begin{pmatrix} a & b \\ cN^2 & d \end{pmatrix}.$$

Hence, studying $X(N)$ can be done by studying $X_1(N^2)$. △

Remark 5.6.8. Fix $\zeta_N \in \mu_N$. We'll define an involution on $X_1(N)$. For each P, there's a Q such that $\langle P, Q\rangle = \zeta_N$, and this Q is unique up to addition by multiples of P. Hence, get

$$(E, p) \mapsto (E/(p), Q + (p)/(p)).$$

$\circ$

Remark 5.6.9. $X_0(N)$ and $X_1(N)$ are both defined over $\mathbb{Q}$.

$X(N)$ is defined over $\mathbb{Q}(\zeta_N)$. $\circ$

There was more stuff he talked about, but I was distracted and missed it.

Definition 5.6.10. An elliptic curve $E/\mathbb{C}$ is called **CM** if $\mathrm{End}(E) \neq \mathbb{Z}$. $\diamond$

If E is CM, then $\mathrm{End}(E) \hookrightarrow K \hookrightarrow \mathbb{C}$ is an order in some imaginary quadratic $K = \mathbb{Q}(\sqrt{-d})$. If $\mathscr{O}_K = \mathbb{Z} + \mathbb{Z}\alpha_0$, then $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}c\alpha_0$ for some **conductor** c, and then the discriminant of $\mathbb{Z} + \mathbb{Z}\alpha$ will be $c^2 D$ (where $D = \mathrm{disc}(K/\mathbb{Q})$).

Conversely, given any order R of discriminant d, there is an elliptic curve E with CM by R. e.g. take $E = \mathbb{C}/R$. Get

$$\{\text{CM elliptic curves over } \mathbb{C}\} = \bigsqcup_d \left\{ \begin{matrix} \text{CM elliptic curves over } \mathbb{C} \\ \mathrm{End}(E) \simeq R_d \end{matrix} \right\}.$$

If $\mathrm{End}(E) = R$, then $E = \mathbb{C}/\Lambda$ with Λ an R-module. In fact, Λ is locally free of rank 1, so get a map

$$\left\{ \begin{matrix} \text{CM elliptic curves over } \mathbb{C} \\ \mathrm{End}(E) \simeq R_d \end{matrix} \right\} \to \mathrm{Pic}(R_d).$$

This map is a bijection. Hence,

$$\{\text{CM elliptic curves over } \mathbb{C}\} = \bigsqcup_d \{E_I \mid I \in \mathrm{Pic}(R_d)\}.$$

Rigidity of CM-elliptic curves Suppose that

$$E : y^2 = x^3 + ax + b \text{ with } a, b \in \mathbb{C}$$

is CM by order R. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be any automorphism. This gives new elliptic curve

$$E^\sigma : y^2 = x^3 + \sigma(a)x + \sigma(b).$$

We also have $\mathrm{End}(E^\sigma) = R$ (e.g. by "transfer of structure"). We get a diagram

$$\begin{tikzcd} E(\mathbb{C}) \arrow[r, "\sigma"] \arrow[d, "\alpha"'] & E^\sigma(\mathbb{C}) \arrow[d, "\alpha^\sigma"] \\ E(\mathbb{C}) \arrow[r, "\sigma"] & E^\sigma(\mathbb{C}) \end{tikzcd}$$

where α is an endormorphism of E and $\alpha^\sigma = \sigma\alpha\sigma^{-1}$. This is crazy because it means that the set of CM elliptic curves with endomorphismm group R_d is fixed by $\mathrm{Aut}(\mathbb{C})$, but this is a finite set! Thinking about

j-invariants, this says that

$$\#\{j(E)^\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{C})\} < \infty$$

when E has CM. Thus, $j(E)$ is algebraic.

He said some more CM stuff, possibly related to stacks. I was distracted so missed it. It seems the point is that you should think of $CM(d)$, the curves with CM by R_d, as all one object (with points defined on the Hilbert class field of R_d).

5.7 Lecture 7 (9/22): modular forms and L-functions

Recall 5.7.1. $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}\, z > 0\}$ via fractional linear transfomrations or whatever they're called

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

The quotient $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ is the course moduli of elliptic curves. Over $\mathscr{F}$, there is a universal family $\mathscr{E} \to \mathfrak{H}$ of elliptic curves ($\mathscr{E}_\tau = \mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$). This has a section section $\mathfrak{H} \xrightarrow{0} \mathscr{E}$, and so we can look at the pull back

$$\omega_{\mathscr{E}/\mathfrak{H}} = 0^*\Omega^1_{\mathscr{E}/\mathfrak{H}}$$

called the **moduli bundle**. This bundle can't descend to $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. On $\omega_{\mathscr{E}/\mathfrak{H}} \cong \mathscr{O}_{\mathfrak{H}} \cdot \mathrm{d}z$, we have

$$\gamma^*\mathrm{d}z = \frac{1}{cz+d}\mathrm{d}z$$

$\odot$

A module form of weight k is essentially a section of $\omega^{\otimes k}$. Since ω can be trivialized, these also correspond to functions on $\mathfrak{H}$ with certain transformation rule.

Definition 5.7.2. Let $k \in \mathbb{Z}$. A function $f : \mathfrak{H} \to \mathbb{C}$ is called **of weight** k if

$$f(\gamma z)\frac{1}{(cz+d)^k} = f(z).$$

$\diamond$

Example. When $k =$ odd, we have $\gamma = -I \in \mathrm{SL}_2(\mathbb{Z})$, so the formula reads

$$f(z) = (-1)^k f(z) = -f(z).$$

Hence, there are no nonzero functions f with weight k. $\triangle$

Assume f is continuous. Note that $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $Tz = z+1$. If f is of weight k, then $f(z+1) = f(z)$, so f is periodic in its x-coordinate. So, we get a Fourier expansion

$$f(z) = \sum a_n(y)e^{2\pi i n x}$$

No harm in using z in the exponent since $a_n(y)$ depends on y, so can write

$$f(z) = \sum_{n \in \mathbb{Z}} a_n(y) e^{2\pi i n z}.$$

Definition 5.7.3. A holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ is called a **modular form of weight** k. $\diamond$

Remark 5.7.4. When f is holomorphic, $a_n(y) = 0$ when $n < 0$ and also $a_n(y) = a_n$ does not depend on y for all n (it's a holomorphic function only depending on x). That is, our Fourier expansion looks like

$$f(z) = \sum_{n \geq 0} a_n e^{2\pi i n z}.$$

$\circ$

Can put $q = e^{2\pi i z}$ and so write $\sum_{n=0}^{\infty} a_n q^n$ instead, so the Fourier expansion is like a Taylor expansion at ∞.

Example (Eisenstein series). Let

$$G_k(z) = \sum_{m,n}{}' \frac{1}{(mz+n)^k}$$

when $k > 2$. Above, the $'$ on the sum means we sum over nonzero $(m, n) \in \mathbb{Z}^2$. Note that

$$G_k\left(\frac{az+b}{cz+d}\right) = \sum_{m,n}{}' \frac{(cz+d)^k}{[m(az+b)+n(cz+d)]^k} = (cz+d)^k \sum_{m,n}{}' \frac{1}{(m'z+n')^k} = (cz+d)^k G_k(z).$$

Above,

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = \begin{pmatrix} ma+nc \\ mb+nd \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix},$$

so we're still summing over nonzero lattice points, just in a different order. $\triangle$

We have already seen these Eisenstein series for Weierstrass equations. The elliptic curve corresponding to the lattice $\mathbb{Z} + \mathbb{Z}\tau$ is given by

$$E_\tau : y^2 = 4x^3 - 60G_4(\tau)x - 140G_6(\tau).$$

What's the Fourier expansion of G_k look like?

Proposition 5.7.5.

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n \geq 1} \sigma_{k-1}(n) e^{2\pi i n z}$$

where

$$\zeta(k) = \sum_{n \geq 1} \frac{1}{n^k} \quad \text{and} \quad \sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1}.$$

When $k = 2$, we define

relevant math overflow question

$$G_2(z) = \lim_{s \to 1^+} \underbrace{\sum_{m,n}{}' \frac{y^s}{(mz+n)^2 \left|mz+n\right|^{2s}}}_{G_{2,s}(z)}$$

The functions $G_{2,s}(z)$, when $s > 1$, are absolutely convergent and modular functions of weight 2. However $G_2(z)$ is a "non-holomorphic modular form." It's Taylor expansion looks like

$$G_2(z) = 2\zeta(2) - \pi y^{-1} + 2(2\pi i)^2 \sum_{n=1}^{\infty} \sigma_1(n) e^{2\pi i n z}.$$

It's Taylor expansion is holomorphic at every term except the single πy^{-1} term above, so it's so close to being holomorphic.

We can normalize the Eisenstein series so that their constant terms are 1. This gives

$$E_k(z) = \frac{G_k(z)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

the **normalized Eisenstein series**. The B_k above is the kth Bernoulli number. Note that this function now has integral coefficients. One can also normalize G_2 to get E_2.

Example.

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} \text{ where } q = e^{2\pi i z}$$

is a modular form of weight 12. This is harder to show by direct computation, but maybe we can make things easier. What do you do you encounter a lot of products? You take logarithms.

$$\frac{1}{2\pi i} \frac{\partial}{\partial z} \log \Delta = E_2(z) \text{ where } E_2(z) = \frac{G_2(z) + \pi/y}{2\zeta(2)}.$$

Note that

$$E_2(\gamma z) = (cz + d)^2 E_2(z) + \frac{12c}{2\pi i}(cz + d).$$

TODO: Make sure this is the right expression

From this, one can show that Δ is holomorphic of weight 12. △

Definition 5.7.6. A modular form is called a **cusp form** if it vanishes at the cusp ∞. In other words, it has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} a_n q^n,$$

i.e. $a_0 = 0$. ◇

Definition 5.7.7. Let M_k be the space of modular forms, and S_k be the space of cusp forms. ◇

Note that $M_k = \mathbb{C}E_k + S_k$. Also note that $\Delta = q \prod_{n=1}^{\infty}(1 - q^n)$ has a zero at ∞ and no zero at $\tau \in \mathfrak{H}$. It's not too hard to see that

$$S_k/\Delta = M_{k-12} \text{ so } M_k = \mathbb{C}E_k + \Delta M_{k-12}.$$

Thus,

$$\dim M_k = 1 + \dim M_{k-12} = 1 + \dim S_k.$$

Theorem 5.7.8. *The space M_k of modular forms is generated, as a ring, by E_4 and E_6.*

He wrote something, but I didn't really get it, so I didn't write. The upshot is that we end up with

$$\dim M_k = \begin{cases} \lfloor k/12 \rfloor & \text{if } k \equiv 2 \pmod{12} \\ \lfloor k/12 \rfloor + 1 & \text{otherwise.} \end{cases}.$$

For details, see Diamond and Shurman or Serre's course in arithmetic or whatever. The above theorem gives us equalities like $E_8 = E_4^2$ and $E_{10} = E_6 E_4$ and whatnot just by dimension counting and matching constant terms (in general, matching low order terms).

5.7.1 L-functions and Hecke operators

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form. Then, its L-function is

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

(note that we start at $n = 1$ always in the L-function).

Example. $f = E_k = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. Then,

$$L(f, s) = -\frac{2k}{B_k} \sum_{n=1}^{\infty} \frac{\sigma_{k-1}(n)}{n^s} = -\frac{2k}{B_k} \sum_{n \geq 1} \frac{\sum_{d|n} d^{k-1}}{n^s} = -\frac{2k}{B_k} \sum_{a,d=1}^{\infty} \frac{d^{k-1}}{(ad)^s} = -\frac{2k}{B_k} \zeta(s)\zeta(s-k+1).$$

△

Theorem 5.7.9. *Let f be a cusp form. Then,*

(1) *$L(f, s)$ is absolutely convergent for $\mathrm{Re}(s) > k/2 + 1$.*

(2) *$L(f, s)$ has a holomorphic continuation to whole complex plane.*

(3) *$L(f, s)$ has a function equation ($s \leftrightarrow k - s$). Set $L^*(f, s) = (2\pi)^{-s} \Gamma(s) L(f, s)$. Then,*

$$L^*(f, s) = (-1)^{k/2} L^*(f, k - s).$$

Recall 5.7.10.

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^s \frac{\mathrm{d}t}{t}.$$

⊙

"When you study mathematics, you want to study something simple but nontrivial."

Let's prove this theorem in steps.

Proposition 5.7.11. *If $f = \sum a_n q^n$ is a cusp form. Then, there is some $C > 0$ such that*

$$|a_n| < C n^{k/2}.$$

Proof. Consider $y^{k/2} |f|$. This function is invariant under $\mathrm{SL}_2(\mathbb{Z})$ (but of course no longer holomorphic), and vanishes at ∞. Thus, $y^{k/2} |f|$ is an entire holomorphic function on $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}$ and so bounded. That is, $y^{k/2}|f| < C$ for some $C > 0$ and all $z \in \mathfrak{H}$. In the Fourier expansion of f, we have

$$e^{2\pi i(iy)n}a_n = \int_0^1 f(z)e^{-2\pi inx}\mathrm{d}x,$$

so

$$|a_n| \leq e^{2\pi ny}\int_0^1 Cy^{-k/2}\mathrm{d}x = Ce^{2\pi iny}y^{-k/2}$$

for *any* choice of $y > 0$ since a_n is a constant. Now, we optimize our choice of y. We can take $y = 1/n$ to get

$$|a_n| < C'n^{k/2}.$$

■

The above proposition gives

$$\sum_{n\geq 1}\left|\frac{a_n}{n^s}\right| \leq C\sum\frac{1}{n^{\mathrm{Re}(s)-k/2}}$$

when $f = \sum a_n a^n$ is a weight k cusp form. Thus, $L(f,s)$ absolutely convergent when $\mathrm{Re}(s) - k/2 > 1$ which gives part **(1)** of the theorem.

We now do parts **(2)**,**(3)**, the holomorphic continuation and function equation. Consider the integration

The Mellin transform of f or of $f(iz)$. Something like this

$$\int_0^\infty f(iy)y^s\frac{\mathrm{d}y}{y} = \int_0^\infty\sum_{n\geq 1}a_n e^{-2\pi ny}y^s\frac{\mathrm{d}y}{y} = \sum_{n\geq 1}a_n\int_0^\infty e^{-2\pi ny}y^s\frac{\mathrm{d}y}{y} = \sum_{n=1}^\infty\frac{a_n}{(2\pi n)^s}\Gamma(s) = L^*(f,s)$$

where we've chosen to not worry too much about convergence yet in swapping our sum and integral, and where we made the transformation $y \mapsto y/(2\pi n)$ in the second-to-last equality. This gives

$$L^*(f,s) = \int_0^\infty f(iy)y^s\frac{\mathrm{d}y}{y}$$

when $\mathrm{Re}(s) > k/2 + 1$, but the RHS above is entire. This is because $f(iy) = O(e^{-2\pi y})$ as $y \to \infty$ so it decays really fast. What about as $y \to 0$? Consider the operator $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. This gives

Fun fact: $\mathrm{SL}_2(\mathbb{Z})$ is generated by S and the T from earlier in class.

$$f\left(\frac{-1}{z}\right) = (-z)^k f(z) = z^k f(z)$$

since k even. Thus, we still have exponential decay as $y \to 0$, specifically, $f(z)$ is like $e^{-2\pi y^{-1}}y^{-k}$ as $y \to 0$. This shows that $L^*(f,s)$ is entire, which gives part **(2)**. For part 3, we do the usual functional equation trick of breaking up the integration and modifying.

$$L^*(f,s) = \int_1^\infty f(iy)y^s\frac{\mathrm{d}y}{y} + \underbrace{\int_0^1 f(iy)y^s\frac{\mathrm{d}y}{y}}_{\text{substitue } iy\mapsto\frac{-1}{iy}} = \int_1^\infty f(iy)y^s\frac{\mathrm{d}y}{y} + \int_1^\infty f\left(\frac{i}{y}\right)y^{-s}\frac{\mathrm{d}y}{y}.$$

Now use $f(-1/z) = (-z)^k f(z)$ with $z = iy$ to get

$$L^*(f,s) = \int_1^\infty f(iy)y^s \frac{\mathrm{d}y}{y} + \int_1^\infty f(iy)(-1)^{k/2}y^{k-s}\frac{\mathrm{d}y}{y} = \int_1^\infty f(iy)\left[y^s + (-1)^{k/2}y^{k-s}\right]\frac{\mathrm{d}y}{y}.$$

Now, one can just visibly see that

$$L^*(f,s) = (-1)^{k/2}L^*(f,k-s).$$

Theorem 5.7.12. *The space S_k has a base $X = \{f_1, \ldots, f_d\}$ such that*

$$L(f_i, s) = \prod_p \left(1 - a_p p^{-s} + p^{k-1-2s}\right)^{-1}.$$

This base is unique, so any cusp form whose L-function as above Euler product is one of these basis elements.

Proof Idea. Use Hecke operators $\{T_n : n \in \mathbb{N}\} \subset \operatorname{End}(S_k)$. These satisfy

- $a_1(T_n f) = a_n(f)a_1(f)$
- $T_n T_m = T_m T_n$
- T_n is sell-adjoint wrt **Peterson inner product** on S_k:

$$\langle f, g\rangle := \int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}} f(z)\overline{g(z)}y^k \frac{\mathrm{d}x\mathrm{d}y}{y^2}.$$

These properties give a diagonalization of S_k, so $S_k = \sum_{i=1}^d \mathbb{C}f_i$. ■

We don't have time for the details of the proof, but can at least define Hecke operators. Start by letting

$$\Delta(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{array}{l} a,b,c,d \in \mathbb{Z} \\ ad - bc = n \end{array} \right\}.$$

Note that $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \Delta(n)$. Let

$$T_n(f) := n^{k/2-1} \sum_{\gamma \in \mathrm{SL}_2(\mathbb{Z})\backslash\Delta(n)} f|_k\gamma.$$

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+$, we define

$$(f|_k\gamma)(z) = f(\gamma z)\frac{(\det\gamma)^{k/2}}{(cz+d)^k}.$$

Proposition 5.7.13.

(1) *If f is a modular form, then so is $T_n f$, and*

$$a_m(T_n f) = \sum_{d|(m,n)} a_{mn/d^2} d^{k-1}.$$

5.8 Lecture 8 (9/24)

Last time talked about modular forms for $\mathrm{SL}_2(\mathbb{Z})$, and then introduced L-functions and mentioned the main properties of Hecke operators. Let's quickly review a little bit.

5.8.1 Review of last time

The upper half plane $\mathfrak{H}$ is acted on by $\mathrm{SL}_2(\mathbb{Z})$. A function $f : \mathfrak{H} \to \mathbb{C}$ is called a modular form of weight k if it is holomorphic and satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \text{ for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Can introduce the **slash operator**

$$(f|_k\gamma)(z) = f(\gamma z)\frac{(\det\gamma)^{k/2}}{(cz+d)^k}$$

for any $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$. With this notation introduced, f is modular of weight $k \iff f|_k\gamma = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Note that $\mathrm{SL}_2(\mathbb{Z})$ is generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ which act by $Tz = z+1$ and $Sz = -1/z$. Thus, f is a modular form of weight k if it is holomorphic and satisfies both of

$$f(z+1) = f(z) \text{ and } f(-1/z) = (-z)^k f(z).$$

The first property gives you a Fourier expansion

This sum starting at 0 is part of the definition of modular form. It needs to be holomorphic at ∞

$$f(z) = \sum_{n=0}^{\infty} a_n q^n.$$

We call f a cusp form when $a_0 = 0$ above, so $f(z) = \sum_{n\geq 1} a_n q^n$.

We let M_k be the space of modular forms of weight k and S_k be the space of weight k cusp forms. Then, $M = \bigoplus M_k$ is a ring and $S = \bigoplus S_k$ is an ideal in this ring. In fact, S is principal, $S = (\Delta)$, where $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$. The main nicety of this Δ is that is has *no zeros in* $\mathfrak{H}$ *and a simple zero at* ∞ and so divides any cusp form. One can show that $M = \mathbb{C}[E_4, E_6]$ is generated by those two Eisenstein series. Furthermore, $M_k = E_k \oplus S_k$.

On the more arithmetic side, we have L-functions. Given modular $f = \sum_{n=0}^{\infty} a_n q^n$, its L-function is $L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}$. When, $f = E_k$, you get "nothing new," you have $L(E_k, s) = -\frac{2k}{B_k}\zeta(s)\zeta(s-k+1)$. Things are more interesting when f is cuspidal. In this case, $L(f,s)$ is absolutely convergent for $\mathrm{Re}(s) > 1 + k/2$, has a holomorphic continuation to whole complex plane, and satisfies a function equation

$$L^*(f, k-s) = (-1)^k L^*(f,s) \text{ where } L^*(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s).$$

In fact one can show the assignment $f \mapsto L(f,1)$ is a bijection (between Hecke eigenforms forms and L-functions with Euler products, analytic continuous, and functional equations of the right form?)

I'm pretty sure there's a rigorous statement of this in Bump's automorphic

5.8.2 Hecke operators

We also mentioned the Hecke operators last time. These form an algebra denoted $\mathbb{T}$ and one has $S_k = \bigoplus_{\lambda:\mathbb{T}\to\mathbb{C}} \mathbb{C}f_\lambda$ where $T_n f = \lambda(T_n)f$. Writing $f_\lambda = \sum a_n q^n$, we have $\lambda(T_n)a_1 = a_n$. In particular, $a_1 \neq 0$ unless $f = 0$, so we can normalize $a_1 = 1$ if we want. These f_λ satisfy an Euler product

$$L(f_\lambda, s) = \prod_p \left(1 - a_p p^{-s} + p^{k-1-2s}\right)^{-1}.$$

Here's something. Consider $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \times \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ which parameterizes pairs of curves. There's a divisor $Z(n) \subset X(1)$ which parameterizes isogenies $(\varphi : E_1 \to E_2)$ of degree $\deg\varphi = n$, so we can write $Z(n) = \sum c_i D_i$. Hecke operators are basically obtained by pullback-pushforward along the (lower half of the) diagram

$$\begin{tikzcd}
 & X(1)\times X(1) \arrow[ddl] \arrow[ddr] & \\
 & Z(n) \arrow[u, hook] \arrow[dl] \arrow[dr] & \\
X(1) & & X(1)
\end{tikzcd}$$

Here's a more analytic approach. Let

$$\Delta(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{matrix} a,b,c,d \in \mathbb{Z} \\ ad - bc = n \end{matrix} \right\}.$$

$\mathrm{SL}_2(\mathbb{Z})$ acts on this on both the left and the right. In cases like this, people like looking at double cosets. Write $\Delta(n) = \bigsqcup_{i=1}^{d(n)} \mathrm{SL}_2(\mathbb{Z})\gamma_i$. We can then set

$$T_n f = n^{k/2-1} \sum_{i=1}^{d(n)} f|_k \gamma_i.$$

By messing around with the effects of $S, T \in \mathrm{SL}_2(\mathbb{Z})$, it is not too hard to show that you can take γ_i to be (some?) matrices of the form

$$\gamma_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $0 \leq b \leq d-1$. Here are some properties.

- $T_n f$ does not depend on the choice of γ_i by modularity of f.
- $T_n f$ is itself a modular form, in fact is is a weight k cusp form (when f is a weight k cusp form).
- $a_m(T_n f) = \sum_{d|(m,n)} a_{mn/d^2}$

Proof. Use the representatives

$$\mathrm{SL}_2(\mathbb{Z})\backslash\Delta(n) = \left\{ \mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \,\middle|\, \begin{matrix} \text{ad} = n \text{ and } a, b > 0 \\ 0 \leq b \leq d-1 \end{matrix} \right\}$$

We can just directly compute

$$T_nf(z)=\sum_{\substack{ad=n\\ b \bmod d}} n^{k-1}f\left(\frac{az+b}{d}\right)d^{-k}=n^{k-1}\sum_m a_m\sum_{\substack{ad=n\\ 0\le b<d}} e^{2\pi im\frac{az+b}{d}}\cdot d^{-k}=n^{k-1}\sum_m a_m\sum_{ad=n} e^{\frac{2\pi imaz}{d}}d^{-k}\sum_{0\le b<d} e^{2\pi imb/d}$$

Note that the rightmost sum is a Gauss sum, a summation of values of a character $(\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}^\times$. Hence, it is equal to d if the character $b\mapsto e^{2\pi imb/d}$ is trivial (i.e. if $d\mid m$), but is equal to 0 otherwise. Thus the above equation equals

$$T_nf(z)=n^{k-1}\sum_m a_m\sum_{d|(m,n)} e^{2\pi imnz/d^2}d^{1-k}.$$

Finishing this proof is left as an exercise... ■

I stopped paying attention for a while, but I think he showed that the Hecke operators commute ($T_mT_n=T_nT_m$) and that $L(f,s)$ satisfies an Euler product when f is an eigenvector for every Hecke operator.

How do we know we can find these simultaneous eigenfunctions? We introduce the Peterson product. For two weight k cusp forms, f,g, we set

$$\langle f,g\rangle=\int_{\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}} f(z)\overline{g(z)}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}.$$

Proposition 5.8.1. $\langle T_nf,g\rangle=\langle f,T_ng\rangle$.

One can show this by direct computation, but it is a big of a mess. Morally, if "$\Delta(n)$ if finite" and "$\mathrm{SL}_2(\mathbb{Z})=1$" then this looks like a sum of

$$\int_{\mathfrak{H}} f|_\gamma(z)\overline{g(z)}y\frac{\mathrm{d}x\mathrm{d}y}{y^2}$$

so one can do the change of variables $z\mapsto\gamma z$.

Alternatively, one can use the Rankin-Selberg method which tells you that $\langle f,g\rangle=$ "$\lim_{s\to1}$" $\sum\frac{a_n\overline{b_n}}{n^s}$, and then do something with this? I didn't really follow either of these approaches, but whatever, can find proofs in books.

Remark 5.8.2. One can extend this theory to congruence subgroups $\Gamma\subset\mathrm{SL}_2(\mathbb{Z})$. ○

Remark 5.8.3. This has applications to elliptic curves over $\mathbb{Q}$. Given $E/\mathbb{Q}$, one gets an L-function $L(E,s)=\prod\left(1-a_pp^{-s}+p^{1-2s}\right)^{-1}$ and Wiles, Taylor-Wiles, and BCDT showed that $L(E,s)=L(f,s)$ for some weight 2 cusp form f.

Geometrically, this is coming from a surjection $\varphi:X\to E$ where X is a modular curve. Inside X, one has CM points coming from $\mathbb{C}/\Lambda$ with $\Lambda\subset\mathbb{Q}(\sqrt{-D})$. φ sends these CM-points to $E(\overline{\mathbb{Q}})$, and these points can be used to construct rational points by taking traces. This can be used to prove (one direction of?) the BSD conjecture in rank ≤ 1 case. This was done by Gross-Zagier and Kolyvagin. Recently, the converse direction was done by Skinner and Wei Zhang. ○

Conjecture 5.8.4 (Discriminant conjecture). *For any elliptic curve $E/\mathbb{Q}$, $\Delta\le c(\varepsilon)N^{6+\varepsilon}$.*

In function field case, this was done by Szpiro.

5.9 Lecture 9 (9/29): Abelian Varieties

Today we start Abelian varieties. Our main reference is Mumford's book which is really long. We will start by working over a algebraically closed fields $k = \overline{k}$.

Assumption. All our k-varieties will be integral (reduced + irreducible), separated, and finite type over k.

Definition 5.9.1. An **abelian variety** X/k is a proper variety with group structure. That is, we have k-morphisms $m : X \times X \to X$, $[-1] : X \to X$, and $e : \operatorname{Spec} k \to X$ which make the obvious diagrams commute (equivalently, which gives a group structure to $X(T) = \mathrm{H}_k(T, X)$ for all k-schemes T) ⋄

Lemma 5.9.2. *Abelian varieties are smooth.*

Proof. Let $U \subset X$ be a smooth open set. For any $x \in X(k)$, the translation $U \cdot x$ is also smooth, so $X = \bigcup_{x \in X(k)} U \cdot x$ is smooth. ■

We will also show that X/k is commutative, but before this, we will need some rigidity properties of abelian varieties. In particular, we will show that any morphism $f : X \to Y$ of abelian varieties, $f(0) = 0 \implies f$ is a homomorphism.

Lemma 5.9.3 (**Rigidity lemma**)**.** *Consider a morphism $f : X \times T \to Y$ such that X is proper and there is some $t_0 \in T$ such that $f|_{X \times \{t_0\}}$ is constant with image $y_0 \in Y$. Then, f factors through the projection*

We're assuming through these are all varieties over $k = \overline{k}$. In particular, Y is separated and T is irreducible

$$\begin{tikzcd} X \times T \arrow[rr, "f"] \arrow[dr] & & Y \\ & T \arrow[ur, "g"] & \end{tikzcd}$$

Proof. First note that this is trivial if Y is affine. For any $t \in T$, $f|_{X \times \{t\}}$ is an proper subvariety of the affine space Y, so it is a point.

Now consider the general case. Let $U \subset Y$ be an affine neighborhood of y_0, and let $Z = Y - U$. Now consider $f^{-1}(Z) \subset X \times T$. The projection map $p_2 : X \times T \to T$ is proper, so maps $f^{-1}(Z)$ to a closed set $p_2(f^{-1}(Z)) \subset T$. Thus, its complement $V = T \setminus p_2(f^{-1}(Z))$ is an open set such that $(X \times V) \cap f^{-1}(Z) = \emptyset$, i.e. $f(X \times V) \subset U$. Since U is affine, this shows that $f|_{X \times V}$ factors through the projection $X \times V \to V$.

Now, Y is separated so the diagonal $\Delta_{Y/k} \subset Y \times Y$ is closed. Fix some $x_0 \in X$, and consider the map $h = (f, f(x_0, -) \circ p_2) : X \times T \to Y \times Y$ given by $h(x, t) = (f(x, t), f(x_0, t))$. So, the subscheme

Question: Do I secretly want $x_0 \in X(k)$?

$$h^{-1}(\Delta_{Y/k}) \subset X \times T$$

where f factors through T is closed. At the same time, it contains the open $X \times V \subset X \times T$. Since T is irreducible, $X \times V$ is a dense open, so we conclude that $h^{-1}(\Delta_{Y/k}) = X \times T$, i.e. that f factors through T. ■

Corollary 5.9.4. *Let $f : X \to Y$ be a morphism of abelian varieties such that $f(e_X) = e_Y$. Then, f is a group homomorphism.*

Proof. Consider

$$\begin{array}{ccc} X \times X & \xrightarrow{f\times f} & Y \times Y \\ {\scriptstyle m_X}\downarrow & & \downarrow{\scriptstyle m_Y} \\ X & \xrightarrow{f} & Y \end{array}.$$

We aim to show that this square commutes. Consider the morphism

$$\begin{array}{cccc} \varphi: & X \times X & \longrightarrow & Y \\ & (x_1, x_2) & \longmapsto & f(x_1)f(x_2)f(x_1x_2)^{-1} \end{array}$$

Note that $\varphi(x_1, e_X) = e_Y$ and $\varphi(e_x, x_2) = e_Y$. We now apply rigidity twice to see that φ is constant with image e_Y. ∎

Corollary 5.9.5. *Any abelian variety is commutative.*

Proof. The map $[-1] : X \to X, x \mapsto x^{-1}$ is a group homomorphism by previous corollary. ∎

Notation 5.9.6. From now on, we use '+' to denote the group structure and replace e_X by 0.

