Math 223b - Algebraic Number Theory

Taught by Alison Miller
Notes by Dongryul Kim

Spring 2018

The course was taught by Alison Miller on Mondays, Wednesdays, Fridays from 12 to 1pm. The textbook was Cassels and Fröhlich's *Algberaic Number Theory*. There were weekly assignments and a final paper. The course assistance was Zijian Yao.

Contents

1 January 22, 2018

Last semester, the big thing we did was local class field theory. Let K be a non-archemedian local field, (i.e., finite extensions of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$), and L/K is Galois. What we showed last semester is that there exists a canonical isomorphism

$$\theta_{L/K} : K^\times/NL^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

The proof was via Galois cohomology. The left hand side is $\hat{H}^0(L/K, L^\times)$ and the right hand side is $\hat{H}^{-2}(L/K, \mathbb{Z})$. We needed two essential facts: Hilbert 90 $H^1(L/K, L^\times) = 0$, and $H^2(L/K, L^\times) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

This semester, we're going to talk about global fields. Now K is a global field, and consider a finite L/K. We want a global reciprocity map

$$\theta_{L/K} : C_K/NC_L \to \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

This C_K is going to be the **adelic class group** or the **idele class group** and is defined as

$$C_K = \mathbb{A}_K^\times/K^\times.$$

The shape of the argument is going to be exactly the same. We're going to need the key lemmas on H^1 and H^2, and then everything else is going to be formal. This formalism that lets us do both local and global class field theory is called class formations. So our agenda is:

- global fields, adeles, statement of global class field theory
- class formations
- algebraic proof of global class field theory
- L-functions, analytic proofs of global class field theory, Chebotarev density theorem
- complex multiplication for elliptic curves, abelian extensions of imaginary quadratic fields

1.1 Global fields and adeles

This material is at the end of Chapter 2 of Cassels and Frölich. Let K be a **global field**. This can be define in two ways. First, it can be defined as a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$. An equivalent definition is that every completion of K is a local field. A local field is valued field that is complete and locally compact. Local fields are classified by $\mathbb{F}_p((t))$, $\mathbb{Q}_p$, their finite extensions, $\mathbb{R}$, and $\mathbb{C}$.

Definition 1.1. A **place** of K is an equivalence class of absolute values on K. It is usually denoted by v. We say that v is **finite** if v comes from a discrete valuation, and **infinite** otherwise, in which case K_v is either $\mathbb{R}$ or $\mathbb{C}$.

We can consider normalized absolute values. If v is finite, K_v is a non-archedemian local field, and so we can consider the uniformizer $\pi \in K_v$ and the residue field $k_v = \mathcal{O}_v/(\pi)$. Then we define the **normalized absolute value** on K_v by

$$|\pi|_v = |k_v|^{-1}.$$

Also, if $K_v \cong \mathbb{R}$ then we define $|a|_v = |a|$, and if $K_v \in \mathbb{C}$ then we define $|a|_v = |a|^2$.

One of the motivations for defining normalization in this way is the product formula. For every $a \in K^\times$, we will have

$$\prod_v |a|_v = 1.$$

We proved this last semester, by first doing it for $K = \mathbb{Q}, \mathbb{F}_p(t)$, and then showing that both sides are preserved by taking finite extensions. Another motivation is that a locally compact abelian group has a Haar measure. So any local field K_v has a Haar measure such that $\mu(E) = \mu(a + E)$ for all $a \in K_v^+$, and such a measure is unique up to scaling. First we normalize it so that $\mu(\mathcal{O}_v) = 1$, in the non-archemedian case. We then consider $|x|_v = \mu(x\mathcal{O}_v)$. It will follow that $\mu(aE) = |a|_v \mu(E)$ for any measurable E. This is because $E \mapsto \mu(aE)$ is another Haar measure, so it is constant times the original Haar measure. Using this, we will give another proof of the product formula.

Now let me define the adeles in 5 minutes. For K a global field, we consider the set $\{K_v\}$ for v the places of K. The field K embeds into each K_v, and we are going to consider the embedding $K \hookrightarrow \prod_v K_v$. But this is too big. In general, let $\{X_i\}$ be a collection of topological groups and let $Y_i \subseteq X_i$ be a subgroup. The **restricted topological product** is defined as

$$\prod_i{}' X_i = \{(x_i)_{i \in I} : x_i \in Y_i \text{ for almost all } i\}.$$

Definition 1.2. We define the **adele** as

$$\mathbb{A}_K^+ = \prod_v{}' K_v^+, \mathbb{A}_K^\times = \prod_v{}' K_v^\times$$

where the restricted products are with respect to $\mathcal{O}_v^+$ and $\mathcal{O}_v^\times$.

2 January 24, 2018

Last time we defined the adeles, but let me go through this more carefully. We first defined the restricted topological product. Let $Y_i \subseteq X_i$ be a collection of topological spaces/groups/rings. We define the restricted product as

$$\prod\nolimits' X_i = \{(a_i)_{i\in I} : a_i \in X_i \text{ for all } i \text{ and } a_i \in Y_i \text{ for almost all } i\}.$$

The basis for the topology is given by

$$\{(a_i) : a_i \in U_i\}$$

where $U_i \subseteq X_i$ are open subsets with $U_i = Y_i$ for almost all i. This is *not* the subspace topology from the product topology for $\prod_i X_i$. If S is any finite subset of I, the restricted product $\prod_i' X_i$ has an open cover of the form

$$\Big(\prod\nolimits' X_i\Big)_S = \prod_{i\in S} X_i \times \prod_{i\notin S} Y_i.$$

The subspace topology here is equal to the product topology.

2.1 Compactness of the adele

Theorem 2.1. *If X_i are locally compact and Y_i are compact, then $\prod' X_i$ is locally compact.*

Proof. Each of $(\prod' X_i)_S$ is locally compact by Tychonoff's theorem. □

As we have defined, the adele

$$\mathbb{A}_K = \prod_v{}' K_v$$

restricted with respect to $\mathcal{O}_v$ is a topological ring. The units

$$\mathbb{A}_K^\times = \prod_v{}' K_v^\times$$

restricted to $\mathcal{O}_v^\times$ is a topological group. For the next few lectures, we are going to focus on the structure and properties.

The topology on $\mathbb{A}_K^\times$ is not the subspace topology from $\mathbb{A}_K$, by the way. This is a natural thing to do because the inverse map is not continuous with the subspace topology. In general, for R a topological ring, the inverse map on $R^\times$ is not necessarily continuous. The correct way to topologize $R^\times$ is to use the injection

$$R^\times \hookrightarrow R \times R; \quad a \mapsto (a, a^{-1})$$

and use the induced subspace topology here. As an exercise, check that this topology on $\mathbb{A}_K^\times$ agrees with the topology by the restricted product. For local fields, we don't need to worry about this issue.

We know that $\mathbb{A}_K$ and $\mathbb{A}_K^\times$ are locally compact. There is a natural embedding

$$K \hookrightarrow \mathbb{A}_K; \quad x \mapsto x = (x)$$

Likewise, we have $K^\times \hookrightarrow \mathbb{A}_K^\times$.

Proposition 2.2. *K^+ is discrete in $\mathbb{A}_K^+$, and is closed. Thus $\mathbb{A}_K^+/K^+$ makes sense, and it is compact and Hausdorff.*

Let first prove the following.

Lemma 2.3. *Let L/K be a finite extension. Then $\mathbb{A}_L \cong \mathbb{A}_K \otimes_K L$ as topological rings. (In this case, we can define the tensor product in the following way. Because $L \cong K^n$ as vector spaces, we topologize $\mathbb{A}_K \otimes_K L$ by the product topology.)*

Proof. The important fact is that if v is a place of K, then $K_v \otimes_K L = \prod_{v'} L_{v'}$ for v' extending v. We can apply this and check the topology. □

Proof of Proposition 2.2. By the lemma, to show for L, it suffices to show for K. (This is because $L \subseteq \mathbb{A}_L^+$ is equivalent to $K^n \subseteq (\mathbb{A}_K^+)^n$.) So we can check for $K = \mathbb{Q}$ and $K = \mathbb{F}_p(t)$.

Let's only do this for $K = \mathbb{Q}$. We take

$$U = \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times (-1, 1) \subseteq \mathbb{A}_\mathbb{Q}.$$

Then $a \in U \cap \mathbb{Q}$ implies that $a \in \mathbb{Z}$, so $a = 0$. So a point is open in $\mathbb{Q}$, which shows that $\mathbb{Q}$ is discrete. You can do $\mathbb{F}_p(t)$ in a similar way.

Now let us show that $\mathbb{A}_\mathbb{Q}/\mathbb{Q}^+$ is compact. If we consider the space

$$D = \prod_{v \neq \mathbb{R}} \mathbb{Z}_v \times \Big[-\frac{1}{2}, \frac{1}{2}\Big],$$

this is compact by Tychonoff. Now the claim is that $D + \mathbb{Q} = \mathbb{A}_\mathbb{Q}$. We first want for $a \in \mathbb{A}_K^+$, an $r \in \mathbb{Q}$ such that $a - r \in D$. There are finitely many finite places such that $a_p \notin \mathbb{Z}_p$. We can make them all into $\mathbb{Z}_p$ by adding a rational number. Then we can add an integer so that the infinite component is in $[-\frac{1}{2}, \frac{1}{2}]$. So $D \twoheadrightarrow \mathbb{A}_\mathbb{Q}^+/\mathbb{Q}^+$ is a surjection. Because D is compact, the image is compact as well. □

3 January 26, 2018

We should last time that $\mathbb{A}_K^+/K^+$ is compact. First of all, $\mathbb{A}_K^+$ has a Haar measure because its a locally compact abelian group. This can also described explicitly as the product of the local Haar measures, so that if $\prod_v E_v \subseteq \mathbb{A}_K^+$ is such that $E_v = K_v^+$ is measurable for each v and $E_v = \mathcal{O}_V^+$ for almost all v, then

$$\mu\biggl(\prod_v E_v\biggr) = \prod_v \mu_v(E_v).$$

This Haar measure descends to a quotient $\mathbb{A}_K^+/K^+$ (by using a fundamental domain). Because $\mathbb{A}_K^+/K^+$ is compact, the measure $\mu(\mathbb{A}_K^+/K^+)$ is going to be finite. As an exercise, show that $\mu(\mathbb{A}_K^+/K^+)$ is the discriminant $\lvert \operatorname{disc} K\rvert$.

Definition 3.1. For $a = (a_i) \in \mathbb{A}_K^\times$, we define its **content** as

$$c(a) = \prod_v \lvert a_v\rvert_v.$$

Proposition 3.2. *If $a \in \mathbb{A}_K^\times$ and $E \subseteq \mathbb{A}_K^+$, then $\mu(aE) = c(a)\mu(E)$.*

Proof. This follows from the local case. It is clear that $\mu(a_v E_v) = \lvert a_v\rvert_v \mu(E_v)$ in the local case. □

Corollary 3.3. *If $a \in K^\times$ then $c(a) = 1$.*

Proof. Consider the action on a on $\mathbb{A}_K^+$ by multiplication. Then $\mu(aE) = c(a)\mu(E)$ for any measurable $E \subseteq \mathbb{A}_K^+/K^+$. Taking $E = \mathbb{A}_K^+/K^+$ shows that $\mu(E) = c(a)\mu(E)$, and so $c(a) = 1$. □

3.1 Compactness of the multiplicative adele

What about the $K^\times \subseteq \mathbb{A}_K^\times$? This is what this course will be ultimately care about.

Proposition 3.4. *$K^\times$ is discrete inside $\mathbb{A}_K^\times$.*

Proof. We have an embedding

$$K^\times \hookrightarrow \mathbb{A}_K \hookrightarrow \mathbb{A}_K^+ \times \mathbb{A}_K^+.$$

But $K^+ \times K^+$ is already discrete inside $\mathbb{A}_K^+ \times \mathbb{A}_K^+$, so $K^\times$ should be discrete as well. □

Likewise, $K^\times$ is a closed subset. So $\mathbb{A}_K^\times/K^\times$ is a Hausdorff topological group. Is this going to be compact? The answer is no, because we have a surjective continuous map

$$c : \mathbb{A}_K^\times/K^\times \to \mathbb{R}_{>0}.$$

(It can be shown that it is continuous.) So define

$$\mathbb{A}_K^1 = \ker(c : \mathbb{A}_K^\times \to \mathbb{R}_{>0}).$$

Theorem 3.5. *$\mathbb{A}_K^1/K^\times$ is compact.*

We will prove this a bit later, but as two important corollaries: finiteness of the class group, and Dirichlet's unit theorem. (Neukirch actually goes the other direction to prove compactness.)

3.2 Applications of the compactness

Definition 3.6. For $a \in \mathbb{A}_K^\times$, define

$$S_a = \{x \in \mathbb{A}_K^\times : |x_v|_v \leq |a_v|_v \text{ for all } v\} \subseteq \mathbb{A}_K^+.$$

Theorem 3.7 (Minkowski)**.** *There exists a constant $C > 1$ (depending on K) such that for all $a \in \mathbb{A}_K^\times$ with $c(a) > C$, there exists $x \in K^\times \cap S_a$.*

Proof. Consider the set

$$B = \prod_{v \text{ fin}} \mathcal{O}_V^+ \times \prod_{v \text{ inf}} B(0, \tfrac{1}{2}) \subseteq \mathbb{A}_K^+.$$

Then you can explicitly compute $\mu(B)$, and it is going to be $\mu(B) < \infty$. If we define $C = \mu(\mathbb{A}_K^+/K^+)/\mu(B)$, then we have

$$\mu(aB) = c(a)\mu(B) > c\mu(B) = \mu(\mathbb{A}_K^+/K^+).$$

So the quotient map $aB \to \mathbb{A}_K^+/K^+$ is non-injective. This shows that there are $b_1, b_2 \in aB$ such that $x = b_1 - b_2 \in aB \cap K^\times$. By the non-archemedian triangle inequality, we have

$$|x_v|_v \leq \max\{|(b_1)_v|_v, |(b_2)_v|_v\} \leq |a_v|_v.$$

For the infinite components, we do the same thing and we get $x \in aB \subseteq S_a$. □

4 January 29, 2018

At the end of last time, we proved the adelic version of Minkowski's lemma.

Theorem 4.1 (Minkowski)**.** *Let K be a global field. There exists a constant c (depending on K) such that for all $a \in \mathbb{A}_K$ and $c(a) > c$ such that there exists an $x \in S_a \cap K^\times$ where*

$$S_a = \{x \in \mathbb{A}_K : |x_v|_v \le |a_v|_v\}.$$

There is another nice theorem that isn't necessary but nice.

Theorem 4.2 (strong approximation)**.** *Let v_0 be any place of K. The map*

$$K \hookrightarrow \mathbb{A}_K^+/K_{v_0}^+ = \prod_{v \neq v_0}{}' K_v.$$

has dense image.

Proof. Let S be a finite set of places, and consider

$$B = \prod_{v \in S} B(x_v, \epsilon) \times \prod_{v \notin S} \mathcal{O}_V^+,$$

where $x \in \mathbb{A}_K^+$ and $\epsilon > 0$. This describes a neighborhood basis for x, and we need to show that any such B contains an element of K^+. We use compactness of $\mathbb{A}_K^+/K^+$ to get that there exists some $a \in \mathbb{A}_K^\times$ such that (the image of) S_a covers $\mathbb{A}_K^+/K^+$. Now we can choose $b \in \mathbb{A}_K^\times$ such that $|b_v|_v < \frac{\epsilon}{|a_v|_v}$ for $v \in S$ and $c(b) > c$. (c is from Minkowski.) Then there exists a $z \in S_k \cap K^\times$. Write

$$\frac{x}{z} = r + s \in \mathbb{A}_K^+ = K^+ + S_a,$$

where $r \in K$ and $s \in S_a$. Now $rz = x - sz$ with $rz \in K$. But $x - sz \in B$ because $|(sz)_v|_v \le |a_v b_v|_v < \epsilon$ for $v \in S$. We also need to show that $(x - sz)_v \in \mathcal{O}_v$ for $v \notin S$, but we can enlarge S to make this true. □

Proposition 4.3. *$\mathbb{A}_K^1/K^\times$ is compact.*

(Here, you'll prove in the homework that $\mathbb{A}_K^1$ has the same topology as a subspace of $\mathbb{A}_K^\times$ and as a subspace of $\mathbb{A}_K$. Also, $\mathbb{A}_K^1$ is closed in $\mathbb{A}_K$.)