Application. On an abelian variety X, one has

$$\Omega_X \simeq \Omega_{X,0} \otimes_k \mathscr{O}_X.$$

To prove this, use translation. Can start with $\alpha_0 \in \Omega_{X,0}$ and use translation to get a section of Ω_X.

Definition 5.9.7. A map $f : X \to \mathbb{Z}$ is **upper semi-continuous** if for any $x \in X$ there exists an open $U \ni x$ such that $f|_U \leq f(x)$, i.e. f can only increase under specialization. ◇

Theorem 5.9.8 (**Semicontinuity theorem**)**.** *Let $f : X \to Y$ be a proper morphism of noetherian schemes, and let $\mathscr{F}$ be a coherent sheaf on X, flat over Y. Then for each $i \geq 0$,*

$$h^i(y, \mathscr{F}) = \dim_{\kappa(y)} \mathrm{H}^i(X_y, \mathscr{F}_y)$$

is an upper semicontinuous function $Y \to \mathbb{Z}$.

Corollary 5.9.9 (**Grauert**)**.** *With the same hypotheses as in the theorem, further suppose that Y is integral, and that for some i, the function $h^i(y, \mathscr{F})$ is constant on Y. Then, $R^i f_*(\mathscr{F})$ is locally free on Y, and for every y the natural map*

$$R^i f_*(\mathscr{F}) \otimes \kappa(y) \to \mathrm{H}^i(X_y, \mathscr{F}_y)$$

is an isomorphism.

Theorem 5.9.10 (**See-Saw Theorem**)**.** *Let X be proper and let T be an arbitrary variety. Let $\mathscr{L}$ be a line bundle on $X \times T$. Then,*

(1) *$S = \{t \in T : \mathscr{L}|_{X\times\{t\}} = \text{trivial}\}$ is a closed subvariety of T.*

(2) *$\mathscr{L}|_{X\times S} = \mathrm{pr}_S^* \mathscr{M}$ is the pullback of some line bundle $\mathscr{M}$ on S.*

Proof. **(1)** Note that $\mathscr{L}|_{X\times\{t\}}$ is trivial $\iff$ $\mathrm{H}^0(X\times\{t\},\mathscr{L}) \neq 0$ and $\mathrm{H}^0(X\times\{t\},\mathscr{L}^{-1}) \neq 0$. Now, by upper semi-continuity of cohomology of flat sheaves, we see that this is a closed property, so S is closed.

(2) On $X\times S$, $1 = \dim \mathrm{H}^0(X\times\{t\},\mathscr{L})$ for all $t\in S$, so the pushforward $(\mathrm{pr}_{S,*}\mathscr{L})$ is a line bundle on S. Further (below, the subscript is fiber, not stalk),

$$\mathrm{H}^0(X\times\{t\},\mathscr{L}) = (\mathrm{pr}_{S,*}\mathscr{L})_t$$

and so $\mathscr{L} = \mathrm{pr}_S^*(\mathrm{pr}_{S,*}\mathscr{L})$. ■

Question: Why do we have this equality?

Answer: The natural map $\mathrm{pr}_S^*\,\mathrm{pr}_{S,*}\mathscr{L} \to \mathscr{L}$ is an isomorphism on fibers, since this is secretly the restriction map $\mathscr{O}_{X\times\{t\}} \to \kappa(x,t)$

Another important theorem is that of the cube.

Theorem 5.9.11 (**Theorem of the cube**)**.** *Say X, Y, Z are varieties with X, Y proper and $\mathscr{L}$ is a line bundle over $X\times Y\times Z$. Fix basepoints $x_0\in X$, $y_0\in Y$, and $z_0\in Z$. Suppose that*

$$\mathscr{L}|_{x_0\times Y\times Z},\quad \mathscr{L}|_{X\times y_0\times Z},\quad \text{and } \mathscr{L}|_{X\times Y\times z_0}$$

are all three trivial. Then, $\mathscr{L}$ is trivial.

The proof is long, so we omit for now. We do give some intuition. $\mathscr{L}$ is determined by $\mathrm{H}^1(X\times Y\times Z, \mathscr{O}^\times_{X\times Y\times Z})$ which sits in a sequence like $\mathrm{H}^1(X\times Y\times Z,\mathscr{O}_{X\times Y\times Z}) \to \mathrm{H}^1(X,\mathscr{O}^\times_{X\times Y\times Z}) \to$ "$\mathrm{H}^2(X,\mathbb{Z})$". The Kunneth formula will tell you that $\mathscr{L}$ can be decomposed into pullback of bundles on at most 2 factors.

Corollary 5.9.12. *Let $X\times Y\times Z$ with $x_0\in X$, $y_0\in Y$, and $z_0\in Z$ as in the theorem of the cube. Then, for any line bundle $\mathscr{L}$ on $X\times Y\times Z$, we have a canonical isomorphism*

$$\mathscr{L} \simeq p_{YZ}^*\mathscr{L}_{YZ}\otimes p_{XZ}^*\mathscr{L}_{XZ}\otimes p_{XY}^*\mathscr{L}_{XY}\otimes p_X^*\mathscr{L}_X^{-1}\otimes p_Y^*\mathscr{L}_Y^{-1}\otimes p_X^*\mathscr{L}_Z^{-1},$$

where, for example, $p_{YZ}: X\times Y\times Z\to Y\times Z$ is a projection map and $\mathscr{L}_{XZ} = \mathscr{L}|_{X\times\{y_0\}\times Z}$ is the restriction to $X\times\{y_0\}\times Z \simeq X\times Z$.

Corollary 5.9.13. *Let X be an abelian variety and let $\mathscr{L}/X$ be a line bundle. Then,*

$$\mathscr{L}^{\square} := \bigotimes_{I\subset\{1,2,3\}} m_I^*\mathscr{L}^{(-1)^{\#I-1}} \simeq \mathscr{O}_{X\times X\times X}$$

where $m_I: X\times X\times X\to X$ is given by $m_I(x_1,x_2,x_3) = \sum_{i\in I} x_i$. Spelled out, we have the inclusion-exclusion type result

$$m_{1,2,3}^*\mathscr{L} - m_{1,2}^*\mathscr{L} - m_{1,3}^*\mathscr{L} - m_{2,3}^*\mathscr{L} + m_1^*\mathscr{L} + m_2^*\mathscr{L} + m_3^*\mathscr{L} - \mathscr{O}_{X\times X\times X} \simeq \mathscr{O}_{X\times X\times X}.$$

Corollary 5.9.14. *Let S be a variety and X an abelian variety. Fix $f,g,h: S\to X$ and a line bundle $\mathscr{L}/X$ over X. Then,*

$$(f+g+h)^*\mathscr{L} \simeq (f+g)^*\mathscr{L}\otimes(g+h)^*\mathscr{L}\otimes(h+g)^*\mathscr{L}\otimes f^*\mathscr{L}^{-1}\otimes g^*\mathscr{L}^{-1}\otimes h^*\mathscr{L}^{-1}.$$

Proof Idea. Consider $(f, g, h) : S \to X^3$ ■

Corollary 5.9.15. *For any line bundle $\mathscr{L}$ on X and integer n, let $n_X : X \to X, x \mapsto nx$ be the multiplication by n map. Then,*

$$n_X^* \mathscr{L} \simeq \mathscr{L}^{\frac{n^2+n}{2}} \otimes ((-1)_X^* \mathscr{L})^{\frac{n^2-n}{2}}.$$

Proof. Apply previous corollary to the morphisms $(n_X, 1_X, -1_X) : X \to X$. Using $+$ instead of $\otimes$ for group operation in $\mathrm{Pic}(X)$, this gives

$$n^* \mathscr{L} \simeq (n+1)^* \mathscr{L} + (n-1)^* \mathscr{L} - n^* \mathscr{L} - \mathscr{L} - (-1)^* \mathscr{L}.$$

That is,

$$(n+1)^* \mathscr{L} - 2n^* \mathscr{L} + (n-1)^* \mathscr{L} \simeq \mathscr{L} + [-1]^* \mathscr{L}.$$

Now use induction. ■

Application. Let $g = \dim X$. Then, ($n_X : X \to X$ is finite) and $\deg n_X = n^{2g}$ (if X is projective[85]).

Remember: finite = proper + quasi-finite. This is one (of many) consequences of the theorem on formal functions

Proof. Let $\mathscr{L}$ be an ample line bundle on X. Note that $c_1(n_X^* \mathscr{L})^g = (\deg n_X) c_1(\mathscr{L})^g$. We may assume that $\mathscr{L}$ is even (i.e. replace $\mathscr{L}$ by $\mathscr{L} \otimes (-1)^* \mathscr{L}$). We have $n^* \mathscr{L} = \mathscr{L}^{n^2}$, so we see that

Question: Why?

Answer: Previous corollary + $\mathscr{L}$ is even

$$n^{2g} c_1(\mathscr{L})^g = (\deg n_X) c_1(\mathscr{L})^g$$

and we win. ■

Remark 5.9.16. How do we show that n_X is finite? If not, some fiber will have positive dimensional component. One can probably then translation to show that all fibers have a positive dimensional component ($\ker[n_x] \curvearrowright X$). We claim that n_X is a separable morphism (at least when $\mathrm{char}\, k = p \nmid n$). Let $m : X \times X \to X$ be multiplications. We claim that $\mathrm{d}m : T_{X,0} \times T_{X,0} \to T_{X,0}$ is addition. This is because $X \xrightarrow{(x,0)} X \times X \xrightarrow{m} X$ and $X \xrightarrow{(0,x)} X \times X \xrightarrow{m} X$ are both the identity (+ linearity). Hence, $dn_X : T_{X,0} \to T_{X,0}$ is multiplication by n, an isomorphism. Since n_X is obviously flat, this means that it is étale. The above application then shows that $\# \ker[n](k) = n^{2g}$; considering this for varying n then shows that $\ker[n](k) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. ○

Remark 5.9.17. What about multiplication by p? On tangent spaces, this induces $T_X \to T_X, x \mapsto px = 0$ so the separable degree of $[p] : X \to X$ is $\le g$ (since the inseparability degree is $\ge g$)[86]. This separable degree is the same as $\# \ker[p](k)$. A little more work will show $X[p] \simeq (\mathbb{Z}/p\mathbb{Z})^i$ for some $0 \le i \le g$. One can then get $X[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^i$ for some $0 \le i \le g$. ○

Theorem 5.9.18 (Theorem of the square). *Let X be an abelian variety with line bundle $\mathscr{L}$, consider the translation map*

$$\begin{array}{rccc} T_x : & X & \longrightarrow & X \\ & y & \longmapsto & y + x \end{array}.$$

[85] Next time we'll show all abelian varieties are projective

[86] Look at function fields $k(Y) \hookrightarrow k(X)$. We know $\Omega_{Y,0} = \sum_{i=1}^{g} k\mathrm{d}x_i$ and that $p^* \mathrm{d}x_i = 0$. We have $k(x_1, \ldots, x_g) \subset k(X)$ pulls back to $k(x_1^p, \ldots, x_g^p) \subset p^* k(X)$

Then,

$$T^*_{x+y}\mathscr{L} + \mathscr{L} = T^*_x\mathscr{L} + T^*_y\mathscr{L}.$$

As a result, $X \to \operatorname{Pic} X, x \to T^*_x\mathscr{L} - \mathscr{L}$ *is a group homomorphism.*

Proof. Consider the three maps $x, y, \mathrm{Id} : X \to X$. The theorem of the cube gives

$$T^*_{x+y}\mathscr{L} \simeq T^*_x\mathscr{L} \otimes T^*_y\mathscr{L} \otimes \mathscr{L}^{-1}.$$

■

5.10 Lecture 10 (10/1)

Last time we started started studying abelian varieties, proper group varieties, over $k = \overline{k}$. Today, we continue studying these, still over an algebraically closed field.

Recall 5.10.1. Abelian varieties are smooth and abelian. The latter of these was a consequence of the rigidity lemma. ⊙

We also introduced the theorem of the cube last time, which had many consequences. One of which was the following

Recall 5.10.2. Let X be an abelian variety and let $\mathscr{L}/X$ be a line bundle. Then,

$$\mathscr{L}_{X^3} := \bigotimes_{I \subset \{1,2,3\}} m_I^*\mathscr{L}^{(-1)^{\#I-1}} \simeq \mathscr{O}_{X\times X\times X}$$

where $m_I : X \times X \times X \to X$ is given by $m_I(x_1, x_2, x_3) = \sum_{i\in I} x_i$. Spelled out, we have the inclusion-exclusion type result

$$m^*_{1,2,3}\mathscr{L} - m^*_{1,2}\mathscr{L} - m^*_{1,3}\mathscr{L} - m^*_{2,3}\mathscr{L} + m^*_1\mathscr{L} + m^*_2\mathscr{L} + m^*_3\mathscr{L} - \mathscr{O}_{X\times X\times X} \simeq \mathscr{O}_{X\times X\times X}.$$

⊙

Can do something similar for $\mathscr{L}_{X^2}$. We have three maps $m, p_1, p_2 : X \times X \to X$ where m is addition and p_1, p_2 are projection maps. Can then define

$$\mathscr{L}_{X^2} = m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1},$$

but this may not be trivial. However, we will study a subgroup

$$\operatorname{Pic}^0(X) = \{\mathscr{L} \in \operatorname{Pic} X : \mathscr{L}_{X^2} = \mathscr{O}_{X^2}\}$$

where it is trivial.

We also introduced the theorem of the square.

Recall 5.10.3 (Theorem of the square)**.** Let X be an abelian variety with line bundle $\mathscr{L}$, consider the translation map

$$\begin{array}{cccc} T_x : & X & \longrightarrow & X \\ & y & \longmapsto & y + x \end{array}.$$

Then,

$$T_{x+y}^*\mathscr{L} + \mathscr{L} = T_x^*\mathscr{L} + T_y^*\mathscr{L}.$$

As a result, $X \to \operatorname{Pic} X, x \to T_x^*\mathscr{L} - \mathscr{L}$ is a group homomorphism. $\odot$

which is an easy consequence of the theorem of the cube.

What are some applications of these?

Application.

$$[n]^*\mathscr{L} \simeq \mathscr{L}^{\frac{n^2+n}{2}} \otimes ([-1]^*\mathscr{L})^{\frac{n^2-n}{2}}.$$

In particular, if $\mathscr{L}$ is **even**, i.e. $\mathscr{L} \simeq [-1]^*\mathscr{L}$, then $[n]^*\mathscr{L} \simeq \mathscr{L}^{n^2}$. If $\mathscr{L}$ is **odd**, i.e. $\mathscr{L}^{-1} \simeq [-1]^*\mathscr{L}$, then $[n]^*\mathscr{L} \simeq \mathscr{L}^n$.

From this, when X is projective, one can see that $[x] : X \to X$ is finite of degree n^{2g} and $X[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ if $p \nmid n$ ($p = \operatorname{char} k$). Also, $X[p] = (\mathbb{Z}/p\mathbb{Z})^i$ for some $i \in \{0, \ldots, g\}$.

Today we will show that X is always projective. The theory of abelian varieties is different from that of elliptic curves. For elliptic curves, your origin is already an ample divisor, and so you get projectivity for free. On an abelian variety, it is harder to construct line bundles. We will show that X is projective using a very general theorem.

Theorem 5.10.4. *Let X be an abelian variety, and let $D \in \operatorname{Div} X$ be an effective divisor. Set $\mathscr{L} = \mathscr{O}_X(D)$. Then, $\mathscr{L}$ is ample iff*

$$H := \{x \in X : T_x^*D = D\}$$

is finite.

Corollary 5.10.5. *Every abelian variety is projective.*

Proof of corollary, assuming Theorems. Let $U \hookrightarrow X$ be any open affine subset around $0 \in X$ such that $X \setminus U =: D$ is a Cartier divisor. Set

$$H := \{x \in X : D + x = D\} = \{x \in X : U + x = U\},$$

so $H \hookrightarrow U$ (since $0 \in U$).

We claim that H is a closed subvariety of X (which is proper). This follows from the seesaw theorem. Since proper subvarieties of affine varieties are finite, we win by the theorem. ∎

TODO: Figure out what's going on here

To prove the theorem, we will add some intermediate steps.

Theorem 5.10.6. *Let X be an abelian variety with D an effective divisor and let $\mathscr{L} = \mathscr{O}_X(D)$. Then, TFAE*

(1) $K(\mathscr{L}) = \{x \in X : T_x^*\mathscr{L} \cong \mathscr{L}\}$ *is finite.*

(2) $H = \{x \in X : T_x D = D\}$ *is finite.*

(3) $X \to \mathbb{P}(\Gamma(\mathscr{O}(2D))) = \mathbb{P}^N$ *is base point free and defines a finite morphism to* $\mathbb{P}^N$.

(4) $\mathscr{L}$ *is ample.*

Proof. ((**(1)** → **(2)**)) is easy.

((**(3)** → **(4)**)) Use Serre's ampleness criterion: $\mathscr{L}$ is ample if for any sheaf $\mathscr{F}$, $\mathrm{H}^i(X, \mathscr{F} \otimes \mathscr{L}^n) = 0$ for all $n \gg 0$ (even enough just to do the case of $i = 1$). We have $\pi : X \to \mathbb{P}^N$ finite with $\pi^*\mathscr{O}(1) = \mathscr{L}^{\otimes 2}$. Thus,

$$\mathrm{H}^1(X, \mathscr{F} \otimes \mathscr{L}^{\otimes 2n}) = \mathrm{H}^1(X, \mathscr{F} \otimes \pi^*\mathscr{O}(n)) = \mathrm{H}^1(\mathbb{P}^N, \pi_*\mathscr{F} \otimes \mathscr{O}((\deg \pi)n)) = 0$$

for $n \gg 0$.

For an affine $f : X \to Y$ between noetherian, separated schemes, one has $\mathrm{H}^i(X, \mathscr{F}) \cong \mathrm{H}^i(Y, f_*\mathscr{F})$ for any quasi-coherent $\mathscr{F}$ on X

((**(4)** → **(1)**)) Use seesaw theorem. This implies that $K(\mathscr{L}) \hookrightarrow X$ is a closed subgroup, so let $Y = K(\mathscr{L})^\circ$ be its connected component, an abelian subvariety. If $\dim Y > 0$ (so $K(\mathscr{L})$ infinite), we can investigate $\mathscr{L}|_Y$ which is ample since $\mathscr{L}$ is. But now we have $T_y^*\mathscr{L}_Y \cong \mathscr{L}_Y$ for all $y \in Y$, so $\mathscr{M}_{Y^2} = 0$ where $\mathscr{M} = \mathscr{L}|_Y$.[87] Consider $i : Y \to Y^2, y \mapsto (y, -y)$. Then,

$$i^*\mathscr{M}_{Y^2} = \mathscr{M}_{Y^2}^{-1} \otimes (-1)^*\mathscr{M}_{Y^2}^{-1}$$

is trivial, and something something anti-ample + seesaw.

TODO: Understand what's going on

((**(2)** → **(3)**)) This is the hard part. We already know $2D$ is base point free. We've seen that $T_{x+y}^*D \cong T_x^*D + T_y^*D - D$ so taking $x + y = 0$ gives $2D \sim T_x^*D + T_{-x}^*D = (D - x) + (D + x)$ for any $x \in X(k)$. For any $y \in X$, we can find x such that $y \notin D - x$ and $y \notin D + x$, so $2D$ is base point free. Now, we can use sections $k^{N+1} \simeq \Gamma(X, \mathscr{O}_X(2D))$ to define a morphism $\pi : X \to \mathbb{P}^N = \mathbb{P}(\Gamma(X, \mathscr{O}_X(2D)))$. We want to show that π is finite, i.e. $\#\pi^{-1}(t) < \infty$ for any t. Suppose not, so there exists some (proper) curve $C \subset \pi^{-1}(t)$ for some fiber. On the other hand, for a hyperplane $H \subset \mathbb{P}^N$ not containing t, we have $\pi^*(H) \cap C = \emptyset$. Since $\pi^*(H) \sim 2D$, we conclude that $\deg \int X(2D)|_C = 0$ (actually $\deg_C(D + x) = 0$ for all x). Thus, for any effective $E \sim D$, either $E \supset C$ or $E \cap C = \emptyset$. For any $x \in C$ and $y \in E$, we have $0 \in C \setminus (x)$ and $0 \in E \setminus (y)$, so $C \cap E + x - y \neq \emptyset \implies C \subset E + x - y$. We have show that for any $x \in C$ and $y \in D$, $C \subset D + x - y$. That is, for any $x, x' \in C$ and $y \in D$, $y + x' - x \in D$. This says exactly $T_{x'-x}^*D = D$ and so $H \supset \{x' - x \mid x', x \in C\}$ which is infinite, a contradiction.

Question: Why?

Question: Why?

If ever I return to understand this, the chain of implications should be something like

$$\begin{aligned}\deg_C D = 0 &\implies \deg_C(D + x) = 0 \implies C \subset D + x \text{ or } C \cap (D + x) = \emptyset \\ &\implies C \subset D + x - y \, (x \in C, y \in D) \implies D + x - x' = D \implies H \supset \{x - x' : x, x' \in C\}\end{aligned}$$

∎

What will we do next time? We'd like to replicate the fact that, for an elliptic curve E, $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$ via $P \mapsto \mathscr{O}_X(P - O)$. For an abelian variety, we can take an ample line bundle $\mathscr{L}$ and consider $X \to \mathrm{Pic}(X), x \mapsto T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. We will show that the image of this map is $\mathrm{Pic}^0(X)$. We know from today that the kernel is finite. We will use this to construct a variety for $\mathrm{Pic}^0(X)$.

5.11 Lecture 11 (10/6)

Recall that abelian varieties are higher dimensional analogues of elliptic curves.

[87] Recall, $\mathscr{M}_{Y^2} = m^*\mathscr{M} \otimes p_1^*\mathscr{M}^{-1} \otimes p_2^*\mathscr{M}^{-1}$

For an elliptic curve E, the identity $O \in E$ already gives an ample line bundle $\mathscr{O}_E(O)$, and its double $\mathscr{O}_E(2O)$ gives a map $E \to \mathbb{P}^1$.

For an abelian variety, $O \in A$ is a point, and so in general not a divisor. This is why, last time, we had to do some work to show that A is projective. In particular, we proved the following.

Theorem 5.11.1. *Let X be an abelian variety with effective divisor D. Then, D is ample $\iff X \setminus D$ is affine. In this case, $\Gamma(\mathscr{O}_X(2D))$ defines a finite morphism $X \to \mathbb{P}^N$.*[88]

We have also defined the morphism

$$\begin{aligned} \varphi_{\mathscr{L}} : \quad X &\longrightarrow \quad \operatorname{Pic}(X) \\ x &\longmapsto T_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned}$$

We showed that $\mathscr{L}$ is ample $\iff$ the kernel $K_{\mathscr{L}} = \ker \varphi_{\mathscr{L}}$ is finite.

Example. Let $X = E \times E$. For m, n can consider the map

$$\begin{aligned} E &\longrightarrow X \\ x &\longmapsto (mx, nx) \end{aligned}$$

Let $D_{m,n}$ be the image of this map. It is ample if $(m, n) = 1$. Note that it has a group law

$$D_{m,n} \times D_{m,n} \to D_{m,n}$$

and $K_{D_{m,n}} = \infty \implies D_{m,n} \neq$ ample. $\triangle$

5.11.1 $\operatorname{Pic}^0(X)$

Setup 5.11.2. X is an abelian variety.

Notation 5.11.3. We define

$$\operatorname{Pic}^0(X) = \{\mathscr{L} \in \operatorname{Pic}(X) : \varphi_{\mathscr{L}}(x) = 0 \, \forall x \in X\},$$

i.e. translation-invariant line bundles $T_x^*\mathscr{L} \simeq \mathscr{L}$ for all $x \in X$.

Note that φ is a bilinear map $\varphi : \operatorname{Pic}(X) \times X \to \operatorname{Pic}(X)$ (use theorem of the square), where $\varphi(\mathscr{L}, x) = \varphi_{\mathscr{L}}(x) = T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$.

Claim 5.11.4. *The image of φ lies in* $\operatorname{Pic}^0(X)$

Proof. We claim $\varphi_{\varphi_{\mathscr{L}}(x)}(y) = 0$ always. This expands to

$$T_y^*\varphi_{\mathscr{L}}(x) \otimes \varphi_{\mathscr{L}}(x)^{-1} = T_y^*(T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}) \otimes T_x^*\mathscr{L}^{-1} \otimes \mathscr{L} = T_{x+y}^*\mathscr{L} \otimes T_y^*\mathscr{L}^{-1} \otimes T_x^*\mathscr{L}^{-1} \otimes \mathscr{L},$$

which is trivial by the theorem of the square. ∎

[88] We won't prove this now, but $\Gamma(\mathscr{O}_X(3D))$ gives an embedding

Thus, φ gives us a map $\mathrm{Pic}(X) \to \mathrm{Hom}(X, \mathrm{Pic}^0(X))$ sitting in a diagram

$$0 \to \mathrm{Pic}^0(X) \to \mathrm{Pic}(X) \to \mathrm{Hom}(X, \mathrm{Pic}^0(X)).$$

Define $\mathrm{NS}(X) :=$ image of φ, the **Néron-Severi group**, so we have a short exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \xrightarrow{\varphi} \mathrm{NS}(X) \longrightarrow 0.$$

Example. When X is an elliptic curve, $\mathrm{Pic}^0(X) = \mathrm{Div}^0(X)/\sim$ and $\mathrm{NS}(X) = \mathbb{Z}$, and φ is just the degree map.

Given $\mathscr{L} = \mathscr{O}_X(D)$, we have $\varphi_{\mathscr{L}} : x \mapsto T_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$. Concretely, T_x^* is translation by $-x$, so if we write $D = \sum n_i p_i$, we have

$$\varphi_{\mathscr{L}}(x) = \sum n_i(p_i - x) - \sum n_i p_i \in \mathrm{Pic}(X).$$

Because of niceties of elliptic curves, we know the above is linearly equivalent to

$$-(\sum n_i)x = -(\deg \mathscr{L})x,$$

so $\varphi_{\mathscr{L}}(x) = -(\deg \mathscr{L})x$. Hence, $\varphi_{\mathscr{L}} = 0 \iff \deg \mathscr{L} = 0$ so $\mathrm{Pic}^0(X) = \{\mathscr{L} \in \mathrm{Pic}(X) : \deg \mathscr{L} = 0\}$ is exactly what we would hope. $\triangle$

Proposition 5.11.5. *Let X be an abelian variety with line bundle $\mathscr{L}$.*

- ***(1)*** *For all $x \in X$, $\varphi_{\mathscr{L}}(x) \in \mathrm{Pic}^0(X)$.*
- ***(2)*** *If $\mathscr{L}^n \in \mathrm{Pic}^o(X)$ $(n \neq 0)$, then $\mathscr{L} \in \mathrm{Pic}^0(X)$.*

Proof. We have shown **(1)** already. For **(2)**, we have

$$0 = \varphi_{\mathscr{L}^n}(x) = n\varphi_{\mathscr{L}}(x) = \varphi_{\mathscr{L}}(nx)$$

and $n : X \to X$ is surjective, so we win. ■

Corollary 5.11.6. $\mathrm{NS}(X)$ *is torsion free. (We'll later show it is finitely generated)*

Theorem 5.11.7. *Let $\mathscr{L} \in \mathrm{Pic}(X)$. Then, TFAE*

- ***(1)*** $\mathscr{L} \in \mathrm{Pic}^0(X)$
- ***(2)*** $\mathscr{L}_{X^2} = \mathscr{O}_{X^2}$ *where, as always,*

$$\mathscr{L}_{X^2} = m_{12}^*\mathscr{L} \otimes m_1^*\mathscr{L}^{-1} \otimes m_2^*\mathscr{L}^{-1}$$

- ***(3)*** $[-1]^*\mathscr{L} \simeq \mathscr{L}^{-1}$ *(i.e. $\mathscr{L}$ is odd) ($\iff$ $[n]^*\mathscr{L} = \mathscr{L}^{\otimes n}$ for all $n \in \mathbb{Z}$)*

Proof. (**(1)** $\implies$ **(2)**) Use see-saw. Consider the projections $p_1, p_2 : X^2 \rightrightarrows X$. Note that

$$\mathscr{L}_{X^2}|_{X \times \{x\}} \simeq T_x^*\mathscr{L} \otimes \mathscr{L}^{-1} = \varphi_{\mathscr{L}}(x) = \mathscr{O}_X$$

with last equality since we assumed **(1)**. Hence $\mathscr{L}_{X^2}$ is trivial on horizontal lines and vertical lines. By see-saw, we get that $\mathscr{L}_{X^2}$ is trivial globally.

(**(2)** $\implies$ **(3)**) Consider the morphism $\delta : x \mapsto (x, -x)$. Then,

$$\delta^* \mathscr{L}_{X^2} \simeq \mathscr{L} \otimes [-1]^* \mathscr{L},$$

but $\delta^* \mathscr{L}_{X^2} \simeq \mathscr{O}_X$, so we win.

(**(3)** $\implies$ **(1)**) Take any $\mathscr{M} \in \operatorname{Pic}(X)$. We want to compute $\varphi_{[-1]^*\mathscr{M}}(x)$. This is

$$\varphi_{[-1]^*\mathscr{M}}(x) = T_x^*[-1]^*\mathscr{M} \otimes [-1]^*\mathscr{M}^{-1} = [-1]^* T_{-x}^* \mathscr{M} \otimes [-1]^*\mathscr{M}^{-1} = [-1]^*\varphi_{\mathscr{M}}(-x) \in \operatorname{Pic}^0(X).$$

Applying **(1)** $\implies$ **(2)** $\implies$ **(3)** to $\mathscr{M}$, we see that

$$[-1]^*\varphi_{\mathscr{M}}(-x) = \varphi_{\mathscr{M}}(x)^{-1} = \varphi_{\mathscr{M}}(x).$$

Take $\mathscr{M} = \mathscr{L}$ so $[-1]^*\mathscr{L} = \mathscr{L}^{-1}$. This tells us that $\varphi_{\mathscr{L}^{-1}} = \varphi_{\mathscr{L}}$, so $\varphi_{\mathscr{L}^2} = 0$. Hence, $\mathscr{L}^2 \in \operatorname{Pic}^0(X)$ which implies $\mathscr{L} \in \operatorname{Pic}^0(X)$. ■

Corollary 5.11.8. $\operatorname{Pic}^0(X) = \{\mathscr{L} \in \operatorname{Pic}(X) : \mathscr{L} = \textit{odd}\}$*, so* $\operatorname{NS}(X) =$*"even part of* $\operatorname{Pic}(X)$*".*

Now let's do something harder and use that X has an ample line bundle.

Theorem 5.11.9. *Let $\mathscr{L}$ be an ample line bundle, and consider $\varphi_{\mathscr{L}} : X \to \operatorname{Pic}^0(X)$ (whose kernel is finite). In fact, $\varphi_{\mathscr{L}}$ is surjective.*

Example. If X is an elliptic curve, then $\mathscr{L}$ ample means $\deg \mathscr{L} > 0$. We calculated $\varphi_{\mathscr{L}}(x) = -(\deg \mathscr{L})x$, but $\operatorname{Pic}^0(X) = X$ so this is indeed surjective. △

Proof Sketch of Theorem. Choose some $\mathscr{M} \in \operatorname{Pic}^0(X)$. We have the projection maps $X \xleftarrow{p_1} X^2 \xrightarrow{p_2} X$. Consider the bundle $\mathscr{N} := \mathscr{L}_{X^2} \otimes p_2^*\mathscr{M}^{-1}$. Note that

$$\mathscr{N}|_{x \times X} \simeq \varphi_{\mathscr{L}}(x) \otimes \mathscr{M}^{-1} \text{ and } \mathscr{N}|_{X \times x} \simeq \varphi_{\mathscr{L}}(x).$$

Hence, we want to show that for some $x \in X$, $\mathscr{N}|_{x \times X}$ is trivial. Suppose this is not the case.

We want to calculate the cohomology $R\Gamma(X^2, \mathscr{N})$. Consider the square

$$\begin{array}{ccc} X^2 & \xrightarrow{p_1} & X \\ {\scriptstyle p_2}\downarrow & & \downarrow \\ X & \longrightarrow & k \end{array}$$

We have

$$R\Gamma(X, Rp_{2,*}\mathscr{N}) = R\Gamma(X^2, \mathscr{N}) = R\Gamma(X, Rp_{1,*}\mathscr{N}).$$

We want to show that the LHS is trivial (I) while the RHS is nontrivial (II).

(I) We want to show $Rp_{2,*}\mathscr{N} = 0$. At each $x \in X$, we have $\mathscr{N}_{x \times X} \neq \mathscr{O}_X$.

Lemma 5.11.10. *If $\mathscr{L} \in \operatorname{Pic}^0(X)$ is nontrivial, then* $\mathrm{H}^*(X, \mathscr{L}) = 0$.

Proof. (Kunneth formula and induction) First prove $\mathrm{H}^0(X, \mathscr{L}) = 0$. Now assume $\mathrm{H}^i(X, \mathscr{L}) = 0$ for all $i < k$. Consider $X \to X^2$ via $x \mapsto (x, 0)$. This composed with multiplication $m : X^2 \to X$ is the identity. Since $\mathscr{L} \in \mathrm{Pic}^0(X)$, we know $\mathscr{L}_{X^2} = 0$ so $m^*\mathscr{L} \simeq p_1^*\mathscr{L} \otimes p_2^*\mathscr{L}$. We have a sequence

$$\mathrm{H}^k(X\mathscr{L}) \to \mathrm{H}^k(X \times X, m^*\mathscr{L}) \to \mathrm{H}^k(X, \mathscr{L})$$

whose composition is the identity. Künneth formula let's us calculate the middle term

$$\mathrm{H}^k(X \times X, m^*\mathscr{L}) = \mathrm{H}^k(X \times X, p_1^*\mathscr{L} \otimes p_2^*\mathscr{L}) = \bigoplus_{i+j=k} \mathrm{H}^i(X, \mathscr{L}) \otimes \mathrm{H}^j(X, \mathscr{L}) = 0$$

(since one of i, j will be less than k), so we win. ■

By lemma, $Rp_2\mathscr{N} = 0 \implies R\Gamma(X, \mathscr{N}) = 0$.

(II) For p_2, $\mathscr{N}|_{X\times x} = \varphi_{\mathscr{L}}(x)$ so $\{x \in X : \varphi_{\mathscr{L}}(x) = 0\} = k(\mathscr{L})$ is finite. For $x \notin K(\mathscr{L})$, $\varphi_{\mathscr{L}}(x) \neq 0$ and $(Rp_2\mathscr{N})_x = 0$ (?). We get

TODO: Come understand this

$$Rp_2\mathscr{N} = \bigoplus_{x \in K(\mathscr{L})} \mathrm{H}^*(\mathscr{O}_X) \otimes \underline{\kappa(x)}_x,$$

so

$$R\Gamma(X^2, \mathscr{N}) = \bigoplus_{x \in K(\mathscr{L})} \mathrm{H}^*(\mathscr{O}_X) \neq 0$$

since $\mathrm{H}^0(\mathscr{O}_X) \neq 0$.

This gives our contradiction. ■

Remark 5.11.11. We have

$$0 \longrightarrow K(\mathscr{L}) \longrightarrow X \twoheadrightarrow \mathrm{Pic}^0(X) \longrightarrow 0$$

with finite kernel $K(\mathscr{L})$, so $\mathrm{Pic}^0(X) = X/K(\mathscr{L})$, as groups. Next time we will give a variety structure to $\mathrm{Pic}^0(X)$. ○

We would like a definition of Pic^0 which works for any variety. Our current ones depend on the group structure on X.

Definition 5.11.12. Let Y be a variety, and choose two line bundles $\mathscr{M}_1, \mathscr{M}_2$. We say that $\mathscr{M}_1$ is **algebraically equivalent** to $\mathscr{M}_2$ if there is a variety S, a line bundle $\mathscr{N}$ on $X \times S$, and two points $a, b \in S$ such that

$$\mathscr{N}|_{X\times\{a\}} \simeq \mathscr{M}_1 \text{ and } \mathscr{M}_2 \simeq \mathscr{N}|_{X\times\{b\}}.$$

◇

Remark 5.11.13. It suffices to take S =curve. You are only connected two points. ○

Remark 5.11.14. If S is rational (e.g. $S \hookrightarrow \mathbb{P}^1$), then $\mathscr{M}_1 \simeq \mathscr{M}_2$. ○

Theorem 5.11.15. *Let $\mathscr{M} \in \mathrm{Pic}(X)$ be a line bundle on an abelian variety X. Then, $\mathscr{M} \in \mathrm{Pic}^0(X) \iff \mathscr{M}$ is algebraically equivalent to 0.*

Proof. ($\rightarrow$) Assume $\mathscr{M} \in \mathrm{Pic}^0(X)$. Previous theorem shows that $\mathscr{M} = \varphi_{\mathscr{L}}(x)$ for some ample $\mathscr{L}$ and $x \in X$. Now consider the line bundle $\mathscr{L}_{X^2}$ on X^2. Well, $\mathscr{L}|_{X\times 0} = \mathscr{O}_X$ and $\mathscr{L}|_{X\times x} = \mathscr{M}$, so $\mathscr{M}$ is algebraically equivalent to 0.

($\leftarrow$) On the other hand, suppose $\mathscr{M}$ is algebrically equivalent to 0, so there is some line bundle $\mathscr{N}$ on $X \times S$ with points $a, b \in S$ such that $\mathscr{O}_X = \mathscr{N}|_{X\times a}$ and $\mathscr{N}|_{X\times b} = \mathscr{M}$. Think of $X_S = X \times S$ as an S-scheme. Using the three morphisms $m_S, p_{1,S}, p_{2,S} : X \times X \times S \to X \times S$ given by addition and projection (onto either X factor):

$$m_s(x, y, s) = (x + y, s) \text{ and } p_{1,S}(x, y, s) = (x, s) \text{ and } p_{2,S}(x, y, s) = (y, s).$$

Consider the bundle $\mathscr{N}_{X_S^2}$ defined as you expect. This bundle is trivial on $0 \times X \times S$, on $X \times 0 \times S$ and on $X \times X \times a$. By the theorem of the cube, $\mathscr{N}_{X_S^2} = \mathscr{O}_{X\times X\times S}$ is trivial. Finally, note that

$$\mathscr{O}_{X^2} = \mathscr{N}|_{X^2\times b} \simeq \mathscr{M}_{X^2}$$

which shows that $\mathscr{M} \in \mathrm{Pic}^0(X)$. ■

5.11.2 Quotients of (Abelian) Varieties

We know $\mathrm{Pic}^0(X)$ is the quotient of an abelian variety by a finite group. We would like to give it a variety structure, so we now study quotients.

Theorem 5.11.16. *Let X be a variety with a free action by a finite group G. Furthermore, assume that for all $x \in X$, there is an affine $U \subset X$ such that $Gx \subset U$. Then there is a morphism $\pi : X \to Y$, unique up to isomorphism, such that*

(1) *As a topological space, $Y = X/G$.*

(2) *On sheaves, $\mathscr{O}_Y \xrightarrow{\sim} (\pi_*\mathscr{O}_X)^G$*

Proof. We first claim that X has a cover by U_i, each invariant under G. For any $x \in X$, there's some $U \supset Gx$ so let $U_x := \bigcap_{g\in G} g(U)$ which is G-invariant. By gluing process, we are reduced to the affine case.

In the affine case $X = \operatorname{Spec} A$ with a G-action. Well, take $Y = \operatorname{Spec} A^G$ and we have a natural map $X \to Y$. There are a few questions.

(1) Is Y a variety? Consider $k \to A^G \hookrightarrow A$. We show that $A^G \to A$ is finite which then implies that A^G is finite type over k. Any $a \in A$ is a root of the polynomial

$$\prod_{\sigma\in G} (x - \sigma(a)) \in A^G[x]$$

which lands in $A^G[x]$ since it is invariant under the G-action. This shows that A is finite over A^G, so Y is indeed a variety.

(2) Does $X \to Y$ satisfy the desired properties? The fact that $Y = X/G$ as topological spaces essentially comes from the fact that a prime of A^G is a G-orbit of primes of A, so $Y \to X$ is a continuous bijection and one easily checks that it's also closed. The second property is essentially by definition.

These spaces are affine, so we can check sheaf things on global sections where **(2)** says that the inclusion $A^G \hookrightarrow A$ induces an iso $A^G \xrightarrow{\sim} A^G$, which I'm at least 80% sure is true. ■

5.12 Lecture 12 (10/8)

Last time we studied $\mathrm{Pic}^0(X)$ when X is an abelian variety, and we ended up with something like 4 different, equivalent definitions.

The goal of the next two lectures is to define a variety structure on $\mathrm{Pic}^0(X)$. This is trivial for elliptic curves ($\mathrm{Pic}^0(X) \cong X(k)$), but much harder in general. In general, $\mathrm{Pic}^0(X) \neq X(k)$, but we do have a map $\varphi = \varphi_{\mathscr{L}}$

$$\begin{array}{rccc} \varphi: & X(k) & \longrightarrow & \mathrm{Pic}^0(X) \\ & x & \longmapsto & T_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \end{array}.$$

We have also shown that φ is surjective with finite kernel when $\mathscr{L}$ is ample. This suggests that $\mathrm{Pic}^0(X)$ is a quotient variety X/K where $K = \ker\varphi$.

In the end of the last lecture, we defined X/K as a variety, so we want to take $\mathrm{Pic}^0(X) = X/K$. However, this K depends on a choice of ample line bundle on X, so how do we know know this description is canonical/natural? More specifically, does "X/K" depend, up to iso, on the choice of $\mathscr{L}$? We would like a more instrisinc description of $\mathrm{Pic}^0(X)$ as a variety.

Definition 5.12.1. Let X be an abelian variety. A **dual abelian variety** is a pair $(\widehat{X}, \wp)$ where $\widehat{X}$ is an abelian variety and $\wp$ is a line bundle on $X \times \widehat{X}$ such that the following 2 conditions hold:

(1) $\wp|_{0\times\widehat{X}} \cong \mathscr{O}_{\widehat{X}}$ and $\wp|_{X\times 0} \cong \mathscr{O}_X$

(2) For any normal variety S and any line bundle Q on $X \times S$ such that

Q is a family of line bundles in $\mathrm{Pic}^0(X)$

- $Q|_{0\times S} \cong \mathscr{O}_S$
- For any $s \in S$, $Q_s := Q|_{X\times s} \in \mathrm{Pic}^0(X)$

Then there is a unique morphism $f : S \to \widehat{X}$ such that $(1\times f)^*\wp = Q$ where $1\times f : X\times S \to X\times\widehat{X}$.

◇

Remark 5.12.2. Informally, this simply says that $\widehat{X}$ parameterizes all of $\mathrm{Pic}^0(X)$. ○

Example. Take $S = \operatorname{Spec} k$. In this case, the definition says for any $\mathscr{M} \in \mathrm{Pic}^0(X)$, there is some $\alpha \in \widehat{X}$ such that $\mathscr{M} \simeq \wp_\alpha (:= \wp|_{X\times\alpha})$. Hence, $\widehat{X}(k) = \mathrm{Pic}^0(X)$. △

Our big theorem for today will be the following.

Theorem 5.12.3. *For any abelian variety X, there is a unique dual abelian variety $(\widehat{X}, \wp)$ (up to unique isomorphism).*

Remark 5.12.4. If you do not require $\widehat{X}$ to come equipped with $\wp$, then you will not get uniqueness. ○

Proof of uniqueness in theorem 5.12.3. Suppose $(\widehat{X}', \wp')$ is another dual abelian variety. Then, we can apply the definition with $S = \widehat{X}'$ and $Q = \wp'$. This satisfies $Q_s \in \mathrm{Pic}^0(X)$ since $\wp'_0$ is trivial and $\widehat{X}'$ is connected (so all other fibers algebrically equiv to 0). Hence, we get some $f : \widehat{X}' \to \widehat{X}$ such that $(1\times f)^*\wp = \wp'$. By symmetry, we also get some $f' : \widehat{X} \to \widehat{X}'$ such that $(1\times f')^*\wp' = \wp$. Finally, uniqueness of these morphisms forces $f \circ f' = \mathrm{id}_{\widehat{X}}$ and $f' \circ f = \mathrm{id}_{\widehat{X}'}$, so we get uniqueness. ■

Example. Let $\mathscr{L}$ be an ample line bundle on X. Then we have constructed

$$\mathscr{L}_{X^2} = m^*\mathscr{L} \otimes p_1^*\mathscr{L}^{-1} \otimes p_2^*\mathscr{L}^{-1} \otimes \mathscr{O}_{X^2}.$$

This satisfies

$$\mathscr{L}_{X^2}|_{X\times 0} \simeq \mathscr{O}_X \text{ and } \mathscr{L}_{X^2}|_{0\times X} \simeq \mathscr{O}_X.$$

Apply definition for $S = X$ and $Q = \mathscr{L}_{X^2}$. This gives a morphism $\varphi : X \to \widehat{X}$ such that $\mathscr{L}_{X^2} \simeq (1\times f)^*\wp$. If you check at the k-points

$$X(k) \ni x \mapsto \varphi(x) = \varphi_{\mathscr{L}}(x) \in \operatorname{Pic}^0(X).$$

This suggests that $\wp$ is in fact a "quotient" of the bundle $\mathscr{L}_{X^2}$ by $\ker\left(1 \times f : X \times X \to X \times \widehat{X}\right)$. △

How do you define a quotient of a bundle by a finite group?

5.12.1 Quotient line bundle by finite group

Let X be an arbitrary variety, and let G be a finite group acting *freely* on X, so the "graph" $G \times X \hookrightarrow X \times X, (g, x) \mapsto (gx, x)$ is an embedding. Last time, we constructed a variety quotient $\pi : X \to X/G$. Hence, we get a pullback $\pi^* : \operatorname{Coh}(X/G) \to \operatorname{Coh}(X)$, and we are interested in its image.

Definition 5.12.5. Let $\mathscr{F}$ be a sheaf on X. An **action of G on the sheaf $\mathscr{F}$** is a collection of isomorphisms – for any $g \in G$, get $\alpha_g : g^*\mathscr{F} \xrightarrow{\sim} \mathscr{F}$ – satisfying $\alpha_e = \operatorname{Id}_{\mathscr{F}}$ and $\alpha_{g_1g_2} = \alpha_{g_2} \circ g_2^*\alpha_{g_1}$, i.e. $\alpha_{g_1g_2}$ is the composition

$$(g_1g_2)^*\mathscr{F} = g_2^*g_1^*\mathscr{F} \xrightarrow{\sim} g_2^*\mathscr{F} \xrightarrow{\sim} \mathscr{F}.$$

⋄

Remark 5.12.6. For any $\mathscr{G} \in \operatorname{Coh}(X/G)$, $\pi^*\mathscr{G}$ has a canonical action by G. Note that $\pi \circ g = \pi : X \to X/G$. ○

Theorem 5.12.7. *The correspondence $\mathscr{G} \mapsto \mathscr{G}^*$ defines an equivalence functor*

$$\operatorname{Coh}(X/G) \xrightarrow{\sim} \operatorname{Coh}_G(X)$$

where $\operatorname{Coh}_G(X)$ is coherent sheaves with G-action. The inverse is denoted $\mathscr{F}/G$.

How to construct $\mathscr{F}/G$? Let $Y = X/G$ and consider $\pi : X \to Y$. Say we have some open $U \subset Y$. We set

$$(\mathscr{F}/G)(U) = \left\{\alpha \in \mathscr{F}(\pi^{-1}(U)) : g\alpha = \alpha\, \forall g \in G\right\} = \mathscr{F}(\pi^{-1}(U))^G.$$

That is, $\mathscr{F}/G := (\pi_*\mathscr{F})^G$ (so maybe a better name is $\mathscr{F}^G$).

Proof of theorem 5.12.7. By gluing process, reduce to the case where $X = \operatorname{Spec} A$ and so $Y = \operatorname{Spec} A^G = X/G$. Now, a G-sheaf on X is simply an $A[G]$-module M and a sheaf on Y is an A^G-module N. Our functors are now $M \mapsto M^G$ and $N \otimes_{A^G} A \leftarrow N$. This is an equivalence since A is a locally free A^G-module. ■

5.12.2 Existence of dual abelian varieties

Let X be an abelian variety, and let $\mathscr{L}$ be an ample line bundle on X. We have $\varphi_{\mathscr{L}} : X \twoheadrightarrow \mathrm{Pic}^0(X)$ with finite kernel $K := \ker \varphi_{\mathscr{L}}$. We only have a line bundle $\mathscr{L}_{X^2}$ on $X \times X$. Let's set $\widehat{X} := X/K$, so we have a natural morphism $1 \times \pi : X \times X \to X \times \widehat{X}$. Note that K acts on $X \times X$ by acting only on the right factor, and $1 \times \pi$ is the corresponding quotient map.

Hence, we want to take $\wp := \mathscr{L}_{X^2}/K$ (maybe clearly to write $\mathscr{L}_{X^2}/0 \times K$), but to do so, we need to know that K acts on $\mathscr{L}_{X^2}$.

Proposition 5.12.8. *There is an unique action of K on $\mathscr{L}_{X^2}$: $(\alpha \in K)$*

$$\psi(\alpha) : T_{0,\alpha}^* \mathscr{L}_{X^2} \xrightarrow{\sim} \mathscr{L}_{X^2}$$

such that when restricted to $0 \times X$, this gives the identity map $\mathscr{L}(0)^{-1} \otimes \mathscr{O}_X = \mathscr{L}(0)^{-1} \otimes \mathscr{O}_X$.

Question: What is $\mathscr{L}(0)$?

Proof. First we calculate $T_{0,\alpha}^* \mathscr{L}_{X^2}$. Recall

$$\mathscr{L}_{X^2} \simeq m^* \mathscr{L} \otimes p_1^* \mathscr{L}^{-1} \otimes p_2^* \mathscr{L}^{-1},$$

so

$$\begin{aligned} T_{0,\alpha}^* \mathscr{L}_{X^2} &\simeq T_{0,\alpha}^* m^* \mathscr{L} \otimes T_{0,\alpha}^* p_1^* \mathscr{L}^{-1} \otimes T_{0,\alpha}^* p_2^* \mathscr{L}^{-1} \\ &\simeq (m \circ T_{0,\alpha})^* \mathscr{L} \otimes (p_1 \circ T_{0,\alpha})^* \mathscr{L}^{-1} \otimes (p_2 \circ T_{0,\alpha})^* \mathscr{L}^{-1} \end{aligned}$$

The first piece is pulling back along $(x, y) \mapsto (x, y + \alpha) \mapsto (x + y + \alpha) = T_\alpha \circ m(x, y)$. The second one is pulling back along $(x, y) \mapsto (x, y + \alpha) \mapsto x = p_1(x)$. The last is pulling back along $(x, y) \mapsto (x, y + \alpha) \mapsto y + \alpha = T_\alpha \circ p_2$. Hence,

$$T_{0,\alpha}^* \mathscr{L}_{X^2} \simeq m^* T_\alpha^* \mathscr{L} \otimes p_1^* \mathscr{L}^{-1} \otimes p_2^* T_\alpha^* \mathscr{L}^{-1}.$$

But, $\alpha \in K = \ker \varphi_{\mathscr{L}}$, so $T_\alpha^* \mathscr{L} \simeq \mathscr{L}$. Hence,

$$T_{0,\alpha}^* \mathscr{L}_{X^2} \simeq m^* \mathscr{L} \otimes p_1^* \mathscr{L}^{-1} \otimes p_2^* \mathscr{L}^{-1} \simeq \mathscr{L}_{X^2}.$$

When restricted on $(0, X)$ both sides naturally isomorphic to $\mathscr{L}(0) \otimes \mathscr{O}_X$. This implies there is a unique isomorphism $T_{0,\alpha}^* \mathscr{L}_{X^2} \xrightarrow{\sim} \mathscr{L}_{X^2}$ compatible with above rigidification. This gives action of $0 \times K$ on $\mathscr{L}_{X^2}$. ∎

In summary, we have constructed a pair $(\widehat{X}, \wp)$ such that the diagram

$$\begin{tikzcd} \mathscr{L}_{X^2} \arrow[r] \arrow[d] & \wp \arrow[d] \\ X \times X \arrow[r] & X \times \widehat{X} \end{tikzcd}$$

is compatible, i.e. $\widehat{X} = X/K$ is a quotient variety and $\wp$ pulls back along the natural map to $\mathscr{L}_{X^2}$.

Theorem 5.12.9. *Assume $\mathrm{char}(k) = 0$. Then, $(\widehat{X}, \wp)$ constructed above is the dual abelian variety of X.*

We'll get rid of this assumption later

Proof. We need to check 2 properties. First, we need

$$\wp|_{0\times\widehat{X}} \simeq \mathscr{O}_{\widehat{X}} \text{ and } \wp|_{X\times 0} \simeq \mathscr{O}_X.$$

Since we have a quotient map $X\times X \xrightarrow{1\times\pi} X\times\widehat{X}$, it is enough to check these identities after pullback (use equiv. of cats). But this is done, since we know $\mathscr{L}_{X^2}|_{0\times X} \simeq \mathscr{O}_X$ and $\mathscr{L}_{X^2}|_{X\times 0} \simeq \mathscr{O}_X$.

For the second property, let S be a normal variety, and let Q be a line bundle on $X\times S$ such that $Q|_{0\times S} = \mathscr{O}_S$ and $Q|_{X\times s} \in \operatorname{Pic}^0(X)$ for all $s\in S$ ($s\in S(k)$?). We want to construct a morphism $f : S \to \widehat{X}$ such that $Q = (1\times f)^*\wp$. Consider the "correspondence" or whatever

$$\begin{tikzcd}
 & & X\times S\times\widehat{X} \arrow[dl, "p_{12}"'] \arrow[dr, "p_{13}"] & & \\
Q & X\times S & & X\times\widehat{X} & \wp
\end{tikzcd}$$

Define $R := p_{12}^*Q\otimes p_{13}^*\wp^{-1}$, and consider

This condition is same as $R_{s,\alpha}\simeq\mathscr{O}_X$? Maybe?

$$\Gamma(k) := \left\{(s,\alpha)\in S\times\widehat{X} : \wp_\alpha \simeq Q_s\right\},$$

the "graph of $S(k)\to\operatorname{Pic}^0(X)$". We want to say that $\Gamma(k)$ has a variety structure; use see-saw. We have

$\Gamma = \overline{\Gamma(k)} \subset S\times\widehat{X}$ is the closure of its k-points

$$\begin{tikzcd}
\Gamma \arrow[r, hook] & S\times\widehat{X} \arrow[r] \arrow[d, "p_1"] & \widehat{X} \\
 & S &
\end{tikzcd}$$

with p_1 inducing an isomorphism $\Gamma(k) \xrightarrow{\sim} S(k)$. In characteristic 0, since S is normal, this implies that $p_1|_\Gamma$ is an isomorphism. This implies that Γ is the graph of some morphism $f : S\to\widehat{X}$, and one easily checks that $(1\times f)^*\wp \simeq Q$. ∎

We used this lemma above.

Lemma 5.12.10. *Assume* $\operatorname{char} k = 0$ *(recall* $k=\overline{k}$*). If* $f : X\to Y$ *is a morphism of normal varieties such that the induced morphism* $X(k)\to Y(k)$ *is bijective, then* f *is an isomorphism.*

Non-example. This is not true in characteristic p. For example consider frobienus $f : \mathbb{P}^n\to\mathbb{P}^n$ given by $(x_0, x_n)\mapsto(x_0^p, x_n^p)$. This is an iso on k-points, but there is no inverse map. ▽

To make the argument work in characteristic p, we will study action by group schemes instead of just by finite groups.

5.13 Lecture 13 (10/13)

Last week we constructed the dual abelian variety. Let X be an abelian variety, then $\widehat{X}$, the dual abelian variety, parameterizes line bundles algebrically equivalent to 0: $\operatorname{Pic}^0(X) = \widehat{X}(k)$ (at least when $\operatorname{char} k = 0$). On $X\times\widehat{X}$, we have the Poincaré bundle $\wp$. For $x\in\widehat{X}$, $\wp_x = \wp|_{X\times\{x\}} \in \operatorname{Pic}^0(X)$. Furthermore, $\wp_0 = \mathscr{O}_X$ and $\wp|_{0\times\widehat{X}} = \mathscr{O}_{\widehat{X}}$. We showed the pair $(\widehat{X},\wp)$ is unique.

Our main tool for constructing $\widehat{X}$ was taking quotients. Given an action $X \times G \hookrightarrow X \times X, (x, g) \mapsto (x, xg)$, we formed "$X/G$" under the assumption that for $x \in X$, "Gx" $\hookrightarrow$ affine $\hookrightarrow X$. We then have $\pi : X \to Y = X/G$ the projection, and any bundle $\mathscr{M} \in \operatorname{Pic}(Y)$ on Y pulls back to a bundle $\pi^*\mathscr{M} \in \operatorname{Pic}_G(X)$ on X with a G-action.

Today we will study isogenies and dual isogenies. Then, we will study complex abelian varieties.

5.13.1 Isogenies

Assumption. We are still assuming $\operatorname{char} k = 0$ (and also $k = \overline{k}$). We will remove this assumption later on, but for now we keep it simple. Also, while I'm at it, remember all varieties are integral, separable, and finite type over k.

Let X be an abelian variety, and $G \hookrightarrow X$ a finite subgroup. Then, we get a surjective, finite homomorphism

$$\pi : X \to X/G = Y$$

with Y an abelian variety.

Theorem 5.13.1. *The above gives an equivalence of categories between*

$$\left\{ \begin{matrix} G \hookrightarrow X \\ \textit{finite} \end{matrix} \right\} \xrightarrow{\sim} \left\{ \begin{matrix} \pi : X \to Y \\ \textit{isogeny} \end{matrix} \right\}$$

The inverse map is $(\ker \pi \hookrightarrow X) \leftarrow\!\shortmid (X \xrightarrow{\pi} Y)$.

Definition 5.13.2. An **isogeny** $\pi : X \to Y$ between abelian varieties is a surjective homomorphism with finite kernel. ◇

Theorem 5.13.3. *For any isogeny $\pi : X \to Y$, there is a* ***dual isogeny***

Don't actually need this to be an isogeny to get a dual morphism

$$\widehat{X} \xleftarrow{\widehat{\pi}} \widehat{Y}$$

such that on k-points

$$\operatorname{Pic}^0(X) \xleftarrow{\pi^*} \operatorname{Pic}^0(Y)$$

we recover the pullback morphism.

Proof. We first show π^* is well defined, i.e. that $\pi^*(\operatorname{Pic}^0(Y)) \subset \operatorname{Pic}^0(X)$. Use that Pic^0 consists of the odd line bundles:

$$\pi^*\mathscr{L}^{-1} = \pi^*[-1]^*\mathscr{L} = [-1]^*\pi^*\mathscr{L} \implies \pi^*\mathscr{L} \in \operatorname{Pic}^0(X).$$

Let $\wp_X$ be the Poincaré bundle on $X \times \widehat{X}$ and $\wp_Y$ the one of $Y \times \widehat{Y}$. Suppose that $\pi : X \to Y$ is any homomorphism of abelian varieties. We then get a morphism

$$X \times \widehat{Y} \xrightarrow{\pi \times \mathrm{Id}} Y \times \widehat{T}$$

and so can consider $(\pi \times 1)^*\wp_Y \in \operatorname{Pic}(X \times \widehat{Y})$. $\widehat{Y}$ parameterizes some line bundles in $\operatorname{Pic}^0(X)$, so the universal property of $\widehat{X}$ gives a unique morphism $\widehat{\pi} : \widehat{Y} \to \widehat{X}$ such that

$$(1 \times \widehat{\pi})^*\wp_X \cong (\pi \times 1)^*\wp_Y.$$

This $\widehat{\pi}$ is our dual morphism. ■

Theorem 5.13.4. *If $X \to Y$ is an isogeny, then there is a perfect pairing between $\ker \pi$ and $\ker \widehat{\pi}$.*

Proof. We have $\pi^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$, and we already know that

Recall Corollary 5.2.6

$$\ker \pi^* \simeq \mathrm{Hom}(\ker \pi, k^\times).$$

Here's a quick sketch of why. Say $\mathscr{L} \in \mathrm{Pic}^0(Y) = \mathrm{Pic}^0(Y/G)$ such that $\pi^*\mathscr{L} \simeq \mathscr{O}_X$. For any section $f \in (\pi^*\mathscr{L})(U)$, we have a G-action $(gf)(x) = f(x+g)$. Since X is compact, can take "$f = \mathrm{Id}$" so $f(x+g)$ is constant. Hence, $gf = \psi(g)f$ for some $\psi : G \to k^\times$.

We now claim that $\ker \pi^*|_{\mathrm{Pic}(X)} = \ker \pi^*|_{\mathrm{Pic}^0(X)}$. This is because $\ker \pi^* \simeq \mathrm{Hom}(\ker \pi, k^\times)$, a finite group, so $\mathscr{L} \in \ker \pi^*$ has finite order, i.e. $\mathscr{L}^{\otimes n} = \mathscr{O}_Y \in \mathrm{Pic}^0(Y) \implies \mathscr{L} \in \mathrm{Pic}^0(Y)$. Thus, we have a perfect pairing

I can never tell when we're making statements about schemes and when we're making statements about k-points of schemes

$$\ker \widehat{\pi} \times \ker \pi \to k^\times.$$

■

Corollary 5.13.5. $\deg \pi = \deg \widehat{\pi}$ *(we're in characteristic 0 so degree is the size of the kernel).*

Theorem 5.13.6. *If X is an abelian variety, then $\widehat{\widehat{X}} = X$. Furthermore, given $\pi : X \to Y$, the double dual $\widehat{\widehat{\pi}} : \widehat{\widehat{X}} \to \widehat{\widehat{Y}}$ is identified with the original π.*

Proof. We already have the Poincaré bundle $\wp_X$ over $X \times \widehat{X}$. For any $x \in X$, $\wp_x := \wp|_{\{x\}\times\widehat{X}} \in \mathrm{Pic}^0(\widehat{X})$. For consistency, let's switch the order of the product, so have $\wp'_X \in \mathrm{Pic}(\widehat{X} \times X)$. By the universal property of $\widehat{\widehat{X}}$, we have a morphism $\eta : X \to \widehat{\widehat{X}}$ such that

$$\wp'_X = (1 \times \eta)^* \wp_{\widehat{X}}.$$

We need to show that η is an isomorphism. Suppose otherwise, that η is not an isomorphism. Since $\dim X = \dim \widehat{X} = \dim \widehat{\widehat{X}}$, this means that $\ker \eta \neq 0$. Note that the connected component $(\ker \eta)^0$ is an abelian variety, so $\ker \eta \supset K$, some finite abelian group. Now factor

$$\eta : X \longrightarrow X/K \xrightarrow{f} \widehat{\widehat{X}}.$$

The picture looks like this

$$\begin{array}{ccccc}
\wp'_X & \longrightarrow & (1\times f)^*\wp_{\widehat{X}} & \longrightarrow & \wp_{\widehat{X}} \\
\downarrow & & \downarrow & & \downarrow \\
\widehat{X} \times X & \longrightarrow & \widehat{X} \times X/K & \xrightarrow{1\times f} & \widehat{X} \times \widehat{\widehat{X}}
\end{array}$$

We can switch the order on the middle guy. $\widehat{X}$ parameterizes line bundles on X/K, so there is a morphism

$\psi : \widehat{X} \to \widehat{X/K}$ such that $(1 \times f)^* \wp_{\widehat{X}} \simeq (\psi \times 1)^* \wp'_{X/K}$. The diagram is now the following

$$\begin{tikzcd}
\wp'_X \arrow[r] \arrow[d] & Q \arrow[r] \arrow[d] & \wp'_{X/K} \arrow[d] \\
\widehat{X} \times X \arrow[r, "1\times\eta"] & \widehat{X} \times X/K \arrow[r, "\psi\times 1"] & \widehat{X/K} \times X/K
\end{tikzcd}$$

What's going on here? On rational points given $\mathscr{L} \in \widehat{X}(k) = \mathrm{Pic}^0(X)$, we have $\pi^*\psi(\mathscr{L}) \simeq \mathscr{L}$ so ψ is injective. However, $\dim X = \dim X/K$, so ψ is then an isomorphism. This implies that π^* is also an isomorphism, so $\# \ker \pi^* = \deg \pi = \# \ker \pi > 1$, a contradiction. ■

Question: Why and what is π?