Proof. Let $D = S_a \cap \mathbb{A}_K^1$, where $c(a) > c$. Note that S_a is closed in $\mathbb{A}_K$, and so S_a is compact by Tychonoff. So $D = S_a \cap \mathbb{A}_K^1$ is also compact. Now it suffices to show that $D \twoheadrightarrow \mathbb{A}_K^1/K^\times$ is a surjection. This means for each $x \in \mathbb{A}_K^1$, there exists a $d \in D$ such that $\frac{x}{d} \in K^\times$. For this, consider $x^{-1}S_a = S_{x^{-1}a}$. Here, $c(x^{-1}a) = c(x)^{-1}c(a) = c(a) > c$, and so there exists an element $r \in K^\times$ such that $r \in S_{x^{-1}a}$. Then $rx \in \mathbb{A}_K^1 \cap S_a = D$. □

4.1 The class group

If K is a number field, it has a ring of integers $\mathcal{O}_K$, and the **class group** of K is defined as

$$\mathrm{Cl}(K) = \mathrm{Cl}(\mathcal{O}_K) = \frac{\text{group of fractional ideals of } \mathcal{O}_K}{\text{group of principal fractional ideals of } \mathcal{O}_K}.$$

More generally, let K be a global field and let S be the finite nonempty set of places of K such that S contains all the archemedian places. If we define

$$\mathcal{O}_{K,S} = \{x \in K : |x_v|_v \leq 1 \text{ for } v \notin S\}.$$

It can be shown that $\mathcal{O}_{K,S}$ is a Dedekind domain and the nonzero primes of $\mathcal{O}_{K,S}$ correspond to places not in S. If S is the set of archemedian places, then we can define $\mathcal{O}_K = \mathcal{O}_{K,S}$. As before, we can define the class group

$$\mathrm{Cl}_S(K) = \mathrm{coker}(K^\times \to I(K,S))$$

where $I(K,S)$ is the group of fractional ideals of $\mathcal{O}_{K,S}$. (By the way, the kernel is $\mathcal{O}_{K,S}^\times$.) Next time we are going to show that $\mathrm{Cl}_S(K)$ is finite and $\mathcal{O}_{K,S}^\times$ is finitely generated of rank $|S| - 1$.

5 January 31, 2018

Last time we showed that $\mathbb{A}_K^1/K^\times$ is compact, if K is a global field.

5.1 Classical theorems from compactness

We will prove the following theorem:

Theorem 5.1. *Let S be a nonempty finite set of places of K, containing all the infinite places. Then*

$$\mathrm{Cl}_S(K) = \mathrm{Cl}(\mathcal{O}_{K,S})$$

is finite and the group of units $\mathcal{O}_{K,S}^\times$ is finitely generated of rank $|S|-1$.

Let us define

$$\mathbb{A}_{K,S}^\times = \{v : |x_v|_v = 1 \text{ for } v \notin S\} = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times.$$

This is the adelic version of $\mathcal{O}_{K,S}^\times$. It is also one of the open sets that define $\mathbb{A}_K^\times$. Also let us define $\mathbb{A}_{K,S}^1 = \mathbb{A}_{K,S} \cap \mathbb{A}_K^1$. This is also open in $\mathbb{A}_K^1$. We have a short exact sequence

$$1 \to \mathbb{A}_{K,S}^1 K^\times/K^\times \to \mathbb{A}_K^1/K^\times \to \mathbb{A}_K^1/\mathbb{A}_{K,S}^1 K^\times \to 1.$$

The middle space is compact, and $\mathbb{A}_{K,S}^1 K^\times$ is an open subgroup of $\mathbb{A}_K^1$. So the first thing is an open subgroup of the second thing, which is compact. Therefore it is also a closed subgroup, and hence compact. Then the second to third map is continuous and the third space is compact as well. But when you quotient by an open subgroup, you get a discrete subgroup. This all shows that

$$\mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 \cdot K^\times)$$

is a finite discrete group.

Proposition 5.2. $\mathbb{A}_K^1/(\mathbb{A}_{K,S}^1 K^\times) \cong \mathrm{Cl}_S(K)$.

Proof. Consider the map

$$\varphi : \mathbb{A}_K^1 \to \mathrm{Cl}_S(K); \quad a \mapsto \Bigl[\prod_{v \notin S} \mathfrak{p}^{v_\mathfrak{p}(a_v)}\Bigr].$$

where $\mathfrak{p}$ is the prime ideal corresponding to the finite place v. The kernel of φ is precisely those that can be expressed as things coming from $K^\times$ and those that give the fractional ideal (1). So it is $\ker \varphi = \mathbb{A}_{K,S}^1 \cdot K^\times$. On the other hand, φ surjective because we can just set a_v as we want. So we get the isomorphism. □

Proposition 5.3. $(\mathbb{A}_{K,S} K^\times)/K^\times \cong \mathbb{A}_{K,S}^1/\mathcal{O}_{K,S}^\times$.

Proof. It suffices to show that $\mathcal{O}_{K,S}^\times \cong \mathbb{A}_{K,S}^1 \cap K^\times$. This is clear. □

We had that $\mathbb{A}^1_{K,S}/\mathcal{O}^\times_{K,S}$ is compact. So we are going to focus on what is happening with the S part.

Lemma 5.4. *The set*

$$\{x \in \mathcal{O}^\times_{K,S} : |x|_v \in [\tfrac{1}{2}, 2] \text{ for all } v \in S\}$$

is finite.

Proof. This is the same as the intersection of $K^\times$ and $\prod_{v \notin S} \mathcal{O}^\times_V \times \prod_{v \in S} B_v$ which is discrete and compact. So it is finite. □

Corollary 5.5. *A number $a \in K^\times$ is a root of unity if and only if $|a|_v = 1$ for all v.*

Proof. One direction is obvious. For the other direction, we note that the group $\{a \in K : |a|_v = 1 \text{ for all } v\}$ is finite, and hence torsion. □

Now define a homomorphism

$$\mathscr{L} : \mathbb{A}^1_{K,S} \to \prod_{v \in S} \mathbb{R}^+; \quad (\mathscr{L}(a))_v = \log(|a_v|_v).$$

Proposition 5.6. *$\mathscr{L}(\mathscr{O}_{K,S})$ is a discrete subgroup of $\prod_{v \in S} \mathbb{R}^+$, and the kernel of $\mathscr{L} : \mathscr{O}^\times_{K,S} \to \prod_{v \in S} \mathbb{R}^+$ is finite.*

Proof. This follows from the lemma, because it is saying that $\mathscr{L}^{-1}$ of some compact region is finite. Then the image has to be discrete, and the kernel should be finite. □

Now we have $\mathscr{L} : \mathbb{A}^1_{K,S} \to (\mathbb{R}^+)^{|S|}$, and this induces a map

$$\mathbb{A}^1_{K,S}/\mathcal{O}^\times_{K,S} \to \mathscr{L}(\mathbb{A}^1_{K,S})/\mathscr{L}(\mathcal{O}^\times_{K,S}).$$

But the condition on $\mathscr{L}(\mathbb{A}^1_{K,S})$ is that all components should add up to 1. It is also true that this is the only condition. This shows that

$$\mathscr{L}(\mathbb{A}^1_{K,S}) = H = \{x \in (\mathbb{R}^+)^s : \textstyle\sum_v x_v = 0\}.$$

On the other hand, $\mathbb{A}^1_{K,S}/\mathcal{O}^\times_{K,S}$ is compact, and so $\mathscr{L}(\mathbb{A}^1_{K,S})/\mathscr{L}(\mathcal{O}^\times_{K,S})$ is compact. This shows that $\mathscr{L}(\mathcal{O}^\times_{K,S})$ is a free group of rank $|S| - 1$. Therefore $\mathcal{O}^\times_{K,S}$ is a finitely generated group of rank $|S| - 1$.

6 February 2, 2018

We have shown that the group $\mathbb{A}_K^1/K^\times$ is compact. In class field theory, we will use $C_K = \mathbb{A}_K^\times/K^\times$. How will we compare it to C_K?

We have a short exact sequence relating the two. Suppose first that K is a number field. Then we have a short exact sequence

$$1 \to \mathbb{A}_K^1/K^\times \to \mathbb{A}_K^\times/K^\times \xrightarrow{c} \mathbb{R}_{>0} \to 1.$$

For each archemedian place v, we have a closed embedding $\mathbb{R} \hookrightarrow K_v^\times$, and then a closed embedding $K_v^\times \hookrightarrow \mathbb{A}_K^\times/K^\times$. This gives a splitting as topological groups.

If K is a function field over $\mathbb{F}_q$, then we have

$$1 \to \mathbb{A}_K^1/K^\times \to \mathbb{A}_K^\times/K^\times \xrightarrow{c} q^{\mathbb{Z}} \to 1.$$

Again, there is a splitting, not in a particularly natural way.

6.1 Statement of global class field theory

Theorem 6.1 (Main theorem of global class field theory)**.** *If K is a global field, we have a reciprocity map*

$$\theta_{/K} : C_K = \mathbb{A}_K^\times/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with dense image, and $\ker(\theta_{/K}) = (C_K)^0$ the connected component of C_K. This can be described as the closure of the image of

$$(\mathbb{A}_K)^0 = \prod_{v \ inf} (K_v^\times)^0$$

which is easy to describe. There is also a local-to-global compatibility

$$\begin{tikzcd}
K_v^\times \arrow[r, "\theta_{/K_v}"] \arrow[d, hook] & \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v) \arrow[d, hook] \\
\mathbb{A}_K^\times/K^\times \arrow[r, "\theta_{/K}"] & \mathrm{Gal}(K^{\mathrm{ab}}/K).
\end{tikzcd}$$

This local-to-global compatibility specifies $\theta_{/K}$ uniquely because K_v generate it topologically. So $\theta_{/K}$ induces a bijection

$$\left\{\begin{matrix}\text{open subgroups of} \\ C_k \text{ of finite index}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{open subgroups of} \\ \mathrm{Gal}(K^{\mathrm{ab}}/K) \text{ of finite index}\end{matrix}\right\}.$$

Then the right hand side is the same as a finite abelian extension L/K. The map from extensions L/K to subgroups of C_K is going to be given by

$$L \mapsto N_{L/K}(C_L) \subseteq C_K.$$

Here, we define

$$N_{L/K} : \mathbb{A}_L^\times \to \mathbb{A}_K^\times; \quad a \mapsto (Na)_v = \prod_{w/v} N_{L_w/K_v}(a_w).$$

It turns out that

$$\begin{tikzcd}
L^\times \arrow[r, "N"] \arrow[d] & K \arrow[d] \\
\mathbb{A}_L^\times \arrow[r, "N"] & \mathbb{A}_K^\times
\end{tikzcd}$$

commutes, so we get a map $C_L \to C_K$. It turns out that $N_{L/K}(\mathbb{A}_L^\times) \subseteq \mathbb{A}_K^\times$ is open.

6.2 Ray class field

Definition 6.2. A **modulus** of a field K is a function $\mathfrak{m} : \{\text{places of } K\} \to \mathbb{Z}_{\geq 0}$ with the property

- $\mathfrak{m}(v) = 0$ for all but finitely many v,
- $\mathfrak{m}(v) = 0$ or 1 if v is real,
- $\mathfrak{m}(v) = 0$ if v is complex.

We write $\mathfrak{m} = \prod_v v^{\mathfrak{m}(v)}$ (so $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\infty_1$ for instance.)

For any $\mathfrak{m}$ we have a congruence subgroup

$$\left(\prod_{\mathfrak{p} \text{ fin}} U_{\mathfrak{p},\mathfrak{m}_\mathfrak{p}} \times \prod_{v \text{ inf } \mathfrak{m}(v)=0} K_v \times \prod_{v \text{ real } \mathfrak{m}(v)=1} \mathbb{R}^{>0}\right) K^\times/K^\times \subseteq C_K,$$

where

$$U_{\mathfrak{p},\mathfrak{m}_\mathfrak{p}} = \{x \in \mathcal{O}_{K_\mathfrak{p}} : x \equiv 1 \pmod{\mathfrak{p}^{\mathfrak{m}_\mathfrak{p}}}\}.$$

Definition 6.3. The **ray class field** $L_\mathfrak{m}$ is the fixed field of $\theta(U_\mathfrak{m})$, so that

$$\mathrm{Gal}(L_\mathfrak{m}/K) \cong C_K/U_\mathfrak{m} \cong \mathbb{A}_K^\times/K^\times\left(\prod_{\mathfrak{p} \text{ fin}} U_{\mathfrak{p},\mathfrak{m}_\mathfrak{p}} \times \prod_{v \text{ fin}} (-)\right).$$

The punchline is that

$$C_K/U_\mathfrak{m} \cong \mathrm{Cl}_\mathfrak{m}(\mathcal{O}_K)$$

is the **ray class group**, which is the fractional ideals of $\mathcal{O}_K$ relatively prime to $\mathfrak{m}$ modulo the principal fractional ideals (a) with $a \in U_{\mathfrak{p},\mathfrak{m}_\mathfrak{p}}$ for all finite $\mathfrak{p}$ and $a_v > 0$ for v real with $\mathfrak{m}(v) = 1$.

7 February 5, 2018

Last Friday I started introducing the adelic statement of global class field theory.

Theorem 7.1 (Main theorem of global class field theory)**.** *Let K be a global field. There exists a canonical $\theta_{/K} : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that*

- $\ker \theta_{/K} = (C_K)^0$ *is the connected component at* 1*,*
- $\mathrm{im}\, \theta_{/K}$ *is dense in* $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varinjlim_{L/K \text{ fin. ab.}} \mathrm{Gal}(L/K)$ *(this means that $\theta_{L/K} : C_K \to \mathrm{Gal}(L/K)$ is surjective for any L/K).*

7.1 Image of the reciprocity map

This map $\theta_{/K}$ that has dense image is actually surjective for K a number field, but not surjective for K a function field.

Proposition 7.2. *If K is a number field, then $C_K/(C_K)^0$ is compact.*

Proof. We know that $\mathbb{A}_K^1/K^\times$ is compact. So it suffices to check that this surjects onto $C_K/(C_K)^0$. This is because we can change only the archemedian component to make the content 1, and this doesn't change the connected component. □

Now $C_K/(C_K)^0$ is compact, so the image of $\theta_{/K}$ in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is compact. This means that the image is closed, and also is dense. So it is the whole space $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ for K a number field.

Let us see what goes wrong when K is a function field. Then all of the localizations are totally disconnected, so $\mathbb{A}_K^\times$ is totally disconnected and C_K is totally disconnected. Then the map $\theta_{/K}$ is injective. If $\theta_{/K}$ were an isomorphism, we would have that C_K is profinite and thus compact. Let $k = \mathbb{F}_q$ be the field of constants, and consider the field extension

$$\overline{k} \cdot K \subseteq K^{\mathrm{ab}}.$$

Then we get a homomorphism

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \widehat{\mathbb{Z}} \cong \mathrm{Gal}(\overline{k}/k).$$

It turns out that the square

$$\begin{tikzcd}
1 \arrow[r] & I_K \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r] & \widehat{\mathbb{Z}} \cong \mathrm{Gal}(\overline{k}/k) \arrow[r] & 1 \\
1 \arrow[r] & \mathbb{A}_K^1/K^\times \arrow[r] \arrow[u, "\cong"] & C_K = \mathbb{A}_K^\times/K^\times \arrow[r, "c"] \arrow[u, "\theta_{/K}"] & q^{\mathbb{Z}} \arrow[r] \arrow[u, "q \mapsto 1"] & 1
\end{tikzcd}$$

commutes, and also both exact sequences split.