Recall that elliptic curves are always self-dual which makes the situation there nicer. This is not the case for general abelian varieties, so we will later introduce the concept of a principle polarization to get around this.

5.13.2 Complex Abelian Varieties

We'll just collect results. There are more details in Mumford's book.

In this section, take $k = \mathbb{C}$. For an abelian variety X/k. For this section, we view $X = X(\mathbb{C})$ as a complex manifold.

Let $\widetilde{X}$ be the universal cover of $(X, 0)$. You can model this as the space of paths in X starting at 0, up to homotopy (or something like that). Here are some facts.

- $\widetilde{X}$ is a complex manifold, and the natural projection $\pi : \widetilde{X} \to X$ is smooth (i.e. analytic)
- $\widetilde{X}$ is an abelian group (a complex Lie group in fact, but not an abelian varity since it is not compact)
- $\pi_1(X, 0) = \pi^{-1}(0)$ and $X = \widetilde{X}/\pi_1(X, 0)$

Note that $\widetilde{X}$ is simply connected, so $\widetilde{X}$ is a $\mathbb{C}$-vector space, canonically isomorphic to $T_{X,0} \simeq \Gamma(X, \Omega_X)^\vee$.

Given $\omega_1, \ldots, \omega_g$ a base for $\Gamma(X, \Omega_X)$, we get a morphism $\widetilde{X} \xrightarrow{\sim} \mathbb{C}^g$ which, on a path $\gamma : [0,1] \to X$, outputs

$$\left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right).$$

This implies that $\pi_1(X, 0)$ is a lattice in $\widetilde{X}$.

Definition 5.13.7. By a "compact" **complex torus** we mean a complex manifold of the form V/Λ where V a $\mathbb{C}$-vector space and Λ a (full-rank) lattice. ◇

We have constructed a functor

$$\{\text{abelian varieties}/\mathbb{C}\} \to \{\text{complex tori}\}$$

which we might write $X \mapsto X^{\mathrm{an}}$. One can show that this is fully faithful (induces a bijection on Hom-sets) using Chow lemma.

Theorem 5.13.8 (Chow Lemma). *Let X be algebraic, proper, and let $Y \hookrightarrow X^{\mathrm{an}}$ be proper. Then Y is algebraic.*

Applying theorem to the graph can show that morphisms are also algebraic.

Question 5.13.9. *What is the essential image of the functor from complex abelian varieties to complex tori? i.e. when is a complex torus algebraic?*

Theorem 5.13.10 (**Riemann**)**.** *Let $X = V/\Lambda$ be a complex torus. Then, X is algebraic iff X has a* ***Riemann form****, a positive-definite hermitian form $H : V \times V \to \mathbb{C}$ such that $\operatorname{Im} H(\Lambda \times \Lambda) \subset \mathbb{Z}$ (i.e. the imaginary part of $H(v, w)$ is integral when $v, w \in \Lambda$).*

Remark 5.13.11. If $X = V/\Lambda$ is algebraic, then it is projective, so have an embedding $\iota : X \hookrightarrow \mathbb{P}^N$. Then, $\mathscr{L} = \iota^*\mathscr{O}(1)$ is an analytic bundle on X, and the embedding is given by sections $s_0, \dots, s_N$ of $\mathscr{L}$, i.e.

$$x \mapsto [s_0(x) : \cdots : s_N(x)] .$$

Such a bundle $\mathscr{L}$ is called *very ample*. An *ample* line bundle is one with a very ample tensor power. ○

Hence, the Riemann theorem says that X has am ample line bundle iff it has a Riemann form.

We want to study bundles on $X = V/\Lambda$. There is a natural map $\pi : V \to X$, inducing $\pi^* : \operatorname{Pic} X \to \operatorname{Pic}_G V$ where $G = \Lambda$. This induced map is an isomorphism. The inverse map is again $\mathscr{M} \mapsto (\pi_*\mathscr{M})^\Lambda$.

At the same time, note that $\operatorname{Pic} V = \{\mathscr{O}_V\}$ is trivial since V is contractible.

Thus, we see that $\operatorname{Pic}(X)$ consists of equivalence classes of actions of Λ on $\mathscr{O}_V$. More on this later...

No class on Thursday. Next week we'll finish these constructions, then talks about Siegal modular curves/forms, and then move back to abelian schemes.

He said one of these words

5.14 Lecture 14 (10/20)

5.14.1 More Complex abelian varieties

Say $X/\mathbb{C}$ an abelian variety. We saw last time that X is a complex torus, so $X = \widetilde{X}/\pi_1(X)$ (with $\widetilde{X}$ a $\mathbb{C}$-vector space, and $\pi_1(X) \hookrightarrow \widetilde{X}$ as a lattice).

Question 5.14.1. *Is every complex torus V/Λ an abelian variety?*

Answer. For elliptic curves (i.e. $\dim_{\mathbb{C}} V = 1$), yes. Can explicitly construct the associated curve using Weierstrass functions. In general though, the answer is no. ⋆

Recall 5.14.2 (Riemann's Theorem)**.** Let $X = V/\Lambda$ be a complex torus. Then, X is algebraic iff X has a **Riemann form**, a positive-definite hermitian form $H : V \times V \to \mathbb{C}$ such that $\operatorname{Im} H(\Lambda \times \Lambda) \subset \mathbb{Z}$ (i.e. the imaginary part of $H(v, w)$ is integral when $v, w \in \Lambda$). ⊙

Remark 5.14.3. TFAE

- X is algebraic
- $X \hookrightarrow \mathbb{CP}^N$
- There is a line bundle $\mathscr{L}$ on X whose sections separate points and tangent lines
- Existence of an ample line bundle

○

We let $\mathrm{Pic}(X)$ denote the group of iso classes of holomorphic line bundles on X.

Proof Sketch of Riemann. ($\leftarrow$) Let $\mathscr{L}$ be a line bundle on $X = V/\Lambda$ and consider the projection $\pi : V \to X$. Note that $\pi^*\mathscr{L}$ is trivial, so we may fix a trivialization $\chi : \pi^*\mathscr{L} \xrightarrow{\sim} \mathscr{O}_V$, so $\mathscr{L} \subset \pi_*\mathscr{O}_V$. Since this is a covering space, if $U \subset X$ is sufficiently small, we get

$$\alpha : \mathscr{L}(U) \hookrightarrow \mathscr{O}_V(\pi^{-1}U) = \left\{f : \pi^{-1}U \to \mathbb{C}\right\}.$$

Define $\psi(\lambda, z)$ (for $\lambda \in \Lambda$ and $z \in \pi^{-1}(u)$) given by

$$\psi(x, z) = \frac{f(z+\lambda)}{f(z)} \text{ with } f \in \mathrm{im}(\alpha).$$

Note that ψ gives a map $\psi : \Lambda \to \mathscr{O}(V)^\times$, and this data determines $\mathscr{L}$. Not all such ψ determine a line bundles; need

$$\psi(\lambda + \mu, z) = \psi(\lambda, z)\psi(\mu, \lambda + z).$$

Write $C^1(\Lambda, \mathscr{O}(U)) = \mathrm{Map}(\Lambda, \mathscr{O}(V)^\times)$, $Z^1(\Lambda, \mathscr{O}(V)) = \left\{\psi \in C^1 : \psi(\lambda+\mu, z) = \psi(\lambda, z)\psi(\mu, \lambda + z)\right\}$, and $B^2(\Lambda, \mathscr{O}(U)) = \{\psi(\lambda, z) = \varphi(z+\lambda)/\varphi(z)\}$. One gets a short exact sequence

$$0 \longrightarrow B^1(X, \mathscr{O}(V)^\times) \longrightarrow Z^1(\Lambda, \mathscr{O}(U)^\times) \longrightarrow \mathrm{Pic}(X) \longrightarrow 1,$$

and so we see that $\mathrm{H}^1(\Lambda, \mathscr{O}(V)^\times) \simeq \mathrm{Pic}(X)$. Furthermore, we're in the land of complex-analytic geometry so we have the **exponential exact sequence**

Question: Have we just been doing a more hands-on version of (the discussion preceding) corollary 5.2.6

This is not quite the usual exponential exact sequence since we're thinking in terms of group cohomology instead of sheaf cohomology

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathscr{O}(V) \xrightarrow{\exp(2\pi i z)} \mathscr{O}(V)^\times \longrightarrow 1$$

which induces the exact sequence

$$\mathrm{H}^1(\Lambda, \mathbb{Z}) \to \mathrm{H}^1(\Lambda, \mathscr{O}(V)) \to \mathrm{H}^1(\Lambda, \mathscr{O}(V)^*) \xrightarrow{\gamma} \mathrm{H}^2(\Lambda, \mathbb{Z}) \to \mathrm{H}^2(\Lambda, \mathscr{O}(V))$$

This then gives

$$0 \longrightarrow \ker\gamma \longrightarrow \mathrm{H}^1(\Lambda, \mathscr{O}(V)^\times) \longrightarrow \mathrm{Im}\,\gamma \longrightarrow 1.$$

Theorem 5.14.4. *Let $U(1)$ denote the group of norm 1 elements in $\mathbb{C}$, and $\mathrm{H}^{1,1}(X)$ the group of Hermitian forms on V with integral values on Λ. Then, we know the following*

- $\ker\gamma = \mathrm{H}^1(\Lambda, \mathscr{O}(V))/\,\mathrm{H}^1(\Lambda, \mathbb{Z}) \xleftarrow{\sim} \mathrm{H}^1(\Lambda, \mathbb{R})/\,\mathrm{H}^1(\Lambda, \mathbb{Z}) = \mathrm{Hom}(\Lambda, \mathbb{R}/\mathbb{Z}) \simeq (S^1)^{2g}$
- *$H \to \mathrm{im}\, H$ defines a bijection $\mathrm{H}^{1,1}(X) \xrightarrow{\sim} \mathrm{Im}\,\gamma$, so we have*

$$0 \longrightarrow \mathrm{Hom}(\Lambda, \mathbb{R}/\mathbb{Z}) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{H}^{1,1}(X) \longrightarrow 0.$$

- *For all $h \in \mathrm{H}^{1,1}(X)$, $\gamma^{-1}(h) \subset \mathrm{Pic}(X)$ are represented by cocycles*

$$\psi(x, z) = \alpha(x)e^{\pi h(z,x) + (\pi/2)h(\lambda,\lambda)}$$

where $\alpha : \Lambda \to U(1)$ *such that*

$$\frac{\alpha(\lambda+u)}{\alpha(\lambda)\alpha(u)} = e^{\pi i h(\lambda,u)} \in \{\pm 1\}.$$

Example. For any hom $\psi : \Lambda \to U(1)$, get $\mathscr{L}_\psi : f(z+\lambda) = \psi(\lambda)f(z)$. Shou-Wu wrote down $\operatorname{Pic}^0(X) \simeq \widehat{\Lambda}$ $\triangle$

Example. Let $h \in 2H$ ($\operatorname{Im} h \subset 2\mathbb{Z}$). Consider $\mathscr{L}_{2h}$ defined by $f(z+\lambda) = e^{2\pi h(z,\lambda)+ih(\lambda,\lambda)}f(z)$ which lives in $2\,\mathrm{H}^{1,1}(\mathbb{Z})$. $\triangle$

Something something the point is that you can construct line bundles on complex tori using hermitian forms or using maps from your lattice something something.

Theorem 5.14.5. *A line bundle* $\mathscr{L}$ *with class* $\gamma(\mathscr{L}) \in \mathrm{H}^{1,1}(X)$ *is ample iff* $\gamma(\mathscr{L})$ $(= c_1(\mathscr{L}))$ *is positive definite. In this case,* $\mathscr{L}^{\otimes 2}$ *is basepoint free, and* $\mathscr{L}^{\otimes 3}$ *is very ample.*

He said a bunch more after this, but I followed almost none of it. ■

TODO: Figure out an understandable way to finish this proof

Example. If $\dim X = 1$, then $X = \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ and the Riemann form is

$$h(z,w) = \frac{z\overline{w}}{\operatorname{Im}\tau}.$$

$\triangle$

Remark 5.14.6. One can show that even in dimension 2, all complex tori and algebraic. ○

Dual complex torus Let $X = V/\Lambda$ be a complex torus. We will define a dual complex torus $\widehat{X} = \widehat{V}/\widehat{\Lambda}$ where $\widehat{V}$ is anti-holomorphic linear $f : V \to \mathbb{C}$ (so $f(az) = \overline{a}f(z)$ and $f(z_1+z_2) = f(z)+f(z_2)$) and $\widehat{\Lambda} = \left\{f \in \widehat{V} : \operatorname{Im} f|_{|\Lambda} \subset \mathbb{Z}\right\}$.

Theorem 5.14.7. *We have the below diagram*

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(\Lambda,\mathbb{Z}) \arrow[r] & \mathrm{H}^1(\Lambda,\mathscr{O}(V)) \arrow[r] & \operatorname{Pic}(X) \\
& \widehat{\Lambda} \arrow[u] \arrow[r] & \widehat{V} \arrow[u] &
\end{tikzcd}$$

where $\widehat{V} \ni f \mapsto \operatorname{Im} f \in \mathrm{H}^1(\Lambda,\mathscr{O}(V))$. *The vertical maps are isomorphisms.*

We can also define a Poincaré bundle for complex tori. We want a bundle $\wp$ on $\widehat{X} \times X = \frac{\widehat{V}\oplus V}{\widehat{\Lambda}\oplus\Lambda}$. We define a hermitian form

Brackets denote evaluation?

$$\begin{array}{rccc} h: & (\widehat{V}\oplus V)\times(\widehat{V}\oplus V) & \longrightarrow & \mathbb{C} \\ & ((\ell_1,v_1),(\ell_2,v_2)) & \longmapsto & \langle \ell_1,\overline{v}_2\rangle + \langle v_1,\overline{\ell}_2\rangle \end{array}$$

as well as

$$\begin{array}{rccc} \alpha: & \Lambda\oplus\widehat{\Lambda} & \longrightarrow & U(1) \\ & (\lambda,\ell) & \longmapsto & e^{2\pi i \operatorname{Im}(\lambda,\ell)}. \end{array}$$

This gives a **Poincaré bundle** $\wp$ on $X \times \widehat{X}$.

Theorem 5.14.8. *If X is algebraic, then so is $\widehat{X}$ and it is the dual abelian variety of X.*

If $\mathscr{L}$ is an ample line bundle on X, then we still have $\varphi_{\mathscr{L}} : X \to \widehat{X}$. We have a diagram

$$\begin{array}{ccc} V & \longrightarrow & \widehat{V} \\ \big\downarrow & & \big\downarrow \\ X & \longrightarrow & \widehat{X} \end{array}$$

and $\varphi_{\mathscr{L}}$ is induced from

$$V \ni z \mapsto (w \mapsto h(z,w)) \in \widehat{V}$$

where $h = c_1(\mathscr{L})$ is a Hermitian form on V.

Note 13. Apparently all this complex-analytic stuff is in chapter one of Mumford, so that might be a good place to go to clear things up.

Next time we'll talk about the moduli space of complex abelian varieties.

5.15 Lecture 15 (10/22)

Let $X/\mathbb{C}$ be an abelian variety, so it has a uniformization $X = V/\Lambda$ along with a Riemann form $h : V \times V \to \mathbb{C}$ Hermitian such that $\operatorname{Im} h|_{\Lambda\times\Lambda} : \Lambda \times \Lambda \to \mathbb{Z}$. There's a more algebraic way to describe the Riemann form which will work for all abelian varieties.

Definition 5.15.1. A **polarization** of an abelian variety X over any field is an isogeny

$$\varphi : X \to \widehat{X} = \operatorname{Pic}^0(X)$$

such that $\widehat{\varphi} = \varphi : X \to \widehat{X}$. $\diamond$

Fact. The following are equivalent data

(1) A polarization $\varphi : X \to \widehat{X}$

(2) A class $[\mathscr{L}] \in \operatorname{NS}(X) = \operatorname{Pic}(X)/\operatorname{Pic}^0(X)$

(3) If $k = \mathbb{C}$, a Riemann form

*Proof of **(1)** $\iff$ **(2)**.* ((**1**) $\implies$ (**2**)) φ is equivalent to a line bundle $\mathscr{M}$ on $X \times X$. We can pull this back along the diagonal $\Delta : X \to X \times X$, and one can see that $\Delta^*\mathscr{M}$ on X is ample and of the form $\Delta^*\mathscr{M} = \mathscr{L}_1^{\otimes 2} \otimes \mathscr{L}_2$ with $\mathscr{L}_1$ even and $\mathscr{L}_2 \in \operatorname{Pic}^0(X)$. Hence, $\varphi \mapsto [\mathscr{L}_1]$ is what we're after.

((**2**) $\implies$ (**1**)) Given $\mathscr{L}$, we get $\varphi_{\mathscr{L}} : X \to \widehat{X}$. ∎

Let's say a little about how **(3)** fits in here. Recall $\widehat{X} = \widehat{V}/\widehat{\Lambda}$ where $\widehat{V} = \{f : V \to \mathbb{C} : f\ \mathbb{C}\text{-antilinear}\}$ and $\widehat{\Lambda} = \left\{\ell \in \widehat{V} : \operatorname{Im} \ell|_\Lambda \subset \mathbb{Z}\right\}$. We get an isomorphism $\widehat{X} \xrightarrow{\sim} \operatorname{Pic}^0(X)$ via

$$\widehat{X} \xrightarrow{\ell \mapsto e \circ \operatorname{Im} \circ \ell} \operatorname{Hom}(\Lambda, U(1)) \simeq \operatorname{Pic}^0(X)$$

where $e(x) = \exp(2\pi i x)$. Given $\psi : \Lambda \to U(1)$, can define bundle $\mathscr{L}_\psi \in \operatorname{Pic}^0(X)$ via transformation rule

$$f(z + \lambda) = \psi(\lambda) f(z).$$

Call $\widehat{V}$ the **Hermitian dual** of V. We have $V \times \widehat{V} \to \mathbb{C}$ which is linear in first slot and anti-$\mathbb{C}$ linear (conjugate-linear) in the second slot. Potentially not standard terminology?

Note that a Riemann form on $X = V/\Lambda$ is $H : V \times V \to \mathbb{C}$ with $\operatorname{Im} H(\Lambda \times \Lambda) \subset \mathbb{Z}$, so it is equivalent to giving $\alpha : V \to \widehat{V}$ such that $\alpha(\Lambda) \subset \widehat{\Lambda}$ so we get $\alpha_H : V/\Lambda \to \widehat{V}/\widehat{\Lambda}$, a polarization.

Given H, get $\psi_H : \Lambda \to \mathbb{C}^\times$, $\psi_H(\lambda) = \alpha(\lambda) e^{???}$, which you can use to construct a line bundle.

5.15.1 Moduli of complex abelian varieties

Let's start with the moduli space of complex tori.

Moduli of complex tori We're looking at $X = V/\Lambda$. Let's fix a base $\alpha : \mathbb{Z}^{2g} \simeq \Lambda$ as well as $\beta : V \xrightarrow{\sim} \mathbb{C}^g$. Then we get

$$\gamma : \mathbb{Z}^{2g} \xrightarrow{\sim} \Lambda \hookrightarrow V \xrightarrow{\sim} \mathbb{C}^g.$$

Then, $X \simeq \mathbb{C}^g / \gamma(\mathbb{Z}^{2g})$.

Note that γ is just a $(2g) \times g$ matrix with $\mathbb{C}$-entries, i.e. $\gamma \in M_{2g \times g}(\mathbb{C})$. Note that $\mathrm{GL}_{2g}(\mathbb{Z})$ acts on the choice of α while $\mathrm{GL}_g(\mathbb{C})$ acts on the set of β. Hence,

$$\left\{ \begin{matrix} \text{complex tori} \\ \text{of dim } g \end{matrix} \right\} / \text{iso} \hookrightarrow \mathrm{GL}_{2g}(\mathbb{Z}) \backslash M_{2g \times g}(\mathbb{C}) / \mathrm{GL}_g(\mathbb{C}).$$

In fact,

$$\left\{ \begin{matrix} \text{complex tori} \\ \text{of dim } g \end{matrix} \right\} / \text{iso} \xrightarrow{\sim} \mathrm{GL}_{2g}(\mathbb{Z}) \backslash U / \mathrm{GL}_g(\mathbb{C})$$

where

$$U = \{ (v_1, \ldots, v_{2g} \mid \text{any } g \text{ columns are linearly independent} \}.$$

Note that $\dim U = g \times 2g = 2g^2$ (Open set in $M_{2g \times g}(\mathbb{C})$) and $\dim \mathrm{GL}_g(\mathbb{C}) = g^2$, so $\dim\{\text{tori}\} = 2g^2 - g^2 = g^2$.

What about "abelian varieties"?

Moduli of polarized abelian varieties Consider pairs (X, h) with $X \cong V/\Lambda$ and $h : V \times V \to \mathbb{C}$ Hermitian with $\operatorname{Im} h(\Lambda \times \Lambda) \subset \mathbb{Z}$. Let $E = \operatorname{Im} h$.

Remark 5.15.2. h is determined by E

$$h(u, v) = E(iu, v) + iE(u, v).$$

(Exercise) ○

Note that V " = " $\Lambda \otimes \mathbb{R}$ carries a symplectic form (i.e. $E(u, v) = -E(v, u)$)

$$E : \Lambda \times \Lambda \to \mathbb{Z}.$$

There is a "normal form" for E. Note that $E : \Lambda \to \Lambda^*$, so we have an exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \Lambda^* \longrightarrow \Lambda^*/\lambda \longrightarrow 0$$

with finite cokernel. Hence, $\Lambda^*/\Lambda \simeq \bigoplus \mathbb{Z}/d_i$ with $d_1 \mid d_2 \mid d_3 \mid \dots$ and $d_1 = \min_{u,v\in\Lambda} |E(u,v)|$.

The upshot is that there are $\lambda_1, \dots, \lambda_g, \mu_1, \dots, \mu_g \in \Lambda$ a $\mathbb{Z}$-basis so that

$$E(\lambda_i, \lambda_j) = E(\mu_i, \mu_j) = 0 \text{ for all } i, j$$

and

$$E(\lambda_i, \mu_j) = 0 \text{ if } i \neq j$$

and

$$E(\lambda_i, \mu_i) = d_i.$$

For any polarized abliean variety (X, h), we have a discrete invariant

$$d = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_g \end{pmatrix}.$$

Take $e_i = d_i^{-1}\mu_i$ as a base for V so

$$E(e_i, e_j) = 0 \text{ and } E(\lambda_i, e_j) = \delta_{ij}.$$

Can find $\tau \in M_{g\times g}(\mathbb{C})$ so that

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_g \end{pmatrix} = \tau \begin{pmatrix} e_1 \\ \vdots \\ e_g \end{pmatrix}.$$

In this way, get a normal form

$$X \simeq \frac{\mathbb{C}^g}{\mathbb{Z}^g\tau + \mathbb{Z}^g d},$$

i.e. writing $\tau = \begin{pmatrix} \tau_1 \\ \vdots \\ \tau_g \end{pmatrix}$, $\Lambda \subset \mathbb{C}^g$ is generated by $\tau_1, \dots, \tau_g, e_1, \dots, e_g$.

Shou-Wu prefers row vectors over column vectors

Let $H \in M_{g\times g}(\mathbb{C})$ represent the Hermitian form h on V with respect to base $e_1, \dots, e_g$, so $H_{ij} = h(e_i, e_j)$. Note that

$$\operatorname{Im} H_{ij} = (\operatorname{Im} h)(e_i, e_j) = E(e_i, e_j) = 0$$

so $H = (H_{ij})$ is real, symmetric, positive definite. Note that

$$h(\lambda_i, e_j) = h\left(\sum_k \tau_{ik} e_k, e_j\right) = \sum_k \tau_{ik} H_{kj} = (\tau H)_{ij}$$

and

$$h(\lambda_i, \lambda_j) = h\left(\sum_m \tau_{im} e_m, \sum_n \tau_{jn} e_n\right) = \sum_{m,n} \tau_{im} H_{mn} \overline{\tau}_{jn} = \left(\tau H \overline{\tau}^t\right)_{ij}.$$

Taking imaginary parts gives

$$I_g = \mathrm{Im}(\tau H) \text{ and } 0 = \mathrm{Im}(\tau H \overline{\tau}^t).$$

Write $\tau = a + bi$ with $a, b \in M_{g\times g}(\mathbb{R})$. The first equation says

$$I_g = bH \implies b = H^{-1}.$$

The second says

$$0 = \mathrm{Im}\left[(a+bi)H(a^t - ib^t)\right] = -aHb^t + bHa^t = -a + a^t$$

Question: Where did last equality come from?

so $\tau = \tau^t$, $\mathrm{Im}\,\tau > 0$ and $H = (\mathrm{Im}\,\tau)^{-1}$.

In summary, we have shown that for any polarized abelian variety (X, h) of type $d = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ can be written (non-uniquely) in the form

$$X = \frac{\mathbb{C}^g}{\mathbb{Z}^g\tau + \mathbb{Z}^g d}$$

with τ symmetric, $\mathrm{Im}\,\tau > 0$, and $h = (\mathrm{Im}\,\tau)^{-1}$ the Hermitian form.

This tells us that the space of polarized abelian varieties of type d is covered by

Looks a lot like an upper half plane

$$\mathfrak{H}_g := \left\{\tau \in M_{g\times g})(\mathbb{C}) : \tau^t = \tau \text{ and } \mathrm{Im}\,\tau > 0\right\}$$

which has dimension $1 + 2 + \cdots + g = \frac{g(g+1)}{2}$. Note that

$$g^2 - \frac{g(g+1)}{2} = \frac{g(g-1)}{2} > 0 \text{ when } g > 1,$$

so elliptic curves are the only dimension of complex tori where every one is algebraic. In dimensions greater than 1, there is also some non-algebraic complex torus.

Now we want to understand the cover

$$\mathfrak{H}_g \twoheadrightarrow \left\{\begin{matrix}\text{polarized abelian varieites} \\ \text{of type } d\end{matrix}\right\}.$$

For symplicity, take

$$d = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}.$$

Remark 5.15.3. In fact, any abelian variety of type d is isogeneous to one of type I_g. These are called **principally polarized abelian varieties**. If $X = \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g d)$ then $X_0 = \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g)$. ◦

Question: Does $X \twoheadrightarrow X_0$ as I've written them?

Consider $(\mathbb{Z}^{2g}, E_0)$, a symplectic form. Let $u_1, \ldots, u_g, v_1, \ldots, v_g$ be a standard basis so the form is given by the matrix

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

That is, $E_0(u_i, u_j) = E_0(v_i, v_j) = 0$ always and $E_0(u_i, v_j) = \delta_{ij}$. Consider

$$\mathbb{Z}^{2g} \xrightarrow{\alpha} \Lambda \hookrightarrow V$$

with α symplectic and an isomorphism. We want

$$\alpha \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} \tau\mu \\ \mu \end{pmatrix}.$$

Hence, τ is equivalent data to $\alpha : \mathbb{Z}^{2g} \to \Lambda$. Now we want to change α. Note that

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \{g \in \mathrm{GL}_{2g}(\mathbb{Z}) : g \text{ preserves } E\}.$$

What happens when we change α, so we consider instead

$$\mathbb{Z}^{2g} \xrightarrow{g} \xrightarrow{\alpha} \Lambda$$

Then,

$$\begin{pmatrix} u \\ v \end{pmatrix} \xrightarrow{g} \begin{pmatrix} au + bv \\ cu + dv \end{pmatrix} \xrightarrow{\alpha} \begin{pmatrix} (a\tau + b)\alpha(v) \\ (c\tau + d)\alpha(v) \end{pmatrix}$$

so we see that τ is changed to $(a\tau + b)(c\tau + d)^{-1}$.

I missed/potentially miswrote some intermediate stuff but this is what you get in the end

Theorem 5.15.4. *The set of principally polarized abelian varieties over $\mathbb{C}$, up to isomorphism, is bijective to*

$$\mathrm{Sp}_{2g}(\mathbb{Z}) \setminus \mathfrak{H}_g.$$

More precisely, each $\tau \in \mathfrak{H}_g$ is associated to

$$X_\tau = \mathbb{C}^g / (\mathbb{Z}^g \tau + \mathbb{Z}^g).$$

For all $g \in \mathrm{Sp}_{2g}(\mathbb{Z})$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we get an isomorphism

$$\begin{tikzcd} X_\tau \arrow[r] \arrow[d, equal] & X_{g\tau} \arrow[d, equal] \\ \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g) \arrow[r] & \mathbb{C}^g/(\mathbb{Z}^g(a\tau + d)(c\tau + d)^{-1} + \mathbb{Z}^g) \end{tikzcd}$$

with bottom arrow given by

$$\begin{array}{ccc} \mathbb{C}^g & \longrightarrow & \mathbb{C}^g \\ z & \longmapsto & z(c\tau + d)^{-1} \end{array}$$

One can again ask if there is a universal family. The answer is again no. I didn't hear the reason, but its probably the same as list time: something something negation in the fibers something something.

5.16 Lecture 16 (10/27)

Missed first 5 minutes due to internet troubles

Recall 5.16.1 (Abelian Varieties over $\mathbb{C}$)**.** $X = V/\Lambda$ with V a g-dim $\mathbb{C}$-vector space and $\Lambda \subset V$ a lattice of rank $2g$. Let h be a Riemann form, so $h : V \times V \to \mathbb{C}$ is Hermitian, positive definitie and restricts to $E = \operatorname{Im} h : \Lambda \times \Lambda \to \mathbb{Z}$. We can write

$$\Lambda = \Lambda_1 \oplus \cdots \oplus \Lambda_g$$

orthogonal w.r.t. E s.t. $\operatorname{rank} \Lambda_i = 2$ and $\Lambda_i = \mathbb{Z}\lambda_i \oplus \mathbb{Z}\mu_i$. We have

$$E(\lambda_i, \mu_i) = \delta_i \text{ with } \delta_1 \mid \delta_2 \mid \cdots \mid \delta_g.$$

The matrix

$$\delta = \begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_g \end{pmatrix}$$

is an invariant of the polarized abelian variety (X, h).

Fix δ, so $X \cong \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g)$. $\mathbb{C}^g, \mathbb{Z}^g$ row matrices and $\tau \in M_{g\times g}(\mathbb{C})$ such that $\tau^t = \tau$ and $\operatorname{Im}\tau > 0$. $\odot$

Hence,

$$\mathfrak{H}_g = \left\{\tau \in M_{g\times g}(\mathbb{C}) : \operatorname{Im}\tau > 0 \text{ and } \tau^t = \tau\right\},$$

the **Siegel upper half space**, surjects onto the moduli of polarized abelian varieties of type δ. This space has dimension $g(g+1)/2$.

More precisely, when $\delta = I_g$, we are looking at principally polarized abelian varieties (X, h) with h a Riemann form on $\widetilde{X}$ such that $\operatorname{Im} h : \pi_1(X) \times \pi_1(X) \to \mathbb{Z}$ is perfect.

Note 14. Internet wonky, so I've been periodically kicked out of Zoom. These notes are incomplete. Missing bits filled in later with help from a friend.

We can decorate this by considering (X, h, α) with $\alpha : \mathbb{Z}^{2g} \longrightarrow \mathrm{H}_1(X, \mathbb{Z}) = \pi_1(X)$ symplectic w.r.t $\mathbb{Z}^g \oplus \mathbb{Z}^g$. Then, $\{(X, h, \alpha)\} = \mathfrak{H}_g$. Different choices of α differ by composition of $\mathrm{Sp}_{2g}(\mathbb{Z})$.

$$\begin{tikzcd} \mathbb{Z}^{2g} \arrow[r, "\alpha"] \arrow[d, "\gamma"'] & \mathrm{H}_1(X, \mathbb{Z}) \arrow[d] \\ \mathbb{Z}^{2g} \arrow[r, "\beta"] & \mathrm{H}_1(X, \mathbb{Z}) \end{tikzcd}$$

with $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$. The takeaway is that

$$\left\{\begin{matrix} \text{prinipally polarized } g\text{-dim} \\ \text{abelian varieites}/\mathbb{C} \end{matrix}\right\} \simeq \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{H}_g.$$

Given $\tau \in \mathfrak{H}_g$, we have $X_\tau = \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}_g)$ and given $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$, we can write

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

as a block-matrix. Then, $\gamma(\tau) = (a\tau + b)(c\tau + d)^{-1}$. We then get a map

$$\begin{tikzcd} \mathbb{C}^g \arrow[r, "\cdot(c\tau+d)^{-1}"] \arrow[d] & \mathbb{C}^g \arrow[d] \\ X_\tau \arrow[r] & X_{\gamma\tau} \end{tikzcd}.$$

Question 5.16.2. *What is the quotient space* $\mathcal{A}_g := \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{H}_g$*?*

When $g = 1$, is is the affine line with parameter given by the j-invariant.

Question 5.16.3. *Does there exist a universal family of abelian varieties?*

Familiarity with the symplectic group The symplectic group Sp_{2g} is a group scheme over $\mathbb{Z}$. For any commutative ring R,

$$\mathrm{Sp}_{2g}(R) = \left\{\gamma \in \mathrm{GL}_{2g}(R) : \gamma^t \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \gamma = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}\right\} = \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_{2g}(R) : \gamma^{-1} = \begin{pmatrix} d^t & -b^t \\ -c^t & a^t \end{pmatrix}\right\}.$$

We can define a symplectic involution on $\mathrm{GL}_{2g}(R)$ via

$$\gamma \mapsto \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}^{-1} \gamma^t \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} =: \overline{\gamma}.$$

Then,

$$\mathrm{Sp}_{2g}(R) = \{\gamma \in \mathrm{GL}_{2g}(R) : \gamma\overline{\gamma} = I\}.$$

Here are some useful subgroups

- $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ for $b \in \mathrm{Sym}_g(R)$
- $\begin{pmatrix} a & 0 \\ 0 & (a^t)^{-1} \end{pmatrix}$ for $a \in \mathrm{GL}_g(R)$
- $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$

One can also consider

$$U_g(R) = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^t a + b^t b = 1\right\} = \mathrm{Sp}_{2g}(R) \cap U_{2g}(R).$$

where $U_{2g}(R)$ on the RHS above is matrices whose inverse is their transpose.

Question: Isn't this $O_{2g}(R)$ instead?

Back to moduli We can reinterpret $\mathcal{H}_g = \left\{\left(V/\Lambda, h, \alpha : \mathbb{Z}^{2g} \xrightarrow{\sim} \Lambda\right)\right\}$. We can instead look at $(V, h, \alpha : \mathbb{R}^{2g} \xrightarrow{\sim} V)$ (in either case, α symplectic). To get from former to latter, tensor with $\mathbb{R}$; to get from latter back to former, set $\Lambda = \mathrm{Im}\,\alpha(\mathbb{Z}^{2g})$.

Note that $\mathrm{Sp}_{2g}(\mathbb{R})$ acts on the second description easily via

$$\gamma \cdot (V, h, \alpha) = (V, h, \alpha \circ \gamma).$$

The corresponding action of $\mathrm{Sp}_{2g}(\mathbb{R})$ on $\mathfrak{H}_g$ under its identification with such triples is $\gamma(\tau) = (a\tau + b)\,(c\tau + d)^{-1}$. What are the stabilizers?

The data of an isomorphism $(V, h, \alpha) \sim (V', h', \alpha')$ consists of $\varphi : V \xrightarrow{\sim} V'$ such that $h \circ \varphi = h'$ and $\varphi \circ \alpha = \alpha'$. So, say $\gamma \cdot (V, h, \alpha) = (V, h\alpha)$; this would give

$$\begin{tikzcd} (h,V) \arrow[r, "\varphi"] & (h,V) \\ \mathbb{R}^{2g} \arrow[u, "\alpha"] \arrow[ur, "\alpha\circ\gamma"] \arrow[r, "\gamma"] & \mathbb{R}^{2g} \arrow[u, "\alpha"] \end{tikzcd}$$

with φ unitary (i.e $h \circ \varphi = h$). Thus,

$$\mathrm{Stab}(V,h,\alpha) = \left\{ \gamma \in \mathrm{Sp}_{2g}(\mathbb{R}) \,\middle|\, \exists \varphi \in U(V,h) \text{ s.t. } \begin{tikzcd} (h,V) \arrow[r, "\varphi"] & (h,V) \\ \mathbb{R}^{2g} \arrow[u, "\alpha"] \arrow[ur, "\alpha\circ\gamma"] \arrow[r, "\gamma"] & \mathbb{R}^{2g} \arrow[u, "\alpha"] \end{tikzcd} \text{ commutes} \right\}$$

Note that the choice of φ determines γ. This is because φ must be symplectic w.r.t. $\mathrm{Im}\, h$, $\varphi \circ \alpha = \alpha \circ \varphi$, so γ is unique. The upshot is that we have $U(v, h) \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{R})$ with image the stabilizer of (V, h, α).

Question: Why? What?

$\mathrm{Sp}_{2g}(\mathbb{R})$ acts on $\mathcal{H}_g$ transitively. In analogy with the upper half plane, we think of $\tau \in \mathfrak{H}_g$ as $\tau = x + iy$ with $x, y \in \mathrm{Sym}_g(\mathbb{R})$ and $y > 0$ (positive definite).

When $g = 1$, showing transitivity is easy. One simply observes that

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} i = \frac{yi + x}{1} = x + iy$$

for any $x \in \mathbb{R}$ and $y > 0$. This is not in $\mathrm{SL}_2(\mathbb{R}) = \mathrm{Sp}_2(\mathbb{R})$, but you can fix this by instead considering the matrix $\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix}$.

For general g, write $\tau = x + iy$ with y positive definite and symmetric. In particular, y is diagonalizable so there exists some symmetric, positive matrix A s.t. $A^2 = y$. Then,

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & A^{-1} \end{pmatrix} = \begin{pmatrix} A & xA^{-1} \\ 0 & A^{-1} \end{pmatrix} =: \gamma$$

and we claim that $\gamma \in \mathrm{Sp}_{2g}(\mathbb{R})$. This is just a simple matrix calculation. Then,

$$\gamma(iI_g) = (Ai + xA^{-1})A = A^2 i + x = x + iy = \tau$$

so $\mathrm{Sp}_{2g}(\mathbb{R}) \curvearrowright \mathfrak{H}_g$ is indeed transitive.

Note that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{R})$ satisfies $\gamma(iI_g) = iI_g$ iff

TODO: Figure out what's going on with this overloaded U_g notation

$$
\begin{aligned}
(ai+b)(ci+d)^{-1} = iI_g \iff ai+b = di-c \\
&\iff (a,b) = (d,-c) \\
&\iff \gamma^{-1} = \begin{pmatrix} d^t & -b^t \\ -c^t & a^t \end{pmatrix} = \begin{pmatrix} a^t & c^t \\ b^t & d^t \end{pmatrix} = \gamma^t \\
&\iff \gamma \in U_{2g}(\mathbb{R}) \\
&\iff \gamma \in \mathrm{Sp}_{2g}(\mathbb{R}) \cap U_{2g}(\mathbb{R}) = U_g(\mathbb{C}).
\end{aligned}
$$

Thus,

$$\mathfrak{H}_g = \mathrm{Sp}_{2g}(\mathbb{R})/U_g(\mathbb{C}).$$

Remark 5.16.4. Apparently, we ended up showing Iwasawa decomposotion for $\mathrm{Sp}_{2g}(\mathbb{R})$ in process of showing transitivity. Don't ask me. $\circ$

We conclude that $\mathfrak{H}_g$ is the set of maximal compact subgroups of $\mathrm{Sp}_{2g}(\mathbb{R})$ or equivalently, the set of conjugacy classes of $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$.

Back to action of $\mathrm{Sp}_{2g}(\mathbb{Z}) \curvearrowright \mathfrak{H}_g$. Let $G = \mathrm{Sp}_{2g}(\mathbb{R})$ and $\Gamma = \mathrm{Sp}_{2g}(\mathbb{Z})$ so $\Gamma \hookrightarrow G$ discretely. The stabilizer of Γ acting on τ is $\Gamma_\tau = G_\tau \cap \mathrm{Sp}_{2g}(\mathbb{Z}) = U(h_\tau) \cap \mathrm{Sp}_{2g}(\mathbb{Z})$ which is finite (discrete subspace of compact, Hausdorff group $U(h_\tau)$). Hence, $\mathrm{Sp}_{2g}(\mathbb{Z}) \curvearrowright \mathfrak{H}_g$ with finite stabilzers.

Lemma 5.16.5. $\Gamma_\tau = \mathrm{Aut}(X_\tau, h_\tau)$

Proof. $\varphi \in \mathrm{Aut}(X_t, h_t)$ means $\varphi : \mathbb{C}^g \to \mathbb{C}^g$ with $\varphi \in U(h_t)$ and $\varphi|_\Lambda = \Lambda$. Since $\Lambda \simeq \mathbb{Z}^{2g}$, get $\varphi \in \Gamma_\tau$. ■

Consider the reduction map $\mathrm{Sp}_{2g}(\mathbb{Z}) \longrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ for $n \geq 1$. Secretly, this map is surjective. Let $\Gamma(n)$ be the kernel, so

$$1 \longrightarrow \Gamma(n) \longrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}) \longrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z}) \longrightarrow 1.$$

Lemma 5.16.6. $\Gamma_\tau \cap \Gamma(n) = 1$ *if* $n \geq 3$, *i.e.* $\Gamma_\tau \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$.

Proof. Γ_τ is finite, so $\Gamma_\tau \cap \Gamma(n)$ is finite as well. It it is nontrivial, then there exists $\gamma \in \Gamma_\tau \cap \Gamma(n)$ with $\gamma^p =$ but $\gamma \neq 1$ (p prime). Then, $\varphi = \frac{1-\gamma}{n} \in M_{2n\times 2n}(\mathbb{Z})$. If ζ is an eigenvalue of γ, then $\zeta^p = 1$ but $\zeta \neq 1$. Note that $\frac{1-\zeta}{n} \in \mathbb{Q}(\zeta)$ is an eigenvalue of φ, so $(1-\zeta)/n$ is an algebraic integer. Note that

$$\mathbb{Z} \ni \mathrm{Nm}\left(\frac{1-\zeta}{n}\right) = \frac{(1-\zeta)(1-\zeta^2)\dots(1-\zeta^{p-1})}{n^{p-1}} = \frac{p}{n^{p-1}}$$

which is nonsense if $n \geq 3$. ■

Corollary 5.16.7. $\Gamma(n) \curvearrowright \mathfrak{H}_g$ *freely if* $n \geq 3$, *so* $\mathcal{A}_{g,n} := \Gamma(n)\backslash\mathfrak{H}_g$ *is a smooth, complex manifold.*

Theorem 5.16.8. $\mathcal{A}_{g,n}$ *is the moduli of tuples* (X, h, κ) *where* X *is an abelian variety,* h *is a principal polarization, and* $\kappa : (\mathbb{Z}/n\mathbb{Z})^{2g} \xrightarrow{\sim} X[n]$ *is a symplectic map; this is called a* ***full level*** n***-structure***.

Theorem 5.16.9. *If* $n \geq 3$, *then* $\mathcal{A}_{g,n}$ *has a universal family of abelian varieites.*

There's a universal family over $\mathcal{H}_g$ given by $\mathscr{X}_H = \mathbb{Z}^{2g}\backslash\mathfrak{H} \times \mathbb{C}^g$ with action

$$(u, v) \cdot (\tau, z) = (\tau, z + u\tau + v).$$

Note that $\Gamma \curvearrowright \mathscr{X}_{\mathfrak{H}_g}$, so the quotient by this action gives a universal family $\Gamma(n)\backslash\mathscr{X}_{\mathfrak{H}_g} =: \mathscr{X}_{g,n} \to \mathcal{A}_{g,n}$ over $\mathcal{A}_{g,n}$. That is, we have

$$\begin{tikzcd} \mathscr{X}_{\mathfrak{H}_g} \arrow[r] \arrow[d] & \mathscr{X}_{g,n} \arrow[d] \\ \mathfrak{H}_g \arrow[r] & \mathcal{A}_{g,n} \end{tikzcd}$$

Next time we introduce Siegal modular forms and sketch proof of quasi-projectivity of Siegal modular variety.

5.17 Lecture 17 (10/29)

We've been studying the moduli space of abelian varieties with principal polarization. These are all of the form $X = \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g)$ with $\tau \in \mathfrak{H}_g$. The iso classes of principally polarized abelian varieties over $\mathbb{C}$ are parameterized by $\mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{H}_g = \mathcal{A}_g$. We have proved

- that the stabilizer of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on any point $z \in \mathfrak{H}_g$ is finite, and has trivial intersection with

  $$\Gamma(n) := \ker\left(\mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})\right)$$

  when $n \geq 3$;

- if we replace $\mathrm{Sp}_{2g}(\mathbb{Z})$ by $\mathrm{Sp}_{2g}(\mathbb{R})$, then the action is transitive, with stabilizer the unitary group defined by h_τ, e.g.

  Did I write down the correct conditions?

  $$\tau = iI_g \implies U_g = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^t a + b^t b = 1 \text{ and } a^t b = b^t a \right\},$$

  so $\mathfrak{H}_g = \mathrm{Sp}_{2g}(\mathbb{R})/U_g(\mathbb{R})$.

- If we replace Γ by $\Gamma(n)$, then $\Gamma(n)$ (for $n \geq 3$) acts freely on $\mathfrak{H}_g$, so $\mathcal{A}_{g,n} := \Gamma(n)\backslash\mathfrak{H}_g$ is a complex manifold. In fact, $\mathcal{A}_{g,n}$ supports a universal family of abelian varieties.

The universal family comes from the quotient $(\mathbb{Z}^{2g} \times \Gamma(n))\backslash(\mathfrak{H}_g \times \mathbb{C}^g)$ with actions $(m,n)\cdot(\tau,z) = (\tau, z + m\tau + n)$ with $m,n \in \mathbb{Z}^g$ and $\gamma(\tau,z) = (\gamma\tau, z\,(c\tau+d)^{-1})$ with $\gamma \in \Gamma(n)$.

This $\mathcal{A}_{g,n}$ has a geometric interpretation. It is the moduli of $\left(X, h, \alpha : (\mathbb{Z}/n\mathbb{Z})^{2g} \xrightarrow{\sim} X[n]\right)$ with α symplectic.

Write $X = V/\Lambda$ so $E = \operatorname{Im} h : \Lambda \times \Lambda \to \mathbb{Z}$ is a symplectic form. We have $X[n] \simeq \frac{1}{n}\Lambda/\Lambda$ with E restricting to

$$\frac{1}{n}\Lambda/\Lambda \times \frac{1}{n}\Lambda/\Lambda \longrightarrow \frac{1}{n^2}\mathbb{Z}/\frac{1}{n}\mathbb{Z},$$

i.e.

$$\Lambda/n\Lambda \times \Lambda/n\Lambda \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

The α decoration is

$$\alpha : (\mathbb{Z}/n\mathbb{Z})^{2g} \xrightarrow{\sim} X[n] \xrightarrow{\sim} \Lambda/n\Lambda.$$

Recall that we have used $\alpha_0 : \mathbb{Z}^{2g} \xrightarrow{\sim} \Lambda$ to identity $\mathfrak{H}_g$ with the space of tuples (X, h, α_0). We claim that

$$\mathcal{A}_{g,n} = \{(X, h, \alpha_n)\}/\mathrm{iso} =: \mathcal{B}_{g,n}.$$

We have a natural map $\mathfrak{H}_g \to \mathcal{B}_{g,n}$ by setting $\alpha_n = \alpha_0 \pmod n$. Consider

$$\begin{tikzcd} & \mathfrak{H}_g \arrow[dl] \arrow[dr] & \\ \mathcal{A}_{g,n} & & \mathcal{B}_{g,n} \end{tikzcd}$$

$$\begin{tikzcd} \mathfrak{H}_g \arrow[d] & \{(x, h, \alpha_0)\} \arrow[l, "\sim"'] \arrow[d] \\ \Gamma(n)\backslash\mathfrak{H}_g \arrow[r, "\varphi"] & \{(x, h, \alpha_n)\} \end{tikzcd}$$

We have a morphism $\varphi : \Gamma(n)\backslash\mathfrak{H}_g \to B_{g,n}$ which we claim is bijective. Injectivity is pretty clear since if you have the same level n structure, then you must be the same. Surjectivity is basically the claim that every mod n level structure can be lifted to a mod 0 level structure.

Say $E : \Lambda \times \Lambda \to \mathbb{Z}$ is an alternating, perfect form. Say $\bar{e}_1, \dots, \bar{e}_{2g}$ a symplectic basis for Λ/n. Then this basis can be lifted to a symplectic basis on Λ: $e_1, \dots, e_{2g}$. Recall symplectic means that E is represented by

$$E : \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}.$$

Can show this by induction on g.

Today we want to show that $\Gamma(n)\backslash\mathfrak{H}_g$ is a quasi-projective variety, and then we'd like to compactify. As always, to show projectivity, we will construct an ample line bundle on $\Gamma(n)\backslash\mathfrak{H}_g$.

For each $\tau \in \mathfrak{H}_g$, we get a corresponding X_τ which has $\bigwedge^g \Omega_{X_\tau}$ = differential forms of degree g on X_τ. There is also ω_τ, the space of invariant forms. If $X_\tau = \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g)$, then $\omega_\tau = \mathbb{C} \cdot \mathrm{d}z_1 \wedge \cdots \wedge \mathrm{d}z_g$. These ω_τ together form a line bundle ω on $\mathfrak{H}_g$.

Note that $\mathrm{Sp}_{2g}(\mathbb{R}) \curvearrowright \mathfrak{H}_g \times \mathbb{C}^g$ via $\gamma \cdot (\tau, \zeta) = (\gamma(\tau), z\,(c\tau + d)^{-1})$. Taker determinants to get action on $\mathfrak{H}_g \times \mathbb{C}$ via $\gamma \cdot (\tau, z) = (\gamma(\tau), z \det{(c\tau + d)}^{-1})$. Take the dual space so action of $\mathfrak{H}_g \times \mathbb{C}$ now $(\gamma(\tau), z \det(c\tau + d))$. Quotient by $\Gamma(n)$ ($n \geq 3$) to get a bundle ω on $\Gamma\backslash\mathfrak{H}_g$ s.t. $\pi^*\omega$ has a base $\mathrm{d}z_1 \wedge \cdots \wedge \mathrm{d}z_g$ ($\pi : \mathfrak{H}_g \longrightarrow \Gamma\backslash\mathfrak{H}_g = \mathcal{A}_\Gamma$). Hence,

$$\Gamma\left(\mathcal{A}_\gamma, \omega^{\otimes k}\right) = \left\{f(\tau)(\mathrm{d}z_1 \wedge \cdots \wedge \mathrm{d}z_g)^k \text{ which are invariant under } \Gamma\right\}$$

In terms of the function $f(\tau)$, this invariance says that

$$f(\tau) = f(\gamma\tau)\det(c\tau + d)^k.$$

Definition 5.17.1. For each $k \in \mathbb{Z}$, the space of **weight k Siegal modular forms** is the span of

$$f : \mathcal{H}_g \longrightarrow \mathbb{C}$$

holomorphic such that

$$f(\gamma\tau) = \det(c\tau + d)^k f(\tau).$$

$\diamond$

Theorem 5.17.2. *The bundle ω is ample. More precisely,*

$$R = \bigoplus_k M_k$$

is a finitely generate module over $\mathbb{C}$, and one can get an embedding $\mathcal{A}_{g,n} \hookrightarrow \operatorname{Proj} R$.

For general Γ, some power of ω will descend to a line bundle on X_Γ.

For $\mathcal{A}_g = \mathcal{A}_{g,1}$, the stabilizer of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on each point is finite; it acts on ω by roots of unity.

In fact, $\omega^{\otimes(g+1)} \simeq \omega_{\mathcal{A}_g} = \bigwedge^{\frac{g(g+1)}{2}} \Omega_{\mathcal{A}_g}$. We have an embedding $\mathcal{H}_g \hookrightarrow \mathrm{Sym}_g(\mathbb{C})$ and

$$\mathrm{d}\tau = \begin{pmatrix} \mathrm{d}\tau_{11} & \dots & \mathrm{d}\tau_{1g} \\ \vdots & \ddots & \vdots \\ \mathrm{d}\tau_{g1} & \dots & \mathrm{d}\tau_{gg} \end{pmatrix}.$$

Since $\gamma\tau = (a\tau + b)(c\tau + d)^{-1}$, we see $\mathrm{d}(\gamma\tau) = \left((c\tau + d)^t\right)^{-1} \mathrm{d}\tau\, (c\tau + d)^{-1}$.

Remark 5.17.3. ω has a natural metric. For $\alpha, \beta \in \Gamma(X, \Omega_X^g) = \omega$, something something

$$i \int_X \alpha\overline{\beta}$$

something something

$$i \int_X \alpha\overline{\alpha} > 0$$

something something

$$\langle \alpha, \beta \rangle \text{ Hermitian}$$

something something. Get a Kähler-Einstein metric? $\circ$

5.17.1 Compactification

Recall 5.17.4. To compactify $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$, we add cusps corresponding to orbits of $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{P}^1(\mathbb{Q})$. $\odot$

Got distracted and missed some stuff and am now completely lost

Note 15. There were several minutes things being said/written that I did not follow before we got to a point where I had enough of an idea of what was going on to return to taking notes.

Start with $\mathbb{C}^{2g}$ with standard symplectic form. Let $\check{\mathfrak{H}}_g$ be the flag variety of $L \hookrightarrow \mathbb{C}^{2g}$ with L a maximal **isotropic subspace**, so $\dim L = g$ (maximal) and any two elements have trivial pairing (trivial). When $g = 1$, $\widehat{\mathfrak{H}}_1 = \mathbb{CP}^1$ (something like this. Don't quote me).

We can embed $\mathfrak{H}_g \hookrightarrow \check{\mathfrak{H}}_g$. Write

$$\tau = \begin{pmatrix} \tau_1 \\ \vdots \\ \tau_g \end{pmatrix} \in \mathfrak{H}_g$$

and set

$$L_\tau = \left\langle \begin{pmatrix} \tau_i & e_i \end{pmatrix} : i = 1, \ldots, g \right\rangle.$$

Note that $\check{\mathfrak{H}}_g$ is compact.

For any $0 \leq i \leq g$, we define $\check{\mathfrak{H}}_i \hookrightarrow \check{\mathfrak{H}}_g$. Write $\mathbb{C}^{2g} = \mathbb{C}^i \oplus \mathbb{C}^{g-i} \oplus \mathbb{C}^g$ and suppose we have $L \hookrightarrow \mathbb{C}^i \oplus \mathbb{C}^i$. Then, we have $\check{\mathfrak{H}}_i \to \check{\mathfrak{H}}_g$ via $L \mapsto L \oplus \mathbb{C}^{g-i}$. Consider

$$\mathfrak{H}_g^* = \bigsqcup_i \mathrm{Sp}_{2g}(\mathbb{Q})\mathfrak{H}_i \hookrightarrow \check{\mathfrak{H}}_g$$

and form $\mathcal{A}_{g,n}^* = \Gamma(n)\backslash\mathfrak{H}_g^*$.

Theorem 5.17.5.

$$\mathcal{A}_{g,n}^* = \operatorname{Proj} R$$

is a projective, normal variety. In fact, it is the minimal compactification of $\mathcal{A}_{g,n}$. It has a lot of singularities.

Note that $\mathcal{A}_{g,n}^* \setminus \mathcal{A}_{g,n} = \bigsqcup_i$ "$\mathcal{A}_i$" with "$\mathcal{A}_i$" like a moduli of abelian varieties of dimension i. Note that

$$\frac{g(g+1)}{2} - \frac{i(i+1)}{2} \geq \frac{g(g+1)}{2} - \frac{(g-1)g}{2} = g,$$

so the boundary has codimension g (so a divisor $\iff$ $g = 1$). This is why we did not put a condition at the cusps.

5.18 Lecture 18 (11/3)

Last time we defined Siegal modular forms and used them to show that the moduli of abelian varities with level structure is quasi-projective. We then gave a compactification and so ended up with an actual projective variety.

One can still wonder if these moduli spaces and be defined over a number field or if they support Hecke operators. To tackle these, we will first need a theory of abelian varieties over more general rings.

5.18.1 Abelian schemes

Definition 5.18.1. Let S be a scheme. A **group scheme** over S is an S-scheme $G \to S$ with "group operations" $m : G \times_S G \to G$ (multiplication), $e : S \to G$ (identity), and $\iota : G \to G$ (inversion) making the obvious diagrams commute. Equivalently, for any S-scheme T, the (set) maps

$$m_T : G(T) \times G(T) \to G(T), \;\; e_T : \{*\} \to G(T), \;\; \text{and} \;\; \iota_T : G(T) \to G(T)$$

turn $G(T)$ into a group. ◇

Example. The **additive group** $\mathbb{G}_a = \operatorname{Spec} \mathbb{Z}[T]$ with multiplication given by $T \mapsto T_1 + T_2$. △

Example. The **multiplicative group** $\mathbb{G}_m = \operatorname{Spec}[T, T^{-1}]$ with multiplication given by $T \mapsto T_1T_2$. △

Example. The general linear group $\mathrm{GL}_n = \operatorname{Spec} \mathbb{Z}[g_{ij}, u]/((\det g)u - 1)$ or the special linear group $\mathrm{SL}_n = \operatorname{Spec} \mathbb{Z}[g_{ij}]/(\det g_{ij} - 1)$. △

Example. The roots of unity $\mu_n = \operatorname{Spec} \mathbb{Z}[T]/(T^n - 1)$ which is a group subscheme of $\mathbb{G}_m$. △

Example. $\alpha = \operatorname{Spec} \mathbb{F}_p[T]/(T^p)$ is a group scheme with no geometric points. △

One naturally defines notions of subgroups, quotient groups, and homomorphisms for group schemes. These can all be test using the functor of points perspective (e.g. passing to $G(T)$).

Definition 5.18.2. Let S be a scheme. By an **abelian scheme** over S, we mean a group scheme $X \to S$ which is proper and smooth with connected geometric fibers. ⋄

Using the rigidity lemma (5.9.3), one can prove

Theorem 5.18.3. *Let $f : X \to Y$ be a morphism of abelian schemes which brings unit element to unit element. Then, f is a group homomorphism.*

Corollary 5.18.4. *Any abelian scheme is commutative.*

Theorem 5.18.5. *Any abelian scheme is **relatively projective**, i.e. if $X \to S$ is an abelian scheme, then we can write $S = \bigcup \operatorname{Spec} A_i$ such that $X_i = X \times_S \operatorname{Spec} A_i$ is projective over A_i.*

Question: Does this imply the pullback of any open affine in S is projective? By like Nike's trick or whatever?

Theorem 5.18.6 (Theorem of cube). *Have $m_I : X \times_S X \times_S X \to X$ as before[89] and $\mathscr{L}$ a line bundle on X. Then,*

$$\bigotimes_{I \subset \{1,2,3\}} (m_I^* \mathscr{L})^{(-1)^{\# I}} \simeq \mathscr{O}_X$$

canonically.

Theorem 5.18.7 (Theorem of square). *Say you have $x \in X(S)$ and $y \in X(S)$. Then,*

$$T_x^* \mathscr{L} \otimes T_y^* \mathscr{L} \simeq T_{x+y}^* \mathscr{L} \otimes \mathscr{L}$$

if $e^* \mathscr{L}$ is trivial.

Definition 5.18.8. A **Rigidified line bundle** $\mathscr{L}$ on X/S is a line bundle equipped with an isomorphism $\mathscr{O}_S \xrightarrow{\sim} e^* \mathscr{L}$. ⋄

Note 16. Since we're working in a commutative setting, the unit section $e : S \to X$ will also be denoted by $0 : S \to X$ and called the zero section. For example, a rigidified line bundle comes equipped with an iso $\mathscr{O}_S \xrightarrow{\sim} 0^* \mathscr{L}$.

Assumption. Unless otherwise state, assume all line bundles are rigidified.

Given a rigidified $\mathscr{L}$ on X, we get a group morphism

$$\begin{array}{rccc} \varphi_{\mathscr{L}} : & X(S) & \longrightarrow & \operatorname{Pic}(X) \\ & x & \longmapsto & T_x^* \mathscr{L} \otimes \mathscr{L}^{-1} \end{array}$$

landing in the subgroup of rigidified line bundles. In fact, for any T, get a map $X(T) \to \operatorname{Pic}(X/T)$. Note that we have an (exact?) sequence

TODO: Come make sense of this

$$\operatorname{Pic}(T) \to \operatorname{Pic}(X) \to \operatorname{Pic}(X/T)$$

[89] $m_\emptyset$ is $X \times_S X \times_S X \to S \to X$

which is split via $\operatorname{Pic}(X) \to \operatorname{Pic}(T)$, $\mathscr{L} \mapsto 0^*\mathscr{L}$. Hence, $\operatorname{Pic}(X) \simeq \operatorname{Pic}(T) \oplus \operatorname{Pic}(X/T)$. The relative Picard group is the rigidified Picard group.

Corollary 5.18.9. *Let X/S be an abelian scheme of relative dimension g. Let n be a natural number. Then the multiplication by n morphism $[n] : X \to X$ is flat, surjective, finite, and of degree n^{2g}; it is étale iff n is inverstibel in $\mathscr{O}_S$. Furthermore, the kernel $X[n] := \ker[n]$ is a finite flat group scheme of degree n^{2g}.*

Remark 5.18.10. Given a homomorphism $f : G \to H$ of group schemes, its kernel is the fiber product

$$\begin{tikzcd} \ker f \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & G \arrow[d, "f"] \\ S \arrow[r, "e"] & H \end{tikzcd} .$$

$\circ$

Definition 5.18.11. A map $f : X \to Y$ of abelian schemes is an **isogeny** if $\ker f$ is finite an f is **surjective** (i.e. f_{top} is surjective on spaces and $f^* : \mathscr{O}_Y \hookrightarrow f_*\mathscr{O}_X$ is injective on sheaves). $\diamond$

Note 17. Got distracted when he was writing the below theorem, so I may not have the statement exactly right.