7.2 Identifying the ray class group

Recall that for K a number field, a modulus is a formal product $\mathfrak{m} = \prod_v v^{\mathfrak{m}(v)}$. Then we can define an open subset $U_\mathfrak{m} \subseteq \mathbb{A}_K^\times$

$$U_\mathfrak{m} = \prod_{\mathfrak{p} \text{ fin}} U_{\mathfrak{p},\mathfrak{m}(\mathfrak{p})} \times \prod_{v \text{ real},\mathfrak{m}(v)=1} \mathbb{R}^{>0} \times \prod_{v \text{ other}} K_v^\times.$$

Then the congruence subgroup $C_K^\mathfrak{m} \subseteq C_K$ is defined as

$$C_K^\mathfrak{m} = U_\mathfrak{m} \cdot K^\times / K^\times \subseteq \mathbb{A}_K^\times / K^\times = C_K.$$

We also defined the ray class field of modulus $\mathfrak{m}$ as the fixed field of $\theta_{/K}(C_K^\mathfrak{m})$. In this case, we have

$$\mathrm{Gal}(L_\mathfrak{m}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)/\theta_{/K}(C_K^\mathfrak{m}) \cong C_K/C_K^\mathfrak{m}$$

Proposition 7.3. *$C_K/C_K^\mathfrak{m}$ is isomorphic to the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$, where*

$$\mathrm{Cl}_\mathfrak{m}(K) = \frac{\textit{frac. ideals rel. prime to } \mathfrak{m}}{\textit{frac. ideals } (a) \textit{ with } a \in U_\mathfrak{m}}.$$

Proof. Exercise. □

We can give the inverse map explicitly. If $\mathfrak{p}$ is relatively prime to $\mathfrak{m}$ then we can send $\mathfrak{p}$ to $[(1, \ldots, 1, \pi, 1, \ldots)]$ where $\pi \in K_\mathfrak{p}^\times$ is an arbitrary uniformizer.

Proposition 7.4. *The field $L_\mathfrak{m}/K$ is unramified at all $\mathfrak{p}$ relatively prime to $\mathfrak{m}$.*

Proof. We have an isomorphism

$$\mathrm{Cl}_\mathfrak{m}(K) \cong C_K/C_K^\mathfrak{m} \xrightarrow{\theta_{/K}} \mathrm{Gal}(L_\mathfrak{m}/K).$$

This sends $\mathfrak{p}$ to $\mathrm{Frob}_\mathfrak{p}$ lying in the decomposition group. This means that $L_\mathfrak{m}$ is a class field in the classical sense. □

8 February 7, 2018

Recall that for K a number field, we defined the ray class field $L_{\mathfrak{m}}$ of modulus $\mathfrak{m}$ by the fixed field of

$$\theta_{L/K}(C_K^{\mathfrak{m}}) = \theta_{L/K}(U_m K^\times/K^\times).$$

8.1 Properties of the ray class field

Proposition 8.1. *(a) $L_{\mathfrak{m}}$ is unramified at all places not dividing $\mathfrak{m}$. (For infinite places, we say that v'/v ramifies if v is is real and v' is complex. Neukirch uses a different convention, that infinite places never ramify.)*

(b) If $\mathfrak{m} \mid \mathfrak{m}'$ then $L_{\mathfrak{m}} \subseteq L_{\mathfrak{m}'}$.

(c) $L_{\mathfrak{m}_1} \cap L_{\mathfrak{m}_2} = L_{\gcd(\mathfrak{m}_1, \mathfrak{m}_2)}$.

(d) $\bigcup_{\mathfrak{m}} L_{\mathfrak{m}} = K^{\mathrm{ab}}$.

Proof. (a) First use the fact that if $\mathfrak{p} \nmid \mathfrak{m}$ then

$$\mathcal{O}_{\mathfrak{p}}^\times \hookrightarrow U_{\mathfrak{m}} \to C_K^{\mathfrak{m}}.$$

For $\mathfrak{p}'$ any prime of $L_{\mathfrak{m}}$ over $\mathfrak{p}$, we have

$$\begin{tikzcd}
K_{\mathfrak{p}}^\times \arrow[r, "\theta_{/K_{\mathfrak{p}}}"] \arrow[d, hook] & \mathrm{Gal}((L_{\mathfrak{m}})_{\mathfrak{p}'}/K_{\mathfrak{p}}) \arrow[d, hook] \\
C_K \arrow[r, "\theta_{L_{\mathfrak{m}}/K}"] & \mathrm{Gal}(L_{\mathfrak{m}}/K).
\end{tikzcd}$$

Now we have $C_K^{\mathfrak{m}} = \ker \theta_{L_{\mathfrak{m}}/K}$ and so $\mathcal{O}_{\mathfrak{p}}^\times \subseteq \ker \theta_{(L_{\mathfrak{m}})_{\mathfrak{p}}/K_{\mathfrak{p}}}$. This shows that $\theta_{(L_{\mathfrak{m}})_{\mathfrak{p}}/K_{\mathfrak{p}}}(\mathcal{O}_{K_{\mathfrak{p}}}^\times)$ is trivial. By local class field theory, this just means that $(L_{\mathfrak{m}})_{\mathfrak{p}}/K_{\mathfrak{p}}$ is unramified. For infinite places, we use $K_{\mathfrak{p}}^\times$ instead of $\mathcal{O}_{\mathfrak{p}}^\times$.

(b) and (c) just follow from the definition of $U_{\mathfrak{m}}$ and $C_K^{\mathfrak{m}}$. For (d), observe that any open subgroup of $\mathbb{A}_K^\times$ contains some $U_{\mathfrak{m}}$. Then any open subgroup of C_K contains some $C_K^{\mathfrak{m}}$. Using global class field theory and Galois correspondence, we see that any finite abelian extension lies in some $L_{\mathfrak{m}}$. □

Example 8.2. Let $K = \mathbb{Q}$. We can take $\mathfrak{m} = m$ or $\mathfrak{m} = m\infty$ where m is a positive integer. First let us figure out $\mathrm{Cl}_{\mathfrak{m}}(K)$ and then figure out $L_{\mathfrak{m}}$. First, if $\mathfrak{m} = m\infty$,

$$\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}) = \frac{\text{frac. ideals rel. prime to } m}{(a) \text{ where } a > 0 \text{ and } a \equiv 1 \bmod m} \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

If $\mathfrak{m} = m$, then we would get $(\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$.

It now follows from the explicit description of $\theta_{/K}$ for cyclotomic fields that $L_{m\infty} = \mathbb{Q}(\zeta_m)$. If we don't allow ∞, we will get $L_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Definition 8.3. Let L be a finite abelian extension of K. The minimal $\mathfrak{m}$ such that $L \subseteq L_{\mathfrak{m}}$ is called the **conductor** of L, and is written $\mathfrak{f} = \mathfrak{f}_{L/K}$.

Another way to describe $\mathfrak{f}$ is that $\mathfrak{f}$ is minimal such that

$$\begin{tikzcd} C_K \arrow[r, "\theta_{L/K}"] \arrow[d] & \operatorname{Gal}(L/K) \\ C_K/C_K^{\mathfrak{f}} \cong \operatorname{Cl}_{\mathfrak{f}}(K) & \end{tikzcd}$$

factors.

We know that L is unramified outside the primes $\mathfrak{p} \nmid \mathfrak{f}$. Then for each $\mathfrak{p} \nmid \mathfrak{f}$, we have

$$\left(\frac{\mathfrak{p}}{L/K}\right) = \operatorname{Frob}_{\mathfrak{p}} \in \operatorname{Gal}(L/K),$$

and $(\frac{p}{L/K})$ is the restriction of $(\frac{\mathfrak{p}}{L/K})$ to $\operatorname{Gal}(L/K)$. Since $(\frac{\mathfrak{p}}{L_{\mathfrak{p}}/K})$ depends only on $[\mathfrak{p}] \in \operatorname{Cl}_{\mathfrak{f}}(K)$, same is true of $(\frac{\mathfrak{p}}{L/K})$.

Also, for $\ker \theta_{L/K} = N_{L/K} C_L$. So $L \subseteq L_{\mathfrak{m}}$ is equivalent to $N_{L/K} C_L \supseteq C_K^{\mathfrak{m}}$. This means that $\mathfrak{f}$ is the minimal $\mathfrak{m}$ that makes this true.

You can show as an exercise that $\mathfrak{p}$ ramifies if and only if $\mathfrak{p} \mid \mathfrak{f}_{L/K}$.

Example 8.4. Take $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{p})$ where $p \equiv 1 \pmod 4$ and p is prime. Then L is ramified only at p and $\mathfrak{f}_{L/\mathbb{Q}} = p$. For q any other prime, we have that

$$\operatorname{Frob}_q(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) = \left(\frac{q}{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}\right) = \left(\frac{q}{p}\right)$$

only depends on the image of q in $(\mathbb{Z}/p\mathbb{Z})^\times/(\pm 1)$.

Let K be an arbitrary field, and let $\mathfrak{m} = 1$. Then

$$\operatorname{Cl}_{\mathfrak{m}}(K) = \operatorname{Cl}(\mathcal{O}_K).$$

Here, $L_1 = H$ is called the **Hilbert class field** that is unramified at all places over K, including the infinite places. For $\mathfrak{m} = \prod_{v \text{ real}} v$, we can similarly define $L_{\mathfrak{m}} = H^+$ the **narrow Hilbert class field**.

9 February 9, 2018

The goal is to set up the abstract theory of class formations. Recall local class field theory. Here, K is a local field. The key fact was homological: if L/K is finite Galois, then

$$K^\times/NL^\times \cong \hat{H}^0(L/K, L^\times) \cong \hat{H}^{-2}(L/K, \mathbb{Z}) \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

Then we took the direct limit over all finite L/K to get

$$\varprojlim K^\times/NL^\times \cong \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

In characteristic zero, this gives $\widehat{K}^\times \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Here are the inputs we put into the Galois cohomology machinery:

- for every finite L/K, a $\mathrm{Gal}(L/K)$-structure on $L^\times$
- the collection of groups $\{\mathrm{Gal}(L/K)\}$ for L finite Galois, and quotient maps $\mathrm{Gal}(E/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ when $E/L/K$
- compatibility conditions on the Gal-module structures with $E^\times = (L^\times)^{\mathrm{Gal}(E/L)}$.

We can also package this whole thing into $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $A = (K^{\mathrm{sep}})^\times$. Then our collection is exactly quotients of G by finite index open subgroups, with $L^\times = ((K^{\mathrm{sep}})^\times)^{\mathrm{Gal}(K^{\mathrm{sep}}/L)}$.

The goal is to be able to replace $K^\times$ with C_K everywhere.

9.1 Ideles with field extensions

For L/K Galois, we know already that $K^\times \hookrightarrow L^\times$ and $K^\times = (L^\times)^{\mathrm{Gal}(L/K)}$. We will need an analogous statement for C_K and C_L.

Let L/K be a finite extension of global fields (not necessarily Galois). We have closed embeddings

$$\mathbb{A}_K \hookrightarrow \mathbb{A}_L, \quad \mathbb{A}_K^\times \hookrightarrow \mathbb{A}_L^\times.$$

Proposition 9.1. *$\mathbb{A}_K^\times$ is closed in $\mathbb{A}_L^\times$. If L/K is Galois, then $(\mathbb{A}_L^\times)^{\mathrm{Gal}(L/K)} = \mathbb{A}_K$ and $\mathbb{A}_K^\times \cap L^\times = K^\times$.*

Proof. All follows immediately form $\mathbb{A}_L \cong \mathbb{A}_K \otimes_K L$ as topological rings. Because L/K is Galois, they are isomorphic as Galois modules. □

So we get an inclusion $\mathbb{A}_K^\times/K^\times \to \mathbb{A}_L^\times/L^\times$. That is, $C_K \hookrightarrow C_L$.

Proposition 9.2. *We have $C_L^{\mathrm{Gal}(L/K)} = C_K$.*

Proof. We use the short exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to C_L \to 1.$$

If we take Galois cohomology, we get

$$1 \to K^\times \to \mathbb{A}_K^\times \to C_L^{\mathrm{Gal}(L/K)} \to H^1(L/K, L^\times) = 1.$$

This shows that $C_L^{\mathrm{Gal}(L/K)} \cong C_K$. □

In general, $\mathrm{Cl}(\mathcal{O}_K) \to (\mathrm{Cl}(\mathcal{O}_L))^{\mathrm{Gal}(L/K)}$ is neither injective nor surjective.

9.2 Formations

Let G be a profinite group. Think of G as some absolute Galois group. In this case, open subgroups as finite extensions of the field. Going back to the general case, consider the set of open subgroup $\{G_K : K \in X\}$ of G. We are going to refer to these indices K as "fields".

In particular, we have a partial ordering of field, with $K \subseteq L$ if and only if $G_L \subseteq G_K$. There is a unique minimal field K_0 corresponding to $G_{K_0} = G$, and we call K_0 the "base field". A pair (K, L) with $K \subseteq L$ is called a "layer" L/K. The "degree" of the layer is defined as $[L : K] = [G_K : G_L]$. We say that L/K is "normal" if $G_L \lhd G_K$ is a normal subgroup. We can define

$$G_{KL} = G_K \cap G_L, \quad G_{K\cap L} = G_K G_L.$$

The group G acts on the set X of all fields by

$$G_{gK} = gG_K g^{-1}.$$

Definition 9.3. A **formation** A is a G-module satisfying the following equivalent conditions:

- G acts continuously on A (using the discrete topology on A)
- $A = \bigcup_K A^{G_K}$

Example 9.4. Suppose that $G = \mathrm{Gal}(K_0^{\mathrm{sep}}/K_0)$. Then $A = (K_0^{\mathrm{sep}})^\times$ is a formation. For global fields, we can instead look at $A = \varinjlim_{K/K_0 \text{ fin}} C_K$.

10 February 12, 2018

We were talking about class formations. This was a profinite group G with $\{G_K : K \in X\}$ indexing the open subgroups of G. These $K \in X$ were called fields. A G-module was an abelian group A with a G-action such that the action is continuous. This can be explicitly described as

$$A = \bigcup_K A^{G_K} = \bigcup_K A^K$$

where we define $A^K = A^{G_K}$. We also say that L/K is a normal layer if $G_L \lhd G_k$ is normal. Then we write $G_{L/K} = G_K/G_L$. Then $G_{L/K}$ acts on A_L and A_L is a $G_{L/K}$-module.

Definition 10.1. We define $H^q(L/K) = H^q(G_{L/K}, A_L)$. Likewise, se define $\hat{H}^q(L/K) = \hat{H}^q(G_{L/K}, A_L)$. We can also define profinite cohomology

$$H^q(/K) = H^q(G_K, A) = \varinjlim_L H^q(G_{L/K}, A_L) = \varinjlim_L H^q(L/K).$$

If $E/L/K$, with E/K and L/K both normal layers, we have inflation maps

$$\inf : H^q(L/K) = H^q(G_{L/K}, A) = H^q(G_{L/K}, (A_E)^{G_L/G_E}) \to H^q(G_{E/K}, A_E) = H_q(E/K).$$

The are also restriction and corestriction. If $E/L/K$ and E/K is normal then E/L is normal. Then we have $G_{E/K} \supseteq G_{E/L}$. So we get restriction and corestriction maps

$$\mathrm{res} : \hat{H}^q(E/K) \to \hat{H}^q(E/L), \quad \mathrm{cores} : \hat{H}^q(E/L) \to \hat{H}^q(E/K).$$

There is also conjugation action. If L/K is a normal layer and $g \in G$, we can define $G_{gK} = gG_Kg^{-1}$. Then we have isomorphisms

$$G_{L/K} \cong G_{gL/gK}; \quad [x] \mapsto [gxg^{-1}].$$

We also have isomorphisms

$$A_L \to A_{gL}; \quad a \mapsto ga,$$

and this induces

$$g^* : H^q(L/K) \to H^q(gL/gK).$$

If $g \in G_K$, then $gK = K$ and $gL = L$ because L/K is normal. In this case, you can check that

$$g^* : H^q(L/K) \to H^q(L/K)$$

is the identity by checking at $q = 0$ and then dimension shifting.

10.1 Class formation

To say something other than formalities with cohomology, you need to input something.

Definition 10.2. (G, A) is a **field formation** if for every layer L/K, $H^1(L/K) = 0$.

Of course, the motivating example here is $G = \mathrm{Gal}(K_0^{\mathrm{sep}}/K_0)$ and $A = (K_0^{\mathrm{sep}})^\times$. From this, we get an inflation-restriction sequence on the second cohomology:

$$0 \to H^2(L/K) \to H^2(E/K) \to H^2(E/L)$$

whenever $E/L/K$ with E/K and L/K normal. Then we have

$$H^2(/K) = \varinjlim H^2(L/K) = \bigcup_{L/K} H^2(L/K).$$

For local fields, we also had the fact that H^2 is cyclic. But we want to say this carefully.