Theorem 5.18.12. *Let X be an abelian scheme. There exists an abelian scheme $\widehat{X}$ and a line bundle P on $X \times_S \widehat{X}$ such that*

(1) *P is trivial on $0 \times \widehat{X}$ and on $X \times 0$*

(2) *For any S-scheme T and any line bundle $\mathscr{L}$ on $X \times T$ such that*

  - *$\mathscr{L}|_{0\times T}$ is trivial*
  - *For any generic point $t \in T$, $\mathscr{L}|_{X\times\{t\}} \in \operatorname{Pic}^0(X_t)$*

  there is a unique $T \to \widehat{X}$ such that $\mathscr{L} \simeq (1 \times f)^*P$.

The proof of this theorem makes use of quotients by finite group schemes. Other than that, its completely analogous to our earlier result for abelian varieties in characteristic 0.

5.18.2 Quotients by finite group scheme

Let G/S be a finite, flat group scheme, so $G = \mathbf{Spec}_S\, \mathscr{O}(G)$ for $\mathscr{O}(G)$ some *sheaf* on S. To keep things simple, let's assume $S = \operatorname{Spec} R$, so $A = \mathscr{O}(G)$ is simply an R-algebra (as an R-module, it is projective with rank n) and $G = \operatorname{Spec} A$.

Definition 5.18.13. Let G/S be a group scheme and X/S be a scheme. By an action of G on X, we mean a morphism

$$G \times_S X \xrightarrow{\mu} X$$

with usual compatibilities

- $X = S \times_S X \xrightarrow{e\times\mathrm{Id}} G \times X \xrightarrow{\mu} X$ is the identity.

- $$\begin{tikzcd} G \times (G \times X) \arrow[r, "1\times\mu"] \arrow[d, "m\times 1"'] & G \times X \arrow[d, "\mu"] \\ G \times X \arrow[r, "\mu"] & X \end{tikzcd}$$

  commutes.

Equivalently, $G(T) \times X(T) \to X(T)$ is a functorial group action. $\diamond$

Can also define the "orbit" of a subvariety.

Remark 5.18.14. Consider

$$X \xleftarrow{p_2} G \times X \xrightarrow{\mu} X.$$

One has

$$\mu^* \mathscr{O}_X \simeq \mathscr{O}_{G\times X} \simeq p_2^* \mathscr{O}_X.$$

For any G-invariant subscheme $U \subset X$, this gives a map

$$\Gamma(U, \mathscr{O}_X) \longrightarrow \Gamma(U, \mu^* \mathscr{O}_X) \longrightarrow \Gamma(G \times U, \mathscr{O}_{G\times X}) \xleftarrow{p_2^*} \Gamma(U, \mathscr{O}_X)$$

so

$$\Gamma(U, \mathscr{O}_X)^G = \{f \in \Gamma(U, \mathscr{O}_X) : \mu^* f = p_2^* f\}.$$

This is basically saying $f(gx) = f(x)$ for all g. $\circ$

Theorem 5.18.15. *Let G be a finite group scheme acting on a scheme X such that the orbit of any point in X is contained in an affine open subset of X. Then, there is a surjective morphism*

$$\pi : X \to Y$$

which represents the quotient, i.e.

- $\pi_{top} : X_{top} \to Y_{top}$ *is a quotient*
- $\mathscr{O}_Y \xrightarrow{\sim} (\pi_* \mathscr{O}_X)^G$

Moreover, if G acts on X ***freely*** *(i.e. $G \times X \to X \times X, (g, x) \mapsto (gx, x)$ is an embedding), then $\pi : X \to Y$ is flat of degree $n = \operatorname{rank} G$ and $G \times X \simeq X \times_Y X$.*

Remark 5.18.16. When $G = \operatorname{Spec} A$ is finite an $X = \operatorname{Spec} B$ is finite, then an action $G \times X \to X$ corresponds to a morphism $B \to A \times B$ satisfying certain compatibility relations. This perspective let's you study group schemes by working with coordinate rings. $\circ$

Corollary 5.18.17. *If X is a group scheme and G is a normal subgroup of X, then X/G is also a group scheme and is called the* ***quotient group scheme****. Conversely, if $f : X \to Y$ is a flat, surjective (so faithfully flat?) finite degree homomorphism of group schemes, then $Y = X/\ker f$.*

Corollary 5.18.18. *For any abelian scheme X/S, the correspondence*

$$G \mapsto X/G$$

gives a bijection (really, an equivalent of categories) between

$$\left\{ \begin{matrix} \text{finite, flat} \\ \text{subgroups of } X \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{isogenies} \\ X \to Y \end{matrix} \right\}.$$

Theorem 5.18.19. *Suppose G acts freely on X. If $\mathscr{F}$ is a coherent sheaf on $Y = X/G$, then $\mathscr{G} := \pi^*\mathscr{F}$ has a natural action by G, i.e. $\alpha : p_2^*\mathscr{G} \xrightarrow{\sim} \mu^*\mathscr{G}$.*[90] *Furthermore, the correspondence*

$$\mathscr{F} \rightsquigarrow \pi^*\mathscr{F}$$

is an equivalence of categories $\mathrm{Coh}(Y) \to \mathrm{Coh}_G(X)$.

Corollary 5.18.20. *Assuming further than X/S is proper. Then,*

$$\ker(f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)) \simeq \mathrm{Hom}_S(G, \mathbb{G}_m).$$

If G is a finite, flat commutative group scheme over S, then their is a dual group scheme $\widehat{G}$ along with a morphism $G \times \widehat{G} \to \mathbb{G}_m$ such that, for any S-scheme T,

$$\mathrm{Hom}_T(G_T, \mathbb{G}_{m,T}) = \widehat{G}(T).$$

Construction 5.18.21. Suppose $S = \operatorname{Spec} R$ and $G = \operatorname{Spec} A$. Then, A is a Hopf algebra (comultiplication coming from multiplication on G). Note that $A^\vee = \mathrm{Hom}_R(A, R)$ is also a Hopf-algebra, so $\widehat{G} = \operatorname{Spec} \widehat{A}$ is a group scheme. Next time we'll show that this is the dual group.

5.19 Lecture 19

For simplicity $S = \operatorname{Spec} R$ affine. Let G/S be an affine group scheme, so $G = \operatorname{Spec} A$ for A an R-algebra. We have multiplication $m : G \times_S G \to G$ as well as a unit $e : S \to G$ and inverse $\iota : G \to G$. In terms of the algebra, these become

$$m^* : A \otimes_R A \leftarrow A, \;\; e^* : R \leftarrow A, \;\; \text{and} \;\; \iota^* : A \leftarrow A.$$

If you think of A as being functions on G (so $A \otimes_R A$ is functions on $G \times_S G$), then you can think of this as $(m^* f)(gh) = f(gh)$, $e^* f = f(e)$ and $(\iota^* f)(g) = f(g^{-1})$. The maps m^*, e^* turn A into an R-coalgebra.

Write $A^\vee = \mathrm{Hom}_R(A, R)$. We get $m^\vee : A^\vee \otimes A^\vee \to A^\vee$ turning $A^\vee$ into an R-algebra. If we assume that A/R is flat of finite rank, then $(A^\vee)^\vee = A$, so A and $A^\vee$ hold the same information when G is a finite flat group scheme over S.

When G is a finite flat group scheme, both $(A, A^\vee)$ have R-algebra structures. Furthermore, one can form the **Carter dual** $\widehat{G}$ associated to $(A^\vee, A)$, i.e. we reverse the role of A and $A^\vee$.

---

[90] This is coming from the commutative square (which is even Cartesian)

$$\begin{tikzcd} G \times X \arrow[r, "\mu"] \arrow[d, "p_2"'] & X \arrow[d] \\ X \arrow[r] & Y \end{tikzcd}$$

Theorem 5.19.1. *Let G be a finite, flat commutative group scheme. $\widehat{G}$ is a finite group scheme which represented the functor of characters*

$$\widehat{G}(T) = \mathrm{Hom}(G_T, \mathbb{G}_{m,T}).$$

(maybe we'll just prove this when when $T = \operatorname{Spec} B$?)

Example. $R = \mathbb{C}$ and $G =$ finite, abelian group. Then, $G = \operatorname{Spec} C(G, \mathbb{C})$ and $\widehat{G} =$ space of characters. By Fourier transform, we have $C(G, \mathbb{C}) = \sum_{\chi \in \widehat{G}} \mathbb{C}\chi$ or something like this. We also have $\widehat{G} = \operatorname{Spec} C(\widehat{G}, \mathbb{C})$. Note there's a canonical pairing $C(\widehat{\widehat{G}}, \mathbb{C}) \times C(G, \mathbb{C}) \to \mathbb{C}$. Given $f_1 \in C(\widehat{G}, \mathbb{C})$ and $f_2 = \sum a_\chi \chi$ ($a_\chi \in \mathbb{C}$), we set $\langle f_1, f_2 \rangle = \sum a_\chi f(\chi)$. △

Example. Take $G = \mathbb{Z}/n\mathbb{Z} = \operatorname{Spec} \underbrace{\bigoplus_{x \in G} R\delta_x}_{\mathscr{O}(G)}$ where

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{otherwise.} \end{cases}.$$

Note that $\mathrm{Hom}(\mathscr{O}(G), R) = \bigoplus_{x \in G} R\delta_x^*$ where

$$\langle \delta_x^*, \delta_y \rangle = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases}.$$

We want(ed) to get $\widehat{\mathbb{Z}/n\mathbb{Z}} = \mu_n := \operatorname{Spec}(R[T]/(T^n - 1))$. △

Now let's prove the theorem.

Proof of theorem 5.19.1. For any R-algebra B, we want so show that

$$\mathrm{Hom}_{B-\mathrm{group}}(G_B, \mathbb{G}_{m,B}) = \widehat{G}(B)$$

where $\widehat{G} = \operatorname{Spec} A^\vee$ (and $G = \operatorname{Spec} A$). The RHS above is

$$\mathrm{Hom}_{R-\mathrm{alg}}(A^\vee, B) \subset \mathrm{Hom}_{R-\mathrm{mod}}(A^\vee, B) = \mathrm{Hom}_{R-\mathrm{mod}}(R, A \otimes B) = A \otimes B$$

since A is a locally free R-module. Given $\varphi \in \mathrm{Hom}_{R-\mathrm{alg}}(A^\vee, B)$, let $\chi \in A \otimes B$ be the corresponding element representing it, so $\varphi(a^\vee) = \langle \chi, a^\vee \rangle$. Since φ is an algebra homomorphism, we have $\varphi(a^\vee b^\vee) = \varphi(a^\vee)\varphi(b^\vee)$ and $\varphi(r) = r$ for $r \in R$. In terms of χ, this forces χ to be a character (i.e. $m^*\chi = \chi \otimes \chi$) and to be invertible (i.e. $\chi \in (A \otimes_R B)^\times$).

We about the LHS? This is

$$\mathrm{Hom}_{B-\mathrm{group}}(G_B, \mathbb{G}_{m,G}) = \mathrm{Hom}_{B-\mathrm{bialgebra}}(B[T, T^{-1}], A \otimes B).$$

Note that $m^*T = T \otimes T$. Note that, for $\psi \in \mathrm{Hom}_{B-\mathrm{bialgebra}}(B[T, T^{-1}], A \otimes B)$, $T \mapsto \psi(T) \in (A \otimes_R B)^\times$ since its inverse is $\psi(T^{-1})$. This finishes the proof. ■

Definition 5.19.2. A homomorphism of abelian schemes $f : X \to Y$ is called an **isogeny** if it is surjective with finite kernel. $\diamond$

Recall 5.19.3. For any abelian scheme X/S, the correspondence

$$G \mapsto X/G$$

gives a bijection (really, an equivalent of categories) between

$$\left\{ \begin{matrix} \text{finite, flat} \\ \text{subgroups of } X \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{isogenies} \\ X \to Y \end{matrix} \right\}.$$

$\odot$

Theorem 5.19.4. *Let f be an isogeny between abelian schemes. The induced $f_T^* : \operatorname{Pic}(Y_T) \to \operatorname{Pic}(X_T)$ for any S-scheme T satisfies*

$$(\ker f_T^*) \simeq \widehat{G}(T)$$

where $G := \ker f$.

We can now construct the dual abelian scheme. Let X/S be an abelian scheme over S. Let $\mathscr{L}$ be a rigidified ample line bundle, so comes equipped with $\mathscr{L}|_0 = \mathscr{O}_S$. Recall $K_{\mathscr{L}}(T) = \ker(X(T) \to \operatorname{Pic} X_T)$ with the map $x \mapsto T_x^* \mathscr{L}_T \otimes \mathscr{L}_T^{-1}$. This $K_{\mathscr{L}}$ is represented by a subgroup scheme of X. Set

$$\mathscr{L}_{X^2} = m^* \mathscr{L} \otimes p_1^* \mathscr{L}^{-1} \otimes p_2^* \mathscr{L}^{-1}$$

where $X^2 = X \times_S X$. Then, $K_{\mathscr{L}}$ is the maximal subscheme of X such that $\mathscr{L}_{X^2}|_{X \times K_{\mathscr{L}}}$ is trivial (think back to seesaw lemma). So we can and do define $\widehat{X} = X/K_{\mathscr{L}}$ with Poincaré bundle $\wp$ the quotient of $\mathscr{L}_{X^2}$, i.e. it fits into

$$\begin{array}{ccc} \mathscr{L}_{X^2} & \longrightarrow & \wp \\ \big\downarrow & & \big\downarrow \\ X \times X & \longrightarrow & X \times \widehat{X} \end{array}$$

Then one can show that $(\widehat{X}, \wp)$ satisfies the universal property for dual abelian scheme. We now get the following

- Let $f : X \to Y$ be any morphism (not necessarily an isogeny). Then you get a dual morphism $\widehat{f} : \widehat{Y} \to \widehat{X}$.
- If f is an isogeny, then $\ker f$ and $\ker f^\vee$ are Cartier dual to each other.
- $\widehat{\widehat{X}} = X$.

Application (Poincaré complete reducibility). Let $Y \hookrightarrow X$ be an abelian subscheme, then there exists an abelian subscheme $Z \hookrightarrow X$ such that

$$Y + Z = X \text{ and } Y \cap Z = \text{finite}.$$

Let $\mathscr{L}$ be ample on X. Consider the square

$$\begin{tikzcd} Y \arrow[r, hook, "i"] \arrow[d, "\varphi_{\mathscr{L}|_Y}"] & X \arrow[d, "\varphi_{\mathscr{L}}"] \\ \widehat{Y} & \widehat{X} \arrow[l, "i^\vee"] \end{tikzcd}$$

Take $Z = \ker(\widehat{i} \circ \varphi_{\mathscr{L}})^\circ$.

Remark 5.19.5. The above is easy over $\mathbb{C}$. We have $X = V/\Lambda$ and a Riemann form h Hermitian on V with restriction $\operatorname{Im} h : \Lambda \times \Lambda \to \mathbb{Z}$. Given $Y \hookrightarrow X$, we write $Y = V_1/\Lambda_1$ with $V_1 \subset V$ and $\Lambda_1 = V_1 \cap \Lambda$. We can take

$$V_2 = V_1^\perp \text{ and } \Lambda_2 = V_2 \cap \Lambda.$$

$\circ$

5.19.1 Tate module

Let's first return to the geometric case, $S = \operatorname{Spec} k$ and $k = \overline{k}$. Choose a prime $\ell \neq \operatorname{char} k$, and consider X/k an abelian variety. We have shown previously that

$$X[\ell^n] = \ker\left([\ell^n] : X \to X\right) \simeq \left(\frac{\frac{1}{\ell^n}\mathbb{Z}}{\mathbb{Z}}\right)^{2g}.$$

Furthermore, we have the inclusion $X[\ell^n] \hookrightarrow X[\ell^{n+1}]$ as well the the multiplication by ℓ map $X[\ell^n] \leftarrow X[\ell^{n+1}]$. Hence, we can form two groups:

$$T_\ell(X) := \varprojlim X[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$$

and

$$V_\ell(X) := \varinjlim X[\ell^n] \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}.$$

In fact, $X[\ell^n] \simeq \frac{1}{\ell^n} T_\ell(X)/T_\ell(X)$ from which we see that

$$V_\ell(X) \simeq T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell / T_\ell(X).$$

If $\widehat{X}$ is the dual abelian variety, we have a natural pairing

$$X[n] \times \widehat{X}[n] \to \mu_n$$

(recall that they are Cartier dual). Taking limits, we get

$$T_\ell(X) \times T_\ell(\widehat{X}) \to \varprojlim \mu_{\ell^n} =: \mathbb{Z}_\ell(1).$$

Remark 5.19.6. Over $\mathbb{C}$, we have $X = V/\Lambda$ with dual space $\widehat{X} = \widehat{V}/\widehat{\Lambda}$ where $\widehat{V} = \operatorname{Hom}_{\text{Hermitian}}(V, \mathbb{C})$ and

$$\widehat{\Lambda} = \left\{\ell \in \widehat{V} : \operatorname{Im} \ell|_\Lambda \subset \mathbb{Z}\right\}.$$

We have $H : V \times \widehat{V} \to \mathbb{C}$ and $E = \operatorname{Im} H : \Lambda \times \widehat{\Lambda} \to \mathbb{Z}$. For Weil pairing, we get

$$\ell^n \cdot E : \frac{1}{\ell^n}\Lambda \times \frac{1}{\ell^n}\widehat{\Lambda} \to \frac{1}{\ell^n}\mathbb{Z} \xrightarrow{\sim} \mu_{\ell^n}$$

with the last map being $\exp(2\pi i(blah))$. Taking the projective limit, we get

$$\underbrace{(\Lambda \otimes \mathbb{Z}_\ell)}_{T_\ell(X)} \otimes \underbrace{(\widehat{\Lambda} \otimes \mathbb{Z}_\ell)}_{T_\ell(\widehat{X})} \longrightarrow \mathbb{Z}_\ell(1).$$

We starting in the beginning with $\Lambda \times \Lambda \to \mathbb{Z}_\ell$. Morally, we just tensored with with $\mathbb{Z}_\ell$ and then mapped $\mathbb{Z}_\ell \to \mathbb{Z}_\ell(1)$ using the canonical element $\zeta = \varprojlim e^{2\pi i/\ell^n} \in \mathbb{Z}_\ell(1)$. ◦

Polarization Let X/k be an abelian variety. A **polarization** $\varphi : X \to \widehat{X}$ is an isogeny which is self-dual.

Remark 5.19.7. When $k = \mathbb{C}$, this means we have $V/\Lambda \xrightarrow{\varphi} \widehat{V}/\widehat{\Lambda}$. With no conditions, this is just saying $\varphi : V \to \widehat{V}$ with $\varphi(\Lambda) \subset \widehat{\Lambda}$, so we have

$$H : V \times V \to \mathbb{C}.$$

To say φ is an isogeny is to say that $H(ax, by) = a\bar{b}H(x, y)$ with $\operatorname{Im} H(\Lambda \times \widehat{\Lambda}) \subset \mathbb{Z}$. To say that φ is a polarization is to add that $\overline{H(x, y)} = H(y, x)$. ◦

For a polarization $\varphi : X \to \widehat{X}$, we get

$$T_\ell(X) \times T_\ell(X) \longrightarrow T_\ell(X) \times T_\ell(\widehat{X}) \longrightarrow \mathbb{Z}_\ell(1).$$

This is an alternating form.

Next time

- moduli interpretation of $\mathcal{A}_{g,n}$ as abelian scheme over $\mathbb{Q}$ with level n structure ("adelic setting"?)
- Endomorphisms
- Shimura varieties of PEL-type

We ended the lecture by checking the status of the election. Biden at 253 and Trump at 214 according to the New York Times. Need 270 to win. Senators at 46 democrat (+ 2 third-party) and 48 republicans. Democrats are leading in the house 208 (or 209? Can't remember which) to 190 (218 for majority).

5.20 Lecture 20 (11/10)

5.20.1 Siegal modular space as a moduli space over number fields

We want a more scheme-theoretic interpretation of $\mathcal{A}_{g,n}$.

Let S be a scheme, let N be a positive integer, invertible on S (i.e. $N \in \Gamma(S, \mathscr{O}_S)^\times$). Let $\mathcal{A}(S)$ be the set of isomorphisms classes of triples (X, φ, η) where

- X is an abelian scheme$/S$ of relative dimension g.
- $\varphi : X \xrightarrow{\sim} \widehat{X}$ is a symmetric isomorphism, i.e. a **principal polarization**. May sometimes accidentally write λ instead of φ

- η is a symplectic simultude (?)
$$\eta : \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^{2n} \xrightarrow{\sim} X[N].$$

Recall 5.20.1. For $f : X \to Y$ isogeny of abelian varieties, we get a perfect pairing

$$\ker f \times \ker \widehat{f} \to \mathbb{G}_m$$

of group schemes. $\odot$

Example. Consider $f = [N] : X \to X$ whose dual morphism is $\widehat{f} = [N] : \widehat{X} \to \widehat{X}$. Hence, we get a pairing
$$\ker[N]_X \times \ker[N]_{\widehat{X}} \to \mathbb{G}_m.$$

Since N is invertible in S, these are actually "étale groups" of rank N^{2g}. Since they have finite order, can write this as
$$\ker[N]_X \times \ker[N]_{\widehat{X}} \to \mu_N.$$

If $\varphi : X \to \widehat{X}$, this gives a pairing $X[N] \times X[N] \to \mu_N$ which is alternating. Note that the geometric points of μ_N are iso to $\mathbb{Z}/N\mathbb{Z}$. $\triangle$

From the above example, we have two symplectic (alternating) pairings

$$X[N] \times X[N] \longrightarrow \mu_N \text{ and } (\mathbb{Z}/N\mathbb{Z})^{2g} \times (\mathbb{Z}/N\mathbb{Z})^{2g} \longrightarrow \mathbb{Z}/N\mathbb{Z}.$$

We require η to satisfy $\langle \eta x, \eta y\rangle = \zeta \langle x, y\rangle$ for some fixed generator $\eta \in \mu_N$.

Remark 5.20.2. *Got distracted* .... $\mu_N \subset \Gamma(S, \mathscr{O}_S)$ since $\zeta \in \Gamma(S, \mathscr{O}_S)$ and is a generator. $\circ$

We just defined a functor $\mathcal{A}_\zeta : \mathrm{Sch}/\mathbb{Z}\left[\frac{1}{N}, \mu_N\right] \longrightarrow \mathrm{Set}$. We can combine these into one functor $\mathcal{A} = \bigsqcup_\zeta \mathcal{A}_\zeta$ where ζ ranges over generators of μ_N.

Theorem 5.20.3.

(1) For $N \geq 3$, $\mathcal{A}$ is represented by a quasi-projective scheme over $\mathbb{Z}\left[\frac{1}{N}, \mu_N\right]$.

(2) For any ζ, consider
$$\begin{array}{ccc} \mathbb{Z}[1/N, \mu_N] & \longrightarrow & \mathbb{C} \\ \zeta & \longmapsto & e^{2\pi i/N}. \end{array}$$

Then, the base change
$$A_\zeta(\mathbb{C}) \simeq \mathcal{A}_{g,N} = \Gamma(N)\backslash\mathfrak{h}_g$$

is the Siegal modular space.

This theorem is due to Mumford, and the proof uses GIT (geometric invariant theory).

Over complex $\mathbb{C} \supset \mathbb{Z}$, $\zeta = e^{2\pi i/N}$, we have $\mathcal{A}(\mathbb{C}) = \{(X, \varphi, \eta)\}$. These can be put in the form $S \simeq \mathbb{C}^g/(\mathbb{Z}^g\tau + \mathbb{Z}^g)$ $(= V/\Lambda)$, $\widehat{X} = \widehat{V}/\widehat{\Lambda}$, $V \times \widehat{V} \xrightarrow{h} \mathbb{C}$ s.t. $\operatorname{Im} h : \Lambda \times \widehat{\Lambda} \to \mathbb{Z}$ is perfect. IIRC, $h = (\operatorname{Im}\tau)^{-1}$. Furthermore, $X[N] = \left(\mathbb{Z}^g\frac{1}{n}\tau + \mathbb{Z}^g\frac{1}{N}\right)/(\mathbb{Z}^g\tau + \mathbb{Z}^g)$ with pairing

$$X[N] \times X[N] \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow \mu_N$$

sending $(x, y) \mapsto \exp(2\pi i N \operatorname{Im} h(xy))$ (with $x, y \in \mathbb{C}^g$?). The level structure is the bottom map in the diagram

$$\begin{tikzcd} \mathbb{Z}^{2g} \arrow[r, "\sim"] \arrow[d] & \Lambda \arrow[d] \\ (\mathbb{Z}/N\mathbb{Z})^{2g} \arrow[r, "\sim"] & X[N] \end{tikzcd},$$

i.e. any level structure can be lifted to $\mathbb{Z}^{2g}$. This lift is unique up to $\Gamma(N)$, so $\mathcal{A}_\zeta(\mathbb{C}) \simeq \Gamma(N)\backslash\mathfrak{H}_g$.

Corollary 5.20.4. *$\mathcal{A}_{g,n}$ is defined over $\mathbb{Q}(\zeta_N)$ and the disjoint union $\mathcal{A}$ is defined over $\mathbb{Q}$.*

Since $\mathbb{Q}(\zeta_N)$ is a $\mathbb{Q}$-scheme, can view $\mathcal{A}_{g,n}$ as a scheme over $\mathbb{Q}$, but it is no long connected. In particular, $\mathcal{A}_{g,n} \times_{\mathbb{Q}} \mathbb{C} = \bigsqcup_\zeta \mathcal{A}_\zeta(\mathbb{C})$.

Remark 5.20.5. For $N \le 3$ (i.e. $N = 1, 2$), $\mathcal{A}_{g,N}$ still has a model defined on $\mathbb{Q}(\zeta_{1,2}) = \mathbb{Q}$, but it is a *coarse* moduli space.

- If $X/S \in \mathcal{A}(S)$, then get $S \to \mathcal{A}_{g,n}$
- For geometric points $x \in \mathcal{A}_{g,n}$, have $\mathcal{A}_x \in \mathcal{A}(k)$.

○

5.20.2 Adelic perspective

This will allegedly make the picture easier.

Start with $\mathbb{Z}^{2g}$ along with its standard symplectic (alternating) structure $\langle -, - \rangle$. We define a group scheme GSp_{2g} over $\mathbb{Z}$ s.t. $\mathrm{GSp}_{2g} \hookrightarrow \mathrm{GL}_{2g} \times \mathrm{GL}_1$ via

$$\mathrm{GSp}_{2g}(R) = \left\{ (\gamma, \lambda) \in \mathrm{GL}_{2g}(R) \times \mathrm{GL}_1(R) : \gamma^t \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \gamma = \lambda \begin{pmatrix} 0 & I_g \\ -I & 0 \end{pmatrix} \right\}$$

In other words,

$$\mathrm{GSp}_{2g}(R) = \left\{ \gamma : R^{2g} \xrightarrow{\sim} R^{2g} : \langle \gamma x, \gamma y \rangle = \lambda \langle x, y \rangle \text{ for some } \lambda \in R^\times \text{ for all } x, y \in R^{2g} \right\}.$$

Let's define $\mathcal{A}'_N$, a new moduli problem (slash scheme over $\mathbb{Z}[1/N]$). It is given by $\mathcal{A}'_N(S) = \{(X, \varphi, \eta)\}$ such that

- X is an abelian scheme over S
- $\varphi : X \to \widehat{X}$ is a (potentially non-principle) polarization of degree prime to N
- $\eta = (\eta_\ell)_{\ell | N}$ is a collection of isomorphisms

$$\eta_\ell : \mathbb{Q}_\ell^{2g} \xrightarrow{\sim} T_\ell(X) \otimes \mathbb{Q},$$

each a symplectic simultudes modulo $K_\ell(N) = \ker\left(\mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell/N)\right)$.

Note 100% sure about this condition. See Mumford, I guess? This might not be Mumford, haven't checked.

A morphism $f : (X, \varphi, \eta) \to (X', \varphi', \eta')$ is a homomorphism $f : X \to X'$ such that

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi'} \\ \widehat{X} & \xleftarrow[\widehat{f}]{} & \widehat{X}' \end{array}$$

commutes up to a scale, i.e.

$$A(\varphi' \circ f) = B(\widehat{f} \circ \varphi)$$

for some $A, B \in \mathbb{Z}_{>0}$. We also want this to be compatible with the level structure.

Theorem 5.20.6. $\mathcal{A} \simeq \mathcal{A}'$

Proof. Given $(X, \varphi, \eta) \in \mathcal{A}(S)$ (so $\eta : (\mathbb{Z}/N\mathbb{Z})^{2g} \to X[N]$), can lift η to a map $\varprojlim_{\ell | N} \mathbb{Z}_\ell^{2g} \to T_\ell(X)$. We then tensor with $\mathbb{Q}$ to get $\prod_{\ell | N} \mathbb{Q}_\ell^{2g} \to V_\ell(X) = \mathbb{T}_\ell(X) \otimes \mathbb{Q}$. This gives an element of $\mathcal{A}(S')$.

Starting with $(X', \varphi', \eta') \in \mathcal{A}'(S)$, we can look at

$$\mathbb{Z}_\ell^{2g} \hookrightarrow \mathbb{Q}_\ell^{2g} \xrightarrow{\eta'_\ell} T_\ell(X') \otimes \mathbb{Q}_\ell.$$

Roughly, this gives a lattice in $V_\ell(X')$ and can use this to construct an abelian variety quasi-iso (?) to X such that this lattice is exactly $T_\ell(X)$. Get $(X, \varphi, \eta) \in \mathcal{A}(S)$. ■

Let's introduce the adeles. We write $\widehat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z} = \prod_\ell \mathbb{Z}_\ell$, and write

$$\widehat{\mathbb{Q}} = \mathbb{Q} \otimes \widehat{\mathbb{Z}} = \prod_\ell{}' \mathbb{Q}_\ell = \left\{ (x_\ell) \in \prod_\ell \mathbb{Q}_\ell : x_\ell \in \mathbb{Z}_\ell \text{ for all but finitely many } \ell \right\}.$$

This is a $\mathbb{Q}$-algebra, so it makes sense to talk about $\mathrm{GSp}_{2g}(\widehat{\mathbb{Q}})$, which is a topological group; it has $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ as an open, compact subgroup. We define

$$K(N) := \ker\left(\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\right).$$

Theorem 5.20.7. $\mathcal{A}_N(\mathbb{C}) \simeq \mathrm{GSp}_{2g}(\mathbb{Q}) \Big\backslash \mathfrak{H}_g \times \left(\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})/K(N)\right)$

Proof. $(X, \varphi, \eta) \in \mathcal{A}_N(\mathbb{C})$ with $X = V/\Lambda$, φ a Hermitian form on V, and $\eta : \widehat{\mathbb{Q}}^{2g} \to \widehat{\Lambda} \otimes \mathbb{Q}_\ell$ a symplectic similitude modulo $K(N)$. Choose $\alpha : \Lambda \otimes \mathbb{Q} \simeq \mathbb{Q}^{2g}$, a symplectic simultude, which is unique up to replacing it with $\gamma \cdot \alpha$ (with $\gamma \in \mathrm{GSp}_{2g}(\mathbb{Q})$). Now we can consider

$$\mathcal{A}_N(\mathbb{C}) = \mathrm{GSp}_{2g}(\mathbb{Q}) \backslash \{(X, \varphi, \eta, \alpha)\}.$$

Given $(X, \varphi, \eta, \alpha)$, we do/consider the following

- $\alpha^{-1} : \mathbb{Q}^{2g} \to V$ gives some $\tau \in \mathfrak{H}_g$ via

$$\alpha^{-1}\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \tau v \\ v \end{pmatrix}.$$

- Have $\widehat{\mathbb{Q}}^{2g} \xrightarrow{\eta} \widehat{\Lambda} \otimes \mathbb{Q}_\ell \xrightarrow{\widehat{\alpha}} \widehat{\mathbb{Q}}^{2g}$ which gives some $x \in \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}})$ unique up to right multiplication by $K(N)$.

In summary, we see that $(X, \varphi, \eta, \alpha)$ is actually bijective to $\mathcal{A}_g \times \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}})$ which then gives the theorem. ■

We get that $\mathcal{A}_{g,N}/\mathbb{Q}$ (not over $\mathbb{Q}(\zeta_N)$) is equal to the double coset space

$$\mathcal{A}_{g,N} \times_{\mathbb{Q}} \mathbb{C} = \mathrm{GSp}_{2g}(\mathbb{Q}) \Big\backslash \mathfrak{H}_g \times \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}}) \Big/ K(N).$$

when basechanged to $\mathbb{C}$ or when looking at its $\mathbb{C}$-points or whatever. This is useful since the RHS "$\mathrm{GSp}_{2g}(\widehat{\mathbb{Q}})/K(N)$" has many automorphisms, so has many Hecke operators.

Hecke correspondences For any $x \in \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}})$, can consider the double coset

$$K(N)xK(N) = \bigsqcup x_i K(N).$$

Then can define the **Hecke operator** $T_{x,N} : \mathcal{A}_{g,N,\mathbb{Q}}(\mathbb{C}) \to \mathcal{A}_{g,N,\mathbb{Q}}(\mathbb{C})$ via

$$T_{x,N} : [\tau, y] \mapsto \sum_{i=1}^{N} [\tau, y x_i].$$

Let $f : \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}}) \to \mathbb{Q}$ be "continuous" (really, with compact support, a Schwartz-Bruhat function or whatever they're called), i.e. $f = \sum c_i \mathbf{1}_{K(N)x_iK(N)}$, can define $T_f = \sum c_i T_{x_i}$. Note that $T_{f_1} \cdot T_{f_2} = T_{f_1 * f_2}$ (where $*$ is convolution or something?). Can take the projective limit

$$\varprojlim_N \mathcal{A}_{g,N,\mathbb{Q}} = \text{“}\, \mathrm{GSp}_{2g}(\mathbb{Q}) \Big\backslash \mathfrak{H}_g \times \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}}) \,\text{”}$$

which is like an algebraic universal cover of $\mathcal{A}_{g,N}$. We can write this as

$$\mathfrak{H}_g \times \overline{\mathrm{GSp}_{2g}(\mathbb{Q})} \backslash \text{“}\mathrm{GSp}_{2g}(\widehat{\mathbb{Q}})\text{”} = \mathfrak{H}_g \times \mathbb{Q}_+^\times \backslash \widehat{\mathbb{Q}}^\times = \mathfrak{H}_g \times \widehat{\mathbb{Z}}^\times$$

(what?), where the first equality comes from applying det, and the second equality is because $\mathbb{Q}$ has class number 1 (gives nice decomposition of ideles over $\mathbb{Q}$). Note that $\widehat{\mathbb{Z}}^\times = \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ from CFT, so the algebraic universal cover is just $\mathfrak{H}_g \times \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$? Note that $\varprojlim_N \mathrm{Spec}(\mathbb{Q}(\mu_N)) \simeq \widehat{\mathbb{Z}}^\times$.

The adelic description is due to Deligne?

Next time we talk about the endomorphism algebra of abelian varieties, and then we talked about Shimura varieties of PEL-type. Today, we talked about Shimura varities of type PL.

5.21 Lecture 21 (11/12)

Let's summarize a little bit about what's been going on. For the last week, we talked about the Cartier dual group scheme. We then used this to construct dual abelian schemes. This was an anti-involution

$X \mapsto \widehat{X}$ on the category Ab/S of abelian S-schemes (S some fixed base scheme). This gives

$$\begin{array}{ccc} \mathrm{Hom}(X,Y) & \longrightarrow & \mathrm{Hom}(\widehat{Y},\widehat{X}) \\ f & \longmapsto & \widehat{f} \end{array}$$

which is actually additive. We didn't show this before, so let's show it now

Proof. Say $f_1, f_2 \in \mathrm{Hom}(X,Y)$. Then, $f_1 + f_2$ is the composition

$$f_1 + f_2 : X \xrightarrow{\Delta} X \times X \xrightarrow{f_1 \times f_2} Y \times Y \xrightarrow{m} Y.$$

Its dual is

$$\widehat{f_1 + f_2} : \widehat{X} \xleftarrow{\widehat{\Delta}} \widehat{X} \times \widehat{X} \xleftarrow{\widehat{f}_1 \times \widehat{f}_2} \widehat{Y} \times \widehat{Y} \xleftarrow{\widehat{m}} \widehat{Y}.$$

Thus, it order to show $\widehat{f_1 + f_2} = \widehat{f}_1 + \widehat{f}_2$, one only need show that $\widehat{\Delta} = m$ and $\widehat{m} = \Delta$. This follows from the theorem of the square. ∎

One consequence is **Poincaré complete reducibility**, any abelian variety A is isogenous to a completely reducible variety

$$A \sim X_1^{n_1} \times X_2^{n_2} \times \ldots \times X_r^{n_r}$$

with X_i a *simple abelian variety*, i.e. has no proper abelian subvariety. Note that, with A as above,

$$\mathrm{End}(A) \otimes \mathbb{Q} \simeq \bigoplus_i M_{n_i}(\mathrm{End}_{\mathbb{Q}}(X_i)).$$

Since X_i is simple, one has that $\mathrm{End}(X_i) \otimes \mathbb{Q}$ is a division algebra over $\mathbb{Q}$.

Recall the Siegal modular space $\mathcal{A}_{g,N}(\mathbb{C}) = \Gamma(N) \backslash \mathfrak{H}_g$ with $\Gamma(N) = \ker(\mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z}))$. We have shown that this is a complex manifold, is quasi-projective (using modular forms), and we discussed the Satake compactification which is the closure of the embedding given by modular forms. Last time we mentioned that this guy has a modular interpretation. It can be realized as a scheme $\mathcal{A}_{g,N}/\mathbb{Z}[1/N, \zeta_N]$ with ζ_N a primitive Nth root of unity. For any $\mathbb{Z}[1/N, \zeta_N]$-scheme S, $\mathcal{A}_{g,N}(S)$ is the set of isomorphism classes of triples

$$\left(X, \varphi : X \to \widehat{X}, \eta : \pmod{\mathbb{Z}} N\mathbb{Z}^{2g} \xrightarrow{\sim} X[N]\right)$$

with φ a polarization and η is **ζ-symplectic**. We have a pairing

The word from last time was actually 'similitude'.

$$X[N] \times X[N] \xrightarrow{e_N} \mu_N = \mathbb{Z}/N\mathbb{Z} \cdot \zeta$$

and we require

ψ_N the standard symplectic form on $(\mathbb{Z}/N\mathbb{Z})^{2g}$

$$e_N(\eta\alpha, \eta\beta) = \zeta \cdot \psi_N(\alpha, \beta).$$

Theorem 5.21.1 (Mumford)**.** *Fix $N \geq 3$. Then, $\mathcal{A}_{g,N}$ is represented by a quasi-projective scheme over $\mathbb{Z}[1/N, \zeta_N]$. Moreover, given $\tau_0 : \mathbb{Z}[1/N, \zeta_N] \to \mathbb{C}, \zeta_N \mapsto \exp(2\pi i/N)$, one has $\mathcal{A}_{g,N} \otimes_{\tau_0} \mathbb{C} \simeq \Gamma(N) \backslash \mathfrak{H}_g$.*

Question 5.21.2. *What about other embeddings in place of τ_0? You can consider $\tau_a : \zeta_N \mapsto \exp(2\pi i a/N)$ with $(a, N) = 1$. This gives another complex manifold $\mathcal{A}_{g,N} \otimes_{\tau_a} \mathbb{C} =: \mathcal{A}_{g,N,a}$; how does it relate to $\Gamma(N) \backslash \mathfrak{H}_g$?*

Let $\mathcal{A}'_{g,N}$ be $\mathcal{A}_{g,N}$ as a $\mathbb{Z}[1/N]$-scheme. Then,

$$\mathcal{A}'_{g,N} \otimes_{\mathbb{Q}} \mathbb{C} = \bigsqcup_{(a,N)=1} \mathcal{A}_{g,N,a}.$$

When looking at adeles last time, we got the nice description

$$\mathcal{A}'_{g,N} \otimes_{\mathbb{Q}} \mathbb{C} = \mathrm{GSp}_{2g}(\mathbb{Q}) \Big\backslash \mathfrak{H}_g^{\pm} \times \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}}) \Big/ K(N).$$

Recall $\mathrm{GSp}_{2g}/\mathbb{Z}$ is a group scheme with

$$\mathrm{GSp}_{2g}(R) = \left\{ \gamma \in \mathrm{GL}_{2g}(R) : \gamma^t \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \gamma = \lambda \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \text{ for some } \lambda \in R^{\times} 0 \right\}.$$

When $g = 1$, we get $\mathrm{GSp}_2 = \mathrm{GL}_2$. Also recall that

$$K(N) = \ker\left(\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\right).$$

The RHS $\mathrm{GSp}_{2g}(\mathbb{Q}) \Big\backslash \mathfrak{H}_g^{\pm} \times \mathrm{GSp}_{2g}(\widehat{\mathbb{Q}}) \Big/ K(N)$ above is what's usually called a *Shimura variety* (assuming I heard Shou-wu correctly[91]). This still has a moduli interpretation.

Over $S = \mathbb{C}$, the moduli problem is easy to describe. We want to represent the functors spitting out triples (X, φ, η) with

- X an abelian scheme
- $\varphi : X \to \widehat{X}$ (principal polarization) modulo $\mathbb{Q}_+^{\times}$ (?)
- $\eta : \widehat{\mathbb{Q}}^{2g} \xrightarrow{\sim} \mathrm{H}_1(X, \widehat{\mathbb{Q}})$ modulo $K(N)$.

The equivalence is defined by isogeny. Given $(X_i, \varphi_i, \eta_i) \in \mathcal{A}'$, $i = 1, 2$, we want $X_1 \xrightarrow{f} X_2$ a **quasi-isogeny** (i.e. $f \in \mathrm{Hom}(X_1, X_2) \otimes \mathbb{Q}$, so Nf =isogeny for some N) with

$$\begin{tikzcd} \widehat{\mathbb{Q}}^{2g} \arrow[r, "\eta_1"] \arrow[dr, "\eta_2"'] & \mathrm{H}_1(X_1, \widehat{\mathbb{Q}}) \arrow[d, "f_*"] \\ & \mathrm{H}_1(X_2, \widehat{\mathbb{Q}}) \end{tikzcd}$$

commuting. Can define Hecke operators.

5.21.1 Tate modules as the first homology group

Remark 5.21.3. When working over $\mathbb{C}$, abelian varieties are $\mathbb{C}^g$ modulo some lattice. This lattice is given by their first homology group, so when looking at maps between $\mathbb{C}$-abelian varieties, you really only need to understand what happens to their H_1. We'd like something similar in general.

This is (related to) "Torelli theorems" or something like that, I think

Fix a field $k = \overline{k}$, and let $\ell \neq \operatorname{char} k$ be a prime. Let X be an abelian variety over k. Then,

$$T_\ell(X) = \varprojlim_n X[\ell^n] =: \mathrm{H}_1^{\mathrm{t}}(X, \mathbb{Z}_\ell).$$

[91] Also assuming I heard him correctly, Shimura varieties are often not connected, I think

Note that $\operatorname{rank} T_\ell(X) = 2g$. We have a "first homology" functor[92]

$$T_\ell : \mathrm{Ab}_{/k} \longrightarrow \mathbb{Z}_\ell - \mathrm{Mod}.$$

For $X, Y \in \mathrm{Ab}/k$, we get $\mathrm{Hom}(X,Y) \to \mathrm{Hom}(T_\ell(X), T_\ell(Y))$.

Example. When $k = \mathbb{C}$, $T_\ell(X) = \mathrm{H}_1(X,\mathbb{Z}) \otimes \mathbb{Z}_\ell$. This is, for example, because $X = \mathrm{Lie}(X)/\mathrm{H}_1(X,\mathbb{Z})$ and

$$X[\ell^n] = \mathrm{H}_1(X, \frac{1}{\ell^n}\mathbb{Z}) = \mathrm{H}_1(X,\mathbb{Z}) \otimes \frac{1}{\ell^n}\mathbb{Z}/\mathbb{Z},$$

so

$$\varprojlim_n X[\ell^n] = \mathrm{H}_1(X,\mathbb{Z}) \otimes \varprojlim \frac{1}{\ell^n}\mathbb{Z}/\mathbb{Z} = \mathrm{H}_1(X,\mathbb{Z}) \otimes \mathbb{Z}_\ell.$$

△

Theorem 5.21.4. *For any $X, Y \in \mathrm{Ab}/k$, the natural map*

$$\mathrm{Hom}(X,Y) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(T_\ell(X), T_\ell(Y))$$

is injective.

Proof idea. Say $T_\ell(\alpha) = 0$. Then, it must factor through $X/\ell^n X$. Use complete reducibility to get a contradiction. ■

Corollary 5.21.5. $\operatorname{rank}\mathrm{Hom}(X,Y) \le 4\dim X \cdot \dim Y$.

Application to Endomorphisms Let Hom^0 denote $\mathrm{Hom} \otimes \mathbb{Q}$. Then, $\mathrm{End}^0(X)$ is a semisimple $\mathbb{Q}$-algebra of rank $\le 4g^2$, so can write $\mathrm{End}^0(X) = \bigoplus_i M_{n_i}(D_i)$ with each D_i a $\mathbb{Q}$-division algebra. Consider some $f : X \to X$. This has a notion of degree $\deg f$, which we define to be 0 if f is not finite (otherwise, it is $\deg f = [k(X) : f^* k(X)]$).

Claim 5.21.6. *$\varphi \mapsto \deg\varphi$ on $\mathrm{End}(X)$ extends to a homogeneous polynomial function of degree $2g$ on $\mathrm{End}^0(X)$.*

Proof. **(1)** Let L be any ample line bundle on X. Then, $c_1(\varphi^* L)^g = (\deg\varphi) c_1(L)^g$. From this, it is clear that $\deg(n\varphi) = n^{2g}\varphi$ since we can take L symmetric (so $n^*L = n^2 L$). This shows homogenity; we still need to show that it is a polynomial. For this, use the theorem of the cube to show that

$$c_1\left[(a\varphi_1 + b\varphi_2)^* L\right]^g$$

is polynomial in a, b. This finishes the proof somehow? ■

Theorem 5.21.7. *Let f be an endomorphism of X. Then, $\deg f = \deg T_\ell(f)$ and $P(n) = \deg(nf) =$ char polynomial of $T_\ell(f)$ (or something like this).*

Question: What is $\deg T_\ell(f)$?

Proof Sketch. Reduce to the case that X is simple. Both sides give a polynomial on the division algebra $D = \mathrm{End}^0(X)$. They are also both conjugate-invariant and have degree $2g$. Apparently this means they differ by a constant multiple. Taking $f = 1$ shows that they are the same. ■

[92] really to the subcategory of free $\mathbb{Z}_\ell$-modules

Definition 5.21.8. For $f \in \mathrm{End}^0(X)$, we can define $\mathrm{tr}(f) := \mathrm{tr}(T_\ell(f))$; this is independent of f. $\diamond$

Application to $D = \mathrm{End}^0(X)$, X =simple Let $C = Z(D)$ be its center, and let $e := [C : \mathbb{Q}]$. Then, $[D : C] = d^2$ for some d.

Fact. If $D/\mathbb{Q}$ is a division algebra with center C (= number field), then

$$D \otimes \overline{C} = M_d(\overline{C})$$

is a matrix algebra over $\overline{C}$. In particular, D is d^2-dimensional over C.

Corollary 5.21.9. *$de \mid (2g)$*

Proof. $D \hookrightarrow T_\ell(X) \otimes \mathbb{Q} \simeq \mathbb{Q}_\ell^{2g}$. ∎

Note that $D \otimes \mathbb{Q}_\ell$ is an algebra over $C \otimes \mathbb{Q}_\ell$ (= local field?). It is the maximal commutative subalgebra over $L = C \otimes \mathbb{Q}_\ell$ of rank de is the L-module $\mathbb{Q}_\ell^{2g}$. Something like this... Maybe this goes in the proof.. Who know, I'm behind.

Example. $k = \overline{\mathbb{F}}_p$, E elliptic. D a division algebra over $\mathbb{Q}$. $2g = 2 = d$, so $d = 2, e = 1$. $\triangle$

Riemann form We have the Cartier dual pairing thing:

$$\mathcal{C}_{\ell^n} : X[\ell^n] \times \widehat{X}[\ell^n] \to \mu_{\ell^n} = \mathbb{G}_m[\ell^n].$$

This paring is compatible with the maps $X[\ell^{n+1}] \to X[\ell^n]$ (an $\mu_{\ell^{n+1}} \to \mu_{\ell^n}$) in the obvious sense, so we can take a projective limit to arrive at

$$e_\ell : T_\ell(X) \times T_\ell(\widehat{X}) \to \mathbb{Z}_\ell(1).$$

Note that e_ℓ is functorial, given $f : X \to Y$, get commuting diagram

Question: If $X = V/\Lambda$ is an abelian variety over $\mathbb{C}$, does one have $\Lambda = \mathrm{H}^1(X, \mathbb{Z}) = \mathrm{H}_1(X^\vee, \mathbb{Z}) = \widehat{\Lambda}$ is some natural sense? Namely, does the middle equality exist canonically?

$$\begin{tikzcd}
T_\ell(X) \arrow[dd, "T_\ell(f)"] & \times & T_\ell(\widehat{X}) \arrow[dr, "e_\ell"] & \\
& & & \mathbb{Z}_\ell(1) \\
T_\ell(Y) & \times & T_\ell(\widehat{Y}) \arrow[uu, "T_\ell(\widehat{f})"'] \arrow[ur, "e_\ell"'] &
\end{tikzcd}$$

i.e.

$$e_\ell(T(f)a, b) = e_\ell(a, T(\widehat{f})b).$$

Example. *Missed example because I wanted to make the diagram above*[93]

Something about realizing this pairing integrally over $\mathbb{C}$. $\triangle$

[93] It was worth it

Recall that we have $\mathrm{Pic}(X) \to \mathrm{Hom}(X, \widehat{X})$ sending L to the map $x \mapsto T_x^* L \otimes L^{-1}$. Can consider the composition

$$\mathrm{Pic}(X) \longrightarrow \mathrm{Hom}(X, \widehat{X}) \longrightarrow \mathrm{Hom}(T_\ell(X), T_\ell(\widehat{X})) \to \mathrm{Hom}(T_\ell(X) \otimes T_\ell(X), \mathbb{Z}_\ell(1)).$$

Definition 5.21.10. For any $L \in \mathrm{Pic}(X)$, denote

$$E^L : T_\ell(X) \times T_\ell(X) \longrightarrow \mathbb{Z}_\ell(1)$$

the morphism defined by $E^L(x, y) = e_\ell(x, \varphi_L y)$. $\diamond$

Theorem 5.21.11. *E^L is skew-symmetric.*

$E^L \in \bigwedge^2 \mathrm{H}_1(X, \mathbb{Z}_\ell)^\vee(1) = \bigwedge^2 \mathrm{H}^1(X, \mathbb{Z}_\ell)(1) = \mathrm{H}^2(X, \mathbb{Z}_\ell)(1)$. We call E^L a **Riemann form** or **Chern class**.

5.22 Lecture 22 (11/17)

Three more lectures.

There are some gaps in material we've covered/want to cover. We never proved Riemann-Roch, we never really talked about étale cohomology, etc.

Let X/k be an abelian variety with $k = \overline{k}$, and let $\ell \neq \mathrm{char}\, k$ be a prime. Recall

$$T_\ell(X) = \varprojlim_n X[\ell^n] = \mathrm{H}_1(X, \mathbb{Z}_\ell).$$

If $\widehat{X}/k$ is the dual abelian variety, we have a natural pairing

$$e_\ell : T_\ell(X) \times T_\ell(\widehat{X}) \to \mathbb{Z}_\ell(1).$$

Now suppose we have a line bundle $\mathscr{L} \in \mathrm{Pic}(X)$; we'd like to define its (first) Chern class $c_1(\mathscr{L}) \in \mathrm{H}^2(X, \mathbb{Z}_\ell(1))$. In our situation, we have

This is using that the cohomology of a torus $(S^1)^n$ is the exterior algebra on its H^1 I guess

$$\mathrm{H}^2(X, \mathbb{Z}_\ell(1)) = \mathrm{Hom}(\bigwedge^2 T_\ell(X), \mathbb{Z}_\ell(1))$$

and the first Chern class can be given as a Riemann form. In Mumford's book, the corresponding form is denoted by $E^{\mathscr{L}}$ and given by

$$E^{\mathscr{L}}(x, y) := e_\ell(x, \varphi_{\mathscr{L}}(y))$$

with

$$\begin{array}{cccc} \varphi_{\mathscr{L}} : & X & \longrightarrow & \widehat{X} \\ & x & \longmapsto & T_x \mathscr{L} \otimes \mathscr{L}^{-1} \end{array}$$

and e_ℓ the Weil pairing.

Theorem 5.22.1. *$E^{\mathscr{L}}$ defined above is alternating. It is non-degenerate iff $\varphi_{\mathscr{L}}$ is an isogeny.*

The first part can be proven by a "brutal calculation."

Theorem 5.22.2. $\mathrm{H}^{2g}(X, \mathbb{Z}_\ell(g)) = \mathrm{Hom}(\bigwedge^{2g} T_\ell(X), \mathbb{Z}_\ell(g))$ *and there is an isomorphism* $\mathrm{tr} : \mathrm{H}^{2g}(X, \mathbb{Z}_\ell(g)) \xrightarrow{\sim} \mathbb{Z}_\ell$ *such that, given* $L_1, \dots, L_g \in \mathrm{Pic}(X)$*, one has*

$$\mathrm{tr}\left(E^{L_1} \wedge E^{L_2} \wedge \cdots \wedge E^{L_g}\right) = L_1 \cdot \cdots \cdot L_g,$$

their intersection product.

Remark 5.22.3. I think, intuitively at least, the idea should be something like E^{L_1} is the fundamental class of $[L_1]$ (or rather of its associated divisor) and this trace map is basically the top Chern class c_{2g}? ○

Proof Sketch. Use Riemann-Roch. For $L \in \mathrm{Pic}(X)$ define $\chi(L) = \sum_{i=0}^{g}(-1)^i \dim \mathrm{H}^i(X, L) \in \mathbb{Z}$. *Riemann-Roch* tells us that

$$\chi(L) = \frac{L^g}{g!} = \sqrt{\deg \varphi_L}.$$

Steps

- Reduce to the case $L_1 = L_2 = \cdots = L_g$ is ample. Use that both sides are multilinear and symmetric. If you set $L = \sum n_i L_i$, then both sides will be a polynomial in the n_i so if they agree, the coefficients agree too.
- Show $\mathrm{tr}(\bigwedge^g E^L) = L^g$. By Riemann-Roch, suffices to show $\mathrm{tr}(\bigwedge^g E^L) = g!\sqrt{\deg \varphi_L}$. Put E^L in normal form, so

  $$E^L = \sum_{i=1}^{g} d_i e_i \wedge e_{g+i} \text{ with } d_i \in \mathbb{Z}_\ell.$$

  One then calculates $\bigwedge^g E^L = g! \prod_{i=1}^{g} d_i$ so we want to show $\sqrt{\deg \varphi_L} = \prod_{i=1}^{g} d_i$. Note that we have

  $$T_\ell(\varphi_L) : T_\ell(X) \to T_\ell(\widehat{X})$$

  and $\deg \varphi_L = \det T_\ell(\varphi_L)$.

  There was some confusion when doing this in class. I think what you want to do is first use modules over a PID to represent $T_\ell(\varphi_L)$ by a diagonal matrix, i.e. $T_\ell(\varphi_L)e_i = d_i e_i'$. Then get $E^L = \sum_{i=1}^{g} d_i e_i \wedge e_{g+i}$ with $d_i \in \mathbb{Z}_\ell$ and $\det T_\ell(\varphi_L) = \prod_{i=1}^{g} d_i$. Now, you need to convince yourself that $\deg \varphi_L = (\det T_\ell(\varphi_L))^2$ and this is hopefully just some simple lattice stuff.

■

Let $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes \mathbb{Q}$. For $\varphi \in \mathrm{End}^0(X)$, we get some $\widehat{\varphi} \in \mathrm{End}^0(\widehat{X})$. Consider

$$\begin{array}{ccc} X & \xrightarrow{\varphi_L} & \widehat{X} \\ {\scriptstyle \varphi'}\downarrow & & \downarrow{\scriptstyle \widehat{\varphi}} \\ X & \xrightarrow{\varphi_L} & \widehat{X} \end{array}$$

with $\varphi' := \varphi_L^{-1}\widehat{\varphi}\varphi_L$. The map $\varphi \mapsto \varphi'$ is an anti-involution of $\mathrm{End}^0(X)$ and is called **Rosati involution** (up to spelling). Here are some properties

- $(\varphi_1\varphi_2)' = \varphi_2'\varphi_1'$
- $(\varphi_1 + \varphi_2)' = \varphi_1' + \varphi_2'$
- $\varphi'' = \varphi$
- $E^L(\varphi x, y) = E^L(x, \varphi' y)$

  Proof. Use functoriality of the Weil paring:

$$\begin{aligned} E^L(\varphi x, y) &= e_\ell(\varphi x, \varphi_L y) \\ &= e_\ell(x, \widehat{\varphi}\varphi_L y) \\ &= e_\ell(x, \varphi_L(\varphi_L^{-1}\widehat{\varphi}\varphi_L)y) \\ &= e_\ell(x, \varphi_L\varphi' y) \\ &= E^L(x, \varphi' y) \end{aligned}$$

■

5.22.1 Positivity of Rosati involution

Theorem 5.22.4. *Let H be an ample divisor on X, and set $\mathscr{L} = \mathscr{O}_X(H)$. Let $\varphi \mapsto \varphi'$ be the Rosati involution. Then for any $\varphi \in \mathrm{End}(X)$, we have*

$$\mathbb{Z} \ni \mathrm{tr}(\varphi\varphi') = \frac{2g}{H^g}\left(H^{g-1} \cdot \varphi^* H\right).$$

Remark 5.22.5. The trace can apparently be defined without using the Tate module. ○

Example. $g = 1$ and $H = 0 \in E$. Then $\varphi' = \widehat{\varphi}$ and $\varphi\widehat{\varphi} = \deg\varphi$. Hence, $\mathrm{tr}(\varphi\varphi') = \mathrm{tr}(\deg\varphi) = 2\deg\varphi$ with $\dim T_\ell(X) = 2$. On the RHS, we have

$$\frac{2}{1}\deg\varphi^{-1}(0) = 2\deg\varphi,$$

so the theorem is easy for elliptic curves. △

Proof of Theorem 5.22.4. We'll use

$$\mathrm{tr}\left(\bigwedge\nolimits_{i=1}^{g} E^{L_i}\right) = L_1 \dots L_g.$$

This tells us that the RHS is

$$2g\frac{H^{g-1}\varphi^* H}{H^g} = 2g\frac{\bigwedge^{g-1} L \wedge E^{\varphi^* L}}{\bigwedge^g E^L}.$$

Thus, it suffices to equate this with $\mathrm{tr}(\varphi\varphi')$. Take a basis of $V_\ell(X) := T_\ell(X) \otimes \mathbb{Q}_\ell$ so that (note: $e_i \in V_\ell(X)$, not necessarily $T_\ell(X)$)

$$E^L = \sum e_i \wedge e_{i+g}.$$

We now compute

$$\frac{\bigwedge^{g-1} E^L \cdot E^{\varphi^* L}}{\bigwedge^g E^L} = \frac{(g-1)!\sum_{i=1}^{g}\prod_{j\neq i} e_j \wedge e_{j+g} \cdot E^{\varphi^* L}}{g!\prod_{i=1}^{g} e_i \wedge e_{i+g}}. \tag{5.1}$$

Note that

$$E^{\varphi^* L}(x,y) = E^L(\varphi x, \varphi y) = E^L(x, \varphi'\varphi y) = E^L(\varphi'\varphi x, y) = \frac{1}{2}\left(E^L(\varphi'\varphi x, y) + E^L(x, \varphi'\varphi y)\right),$$

so

$$E^{\varphi^* L} = \frac{1}{2}\left(\sum_i (\varphi'\varphi e_i) \wedge e_{i+g} + \sum_i e_i \wedge (\varphi'\varphi e_{i+g})\right).$$

Plugging this into (5.1), we see that the RHS is equal to[94]

$$\frac{\frac{1}{2}(g-1)!\,\mathrm{tr}(\varphi'\varphi)\prod_{i=1}^g e_i \wedge e_{i+g}}{g!\prod_{i=1}^g e_i \wedge e_{i+g}} = \frac{1}{2g}\,\mathrm{tr}(\varphi'\varphi),$$

so we win. ■

Corollary 5.22.6. $\mathrm{tr}(\varphi\varphi') = \mathrm{tr}(\varphi'\varphi) > 0$ *if* $\varphi \neq 0$.

Proof. $\varphi^* H$ is effective and H^{g-1} is ample, so $H^{g-1}\varphi^* H / H^g \geq 0$. ■

Corollary 5.22.7. *If X is an abelian variety with a polarization $\varphi_L : X \to \widehat{X}$, then $\mathrm{End}^0(X)$ is a semisimple algebra over $\mathbb{Q}$ with a positive involution.*

Example. If X is simple, then $\mathrm{End}^0(X) = D$ is a division algebra. △

5.22.2 Reduced trace and reduced norm

Let $D/\mathbb{Q}$ be a division algebra with center $K \hookrightarrow D$ (so K a number field). Then, $[D : K] = d^2$ for some $d \in \mathbb{Z}$. There is a unique K-linear function $\mathrm{tr} : D \to K$ such that $\mathrm{tr}(xy) = \mathrm{tr}(yx)$ and $\mathrm{tr}(1) = d$. The **reduced trace** is the composition

$$\mathrm{tr}_{D/\mathbb{Q}} : D \xrightarrow{\mathrm{tr}} K \xrightarrow{\mathrm{tr}_K} \mathbb{Q}.$$

Definition 5.22.8. An anti-involution $x \mapsto x'$ is called **positive** if $\mathrm{tr}(xx') > 0$ for $x \neq 0$. ⋄

We will give a full classification of division algebras with positive involutions.

Let K be a number field, and let D/K be a central (i.e. center $= K$) division algebra. Then, for each place v of K, D has an invariant $\mathrm{Inv}_v(D) \in \mathbb{Q}/\mathbb{Z}$ such that $\sum_v \mathrm{Inv}_v(D) = 0$. These local invariants characterize D.