Definition 10.3. A is a **class formation** if for every L/K we provide an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},$$

with compatibility conditions

$$\begin{tikzcd}
H^2(L/K) \arrow[r, "\mathrm{inv}_{L/K}"] \arrow[d, "\mathrm{inf}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, hook] \\
H^2(E/K) \arrow[r, "\mathrm{inv}_{E/K}"] & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

for all normal $E/L/K$, and

$$\begin{tikzcd}
H^2(E/K) \arrow[r, "\mathrm{inf}_{E/K}"] \arrow[d, "\mathrm{res}"] & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "\times{[L:K]}"] \\
H^2(E/L) \arrow[r, "\mathrm{inf}_{E/L}"] & \frac{1}{[E:L]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

for $E/L/K$ with E/K normal.

Try to deduce the diagram for corestriction.

11 February 14, 2018

A class formation is a formation $(G, (G_K)_{K\in X}, A)$ satisfying the axioms

(i) (Hilbert 90) $H^1(L/K) = 0$ for all normal L/K,

(ii) there are invariant maps inv : $H^2(G_{L/K}, A_L) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ compatible with inflation and restriction (and thus correstriction)

Example 11.1. Suppose $G = \widehat{Z}$ and suppose $A = \mathbb{Z}$ with the trivial action. The fields are $K_n = n\widehat{Z}$ with $A^{K_n} = \mathbb{Z}$. Then for $m \mid n$,

$$H^1(K_n/K_m) = H^1(n\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = 0$$

and

$$H^2(K_n/K_m) = H^2(n\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}/(\tfrac{n}{m}\mathbb{Z}).$$

You can of this as something over finite fields.

Example 11.2. By last semester, we know that for K a local field, $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ with $A = (K^{\mathrm{sep}})^\times$ is a class formation.

Our goal is to show that for K_0 global,

$$G = \mathrm{Gal}(K_0^{\mathrm{sep}}/K), \quad A = \bigcup_{L/K} C_L$$

is a class formation. In this case, $A_L = C_L$.

11.1 Consequences of the class formation axiom

Proposition 11.3. *Let A be a class formation.*

(a) For $E/L/K$ with E/K normal, the following commutes.

$$\begin{tikzcd} H^2(E/L) \arrow[r, "\mathrm{inv}_{E/L}"] \arrow[d, "\mathrm{cor}"] & \frac{1}{[E:L]}\mathbb{Z}/\mathbb{Z} \arrow[d, hook] \\ H^2(E/K) \arrow[r, "\mathrm{inv}_{E/K}"] & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} \end{tikzcd}$$

(b) For normal L/K and $g \in G$, the following commutes.

$$\begin{tikzcd} H^2(L/K) \arrow[r, "\mathrm{inv}_{L/K}"] \arrow[d, "g^*"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, equal] \\ H^2(gL/gK) \arrow[r, "\mathrm{inv}_{L/K}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \end{tikzcd}$$

Proof. For (a), we simply note that

$$H^2(E/K) \xrightarrow{\text{res}} H^2(E/L) \xrightarrow{\text{cor}} H^2(E/K)$$

is multiplication by $[L : K]$. For (b), if $g \in G_K$ then we are done because $g^* : H^2(L/K) \to H^2(L/K)$ is the identity map as we have shown. In general, we have $g \in G_{K_0} = G$, so we can find $L' \supseteq L$ such that L'/K is normal. Then you compute the diagrams for L/K and L'/K_0. □

If (G, A) is a class formation, we define the fundamental class

$$u_{L/K} \in H^2(L/K) \text{ by } \operatorname{inv}(u_{L/K}) = \frac{1}{[L : K]}.$$

Clearly $u_{L/K}$ generates $H^2(L/K)$.

Proposition 11.4. *Let $E/L/K$ be fields with E/K normal (and L/K normal if necessary).*

(a) $\operatorname{res} u_{E/K} = u_{E/L}$.

(b) $\inf u_{L/K} = [E : L]u_{E/K}$.

(c) $\operatorname{cor} u_{E/L} = [L : K]u_{E/K}$.

(d) $g^*(u_{E/K}) = u_{gE/gL}$.

Theorem 11.5. *For any normal layer L/K, cup product with $u_{L/K}$ gives an isomorphism*

$$\hat{H}^q(G_{L/K}, \mathbb{Z}) \to \hat{H}^{q+2}(L/K).$$

Proof. This is literally Tate's theorem. □

In particular, for $q = -2$ we get an isomorphism

$$- \smile u_{L/K} : G_{L/K}^{\text{ab}} = \hat{H}^{-2}(G_{L/K}, \mathbb{Z}) \to \hat{H}^0(L/K) \cong A_K/N_{L/K}A_L.$$

So if we can show that $(\operatorname{Gal}(K_0^{\text{sep}}/K), \bigcup_{L/K} C_L)$ is a class formation for any global base field K_0, then we get

$$\operatorname{Gal}(L/K)^{\text{ab}} \cong C_K/NC_L$$

for all L/K normal.

11.2 Strategy for verifying the axioms

We will need to check Hilbert 90, and we will also need to construct this invariant map. Let me outline the strategy.

Lemma 11.6 (first inequality)**.** *For L/K cyclic, $|H^2(L/K)| \geq [L : K]$.*

We will prove this by looking at the Herbrand quotient. In fact, we will show

$$\frac{|H^2(L/K)|}{|H^1(L/K)|} = [L : K].$$

Lemma 11.7 (second inequality)**.** *For L/K cyclic and $[L : K]$ prime, $|H^2(L/K)| \leq [L : K]$.*

This is actually easier to prove analytically. But Chevalley managed to prove this algebraically in the 1940s. This formally implies $|H^1(L/K)| = 1$ and $|H^2(L/K)| \leq [L : K]$ for all L/K. We will then construct an invariant map

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

by patching the local invariant maps together.

12 February 16, 2018

Our goal is now to find $H^q(L/K, C_L)$ for $q = 1, 2$. The first step is to look at $H^q(L/K, \mathbb{A}_L^\times)$.

12.1 Cohomology of the ideles

Let S be a finite set of places of K, and $\overline{S}$ be the places of L lying over S. Then $\mathbb{A}_L^\times$ is covered by

$$\mathbb{A}_{L,S}^\times = \mathbb{A}_{L,\overline{S}}^\times = \prod_{w \in \overline{S}} L_w^\times \times \prod_{w \notin \overline{S}} \mathcal{O}_w^\times.$$

We can then compute

$$\begin{aligned} H^q(L/K, \mathbb{A}_{L,S}^\times) &= H^q\Big(G, \prod_{v \in S}\Big(\prod_{v' \mid v} L_v^\times\Big) \times \prod_{v \notin S}\Big(\prod_{v' \mid v} \mathcal{O}_v^\times\Big)\Big) \\ &= \prod_{v \in S} H^q\Big(G, \prod_{v' \mid v} L_v^\times\Big) \times \prod_{v \notin S} H^q\Big(G, \prod_{v' \mid v} \mathcal{O}_v^\times\Big). \end{aligned}$$

For each v, choose $w \mid v$ and let G_w be the decomposition group of w. We know that G acts on the set $v' \mid v$ transitively. So we can say that

$$\prod_{v' \mid v} \prod_{g \in G/G_w} L_{gw}$$

is the coinduced module. So

$$H^q(G, \textstyle\prod_{v' \mid v} L_{v'}^\times) \cong H^q(G_w, L_w^\times).$$

This isomorphism can be realized explicitly as

$$H^q(G, \textstyle\prod_{v' \mid v} L_{v'}^\times) \xrightarrow{\text{res}} H^q(G_w, \prod_{v' \mid v} L_{v'}^\times) \xrightarrow{\pi_*} H^q(G_w, L_w^\times) \cong H^q(L_w/K_v, L_w^\times).$$

Likewise, we have

$$H^q(G, \textstyle\prod_{v' \mid v} \mathcal{O}_{v'}^\times) \cong H^q(G_w, \mathcal{O}_w^\times) \cong H^q(L_w/K_v, \mathcal{O}_w^\times).$$

The statements are also true for also $\hat{H}^q$.

Suppose that v is unramified in L. Then $\hat{H}^q(K_w/K_v, \mathcal{O}_w^\times)$ vanishes. In particular, if we assume that S contains all ramified places of K, then

$$H^q(L/K, \mathbb{A}_{L,S}^\times) \cong \prod_{v \in S} H^q(L_w/K_v, L_w^\times).$$

Now we can write

$$\mathbb{A}_L^\times = \varinjlim_S \mathbb{A}_{L,S}^\times$$

where S runs over all finite sets containing all ramified places. Then

$$\begin{aligned}\hat{H}^q(L/K, \mathbb{A}_L^\times) &= \varinjlim H^q(L/K, \mathbb{A}_{L,S}^\times) \\ &= \varinjlim_S \prod_{v \in S} H^q(L_w/K_v, K_w^\times) = \bigoplus_v H^q(L_w/K_v, L_w^\times).\end{aligned}$$

An immediate consequence is that

$$H^1(L/K, \mathbb{A}_L^\times) \cong 1.$$

That is, the ideles give a field formation. That is, if we define

$$\mathbb{A}_{K^{\mathrm{sep}}}^\times = \bigcup_{L/K} \mathbb{A}_L^\times,$$

then $(\mathrm{Gal}(K^{\mathrm{sep}}, K), \mathbb{A}_{K^{\mathrm{sep}}}^\times)$ form a field formation.

But this is not a class formation, because we can also compute

$$H^2(L/K, \mathbb{A}_L^\times) \cong \bigoplus_v H^2(L_w/K_v, L_w^\times) \cong \bigoplus_v \tfrac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z}$$

and it is infinite. So this is far off from what we need for a class formation. Later, we are going to see that

$$\bigoplus_v \tfrac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z} \cong H^2(L/K, \mathbb{A}_L^\times) \to H^2(L/K, C_k) \cong \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

is given by adding up the components.

The other interesting thing we can compute is

$$\mathbb{A}_K^\times / N\mathbb{A}_L^\times = \hat{H}^0(L/K, \mathbb{A}_L^\times) \cong \bigoplus_v \hat{H}^0(L_w/K_v, L_w^\times) = \bigoplus_v K_v^\times / NL_w^\times.$$

This is equivalent to the norm theorem for ideles.

Theorem 12.1. *For $(a_v) \in \mathbb{A}_K^\times$, we have $a \in N\mathbb{A}_L^\times$ if and only if $a_v \in NL_w^\times$ for all v.*

There is an analogue for principal ideles, which requires the second inequality.

Theorem 12.2 (Hasse)**.** *For $a \in K^\times$ with $a_v \in K_v^\times$ the v-component, $a \in NL^\times$ if and only if $a_v \in NL_w^\times$ for all v.*

Next, we want to get the Herbrand quotient of $C_L = \mathbb{A}_L^\times / L^\times$ when L/K is cyclic. The problem is that the Herbrand quotient of $\mathbb{A}_L^\times$ is infinite, so we can't use this directly. So we are going to choose S large enough so that $\mathbb{A}_{L,S}^\times \to C_L$ is surjective. This can be done by making $\overline{S}$ generate $\mathrm{Cl}(\mathcal{O}_L)$. Also, let S contain all the ramified primes, all infinite primes, and make S generate $\mathrm{Cl}(K)$. Then we get a short exact sequence

$$1 \to \mathcal{O}_{K,S}^{\times} \to \mathbb{A}_{L,S}^{\times} \to C_L \to 1.$$

So

$$h(C_L) = \frac{h(\mathbb{A}_{L,S}^{\times})}{h(\mathcal{O}_{L,S}^{\times})} = \frac{\prod_{v \in S} [L_w : K_v]}{h(\mathcal{O}_{L,S}^{\times})}.$$

Next time we will calculate the Herbrand quotient of $\mathcal{O}_{L,S}^{\times}$.

13 February 21, 2018

Our goal today is to get something for L/K cyclic extension of global fields. If $G = \mathrm{Gal}(L/K)$ and $|G| = n = [L:K]$, we want to show that $\hat{H}^0(L/K) \geq n$.

13.1 First inequality

We want to compute the Herbrand quotient

$$h(C_L) = \frac{|\hat{H}^0(G, C_L)|}{|\hat{H}^1(G, C_L)|}.$$

If S is a sufficiently large finite set of places of K, we have a short exact sequence

$$1 \to \mathcal{O}_{L,S}^\times \to \mathbb{A}_{L,S}^\times \to C_L \to 1.$$

Last time we showed that

$$h(\mathbb{A}_{L,S}) = \frac{\prod_{v \in S}[L_w : K_v]}{h(\mathcal{O}_{L,S}^\times)},$$

so we need to find $h(\mathcal{O}_{L,S}^\times)$.

Recall that we have the log map of G-modules

$$\mathscr{L} : \mathcal{O}_{L,S}^\times \to \prod_{v' \in \overline{S}} \mathbb{R}^+; \quad (a \mapsto (\log|a|_{v'})_{v' \in \overline{S}}$$

whose image lies in the hyperplane $\sum_{v'} r_{v'} = 0$. The image is a lattice, and so induces an isomorphism

$$\mathcal{O}_{L,S}^\times \otimes_{\mathbb{Z}} \mathbb{R} \cong H.$$

Lemma 13.1. *Let G be a finite group. Let L/K be an extension, with K is infinite. Two finite-dimensional $K[G]$-modules V_1 and V_2 are isomorphic if and only if $V_1 \otimes_K L$ and $V_2 \otimes_K L$ are isomorphic as $L[G]$-modules.*

Proof. Suppose $V_1 \otimes_K L$ and $V_2 \otimes_K L$ are isomorphic as $L[G]$-modules. First, we can reduce to the case when L/K is finitely generated, because the isomorphism is going to be given by some finite number of coefficients. Then by Noether normalization, L is a finite extension of a transcendental extension of K, and the transcendental extension can be taken care easily by specialization. So we only need to consider when L/K is finite.

Now use that there is an isomorphism

$$\mathrm{Hom}_{L[G]}(V_1 \otimes_K L, V_2 \otimes_K L) \cong \mathrm{Hom}_{K[G]}(V_1, V_2) \otimes_K L.$$

Because $V_1 \otimes_K L \cong V_2 \otimes_K L$, there is a determinant map $\mathrm{Hom}_{L[G]}(V_1 \otimes_K L, V_2 \otimes_K L) \to L$, which is nonzero. But this is a polynomial function on $\mathrm{Hom}_{K[G]}(V_1, V_2) \otimes_K L$. So there must be some $\varphi \in \mathrm{Hom}_{K[G]}(V_1, V_2)$ such that $\det \varphi \neq 0$. □

There is another proof using Galois descent. Consider

$$\mathrm{Isom}_{L[G]}(V_1 \otimes L, V_2 \otimes L)$$

which is a torsor for the group $\mathrm{Aut}_{L[G]}(V_1 \otimes L)$. But this is isomorphic to the product of factors $\mathrm{GL}_n(L)$, and $H^1(G, \mathrm{GL}_n(L)) \cong 1$. This shows that there is some $\varphi \in (V_1 \otimes L, V_2 \otimes L)^G$ that gives an isomorphism $V_1 \cong V_2$.

understand

Proposition 13.2. *If A, B are G-modules, finitely generated as abelian groups, and $A \otimes_{\mathbb{Z}} \mathbb{R} \cong B \otimes_{\mathbb{Z}} \mathbb{R}$, then $h(A) = h(B)$.*

Proof. The lemma gives $A \otimes_{\mathbb{Z}} \mathbb{Q} \cong B \otimes_{\mathbb{Z}} \mathbb{Q}$. Then there exists a finite index subgroup $A' \subseteq A/T(A)$ and $B' \subseteq B/T(B)$ such that $A' \cong B'$. Then

$$h(A) = h(A') = h(B') = h(B)$$

because finite groups have Herbrand quotient 1. □

We have an isomorphism

$$\mathcal{O}_{L,S}^\times \otimes_{\mathbb{Z}} \mathbb{R} \cong H \subseteq \prod_{v' \in \overline{S}} \mathbb{R}^+$$

which extends to an isomorphism

$$(\mathcal{O}_{L,S}^\times \oplus \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \prod_{v' \in \overline{S}} \mathbb{R}^+$$

with $(\mathrm{id} \oplus 1) \otimes 1 \mapsto (1, \dots, 1)$. This shows that

$$h(\mathcal{O}_{L,S}^\times \oplus \mathbb{Z}) = h(\mathcal{O}_{L,S}^\times) \cdot n$$

is equal to

$$\begin{aligned} h(\textstyle\prod_{v' \in \overline{S}} \mathbb{Z}) = h(\textstyle\prod_{v \in S} \prod_{v' \mid v} \mathbb{Z}) &= \prod_{v \in S} h(\mathrm{coind}_{G_w}^G \mathbb{Z}) \\ &= \prod_{v \in S} h(G_w, \mathbb{Z}) = \prod_{v \in S} |G_w| = \prod_{v \in S} [L_w : K_v]. \end{aligned}$$

Therefore

$$h(\mathcal{O}_{L,S}^\times) = \frac{\prod_{v \in S} [L_w : K_v]}{n}$$

and so

$$h(C_L) = \frac{h(\mathbb{A}_{L,S}^\times)}{h(\mathcal{O}_{L,S})} = n.$$

The conclusion is that

$$|\hat{H}^0(L/K, C_L)| = [L : K] |H^1(L/K, C_L)| \geq [L : K].$$

Here, we have

$$C_K / N C_L = \mathbb{A}_K^\times / K^\times \cdot N \mathbb{A}_L^\times.$$

14 February 23, 2018

We showed that $|\hat{H}^0(L/K, C_L)| \geq [L : K]$ for L/K a cyclic extension of global fields. By the way we have

$$C_K/NC_L \cong \mathbb{A}_K^\times/N\mathbb{A}_L^\times \cdot K^\times.$$

14.1 Algebraic weak Chebotarev

Corollary 14.1. *Suppose L/K is abelian, and let $D \subseteq N_{L/K}\mathbb{A}_L^\times \subseteq \mathbb{A}_K^\times$ be a subgroup. If $K^\times D$ is dense in $\mathbb{A}_K^\times$, then $L = K$.*

Proof. First we reduce to when L/K is cyclic. If L/K is abelian, there exists a $L' \subseteq L$ with L'/K cyclic. Then we can replace L by L'.

Observe that $N_{L/K}\mathbb{A}_L^\times$ is open in $\mathbb{A}_K^\times$. So $K^\times \cdot N_{L/K}\mathbb{A}^\times$ is open in $\mathbb{A}_K^\times$, and hence closed. But $K^\times D$ is dense. This shows that $K^\times \cdot N_{L/K}\mathbb{A}_L^\times = \mathbb{A}_K^\times$. So $1 = |\mathbb{A}_K^\times/N_{L/K}\mathbb{A}_L^\times| \geq [L : K]$. So $L = K$. □

Corollary 14.2. *Let L/K be a finite abelian extension with $L \neq K$. Then there are infinitely many primes of K that do not split completely in L.*

Proof. Suppose there are finitely many prime that are not split completely. Let S be this set of primes that don't split completely, and also the infinite primes, and set

$$D = \{x \in \mathbb{A}_K^\times : x_v = 1 \text{ for all } v \in S\}.$$

I need to check that $D \subseteq N_{L/K}\mathbb{A}_L^\times$. If $v \notin S$ then $L_w = K_v$ so $NL_w^\times = K_v^\times$. We also need to check that $K^\times D$ is dense in $\mathbb{A}_K^\times$. This is equivalent to $K^\times$ being dense in $\prod_{v \in S} K_v^\times$. This is the weak approximation. So the technical lemma implies that $L = K$. □

Corollary 14.3. *If S is a finite set of places of K, and L/K is finite abelian, then* $\mathrm{Gal}(L/K)$ *is generated by*

$$\left(\frac{L/K}{v}\right) = \mathrm{Frob}_v \in \mathrm{Gal}(L/K)$$

for $v \notin S$.

Proof. Without loss of generality, assume that S contains all ramified and infinite primes. Let $H \subseteq \mathrm{Gal}(L/K)$ be generated by $\{\mathrm{Frob}_v : v \notin S\}$. Let $M \subseteq L$ be the subfield fixed by H. For any $v \notin S$, we then have that Frob_v fixes M. But Frob_v is the generator of the decomposition group, and so v splits completely in M/K. This shows that $H = \mathrm{Gal}(L/K)$. □

14.2 Reduction of the second inequality to Kummer extensions

We now want to prove the second inequality. We want to prove that

Proposition 14.4. *If L/K and $[L:K]=p$, then*

$$|\hat{H}^0(L/K, C_L)| = |C_K/N_{L/K}C_L| \leq p.$$

First we reduce to the case where K contains μ_p. If $[L:K]=p$ as above, let $L' = L(\zeta_p)$ and $K' = K(\zeta_p)$. Because $d = [K':K]$ divides $p-1$, it is relatively prime to p and so $[L':K'] = p$ and $[L':L] = d$. Now we have

$$\begin{tikzcd}
C_L \arrow[r, hook] \arrow[d, "N_{L/K}"] & C_{L'} \arrow[r, "N_{L'/L}"] \arrow[d, "N_{L'/K'}"] & C_L \arrow[d, "N_{L/K}"] \\
C_K \arrow[r, hook] \arrow[d] & C'_K \arrow[r, "N_{K'/K}"] \arrow[d] & C_K \arrow[d] \\
C_K/N_{L/K}C_L \arrow[r] \arrow[d] & C_{K'}/N_{L'/K'}C_{L'} \arrow[r] \arrow[d] & C_K/N_{L/K}C_L \arrow[d] \\
1 & 1 & 1.
\end{tikzcd}$$

But $C_K^p \subseteq N_{L/K}C_L$ and so $C_K/N_{L/K}C_L$ has exponent p. Also, the composite of two horizontal arrows is multiplication by d. So $\times d : C_K/NC_L \to C_K/NC_L$ is an isomorphism, and this shows that

$$|C_K/N_{L/K}C_L| \leq |C_{K'}/N_{L'/K'}C_{L'}|.$$

Therefore it is enough to show the second inequality for L'/K'. So we may assume that L/K is a cyclic extension with $\mu_p \subseteq K$. By Kummer theory, we have

$$L = K(\sqrt[p]{a})$$

for some $a \in K^\times$.

We need to bound $[\mathbb{A}_K^\times : K^\times \cdot \mathbb{A}_L^\times]$. We will replace $N\mathbb{A}_L^\times$ with a smaller subgroup $F \subseteq N\mathbb{A}_L^\times$ and then bound $[\mathbb{A}_K^\times : K^\times F]$. Let S be a finite set of places of K containing all ramified places, and let $v_1, \ldots, v_k$ be places of K that split completely in L. Let $S^* = S \cup \{v_1, \ldots, v_k\}$. Then we take

$$F = \prod_{v \in S} (K_v)^p \cdot \prod_{1 \leq i \leq k} K_{v_i}^\times \times \prod_{v \notin S^*} \mathcal{O}_v^\times.$$

Then $F \subseteq N\mathbb{A}_L^\times$ because $(K_v)^p \subseteq NL_w^\times$ for $v \in S$, $K_{v_i} = NL_{w_i}^\times$, and $\mathcal{O}_v^\times \subseteq NL_w^\times$ because L_w/K_v is unramified.

15 February 26, 2018

Let L/K be cyclic with $[L:K]=p$. Assume $K \supseteq \mu_p$. We need to show that

$$|\mathbb{A}_K^\times / N\mathbb{A}_L^\times \cdot K| \leq p.$$

We will choose $F \subseteq N\mathbb{A}_L^\times$ and show that $|\mathbb{A}_K^\times / K^\times F| \leq p$. We will take

$$F = \prod_{v \in S} (K_v^\times)^p \times \prod_{1 \leq i \leq k} K_{v_i} \times \prod_{v \in S^*} \mathcal{O}_V^\times.$$

Last time we checked that $F \subseteq NL^\times$ provided that S contains all ramified primes in L/K.

Proposition 15.1. *Let K be a global field, and v a finite place of K. Assume that K_v does not have residue characteristic p, with $b \in K^\times$. Then v is ramified in $K(\sqrt[p]{b})/K$ if and only if $b \in \mathcal{O}_v^\times \cdot (K_v^\times)^p$. Also, v is split if and only if $b \in (K_v^\times)^p$.*

Proof. Exercise. □

Corollary 15.2. *If we choose S such that S contains primes of K dividing p, and also all v such that $|a|_v \neq 1$, then L/K is unramified outside S.*

15.1 Computing the size of the quotient

We also want S large enough that $\mathbb{A}_{K,S}^\times \twoheadrightarrow C_K$. Then

$$\mathbb{A}_{K,S^*}^\times \twoheadrightarrow \mathbb{A}_K^\times / K^\times \cdot F.$$

The kernel is going to be

$$\mathbb{A}_{K,S^*}^\times \cap K^\times F = F \cdot (K^\times \cap \mathbb{A}_{K,S^*}^\times) = F \cdot \mathcal{O}_{K,S^*}^\times.$$

So we get

$$1 \to F \cdot \mathcal{O}_{K,S^*}^\times \to \mathbb{A}_{K,S^*}^\times \to \mathbb{A}_K^\times / K^\times F \to 1.$$

In particular,

$$[\mathbb{A}_K : K^\times F] = |\mathbb{A}_{K,S^*}^\times / F \cdot \mathcal{O}_{K,S^*}^\times|.$$

We also have

$$1 \to \mathcal{O}_{K,S^*}/(F \cap \mathcal{O}_{K,S^*}) \cong F \cdot \mathcal{O}_{K,S^*}/F \to \mathbb{A}_{K,S^*}^\times / F \to \mathbb{A}_{K,S^*}^\times / F \cap \mathcal{O}_{K,S^*}^\times \to 1.$$

That is,

$$|\mathbb{A}_K^\times / K^\times F| = \frac{|\mathbb{A}_{K,S^*}^\times / F|}{|\mathcal{O}_{K,S^*}^\times / F \cap \mathcal{O}_{K,S^*}^\times|}.$$

So we have broken up this into a local computation and a global computation.

Let us first look at the local component. We have

$$|\mathbb{A}_{K,S^*}/F| = \left|\prod_{v\in S} K_v^\times/(K_v^\times)^p\right|.$$

But by the homework, we have

$$|K_v^\times/(K_v^\times)^p| = p^2 \cdot |p|_v^{-1}$$

if $\mu_p \subseteq K$. This shows that

$$|\mathbb{A}_{K,S^*}^\times/F| = \prod_{v\in S} p^2|p|_v^{-1} = p^{2|S|},$$

because S contained all v such that $|p|_v \neq 1$.

Now let us do the global computation. Observe that

$$F \cap \mathcal{O}_{K,S^*}^\times \supseteq \mathcal{O}_{K,S^*}^p.$$

Then

$$|\mathcal{O}_{K,S^*}^\times/F \cap \mathcal{O}_{K,S^*}^\times| = \frac{|\mathcal{O}_{K,S^*}^\times/(\mathcal{O}_{K,S^*}^p|}{|F \cap \mathcal{O}_{K,S^*}/(\mathcal{O}_{K,S^*}^\times)^p|}.$$

By Dirichlet's unit theorem, we have

$$\mathcal{O}_{K,S^*}^\times \cong \mathbb{Z}^{|S_*|-1} \oplus \text{torsion},$$

where the torsion group contains μ_p. So we get

$$|\mathcal{O}_{K,S^*}^\times/(\mathcal{O}_{K,S^*}^\times)^p| = p^{|S_*|} = p^{|S|+k}.$$

Combining everything we have, we get

$$|\mathbb{A}_K^\times/K^\times F| = \frac{|\mathbb{A}_{K,S^*}^\times/F|}{|\mathcal{O}_{K,S^*}^\times/F \cap \mathcal{O}_{K,S^*}|} = p^{|S|-k}[F \cap \mathcal{O}_{K,S^*}^\times : (\mathcal{O}_{K,S^*}^\times)^p].$$

The claim is that we can pick $v_1, \dots, v_k$ such that $k = |S| - 1$ and $F \cap \mathcal{O}_{K,S^*}^\times = (\mathcal{O}_{K,S^*}^\times)^p$. Also, recall that $v_1, \dots, v_k$ had to be split completely in L.

15.2 Choosing the completely split places

Proposition 15.3. *Suppose $v_1, \dots, v_k$ are places of K such that if $K(\sqrt[p]{b})$ is unramified outside $v_1, \dots, v_k$ and split at all places of S, then $b \in (K^\times)^p$. Then $F \cap \mathcal{O}_{K,S^*}^\times = (\mathcal{O}_{K,S^*}^\times)^p$.*

Proof. Suppose that $b \in F \cap \mathcal{O}_{K,S^*}^\times$. By the exercise, we know that $K(\sqrt[p]{b})/K$ is split at all $v \in S$, and also that $K(\sqrt[p]{b})$ is split at all $v \in S$. Then $b \in (K^\times)^p$, and because $b \in \mathcal{O}_{K,S^*}^\times$, we have $b \in (\mathcal{O}_{K,S^*}^\times)^p$. □

Now we would like to choose $v_1, \ldots, v_k$ given only S. Consider the auxiliary extension

$$T = K(\sqrt[p]{\mathcal{O}_{K,S}^\times}),$$

which has exponent p. Then

$$\mathrm{Gal}(T/K) \cong \mathrm{Hom}(\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p, \mu_p) \cong (\mathbb{Z}/p\mathbb{Z})^{|S|}.$$

Note that $L = K(\sqrt[p]{a}) \subseteq T$. Now we choose places $w_1, \ldots, w_k$ of L such that

$$\mathrm{Frob}(w_i) = \left(\frac{T/L}{w_i}\right) \in \mathrm{Gal}(T/L)$$

form a basis for the $\mathbb{F}_p$-vector space $\mathrm{Gal}(T/L)$.

16 February 28, 2018

Last time we reduced the second inequality to, given S, finding additional places $v_1, \dots, v_k$ with $k = |S| - 1$ such that

- $v_1, \dots, v_k$ all split totally in L/K, and
- if $K(\sqrt[p]{b_i})$ is unramified outside $v_1, \dots, v_k$ and completely splits at all $v \in S$ then $b \in (K^\times)^p$.

16.1 Finishing the second inequality

To do this, we looked at the auxiliary extension

$$T = K\big(\sqrt[p]{\mathcal{O}_{K,S}^\times}\big)$$

and tried to find L inside T. Choose $w_1, \dots, w_k$ be places of L such that $\mathrm{Frob}_{w_1}, \dots, \mathrm{Frob}_{w_k}$ form a basis for $\mathrm{Gal}(T/L) \cong (\mathbb{Z}/p\mathbb{Z})^k$. Then take v_i to be places of K below w_i. First of all, note that

$$\mathrm{Frob}_{w_i} = \mathrm{Frob}_{v_i}^{e_i}$$

where e_i is the inertia degree. But $e_i = 1$ or $e_i = p$, but it can't be that $e_i = p$ because then $\mathrm{Frob}_{w_i} = \mathrm{Frob}_{v_i}^p = \mathrm{id}$. So we get $e_i = 1$ so that v_i is split.

So we have $\mathrm{Frob}_{v_i} = \mathrm{Frob}_{w_i}$ inside $\mathrm{Gal}(T/K)$. So they generate the subgroup $\mathrm{Gal}(T/L)$ which is of index p in $\mathrm{Gal}(T/K)$. Let v_{k+1} be a place such that $(\mathrm{Frob}_{v_i})_{1 \le i \le k+1}$ generate $\mathrm{Gal}(T/K)$.

Lemma 16.1. $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \to \prod_{i=1}^{k+1} \mathcal{O}_{v_i}^\times/(\mathcal{O}_{v_i}^\times)^p$ *is bijective.*

Proof. For injectivity, we use Kummer theory. If $[c] \in \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p$ is in the kernel, then $K(\sqrt[p]{c})$ is a Kummer extension. For $1 \le i \le k+1$ and $c \in (\mathcal{O}_{v_i}^\times)^p$, so v_i splits completely in $K(\sqrt[p]{c}$. This means that Frob_{v_i} is the identity on $K(\sqrt[p]{c})$. So all of $\mathrm{Gal}(T/K)$ acts trivially on $K(\sqrt[p]{c})$, and this shows that $K(\sqrt[p]{c}) = K$.