Something something Brauer group something something?

Example. The central division algebras over $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{H}$. The invariant of $\mathbb{R}$ is 0 and the invariant of $\mathbb{H}$ is $\frac{1}{2} \mod 1$.

The only central division algebra over $\mathbb{C}$ is $\mathbb{C}$ with invariant 0. △

Example. When $K/\mathbb{Q}_p$ a finite extension, write $[D : K] = d^2$ and $L \subset D$ the maximal unramified extension of K (in D). Then,

$$\mathrm{Nom}_D(L) = \left\{x \in D^\times : xLx^{-1} \subset L\right\}$$

satisfies $\mathrm{Nom}_D(L)/L^\times \simeq [L : K] \simeq \mathbb{Z}/d\mathbb{Z} \simeq \mathrm{Gal}(L/K)$. Frobenius $\mathrm{Frob} \in \mathrm{Gal}(L/K)$ corresponds to some $\alpha \in \mathrm{Nom}_D(L)/L^\times$ (so some $\alpha \in D$ up to scaling). The invariant here is $\mathrm{Inv}(D) := \mathrm{val}(\alpha) \in \frac{1}{d}\mathbb{Z}/\mathbb{Z}$. △

Question: What?

[94] If you write $\varphi'\varphi e_i = n_i e_i + (\text{other terms})$, then $\mathrm{tr}(\varphi'\varphi) = \sum n_i$.

There was another example with $K = \mathbb{Q}_p$, but it made about as much sense to me as the previous one, so I didn't bother typing anything.

For any division algebra, have an opposite algebra, and $\mathrm{Inv}(D) + \mathrm{Inv}(D^{\mathrm{op}}) = 0$.

Next time we may define Shimura varieties of PEL type.

5.23 Lecture 23 (11/19)

3 minutes late

Last time, we looked at $\varphi_L : X \to \widehat{X}$ (X an abelian variety over k). We showed that on $\mathrm{End}^0(X)$, there is an involution $\varphi \mapsto \varphi' = \varphi_L^{-1}\widehat{\varphi}\varphi_L$, and that $\mathrm{End}^0(X)$ is a semisimple algebra over $\mathbb{Q}$ of finite rank.

We've seen previously that we can write $X \sim \prod_i X_i^{n_i}$ with X_i simple and $X_i \not\sim X_j$ (here $\sim$ denote isogeny). Then,

$$\mathrm{End}^0(X) \cong M_{n_i}(D_i)$$

where $D_i = \mathrm{End}^0(X_i)$ is a division algebra. Note that $M_{n_i}(D_i)$ is a **simple $\mathbb{Q}$-algebra** (i.e. no 2-sided ideal). The division algebras D_i are classified by the Brauer group.

Let D_0 be a division algebra over $\mathbb{Q}$ with center K, a field. Locally, for each v of K, $D_v = D \otimes_v K_v$ is a simple algebra, but not necessarily a division algebra.

Actually let's start with a simple algebra B over $\mathbb{Q}$ with center K, a field. For v a place of K, we write $B_v = B \otimes K_v$ which is a simple algebra over K_v, so $B_v = M_{n_v}(D_v)$ for some division algebra D_v/K_v. We which to classify these D_v.

The first case is $K_v = \mathbb{C}$. Then, $D_v = K_v = \mathbb{C}$, so $B_v = M_{n_v}(\mathbb{C})$. We see that invariant of v is 0.

The second case is $K_v = \mathbb{R}$. Then, $D_v = \mathbb{R}$ (invariant $= 0$) or $D_v = \mathbb{H}$ (invariant $= \frac{1}{2}$). Note that $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{C} + \mathbb{C}j = \left\langle \mathbb{C}, j : jxj^{-1} = \overline{x}, j^2 = -1, x \in \mathbb{C} \right\rangle$. Note that if you set $j^2 = 1$ instead of $j^2 = -1$, then you get $M_2(\mathbb{R})$ instead of $\mathbb{H}$.

Now say K_v is non-archimedean, and L_v/K_v an unramified degree d field extension. Then, we'll construct D_v s.t. $[D_v : K_v] = d^2$. Let $D_v = \langle L_v, j\rangle$ where $jxj^{-1} = x^F$ (F is frobenius) and $j^d \in L_v$. We have $r = \mathrm{val}(j^d) \in \mathbb{Z}$ and one can show that $(r, d) = 1$. We define $\mathrm{Inv}(D_v) := \frac{r}{d} \pmod 1$.

Remark 5.23.1. If $\gcd(r, d) \neq 1$, then $D_v = M_{d/e}(D')$ is a matrix algebra, not a division algebra. ◦

We define Brauer groups.

$$\mathrm{Br}(K_v) := \begin{cases} 0 & \text{if } K_v = \mathbb{C} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } K_v = \mathbb{R} \\ \mathbb{Q}/\mathbb{Z} & \text{otherwise} \end{cases}.$$

Note that we can define invariants for any simple algebra B_v/K_v. We set $\mathrm{Inv}(B_v) = \mathrm{Inv}(D_v)$ where $B_v = M_{n_v}(D_v)$.

Let B/K be a central simple algebra of degree d^2. Then,

$$\left(\mathrm{Inv}(B_v)\right)_v \in \mathrm{Br}(K_v)[d]$$

so we get an element of $\bigoplus_v \mathrm{Br}(K_v)$. The sum of these components will be $0 \in \mathbb{Q}/\mathbb{Z}$.

Theorem 5.23.2.

(1) $\sum \mathrm{Inv}(B_v)_v = 0$

(2) $B \mapsto (\operatorname{Inv}(B_v)_v)_v$ *defines a bijection between* $\operatorname{Br}(K)[d]$ *and central simple algebras over* k *of degree* d^2*.*

Definition 5.23.3. Above,

$$\operatorname{Br}(k) := \ker\left(\bigoplus \operatorname{Br}(k_v) \to \mathbb{Q}/\mathbb{Z}\right).$$

◇

Example. When $d = 2$, $\operatorname{Br}(k_v) = \begin{cases} 0 & \text{if } K_v = \mathbb{C} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{otherwise.} \end{cases}$. So we get

$$\{\text{quaternion over } /k\} \xrightarrow{\sim} \{S \subset \Sigma(k) : \#S = \text{even}\}$$

A quaternion algebra is just a choice of evenly many non-arch places on k. △

What about $(B,')$ a simple algebra with positive involution? This gives some constraints.

- Gives center K a positive involution. Let $K_0 \subset K$ be the subfield fixed by the involution. Then K/K_0 has degree 1 or 2. For $x \in K_0$, we have $x' = x$ so $\operatorname{tr}_{K_0/\mathbb{Q}}(x^2) > 0$. hence, K_0 is totally real, i.e. $K_0 \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^e$ (as algebras) where $e := [K_0 : \mathbb{Q}]$.

  If $K \neq K_0$, then K/K_0 is CM. Hence, K is totally real or CM.

- We have a square

$$\begin{tikzcd} K \arrow[r, "\sigma"] \arrow[d] & K \arrow[d] \\ B \arrow[r, "'"] & B^{\mathrm{op}} \end{tikzcd}$$

  where σ is conjugation (element of $\operatorname{Gal}(K/K_0)$). Hence, $x \mapsto x'$ defines isomorphism

$$B \otimes_{K,\sigma} K \xrightarrow{\sim} B^{\mathrm{op}}.$$

  Hence, $\operatorname{Inv}(B_{\sigma v}) = -\operatorname{Inv}(B_v)$. If K is totally real, then this gives $\operatorname{Inv}(B_v) \in \{0, 1/2\}$.

  When K totally real, we have $B = M_d(K)$ or $M_{d/2}(D)$ with D/K a quaternion algebra. We also can find a ' with positive trace pairing.

  He wrote something like this. I'm not keeping up with lecture well

$$B \otimes_K \mathbb{R} \in \left\{\bigoplus M_d(\mathbb{R}), \bigoplus M_{d/2}(\mathbb{H})\right\}.$$

  Depending on which case you're in, the positive involution should look like $A \mapsto A^t$ or $A \mapsto \overline{A}^t$.

- If K is CM, have extra condition: $\operatorname{Inv}(B_v) = 0$ if $\sigma v = v$. Then,

$$B \otimes_{\mathbb{Q}} \mathbb{R} = B \otimes_K (K \otimes_{\mathbb{Q}} \mathbb{R}) = B \otimes_K \mathbb{C}^e = \bigoplus M_d(\mathbb{C}).$$

  For the positive involution, use $A \mapsto \overline{A}^t$.

5.23.1 Shimura Varieties of PEL-type

Let X/S be an abelian scheme, and let $\varphi : X \to \widehat{X}$ be a polarization. For some B (central simple algebra with positive involution?), say we have a morphism $\iota : B \to \mathrm{End}^0(X)$ compatible with the Rosatti involution, and let η be a level structure.

Say $S = \operatorname{Spec}\mathbb{C}$. $(B, *)$ is a simple algebra with a positive involution. Fix an order $\mathscr{O}_B \hookrightarrow B$ (not necessarily maximal) stable under involution.

Can replace B by $\mathscr{O}_B$ is the definition of ι

- $\Lambda := \mathrm{H}_1(X, \mathbb{Z})$ is an $\mathscr{O}_B$-module with a symplectic form ψ $(= \operatorname{Im} H)$ with $\psi : \Lambda \times \Lambda \to \mathbb{Z}$. We also have
$$\psi(bx, y) = \psi(x, b^* y).$$
We say (Λ, ψ) is a **skew Hermitian $\mathscr{O}_B$-module**.

- $\mathscr{O}_B$ acts on $\mathrm{Lie}(X)$. If you write $X = V/\Lambda$, then $\mathrm{Lie}(X) = V$ itself and we have $\mathscr{O}_B \xrightarrow{i_V} \mathrm{End}(V)$. Also get $t : \mathscr{O}_B \to \mathbb{C}$ via $t(b) = \mathrm{tr}(i_v(b))$. This lets us define the **reflex field of** X, $E = \mathbb{Q}(t(\mathscr{O}_B)) \subset \mathbb{C}$.

Definition 5.23.4. Let B be a simple $\mathbb{Q}$ algebra and let E be a number field. Then, a **trace map** $t : B \to E$ is a $\mathbb{Q}$-linear map factoring as $B \xrightarrow{\mathrm{tr}_{B/K}} K \to E$ where K is the center of B. ⋄

Definition 5.23.5. A **PE-data** is a triple $(B, *) =$ simple $\mathbb{Q}$ algebra with positive involution, $(\Lambda, \psi) =$ skew $\mathscr{O}_B$-module, and (E, t) a trace map $t : B \to E$. So the triple is

$$((B, *), (\Lambda, \psi), (E, t)).$$

⋄

Given a fixed PE-structure, when it there an abelian variety X with that structure? If such an X exists, we call the structure **honest**. Say out PE-structure is

$$\Big((B, *), (\Lambda, \psi), (E, t)\Big).$$

First thing we notice is that we get a real torus $\Lambda \otimes \mathbb{R}/\Lambda$. For a complex structure, we need to multiply by $\mathbb{C}$, we need $h : \mathbb{C} \to \mathrm{End}(\Lambda \otimes \mathbb{R})$ commuting with B-action. We really need

$$h : \mathbb{C}^\times \longrightarrow \mathrm{GL}_B(\Lambda \otimes \mathbb{R})$$

(a "weight 1" homomorphism?). $\mathbb{C}^\times$ acts on $V = \Lambda \otimes \mathbb{R}$ and $V \otimes \mathbb{C} = \bigoplus V_\chi$ with $\chi : \mathbb{C}^\times \to \mathbb{C}^\times$ of the form
$$z = \rho e^{2\pi i \theta} \mapsto \rho^s e^{2\pi i m \theta}.$$
"Weight 1" means $s = 1$ and $m = \pm 1$.

The upshot is complex structures on $\Lambda \otimes \mathbb{R}/\Lambda$ which are compatible with the $\mathscr{O}_B$-action are in bijection with $h : \mathbb{C}^\times \to \mathrm{GL}_B(\Lambda \otimes \mathbb{R})$.

Fix such an h. Then, H is a Riemann form determined by ψ:

This comes from the PE-data and $\psi = \operatorname{Im} H$ with this PE-data comes from an abelian

$$H(x, y) = R(x, y) + i\psi(x, y)$$

and $H(h(i)x,y) = iH(x,y)$ shows that $R(x,y) = \psi(ix,y)$. Similarly, $H(x,y) = H(y,x)$ shows that $\psi(ix,y) = \psi(iy,x)$. The fact that H is Hermitian tells us that

$$\psi(h(z)x, h(z)y) = |z|^2\, \psi(x,y)$$

so $\psi(x,x) > 0$ for $x \neq 0$.

For out PE-data to come from an abelian variety, we need $\psi(h(z)x,h(z)y) = |z|^2\,\psi(x,y)$, so we see that h must be a morphism $h : \mathbb{C}^\times \to G(R)$ where $G = \mathrm{GSp}_B(V,\psi)$ (a $\mathbb{Z}$-group scheme), i.e.

$$G(R) = \left\{(\gamma,\lambda) \in \mathrm{GL}(\Lambda \otimes R) \times R^\times : \psi(\gamma x, \gamma y) = \lambda\psi(x,y) \text{ and } \gamma b = b\gamma\right\}$$

Theorem 5.23.6. *Polarized abelian varieties X with PE-type such that $\mathrm{H}_1(X,\mathbb{Z}) = \Lambda$ (up to isomorphism) are in bijection with $h : \mathbb{C}^\times \to G(\mathbb{R})$ of weight 1 such that $\psi(h(i)x,x) > 0$ for $x \neq 0$.*

Note that h above gives rise to a trace map $t_h : B \to \mathbb{C}$.

Lemma 5.23.7. *Let $h_1, h_2 : \mathbb{C}^\times \to G(\mathbb{R})$ be two polarized complex structure. Then, TFAE*

(1) $(V \otimes \mathbb{R}, h_1) \sim (V \otimes \mathbb{R}, h_2)$ *as $B \otimes \mathbb{C}$-modules*

(2) h_1, h_2 *are conjugate to each other*

(3) $t_{h_1} = t_{h_2}$.

An **admissible PE-structure** is a triple

$$\Big((B,*), (\Lambda,\psi), (E,t)\Big)$$

where t comes from a complex variety, i.e. $\exists h : \mathbb{C}^\times \to G(\mathbb{R})$ of weight one such that $\psi(h(i)x,x) > 0$ and $t = t_h$.

Example. Say $B = \mathbb{Q}$ with trivial involution, PE-type $\mathbb{Q} \to \mathbb{C}$. So have (Λ,ψ) with $\dim \Lambda = 2g$ and $\tau : \mathbb{Q} \to \mathbb{C}, x \mapsto gx$. Above work allegedly shows that polarized abelian varieties $X/\mathbb{C}$ with iso

Question: What's g?

$$\alpha : (\mathrm{H}_1(X,\mathbb{Z}), E) \xrightarrow{\sim} (\Lambda,\psi)$$

are in bijection with weight 1 homomorphisms $h : \mathbb{C}^\times \to \mathrm{GSp}_{2g}(\mathbb{R})$ s.t. $\psi(h(i)x,x) > 0$ which is in turn in bijection with $\mathfrak{H}_g$.

Choose some fixed $h_0 : \mathbb{C}^\times \to \mathrm{GSp}_{2g}$, e.g.

$$a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Conjugacy class of h_0 is $\mathfrak{H}_g^{???}$ via $\gamma h_0 \gamma^{-1} \mapsto \gamma(iI_g)$. △

There some something else written here I couldn't make out

5.24 Lecture 24 (11/24): Last Class

3 minutes late, off to a good start

Start with one complex abelian variety with PEL type. Then look at moduli of this structure, and then the components of this moduli space will be Shimura varieties (or something like this).

Let $X/\mathbb{C}$ an abelian variety with polarization $\varphi : X \to \widehat{X}$ as well as $\iota : (B, *) \to (\mathrm{End}^0(X), ')$ where B a simple algebra/$\mathbb{Q}$ with positive involution. I think Shou-Wu said something about this being like the level structure $\eta : (\mathbb{Z}/N\mathbb{Z})^{2g} \to X[N]$ we're familiar with from before.

I'm currently fairly distracted, so these notes may be even worse than usual

Let $(B, *)$ be a simple $\mathbb{Q}$-algebra with a positive involution. Let $\mathscr{O}_B$ be an order of B stable under $*$. Let $(X_0, \varphi_0, \iota_0)$ be an abelian variety with a polarization $\varphi_0 : X_0 \to \widehat{X}_0$ and $\iota : \mathscr{O}_B \to \mathrm{End}(X_0)$ compatible under involution.

Warning 5.24.1. $\mathrm{End}(X_0)$ itself is not stable under involution, so we really mean $\mathscr{O}_B \to \mathrm{End}({}_0X) \hookrightarrow \mathrm{End}^0(X_0)$ with $\mathrm{End}^0(X_0)$ having an actual involution. •

We also have $\Lambda := \mathrm{H}_1(X, \mathbb{Z})$ with a non-degenerate symplectic form $\psi : \Lambda \times \Lambda \to \mathbb{Z}$ (which is perfect iff φ_0 is principal) coming from the imaginary part of the Riemann form. Furthermore $\mathscr{O}_B \curvearrowright \Lambda$ since

$$\psi(bx, y) = \psi(x, b^* y).$$

Definition 5.24.2. (Λ, ψ) is called a **skew-Hermitian $\mathscr{O}_B$-module**. ◇

Fix an integer N (maybe want $N \geq 3$?). Let $\mathcal{M}_N$ be the moduli functor/$\mathbb{Q}$ we currently care about. Let $S/\mathbb{Q}$ be an scheme[95]. Then,

$$\mathcal{M}_N(S) = \{(X, \varphi, \iota, \eta)\}$$

where

- X is an abelian scheme over S.
- $\varphi : X \to \widehat{X}$ is a polarization (i.e. choice of ample line bundle L and then $\varphi = \varphi_L$).
- $\iota : \mathscr{O}_B \to \mathrm{End}(X)$ compatible with involution.
- $\overline{\eta} : \Lambda/N\Lambda \xrightarrow{\sim} X[N]$, liftable to $\eta : \Lambda \otimes \widehat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{H}_1(X, \widehat{\mathbb{Z}})$, a skew Hermitian similitude, i.e.

$$\psi_X(\eta(x), \eta(y)) = \lambda \psi(x, y)$$

  for some $\lambda \in \mathbb{Z}/N\mathbb{Z}(1) = \mu_N$ (independent of x, y)

Theorem 5.24.3. *If $N \geq 3$, then $\mathcal{M}_N$ is representable by a smooth scheme over $\mathbb{Q}$.*

Remark 5.24.4. Seems we don't use the abelian variety we start with at all. It's just there to know the moduli space is non-empty?

Might not have been clear before; let's write condition on η. We want $\overline{\eta} : \Lambda/N\Lambda \to X[N]$ such that, at each geometric point $s \in X$,

$$\overline{\eta}_s : \Lambda/N\Lambda \to X_s[N]$$

can be lifted to a skew-Hermitian similitude

$$\Lambda \otimes \overline{\mathbb{Z}} \to \prod_{\ell} T_\ell(X_s).$$

[95] Possible to make things work over smaller rings

$\circ$

Proof. We have a natural map $\mathcal{M}_N \to \mathcal{A}_N$ and we know that $\mathcal{A}_N$ is representable. Something something have $\mathscr{X} \in \mathcal{A}_N/\mathbb{Q}$ and $\mathcal{M}_N$ "is what you get" by adding $\iota : \mathscr{O}_B \to \operatorname{End}(\mathscr{X})$ to the data of $\mathscr{X}$. Something something $\operatorname{End}(\mathscr{X})$ is a sheaf, and something something functions are determined by their graphs so something something can prove this by making use of Hilbert schemes something something. ∎

Example. Take $B = K$ and $* = x \mapsto \overline{x}$. $\sqrt{D} \in K$ and $\Lambda = K$.

$$\psi(x, y) = \operatorname{Re}\left(\frac{\overline{x}y}{\sqrt{D}}\right).$$

So if $x = a + b\sqrt{D}$ and $y = c + d\sqrt{D}$, then we're saying $\psi(x, y) = ad - bc$.

Take $\mathscr{O}_B = \mathscr{O} \subset K$ to be some order in K. What does $\mathcal{M}$ look like? Say $X = E$ elliptic, then $\iota : \mathscr{O}_B \to \operatorname{End}(X)$ makes X CM (I think, maybe). We also have

$$\mathscr{O}_B/N \to E[N].$$

Note that there are two ways to make E CM. You can use ι of its conjugate ι^*, so we see that the map $\mathcal{M}_N \to \mathcal{A}_N$ is not always injective. In this case, the map $\mathcal{M}_N \to \mathcal{A}_N$ is $2 : 1$ (he wrote $\mathcal{A}_N = M(\Gamma(N))$, but I'm not sure what that means). △

Can we study $\mathcal{M}_N(\mathbb{C})$? Allegedly yes and allegedly doing so will give us Shimura varieties.

Consider $(X_0, \varphi_0, \iota_0, \overline{\eta}_0) \in \mathcal{M}_N(\mathbb{C})$. We have $\Lambda = \mathrm{H}_1(X, \mathbb{Z})$ and then $X_0(\mathbb{C}) = \mathrm{H}_1(X, \mathbb{R})/\mathrm{H}_1(X, \mathbb{Z})$ which is ostensibly a real manifold, but actually $\mathrm{H}_1(X, \mathbb{R})$ has a complex structure

$$h : \mathbb{C} \longrightarrow \operatorname{End}_{\mathbb{R}}(\mathrm{H}_1(X, \mathbb{R})).$$

This commutes with the B-action, so we really get

$$\mathbb{C}^\times \longrightarrow \mathrm{GL}_B(\mathrm{H}_1(X, \mathbb{R})).$$

We also have a Hermitian for. $H = R + i\psi$ with $R = \operatorname{Re} H$ and $\psi = \operatorname{Im} H$, a symplectic form on $\mathrm{H}_1(X, \mathbb{Z})$. Note that

$$H(x, y) = \overline{H(y, x)} \text{ and } H(h(z)x, y) = zH(x, y).$$

From this, one can see that

$$H(x, y) = \psi(ix, y) + i\psi(x, y)$$

(so R is almost ψ too). Furthermore,

$$\psi(h(z)x, h(z)y) = |z|^2 \psi(x, y) \text{ for } z \in \mathbb{C}.$$

and $\psi(h(i)x, x) > 0$ if $x \neq 0$.

We would like to package these two properties of ψ into conditions on

$$h : \mathbb{C}^\times \longrightarrow \mathrm{GL}_B(\mathrm{H}_1(X, \mathbb{R}))$$

(note $\mathrm{H}_1(X,\mathbb{R}) = \Lambda \otimes \mathbb{R}$).

- The first one is telling us that $\mathbb{C}^\times \to G(\mathbb{R})$ where $G/\mathbb{Z}$ is the group scheme such that, for any ring R,
$$G(R) = \left\{(\gamma,\lambda) \in \mathrm{GL}(\Lambda \otimes_{\mathbb{Z}} R) \times R^\times : \psi(\gamma x, \gamma y) = \lambda\psi(x,y)\right\}.$$
This is a reductive group scheme.

Let $D_\psi \subset \mathrm{Hom}(\mathbb{C}^\times, G_\psi(\mathbb{R}))$ be the homomophisms satisfying

- weight 1: the induced action
$$\mathbb{C}^\times \xrightarrow{h} G_\psi \hookrightarrow \mathrm{GL}_2(\Lambda \otimes \mathbb{R})$$
of $\mathbb{C}^\times$ on $\Lambda \otimes \mathbb{R}$ has eigenvalues z (weight $(1,0)$) or $\overline{z}$ (weight $(0,1)$)
- $\psi(h(i)x, x) > 0$ if $x \neq 0$

In summary, we have proven the following:
$$\{(X,\varphi,\iota,\eta)\} \simeq D_\psi$$
where

- $X/\mathbb{C}$ an abelian variety
- $\varphi : X \to \widehat{X}$ is a polarization
- $\iota : \mathscr{O}_B \to \mathrm{End}(X)$
- $\eta : \mathrm{H}_1(X,\mathbb{Z}) \xrightarrow{\sim} \Lambda$

Maybe call this a "framed abelian variety" or something. Move of the above data above is encapsulated in h.

Example. If $B = \mathbb{Q}$, $\mathscr{O}_B = \mathbb{Z}$, and $\Lambda = \mathbb{Z}^2$, we've shown that
$$\mathfrak{H}^\pm = \left\{\left(E, E \xrightarrow{\sim} \widehat{E}, \iota : \mathscr{O}_B \to \mathrm{End}(E), \mathrm{H}_1(E,\mathbb{Z}) \simeq \mathbb{Z}^2\right)\right\}$$
or something. △

More stuff I don't really follow... something about D_ψ and G_ψ. Potentially $G_\psi(\mathbb{R}) \curvearrowright D_\psi$ (via conjugation or something)? Something about D_ψ and complex structures?

Can write $D_\psi = \bigsqcup D_\psi^t$ is a union of conjugacy classes, and $D_\psi^t = G_\psi(\mathbb{R})/\mathrm{Stab}_{G_\psi(\mathbb{R})}(h)$ (with $h \in D_\psi^t$) and this stabilizer is a maximal compact group K (Think $\mathfrak{H} = \mathrm{GL}_2(\mathbb{R})/O_2(\mathbb{R})$). Can also put a complex structure on D_ψ? Have map $G_\psi \to \mathrm{Sp}_\psi$ inducing $D_\psi \to \mathfrak{H}_g$ where $2g = \mathrm{rank}\,\Lambda$. This turns out to induce a complex structure on D_ψ and one can show that $D_\psi \to \mathfrak{H}_g$ is étale? How do we distinguish conjugacy classes in the decomposition
$$D_\psi = \bigsqcup D_\psi^t?$$

This is the word that was said, but I think it should be "$G_\psi(\mathbb{R})$-orbit" instead of "conjugacy class."

Lemma 5.24.5. *Let $h_1, h_2 \in D_\psi$. Then, TFAE*

- *h_1, h_2 are conjugation under $G_\psi(\mathbb{R})$*
- *h_1, h_2 induce isomorphism of $(\Lambda \otimes \mathbb{R}, h_1)$ and $(\Lambda \otimes \mathbb{R}, h_2)$ as $B \otimes \mathbb{C}$-modules.*
- *The traces induced by h_1, h_2 coincide.*

Now, we describe the second moduli problem. We'll use quasi-isogenies and adeles
Let $K \subset G_\psi(\widehat{\mathbb{Q}})$ be open and compact. We consider

$$\mathcal{M}_K(\mathbb{C}) = \{(X, \varphi, \iota, \overline{\eta})\}$$

- $X/\mathbb{C}$ an abelian variety
- $\varphi : X \to \widehat{X}$ a polarization
- $\iota : B \to \mathrm{End}^0(X)$ (we no longer use $\mathscr{O}_B$)
- $\overline{\eta}$ is a mod K class of Skew-Hermitian similitudes

$$\eta : \Lambda \otimes \widehat{\mathbb{Q}} \longrightarrow \mathrm{H}_1(X, \widehat{\mathbb{Q}}).$$

We say $(X_1, \varphi_1, \iota_1, \overline{\eta}_1) \sim (X_2, \varphi_2, \iota_2, \overline{\eta}_2)$ are equivalent if there is a quasi-isogeny $f : X_1 \to X_2$ (i.e. $f \in \mathrm{Hom}(X_1, X_2) \otimes \mathbb{Q}$) s.t.

$$\begin{tikzcd} X_1 \arrow[r, "\varphi_1"] \arrow[d, "f"] & \widehat{X}_1 \\ X_2 \arrow[r, "\varphi_2"] & \widehat{X}_2 \arrow[u, "\widehat{f}"'] \end{tikzcd}$$

$$\widehat{f}\varphi_2 f = c\varphi_1 \ \text{ for some } \ c \in \mathbb{Q}^\times.$$

We also want

$$\begin{tikzcd} \Lambda \otimes \widehat{\mathbb{Q}} \arrow[r, "\eta_1"] \arrow[d, "="'] & \mathrm{H}_1(X_1, \widehat{\mathbb{Q}}) \arrow[d, "\mathrm{H}_1(f)"] \\ \Lambda \otimes \widehat{\mathbb{Q}} \arrow[r, "\eta_2"] & \mathrm{H}_1(X_2, \widehat{\mathbb{Q}}) \end{tikzcd}$$

to commute.

One can show that $\mathcal{M}_N \simeq \mathcal{M}_{K(N)}$ where

$$K(N) := \ker\left(G_\psi(\widehat{\mathbb{Z}}) \to G_\psi(\mathbb{Z}/N\mathbb{Z})\right).$$

So we only need to describe $\mathcal{M}_K(\mathbb{C})$. Choose some $(X, \varphi, \iota, \overline{\eta}) \in \mathcal{M}_K(\mathbb{C})$. Write $V_X := \mathrm{H}_1(X, \mathbb{Q})$ and $V = \Lambda \otimes \mathbb{Q}$. We want to compare (V, ψ) (initial data) and (V_X, ψ_X).

Fact. $V_X \otimes \widehat{\mathbb{Q}} \simeq V \otimes \widehat{\mathbb{Q}}$ (respecting the symplectic forms).
At ∞, $(V_X \otimes \mathbb{R}, \psi_X) \simeq (V \otimes \mathbb{R}, \psi)$.

Let $\Xi(\psi) = \{$isomorphism classes of (W, ψ_W) s.t. $W \otimes \mathbb{A} \simeq V \otimes \mathbb{A}$ as skew B-modules$\}$.

Fact. $\Xi(\psi) =$ finite.

This is this thing as some sort of analogue of $\text{Ш}(E)$ for E elliptic.

$$\mathcal{M}_K(\mathbb{C}) = \bigsqcup_{\xi \in \Xi(\psi)} \mathcal{M}_K^\xi(\mathbb{C}).$$

In $\mathcal{M}^\xi$ we require $(\mathrm{H}_1(X, \mathbb{Q}), \psi_X) \simeq (V^\xi, \psi_\xi)$. Can define a $G^\xi = G^\xi_\psi$ apparently with $G^\xi(\mathbb{A}) = G(\mathbb{A})$, and then show that

$$\mathcal{M}_K^\xi(\mathbb{C}) = G^\xi(\mathbb{Q}) \backslash D_\psi \times G(\widehat{\mathbb{Q}})/K.$$

In the end, we get a decomposition

$$\mathcal{M}_K(\mathbb{C}) = \bigsqcup_\xi G^\xi(\mathbb{Q}) \backslash D_\psi \times G(\widehat{\mathbb{Q}})/K.$$

What's the next question? We know $\mathcal{M}_K$ is defined over $\mathbb{Q}$? What about the pieces

$$G^\xi(\mathbb{Q}) \backslash D_\psi \times G(\widehat{\mathbb{Q}})/K?$$

Recall the composition $D_\psi = \bigsqcup D_\psi^t$ with $t : B \to \mathbb{C}$. Let $E_t = t(B)$ be its image. Then, That is not what I thought t was... oops

$$\bigsqcup G^\xi(\mathbb{Q}) \backslash D_\psi^t \times G(\widehat{\mathbb{Q}})/K$$

is defined over E_t.

Definition 5.24.6.

$$G^\xi(\mathbb{Q}) \backslash D_\psi^t \times G(\widehat{\mathbb{Q}})/K$$

is called a **Shimura variety associated to** (G^ξ, D_ψ^t) and E_t is called a **reflex field**. $\diamond$

Shou-Wu continued saying things after this, but I was too distracted to get it.

6 List of Marginal Comments

Index