For surjectivity, we count the size. We have

$$|\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p| = p^{|S|} = p^{k+1}.$$

By the homework, we have $|\mathcal{O}_{v_i}^\times/(\mathcal{O}_{v_i}^\times)^p| = p$ for all i. So the right hand side also has order p^{k+1}. □

Corollary 16.2. $\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p \twoheadrightarrow \prod_{i=1}^{k} \mathcal{O}_{v_i}^\times/(\mathcal{O}_{v_i}^\times)^p$ *is surjective.*

Now let us check the second condition on v_i. Suppose $M = K(\sqrt[p]{b})$ is a Kummer extension such that M/K is unramified outside $v_1, \dots, v_k$ and completely split at S. We need to show that $b \in (K^\times)^p$. Let

$$D = \prod_{v \in S} K_v^\times \times \prod_{v_i} (K_{v_i}^\times)^p \times \prod_{v \notin S^*} \mathcal{O}_v^\times.$$

Then $D \subseteq N\mathbb{A}_M^\times$ because we can check this locally. Note that $D \cdot K^\times$ contains $D \cdot \mathcal{O}_{K,S}^\times$. By the corollary, it includes $\mathbb{A}_{K,S}^\times = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$. That is, $D \cdot K^\times \supseteq \mathbb{A}_S^\times$. Recall that

$$\mathbb{A}_{K,S}^\times \twoheadrightarrow \mathbb{A}_K^\times / K^\times$$

by definition of S. Therefore $D \cdot K^\times = \mathbb{A}_K^\times$. By the corollary the first inequality, we get $[M : K] = 1$ as needed. This completes the proof of the second inequality.

16.2 Immediate corollaries

In the first inequality, for L/K cyclic, we showed that

$$\frac{|\hat{H}^0(L/K, C_L)|}{|H^1(L/K, C_L)|} = [L : K].$$

From the second inequality, for L/K cyclic and prime, we showed that

$$|\hat{H}^0(L/K, C_L)| \leq [L : K] = p.$$

Then we immediately get

$$H^1(L/K, C_L) = 1, \quad |\hat{H}^0(L/K, C_L)| = |H^2(L/K, C_L)| = p.$$

By the homework, this implies that

$$H^1(L/K, C_L) = 1, \quad |H^2(L/K, C_L)| \mid [L : K]$$

for all L/K. (This was done by first showing for p-groups, and then showing it for all groups using Sylow subgroups.)

Corollary 16.3. *If L/K is abelian, then the map*

$$H^2(L/K, L^\times) \to H^2(L/K, \mathbb{A}_L^\times) \cong \bigoplus_v H^2(L_w/K_v, L_w^\times)$$

is injective.

Proof. Use the sequence $1 \to L^\times \to \mathbb{A}_L^\times \to C_L \to 1$. □

Corollary 16.4 (Hasse norm theorem)**.** *Let L/K be a cyclic extension of number fields, and $a \in K^\times$. Then $a \in NL^\times$ if and only if $a \in NL_w^\times$ for all primes w of L.*

Proof. This is equivalent to the injectivity of

$$K^\times/NL^\times \cong \hat{H}^0(L/K, L^\times) \to \bigoplus \hat{H}^0(L_w/K_v, L_w^\times) \cong \bigoplus K_v^\times/NL_w^\times.$$

This follows from $\hat{H}^{-1}(L/K, C_L) \cong H^1(L/K, C_L) = 0$. □

Note that this only true for cyclic extensions. Here is a counter example. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, and $a = -1$.

Next, we will build the invariant map

$$\text{inv} : H^2(L/K, C_L) \to \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

we will construct this as the direct sum of local invariant maps, but it will take some work to show that this gives a well-defined map. Here we are going to do for "nice extensions", i.e., cyclic cyclotomic extensions.

17 March 2, 2018

From this point on, all fields are number fields unless stated otherwise. For Kummer theory, we already needed characteristic zero. We have two recprocities we want to prove:

- inv-reciprocity: if $a \in H^2(L/K, L^\times) \to H^2(L_w/K_v, L_w^\times)$ then
$$\sum_v \operatorname{inv}_v \alpha = 0.$$
- θ-reciprocity: if L/K is abelian, for $a \in K^\times$
$$\prod_v \theta_{L_w/K_v}(a) = 1.$$

Note that last time we showed for L/K finite Galois, we have
$$H^2(L/K, L^\times) \hookrightarrow \bigoplus_v H^2(L_w/K_v, L_w^\times).$$

If we put all L together, we get
$$\operatorname{Br}(K) = H^2(K, \overline{K}^\times) \hookrightarrow \bigoplus_v H^2(K_v, \overline{K}_v^\times) = \bigoplus_v \operatorname{Br}(K_v) \cong \bigoplus_v \mathbb{Q}/\mathbb{Z}.$$

That is, $\alpha \in \operatorname{Br}(K)$ is zero if and only if $\operatorname{inv}_v(\alpha) = 0$ for all v.

17.1 Reduction to cyclic cyclotomic extensions

Proposition 17.1. *Let K be a number field, and $\alpha \in \operatorname{Br}(K) = H^2(K, \overline{K}^\times)$. Then there exists a cyclic cyclotomic extension L/K such that $\operatorname{res}_{L/K} \alpha = 0 \in \operatorname{Br} L$.*

We are going to say that "L splits α" in this case. By the inflation-restriction sequence, this is equivalent to α being in the image of $\inf : H^2(L/K, L^\times) \to \operatorname{Br}(K)$.

Proof. Consider
$$\begin{tikzcd}
\operatorname{Br}(K) \arrow[r, "\operatorname{res}"] \arrow[d] & \operatorname{Br}(L) \arrow[d] \\
\operatorname{Br}(K_v) \arrow[r, "\operatorname{res}"] \arrow[d, "\cong"', "\operatorname{inv}_v"] & \operatorname{Br}(L_w) \arrow[d, "\cong"', "\operatorname{inv}_w"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\times[L_w:K_v]"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

So for L to split α, we just need $[L_w : L_v] \operatorname{inv}_v(\alpha) = 0$ for all v. In other words, for any v with $\operatorname{inv}_v(\alpha) \neq 0$ in $\mathbb{Q}/\mathbb{Z}$ (this happens for only finitely many v) we need $[L_w : K_v]$ to be a multiple of the order of $\operatorname{inv}_v(\alpha) \in \mathbb{Q}/\mathbb{Z}$. It follows from the following lemma. □

Lemma 17.2. *Let S be a finite set of finite primes of K, and let $m > 0$ be an integer. There exists a totally complex cyclic cyclotomic extension L/K such that $m \mid [L_w : K_v]$ for all $v \in S$.*

Proof. We reduce to the case $K = \mathbb{Q}$ by replacing m with $m \cdot [K : \mathbb{Q}]$. Then for each prime ℓ, take $\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q}$ which contains a cyclic subfield of order ℓ^{r-1} or ℓ^{r-2}, and combine them for different ℓ. □

17.2 Invariant and reciprocity maps

Definition 17.3. We define

$$\operatorname{inv}_{L/K} : H^2(L/K, \mathbb{A}_L^\times) \to \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}; \quad c \mapsto \sum_v \operatorname{inv}_{L_w/K_v} c.$$

inv-reciprocity then states that inv vanishes on $H^2(L/K, L^\times) \hookrightarrow H^2(L/K, \mathbb{A}_L^\times)$. There are compatibilities

- $\operatorname{inv}_{N/K}(\operatorname{inf}_{N/L} c) = \operatorname{inv}_{L/K}(c)$,
- $\operatorname{inv}_{N/L}(\operatorname{res}_{L/K} c) = [L : K] \operatorname{inv}_{N/K}(c)$,
- $\operatorname{inv}_{N/L}(\operatorname{cor}_{L/K} c) = \operatorname{inv}_{N/K}(c)$,

following from the local compatibilities. For instance,

$$\begin{aligned}\operatorname{inv}_{N/L}(\operatorname{res}_{L/K} c) &= \sum_w \operatorname{inv}_{N_{w'}/L_w}(\operatorname{res}_{L_w/K_v} c) = \sum_w [L_w : K_v] \operatorname{inv}_{N_{w'}/K_v} c \\ &= \sum_v \sum_{w|v} [L_w : K_v] \operatorname{inv}_{N_{w'}/K_v}(c) = \sum_v [L : K] \operatorname{inv}_{N_{w'}/K_v} c \\ &= [L : K] \operatorname{inv}_{N/K} c.\end{aligned}$$

So $\bigcup_{L/K} \mathbb{A}_L^\times$ looks almost like a class formation, except that the map inv is not an isomorphism. The inv is clearly not injective, and it even is sometimes not surjective, because the image of $\operatorname{inv}_{L/K}$ is $\frac{1}{\operatorname{lcm}([L_w:K_v])}\mathbb{Z}/\mathbb{Z}$. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$ for instance.

Definition 17.4. For L/K abelian, we define

$$\theta_{L/K} : \mathbb{A}_K^\times \to \operatorname{Gal}(L/K); \quad a \mapsto \prod_v \theta_{L_w/K_v}(a).$$

Proposition 17.5. *For any character $\chi : \operatorname{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$, considered as an element of $H^1(L/K, \mathbb{Q}/\mathbb{Z})$, we have*

$$\chi(\theta_{L/K}(a)) = \operatorname{inv}_{L/K}([a] \smile \delta\chi)$$

Proof. It follows from the local case. □

Corollary 17.6. *If L/K is abelian, then* inv*-reciprocity implies θ-reciprocity. If L/K is cyclic, then θ-reciprocity implies* inv*-reciprocity.*

Proof. Suppose L/K is abelian and we have inv-reciprocity. Then

$$\chi(\theta_{L/K}(a)) = 0$$

for all $a \in K^\times$ and χ, and so $\theta_{L/K}(a) = 1$.

If L/K is cyclic and we have θ-reciprocity, take χ to be a generator of $H^1(L/K, \mathbb{Q}/\mathbb{Z})$. Then $\delta\chi$ generates $H^2(L/K, \mathbb{Z})$ and so taking cup product with $\delta\chi$ is an isomorphism. θ-reciprocity gives that

$$\mathrm{inv}_{L/K}([a] \smile \delta\chi) = 0$$

for all $a \in K^\times$, and so $\mathrm{inv}_{L/K} = 0$. □

We will first prove θ-reciprocity for $L/\mathbb{Q}$ cyclotomic, deduce inv-reciprocity for $L/\mathbb{Q}$ cyclic cyclotomic, deduce inv-reciprocity for L/K Galois, and then θ-reciprocity for L/K abelian.

18 March 5, 2018

We had two reciprocities we wanted to check:

- θ-reciprocity: for all $a \in L^\times$, $\prod_v \alpha_v(a) = 1$.
- inv-reciprocity: for all L/K and $a \in H^2(L/K, L^\times)$, $\sum_v \operatorname{inv}_v a = 0$.

We proved two things:

- if L/K is cyclic, then θ-reciprocity implies inv-reciprocity.
- if L/K is abelian, then inv-reciprocity implies θ-reciprocity.

18.1 θ-reciprocity for cyclotomic fields

We are going to first check θ-reciprocity for $K = \mathbb{Q}$ and L cyclotomic. This means that L is contained in $\mathbb{Q}(\zeta_n)$, but it is enough to check for $L = \mathbb{Q}(\zeta_n)$ by the compatibility conditions, and further more, check for $L = \mathbb{Q}(\zeta_{\ell^r})$. We want to check that

$$\theta : \mathbb{Q}^\times \to \operatorname{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q}); \quad \theta(a) = \prod_v \theta_v(a)$$

is zero. We can check this for a primes and -1.

For $a = p \neq \ell$, we have

$$\theta_{p'}(p) = 1 \text{ for } p' \neq p, \ell, \quad \theta_p(p) = \operatorname{Frob}_p(\zeta \mapsto \zeta^p)$$

because $\mathbb{Q}_v(\zeta_{\ell^r})/\mathbb{Q}$ is unramified. On the other hand, because $\mathbb{Q}_\ell(\zeta_{\ell^r})$ is a Lubin–Tate extension, we have

$$\theta_\ell(p) : \zeta \mapsto \zeta^{(p^{-1})}.$$

Also, $\theta_\infty(p) = 1$, so we get cancellation.

For $a = \ell$, we have $\theta_{p'}(\ell) = 1$ for $p' \neq \ell$ and $\theta_\ell(\ell) = 1$ and $\theta_\infty(\ell) = 1$. For $a = -1$, we have $\theta_{p'}(-1) = 1$ for $p' \neq \ell$ and $\theta_\ell(-1) : \zeta \mapsto \zeta^{-1}$ and $\theta_\infty(-1)$ is complex conjugation.

So we have checked θ-reciprocity for $L/\mathbb{Q}$ cyclic cyclotomic, and so inv-recipcority for $L/\mathbb{Q}$ cyclic cyclotomic. But from last time we have that

$$\operatorname{Br}(\mathbb{Q}) = \bigcup_{L/\mathbb{Q}} H^2(L/\mathbb{Q}, L^\times)$$

for $L/\mathbb{Q}$ cyclic cyclotomic. So we get inv-reciprocity for $L/\mathbb{Q}$ arbitrary.

For arbitrary L/K, we can enlarge L to L' with $L'/\mathbb{Q}$ Galois. Then we get

$$\begin{tikzcd}
H^2(L/K), L^\times) \arrow[r, "\text{inf}"] \arrow[d, "\text{inv}"] & H^2(L'/K, (L')^\times) \arrow[r, "\text{cor}"] \arrow[d, "\text{inv}"] & H^2(L'/\mathbb{Q}, (L')^\times) \arrow[d, "\text{inv}=0"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Because the horizontal maps on the top row are injective, we get that the invariant map $H^2(L/K, L^\times) \to \mathbb{Q}/\mathbb{Z}$ is zero. This shows inv-reciprocity, and thus θ-reciprocity for any L/K abelian.

18.2 Invariant map on the class group

Now we have (for L/K abelian) a map

$$\theta_{L/K} : C_K/NC_L = \mathbb{A}_K^\times/N\mathbb{A}_L^\times \cdot K^\times \to \mathrm{Gal}(L/K).$$

Also, by inv-reciprocity, we have

$$H^2(L/K, L^\times) \hookrightarrow H^2(L/K, \mathbb{A}_L^\times) \xrightarrow{\mathrm{inv}} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

This is not always a short exact sequence, because we don't always have surjectivity on the right.

Proposition 18.1. *If L/K is cyclic, then*

$$1 \to H^2(L/K, L^\times) \xrightarrow{i_*} H^2(L/K, \mathbb{A}_L^\times) \xrightarrow{\mathrm{inv}} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact.

Proof. We first show that the invariant map is surjective. We can describe explicitly the image, because $H^2(L/K, \mathbb{A}_L^\times) \cong \bigoplus_v H^2(L_w/K_v, L_w^\times)$. Then it is enough to show that $\mathrm{lcm}([L_w : K_v]) = [L : K]$. Recall that $\mathrm{Frob}_v \in \mathrm{Gal}(L/K)$ generate, because the order of Frob_v is equal to $[L_w : K_v]$, we get $\mathrm{lcm} = [L : K]$.

Now we show that the kernel of inv is equal to the image of i_*. We have an exact sequence

$$1 \to H^2(L/K, L^\times) \xrightarrow{i_*} H^2(L/K, \mathbb{A}_L^\times) \xrightarrow{j_*} H^2(L/K, C_L) \to H^3(L/K, L^\times) = 1.$$

But we know that by the second inequality,

$$|H^2(L/K, C_L)| \leq [L : K].$$

By comparing the two sequences, we get that both sequences are exact. □

Moreover, we get an isomorphism

$$\mathrm{inv} : H^2(L/K, C_L) \xrightarrow{\cong} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

This works to define the correct invariant map for L/K cyclic. We are going to do the same thing we did last time, which is to first define the map for special (last semester, for unramified extensions) and then extend it to the general case.

Lemma 18.2. *Let L/K be Galois, and let L'/K be cyclic with $[L' : K] = [L : K]$. Then $H^2(L/K, C_L)$ and $H'(L'/K, C_{L'})$ have the same image inside $H^2(\overline{K}/K, C_{\overline{K}} = \bigcup_M C_M)$.*

19 March 7, 2018

Today we are going to finish proving that everything is a class formation. Last time we defined the invariant map

$$\mathrm{inv} : H^2(L/K, C_L) \to \tfrac{1}{[L:K]}\mathbb{Z} \to \mathbb{Z}$$

for L/K cyclic. We will extend this to all L/K finite Galois.

19.1 C_K form a class formation

Lemma 19.1. *If L/K is Galois and L'/K is cyclic, and $[L' : K] = [L : K]$ then $H^2(L/K)$ and $H^2(L'/K)$ have the same image in $H^2(\overline{K}/K)$.*

Proof. First we want to show that $\inf(H^2(L'/K)) \subseteq \inf(H^2(L/K))$. Take $K = L \cdot L'$ the compositum. Then L'/K is cyclic, the extension N/L is also cyclic with degree $[N : L] \mid [L' : K]$. If $c \in H^2(L'/K)$, I need to show that

$$\inf_{N/L'}(c) \in \operatorname{im} \inf_{N/L} = \ker \operatorname{res}_{L/K}.$$

(Here, we are using the inflation-restriction sequence.) Choose $\tilde{c} \in H^2(L'/K, \mathbb{A}_{L'}^\times)$ such that $j_*(\tilde{c}) = c$. Then we need to check that

$$\mathrm{inv}_{N/L} \operatorname{res}_{L/K} \inf_{N/L'} j_*(\tilde{c}) = 0 \in \tfrac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}.$$

But this thing is

$$\mathrm{inv}_{N/L} j^* \operatorname{res}_{L/K} \inf_{N/L'}(\tilde{c}) = \mathrm{inv}_{N/L} \operatorname{res}_{L/K} \inf_{N/L}(\tilde{c}) = [L : K] \,\mathrm{inv}_{L'/K}(\tilde{c}) = 0$$

because the invariant map $\mathrm{inv}_{N/L}$ from the second term is on $\mathbb{A}^\times$ and so is local. This shows that $\inf(H^2(L'/K))$ is contained in $\inf(H^2(L/K))$. But note that the size of $H^2(L'/K)$ is equal to $[L' : K]$ and the second inequality shows that the size of $H^2(L/K)$ is at most $[L : K]$. This shows the other containment as well. □

Now we can define

$$\mathrm{inv} : H^2(\overline{K}/K) \to \mathbb{Q}/\mathbb{Z}$$

by considering

$$H^2(\overline{K}/K) \cong \varinjlim_{L/K} H^2(L/K) \cong \varinjlim_{L'/K \text{ cyclic}} H^2(L'/K).$$

For any L/K, this restricts to an isomorphism

$$H^2(L/K) \xrightarrow{\mathrm{inv}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

Thus we have verified all the axioms of class formations.

19.2 Consequences

We can identify a fundamental class $u_{L/K}$ with

$$\operatorname{inv}_{L/K}(u_{L/K}) = \frac{1}{[L:K]}.$$

We then have, by Tate's theorem, an isomorphism

$$\smile u_{L/K} : \hat{H}^i(L/K, \mathbb{Z}) \to \hat{H}^{i+2}(L/K, C_L)$$

is an isomorphism for all i. The i that we really care about is $i = -2$, and this gives us

$$\smile u_{L/K} : \operatorname{Gal}(L/K)^{\mathrm{ab}} = \hat{H}^{-2}(L/K, \mathbb{Z}) \to \hat{H}^0(L/K, C_L) = C_K/NC_L.$$

The inverse map is what we denote by

$$\theta : C_K/NC_L \to \operatorname{Gal}(L/K)^{\mathrm{ab}}.$$

This map is actually going to be the same as the product of the local θs. By the argument as last semester, for all characters $\chi : \operatorname{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ and $a \in C_K$, we have an equality

$$\chi(\theta_{L/K}(a)) = \operatorname{inv}_{L/K}(a \smile \delta\chi).$$

This characterizes $\theta_{L/K}$, so if I consider $\theta'_{L/K} : C_K/NC_L = \mathbb{A}_K^\times/K^\times N\mathbb{A}_L^\times \to \operatorname{Gal}(L/K)$ by the product of the local reciprocity maps, we previously checked that

$$\chi(\theta'(a)) = \operatorname{inv}(a \smile \delta\chi)$$

using the invariant map $H^2(L/K, \mathbb{A}_L^\times) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

Note that $\theta_{L/K} : C_K/NC_L \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$ is continuous using the adelic topology on C_K. This is because $N_{L/K}C_L$ are closed in C_K. To see this, just note that

$$C_L \cong C_L^0 \times \mathbb{R}^{>0}, \quad C_K \cong C_K^0 \times \mathbb{R}^{>0}$$

with the image of $N_{L/K}C_L^0$ being closed in C_K^0 by compactness. Taking them all together gives a continuous map

$$\theta_{/K} : C_K \to \varprojlim_L \operatorname{Gal}(L/K)^{\mathrm{ab}} = \operatorname{Gal}(K^{\mathrm{ab}}/K).$$

This has dense image, because each $C_K \to \operatorname{Gal}(L/K)^{\mathrm{ab}}$ is surjective. The kernel is the intersection

$$\ker \theta_{/K} = \bigcap_{L/K} NC_L.$$

So we need to ask again which subgroups $A \subseteq C_K$ are normic, i.e., equal to NC_L for some L/K finite Galois. Note that it must be a finite index open subgroup. We are going to show that this is actually enough. Roughly, this is going to be the same argument from last semester, which is doing a lot of Kummer theory.

Note that if A is normic, so is $A' \supseteq A$, because we have our finite reciprocity map θ. If A and B are normic, so is $A \cap B$. What we are going to do is to pick a sequence of open subgroups and show that each of them are normic.

20 March 9, 2018

Recall that we now have the reciprocity map

$$\theta_{/K} : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

that is continuous with dense image. Moreover, we can only take the image of C_K^0 the content zero stuff, because we can adjust the infinite part to make anything have content zero. So the image is compact and hence closed, and this shows that θ/K is surjective. We also showed that the kernel is the intersection of all normic subgroups $N_{L/K}C_L$.

20.1 Classification of normic subgroups

Proposition 20.1. *$A \subseteq C_L$ is normic if and only if $A \subseteq C_L$ is finite index open.*

I justified last time that normic subgroups are finite index and open. If $A \subseteq C_L$ is finite index, it is going to contain some C_L^n. Because A is open, A also contains some subgroup of the form

$$U_S = \prod_{v\in S} 1 \times \prod_{v\notin S} \mathcal{O}_v^\times \subseteq C_K.$$

(This is not open, but at least A contains some U_S.) Combining these two facts, we see that it is enough to show that $C_L^n U_S$ is normic for large enough S.

Lemma 20.2. *Suppose S contains all infinite primes and all primes dividing n, and suppose $\mathbb{A}_{K,S}^\times \twoheadrightarrow C_K$. If $K \supseteq \mu_n$ then*

$$(C_K)^n U_S = N_{T/K}T$$

where $T = K(\sqrt[n]{\mathcal{O}_{K,S}})$. In general, $(C_K)^n U_S$ is still normic.

Proof. This is going to be a lot like what we did for the second inequality. We have

$$\mathrm{Gal}(T/K) \cong \mathrm{Hom}(\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n, \mu_n).$$

Here, we can non-canonically compute $\mathcal{O}_{K,S}^\times(\mathcal{O}_{K,S}^\times)^n \cong (\mathbb{Z}/n\mathbb{Z})^S$. So $|\mathrm{Gal}(T/K)| = n^{|S|}$. We have a map

$$\theta_{T/K} : C_K \to \mathrm{Gal}(T/K),$$

and $(C_K)^n \subseteq \ker\theta_{T/K}$. We also check that $U_S \subseteq N_{T/K}C_T$ locally. Clearly $1 \in K_v^\times$ a norm for $v \in S$, and for $v \notin S$, $T = K(\sqrt[n]{\mathcal{O}_{K,S}})$ implies that T/K is unramified, and hence $\mathcal{O}_v^\times \subseteq NT_w^\times$. This shows

$$(C_K)^n U_S \subseteq N_{T/K}C_T.$$

Now we compute the index of both groups and show that they are equal. We first immediately see

$$[C_K : N_{T/K}C_T] = |\mathrm{Gal}(T/K)| = n^{|S|}.$$

For the other inclusion, we note that there is an exact

$$\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^n \to \prod_{v\in S}(K_v^\times)/(K_v^\times)^n \to C_K/(C_K)^n \cdot U_S \to 1.$$

(The second map is surjective because $\mathbb{A}_{K,S}^\times \twoheadrightarrow C_K$ is assumed to be surjective.) But the first term has size $n^{|S|}$ and the second term has size $n^{2|S|}$. So it suffices to check that $(\mathcal{O}_{K,S}^\times)/(\mathcal{O}_{K,S}^\times)^n$ injects into $K_v^\times/(K_v^\times)^n$.

If $a \in \mathcal{O}_{K,S}^\times$ and $a \in (K_v^\times)^n$ for all $v \in S$, consider the extension $L = K(\sqrt[n]{a})/K$. This is unramified outside S and split completely . So todo

Let us now look at the general case. If K does not contain μ, we let $K' = K(\mu_n)$ and S' be the set of primes of K' above S. Then there exists a L'/K' such that $(C_{K'})^n U_{S'} = N_{L'/K'} \cdot C_{L'}$ by taking $L \supseteq L'$ with L'/K Galois. WE then have

$$N_{L/K}C_L \subseteq N_{L'/K}C'_L = N_{N'/K}C'_L = N_{K'/K}(N_{L'/K'}C_{L'}) = N_{K'/K}(C_{K'}^n U_{S'}) \subseteq C_K^n U_S.$$

This shows that $C_K^n U_S$ is normic. □

Now we have shown that

$$\theta_{/K} = \bigcap_{U\subseteq C_K \text{ finite index}} U.$$

We claim that this is equal to

$$D_K = \text{connected comp. of } 1 \in C_K = \text{closure of } \Bigg(\prod_{v \text{ real}} \mathbb{R}^{>0}\Bigg)\Bigg(\prod_{v \text{ complex}} \mathbb{C}^\times\Bigg).$$

It is clear that $D_K \subseteq \bigcap U$, and on the other hand C_K/D_K is profinite because it is compact and totally disconnected. We also can characterize this as

$$D_K = \text{divisible elements of } C_K = \bigcap_n (C_K)^n.$$

21 March 19, 2018

For L/K a finite extension of number fields, we now have

$$\theta_{L/K} : C_K/NC_L \xrightarrow{\cong} \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

The map is natural in L and K with inflation and restriction:

$$\begin{tikzcd}
C_K/N_{L/K}C_L \arrow[r, "\theta_{L/K}"] \arrow[d] & \mathrm{Gal}(L/K)^{\mathrm{ab}} \arrow[d, "\text{transfer}"] \\
C_M/N_{L/M}C_L \arrow[r, "\theta_{L/M}"] & \mathrm{Gal}(L/M)^{\mathrm{ab}}
\end{tikzcd}$$

21.1 Properties of the Hilbert class field

The Hilbert class field H of a number field K is the ray class field of (1). This is the maximal abelian extension of K that is unramified at all places (including infinite fields). Then there is a canonical isomorphism

$$\mathrm{Cl}(\mathcal{O}_K) \xrightarrow{\cong} \mathrm{Gal}(H/K)$$

given by the Artin map.

Example 21.1. For $K = \mathbb{Q}$, we have $H = \mathbb{Q}$. If $K = \mathbb{Q}(\sqrt{-5})$, then $H = \mathbb{Q}(\sqrt{-5}, i)$. For $K = \mathbb{Q}(\sqrt{-23})$, we get $H = K(\alpha)$ where $\alpha^3 - \alpha + 1 = 0$. (This has discriminant 23.)

Because this extension H/K is unramified at every prime, a prime $\mathfrak{p} \in \mathrm{Cl}(\mathcal{O}_K)$ is mapped to the Frobenius $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$. So $\mathfrak{p}$ is principal if and only if $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$ if and only if $\mathfrak{p}$ splits completely in H/K.

Corollary 21.2. *Given p a prime of $\mathbb{Q}$, the prime p is a norm from $\mathcal{O}_K$ if and only if p splits completely in $\mathcal{O}_H$.*

Proof. If (p) does not split completely in $\mathcal{O}_K$, then it is not a norm in $\mathcal{O}_K$ and also it does not split completely in $\mathcal{O}_H$. If (p) does split completely in $\mathcal{O}_K$, write $(p) = N\mathfrak{p}$. Then $\mathfrak{p}$ is a principal ideal if and only if $\mathfrak{p}$ splits completely in $\mathcal{O}_H$ if and only if (p) splits completely in $\mathcal{O}_H$. □

Example 21.3. Let $K = \mathbb{Q}(\sqrt{-5})$. We have that $p = x^2 + 5y^2$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-5}, i)$. Because $\mathbb{Q}(\sqrt{-5}, i) \subseteq \mathbb{Q}(\zeta_{20})$, this is going to be a condition on p modulo 20.

Theorem 21.4 (principal ideal theorem of class field theory)**.** *If $\mathfrak{a}$ is any fractional ideal of $\mathcal{O}_K$, then $\mathfrak{a}\mathcal{O}_K$ is principal.*

This property does not uniquely determine $\mathcal{O}_H$. This also does not mean that $\mathcal{O}_H$ have class number 1. The theorem follows from the following group theory fact.

Theorem 21.5. *Let G be a group, $G' = [G,G]$, and $G'' = [G',G']$. Then the transfer map $G/G' \to G'/G''$ is trivial.*

Proof. Let us start out with H/K and let H_1 be the Hilbert class field of H, so that $\mathrm{Gal}(H_1/H) = \mathrm{Cl}(H)$. Now H is going to be the maximal abelian subextension of H, because H_1/K is unramified. Let $G = \mathrm{Gal}(H_1/K)$ so that $\mathrm{Gal}(H/K) = G^{\mathrm{ab}}$ and $\mathrm{Gal}(H_1/H) = G'$. We have

$$\begin{tikzcd}
C_K/N_{H_1/K}C_{H_1} \arrow[r, "\theta_{H_1/K}"] \arrow[d] & \mathrm{Gal}(H_1/K)^{\mathrm{ab}} = G^{\mathrm{ab}} \arrow[d, "\text{transfer}"] \\
C_H/N_{H_1/H}C_{H_1} \arrow[r, "\theta_{H_1/H}"] & \mathrm{Gal}(H_1/H)^{\mathrm{ab}} = (G')^{\mathrm{ab}}.
\end{tikzcd}$$

But note that $\mathrm{Gal}(H_1/K)^{\mathrm{ab}} \cong \mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O}_K)$. So we get that the map $\mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_H)$ is trivial. □

22 March 21, 2018

Last time we showed the following:

Theorem 22.1 (principal ideal theorem)**.** *If H is the Hilbert class field of K, then* $\mathrm{Cl}(K) \to \mathrm{Cl}(H)$ *is trivial.*

22.1 Class field tower

Then people started wondering about whether one can always find L/K such that $\mathrm{Cl}(L)$ is trivial. Examples last time had $\mathrm{Cl}(H)$ trivial, so $L = H$ works. Historically, this was to enlarge the field so that unique factorization works. One thing you can do is to take the class field tower $K \subseteq H \subseteq H_1 \subseteq H_2 \subseteq \cdots$. For small cases, this appears to always terminate and you eventually hit some H_n which has $\mathrm{Cl}(H_n) = 1$, in which case the tower stabilizes. Actually this is a natural thing to do.

Lemma 22.2. *If L/K is such that* $\mathrm{Cl}(L) = 1$*, then L contains H the Hilbert class field of K. (So $L \supseteq H_n$ for all n.)*

So such L exists if and only if the class field tower stabilizes.

Proof. Note that HL/L is an unramified extension but $\mathrm{Cl}(L) = 1$. So $H_0L = L$ and $H_0 \subseteq L$. □

This is related to $\mathrm{Gal}(K^{\mathrm{unr}}/K) = G$, where K^{unr} is the maximal (not-abelian) everywhere unramified extension. The entire tower then lies in K^{unr}. Also, H_0 is the fixed field of $G_1 = [G, G]$, then H_1 is the fixed field of $[G_1, G_1]$, and so on. It is easier to study p-groups for a fixed p. Let $H_{0,p}$ be the fixed field of the p-group of H_0, and so on $K \subseteq H_{0,p} \subseteq H_{1,p} \subseteq \cdots$. This is called the p-class field tower of K.

Theorem 22.3 (Golod–Shafarevich)**.** *If the p-class field tower stabilizes, then it must be that the p-rank of* $\mathrm{Cl}(K)$ *is at most* $2 + 2\sqrt{[K : \mathbb{Q}] + 1}$.

If the latter condition fails, then it should have infinite p-class field tower, and hence infinite class field tower. For instance we just need it to have the 2-rank of $\mathrm{Cl}(K)$ to be at least 6. This holds for any imaginary quadratic fields with ≥ 6 ramified primes or real quadratic fields with ≥ 8 ramified primes. (This is genus theory.)

22.2 L-functions

A **Dirichlet series** is a series of the form

$$\sum_{n \geq 1} \frac{a_n}{n^s}.$$

Then $\zeta(s)$ is the case $a_n = 1$ for all n. This series generally converges for $\Re(s) \gg 0$. For $\zeta(s)$, the series converges for $\Re(s) > 1$. But one important thing is that there is a meromorphic continuation to all of $\mathbb{C}$, using a functional equation.

We can write

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}},$$

and more generally if K is a number field, an **Euler product** is a product of the form

$$\prod_{\mathfrak{p}\subseteq\mathcal{O}_K} \frac{1}{(1-a_{1,\mathfrak{p}}(N\mathfrak{p})^{-s})\cdots(1-a_{k_\mathfrak{p},\mathfrak{p}}(N\mathfrak{p})^{-s})}$$

where $N\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$. L-functions are Dirichlet series with Euler products. For instance, the **Dedekind ζ-function** of a number field K is

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{1}{|N\mathfrak{a}|^{-s}} = \prod_{\mathfrak{p}\subset -\mathcal{O}_K} \frac{1}{1-(N\mathfrak{p})^{-s}}.$$

We can actually do this for function fields. Let us take $K = \mathbb{F}_q(t)$ for instance. Let us take $\mathcal{O}_{K,\infty} = \mathbb{F}_q[t]$. Then we are looking at

$$\sum_{\mathfrak{a}\subseteq\mathbb{F}_q[t]} \frac{1}{(N\mathfrak{a})^{-s}}.$$

But every $\mathfrak{a}$ is principal and if we write $\mathfrak{a} = (f)$ then $N\mathfrak{a} = q^{-\deg f}$. So

$$\zeta_K(s) = \sum_{d\geq 0} \frac{q^d}{q^{-ds}} = \frac{1}{1-q^{(1-s)}}$$

This kind of thing always happens for function fields. If we take the Euler product formula, we get

$$\prod_{v \text{ of } \mathbb{F}_q(t)} \frac{1}{1-|k_v|^{-s}} = \frac{1}{1-q^{-s}}\zeta_K(s) = \frac{1}{(1-q^{-s})(1-qq^{-s})}.$$

This is the zeta function of $\mathbb{P}^1_{\mathbb{F}_q}$. It is a rational function in $t = q^{-s}$. For any function field $K(C)$, the zeta function of C is going to be of the form

$$\frac{\prod_i (1-\alpha_i q^{-s})}{(1-qq^{-s})(1-q^{-s})}$$

where all α_i has $|\alpha_i| = \sqrt{q}$. This is the Riemann hypothesis for curves over finite fields.

23 March 23, 2018

We defined the Dedekind ζ function of $\mathcal{O}_k$ as

$$\sum_{\mathfrak{a}\subseteq\mathcal{O}_K}\frac{1}{(N\mathfrak{a})^s}=\prod_{\mathfrak{p}\subseteq\mathcal{O}_K}\frac{1}{1-(N\mathfrak{p})^s}.$$

23.1 L-functions

Then we can define the Dirichlet L-function over $\mathcal{O}_K$ as the following. First choose a module $\mathfrak{m}$ and look at

$$\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)=\mathrm{Frac}_{\mathfrak{m}}(\mathcal{O}_K)/\operatorname{Prin}_{\mathfrak{m}}(\mathcal{O}_K)$$

and choose a character χ of $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$. Now we define the **Dirichlet L-function** as

$$L(s,\chi)=\sum_{(\mathfrak{a},\mathfrak{m})=1}\frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s}=\prod_{\mathfrak{p}\subseteq\mathcal{O}_K,\mathfrak{p}\nmid\mathfrak{m}}\frac{1}{1-\chi(\mathfrak{p})(N\mathfrak{p})^s}.$$

For instance, if $K=\mathbb{Q}$ and $\mathfrak{m}=m\infty$ then $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Z})\cong(\mathbb{Z}/m\mathbb{Z})^\times$ and $\chi:(\mathbb{Z}/m\mathbb{Z})^\times\to S'$. Then

$$L(s,\chi)=\sum_{(a,m)=1}\frac{\chi(a)}{a^s}.$$

We can consider $\chi:\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)\to S'$ as a character of $C_K\to S^1$, because there is a map $C_K\twoheadrightarrow S^1$. Hecke L-functions generalize Dirichlet L-functions by allowing arbitrary characters $\chi:C_K\to S^1$ with non-discrete image. You can prove using this that primes in $\mathbb{Z}[i]$ have equidistributed arguments, for instance.

There is another point of view. Note that there is a map

$$\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)\to\mathrm{Gal}(L_{\mathfrak{m}}/K);\quad\mathfrak{p}\mapsto\mathrm{Frob}_{\mathfrak{p}}.$$

So if V is a finite-dimensional representation of $\mathrm{Gal}(L/K)$, we can take the trace χ_V and we can define the Artin L-series

$$\prod_{\mathfrak{p}}\frac{1}{1-\chi(\mathrm{Frob}_{\mathfrak{p}})(N\mathfrak{p})^{-s}}.$$

23.2 Convergence of Dirichlet series

If a_n is $O(n^b)$, then the series $\sum a_n n^{-s}$ converges locally uniformly and absolutely in the half-plane $\Re(s)>b+1$.

Proposition 23.1. *Let $S(x)=\sum_{n\leq x}a_n$. If $S(x)=O(x^b)$ then $\sum a_n n^s$ can be extended to a holomorphic function on $\Re(s)>b$.*

Proof. This is just analysis. The basic idea is that we can do summation by parts and write

$$\sum_{n\geq 0} \frac{a_n}{n^s} = \sum_{n\geq 0} s_n\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big).$$

Here $s_n = O(n^b)$ and the difference is $O(n^{-s-1})$. □

Proposition 23.2. *$\zeta(s)$ has a meromorphic continuation to $\Re(s) > 0$, with a pole at $s = 1$ an no other poles.*

Proof. Consider $\zeta_2(s) = \zeta_s(1 - 2^{-s})$. Then

$$\zeta_2(s) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n^s}$$

on $\Re(s) > 1$. By our proposition, this can be extended to $\Re(s) > 0$ holomorphically, so $\zeta(s)$ is meromorphic on $\Re(s) > 0$ with poles possibly as $s = 1 + k\frac{2\pi i}{\log 2}$. If we define $\zeta_3(s)$ similarly, we see that $\zeta(3)$ can have a pole only at $s = 1$. It actually does have a pole. □

Proposition 23.3. *$\zeta(s)$ has a pole at $s = 1$ of residue 1.*

Proof. We look at $\zeta(s)$ for $s > 1$. We have

$$\sum_{n\geq 1} \frac{1}{n^s} \geq \int_{x=1}^{\infty} \frac{1}{x^s} dx = \frac{1}{s-1} \geq \sum_{n\geq 2} \frac{1}{n^s} = \zeta(s) - 1,$$

so the residue should be 1. □

For the Dedekind zeta function, we will show that $\zeta_K(s)$ also have a simple pole at $s = 1$ and will give a formula for the residue involving the class number.

24 March 26, 2018

We showed the following last time. If $S(x) = \sum_{n \le x} a_n$ has $S(x) = O(x^b)$, then $\sum a_n n^{-s}$ converges to a holomorphic function on $\Re(s) > b$. Using this, we showed that

$$\zeta(s) = \sum \frac{1}{n^s}$$

has a meromorphic continuation to $\Re(s) > 0$ with a simple pole at $s = 1$ with residue 1.

24.1 Meromorphic continuation of L-functions

Proposition 24.1. *If there exists some a_0 such that $S(n) = a_0 n + O(x^b)$ with $0 \le b < 1$, then $\sum a_n n^{-s}$ can be analytically continued to a meromorphic function on $\Re(s) > b$ with a simple pole at $s = 1$ having residue a_0.*

Proof. We have $\sum a_n n^{-s} = a_0 \zeta(s) + \sum (a_n - a_0) n^{-s}$. □

We will apply this to ζ_K, and more generally, $L(s, \chi)$ for $\chi : \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K) \to S^1$ given by

$$L(s, \chi) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K, (\mathfrak{a}, \mathfrak{m}) = 1} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s}.$$

Definition 24.2. We define, for $\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$,

$$\zeta(s, \mathfrak{K}) = \sum_{\mathfrak{a} \in \mathfrak{K}} \frac{1}{(N\mathfrak{a})^s}.$$

Then we can write

$$L(s, \chi) = \sum_{\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)} \chi(\mathfrak{K}) \zeta(s, \mathfrak{K}).$$

The goal is to apply the proposition to $\zeta(s, \mathfrak{K})$. Consider the partial sum function

$$S(x, \mathfrak{K}) = \#\{\mathfrak{a} \in \mathfrak{K} : N\mathfrak{a} \le x\}.$$

Proposition 24.3. *We have $S(x, \mathfrak{K}) = g_{\mathfrak{m}} x + O(x^{(1 - \frac{1}{d})})$. Thus, $\zeta(s, \mathfrak{K})$ has a pole or residue $g_{\mathfrak{m}}$ at $s = 1$. Here,*

$$g_{\mathfrak{m}} = \frac{2^r (2\pi)^s \operatorname{reg}(\mathfrak{m})}{w_{\mathfrak{m}} (N\mathfrak{m}) \sqrt{|\operatorname{disc}(K)|}},$$

where r is the number of real places, s is the number of complex places, $\operatorname{reg}(\mathfrak{m})$ *is the regulator, $w_{\mathfrak{m}}$ is the number of roots or unity in $\mathcal{O}_{K,\mathfrak{m}}^\times = \{a \in \mathcal{O}_K^\times : a \equiv 1 \bmod \mathfrak{m}$, a positive at reals of $\mathfrak{m}\}$, $N\mathfrak{m}$ is the norm of $\mathfrak{m}$ as an ideal (ignoring places at infinity),* $\operatorname{disc}(K)$ *is the discriminant.*

Definition 24.4. The **regulator** is the "size of $\mathcal{O}_{K,\mathfrak{m}}^\times$". Consider the log map

$$\mathcal{L} : \mathcal{O}_K^\times \to H \hookrightarrow \prod_{v|\infty} \mathbb{R}^+; \quad a \mapsto (\log|a|_{v_1}, \dots, \log|a|_{v_{r+s}}).$$

Then $\mathcal{L}(\mathcal{O}_{K,\mathfrak{m}}^\times)$ is a lattice in H, and now we take $\operatorname{reg}(\mathfrak{m})$ as the covolume of $\mathcal{L}(\mathcal{O}_{K,\mathfrak{m}}^\times)$ inside H.

If $\mathfrak{m} = 1$, we also say $\operatorname{reg}(\mathfrak{m}) = \operatorname{reg}(\mathcal{O}_K)$. If K is real quadratic, we have $\operatorname{reg}(\mathfrak{m}) = \log|u|$ where u is the generator of the unit with $|u| > 1$.

Proof. For a completely proof, read Lang's *Algebraic number theory*. First choose $\mathfrak{c} \in \mathfrak{K}$. Then any $\mathfrak{a} \in \mathfrak{K}$ is going to look like $\mathfrak{a} = a\mathfrak{c}$ where $a \equiv 1 \bmod \mathfrak{m}$ and $a \in \mathfrak{c}^{-1}$. Then $Na = N\mathfrak{c}^{-1}Na \leq (N\mathfrak{a})x$ for some $x > 0$. This means that a belongs to an additive coset of $\mathfrak{m}\mathfrak{c}^{-1}$, which is going to be some lattice in $\prod_{v|\infty} K_v$. Then the number of these points in some ball is going to be approximately

$$\frac{\text{vol(ball)}}{\text{covolume of lattice}} + O(x^{1-\frac{1}{d}}) = \frac{x \cdot N\mathfrak{c}^{-1} \cdot (\cdots)}{\sqrt{\operatorname{disc}(K)} N\mathfrak{m} N\mathfrak{c}^{-1}} + O(x^{1-\frac{1}{d}}).$$

If you work out the coefficients out, you are going to get that. If you have a real quadratic field, for instance, you actually have a hyperbola, and you have to quotient by the unit group. Here is where you get the regulator. □

25 March 28, 2018

We were counting

$$S(x,\mathfrak{K}) = \#\{\text{ideals } \mathfrak{a} \in \mathfrak{K} : N\mathfrak{a} \le x\},$$

where $\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$. We had the following proposition.

Proposition 25.1. *$S(x,\mathfrak{K}) = g_{\mathfrak{m}} x + O(x^{1-\frac{1}{d}})$, where*

$$g_{\mathfrak{m}} = \frac{2^r (2\pi)^s \operatorname{reg}(\mathfrak{m})}{w_{\mathfrak{m}} N\mathfrak{m} \sqrt{|\operatorname{disc} K|}}$$

and $N\mathfrak{m} = N\mathfrak{m}_{\mathrm{fin}} 2^{r_{\mathfrak{m}}}$ for $r_{\mathfrak{m}}$ the number of real places in $\mathfrak{m}$.

Proof. We first chose $\mathfrak{c} \in \mathfrak{K}$ so that $\mathfrak{a} = a\mathfrak{c}$. Here, the set of possible a is then some lattice in $\prod_{v|\infty} K_v$ interesected with a fundamental domain for the action of $\mathcal{O}_{K,\mathfrak{m}}^{\times}$. □

Theorem 25.2. *Let χ be a Dirichlet character of modulus $\mathfrak{m}$. If $\chi \neq 1$, then $L(s,\chi)$ is holomorphic at $s = 1$. If $\chi = 1$, then $L(s,\chi)$ has a pole of order 1 at $s = 1$, with reseidue $|\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)| g_{\mathfrak{m}}$.*

Proof. This immediately follows from

$$L(s,\chi) = \sum_{\mathfrak{K} \in \mathrm{Cl}_{\mathfrak{m}}} \chi(\mathfrak{K}) \zeta(s,\mathfrak{K}).$$

Here, each $\zeta(s,\mathfrak{K})$ has a pole of order 1 at $s = 1$, with residue $g_{\mathfrak{m}}$. So if χ is not the trivial character, we get cancellation, and if χ is trivial, we get the correct thing. □

Corollary 25.3. *For $\mathfrak{m} = 1$, we get that $\zeta_{K,s}(s) = L(s,1)$ has pole at $s = 1$ with residue given by*

$$h_K g_1 = \frac{2^r (2\pi)^s \operatorname{reg}(K) h_K}{w_K \sqrt{|\operatorname{disc}(K)|}}.$$

For instance, if K is imaginary quadratic, then the residue is

$$\frac{2\pi h_K}{w_K \sqrt{-\Delta}}.$$

If K is real quadratic, then the residue is

$$\frac{2 \log|u| h_K}{2\sqrt{\Delta}}.$$

There's something called the Stark's conjecture that generalize this to other L-functions. This is also very similar to the Birch–Swinnerton-Dyer conjecture.

25.1 Densities of sets of primes

I'm going to give you three different notions of density. Let T be a set of primes of $\mathcal{O}_K$.

- The **Dirichlet density** is a number δ satisfying
$$\sum_{\mathfrak{p}\in T} \frac{1}{(N\mathfrak{p})^s} = \delta \log \frac{1}{1-s} + O(1)$$
as $s \to 1+$.
- The **natural density** is
$$\delta = \lim_{x\to\infty} \frac{\#\{\mathfrak{p}\in T : N\mathfrak{p} \le x\}}{\{\mathfrak{p} : N\mathfrak{p} \le x\}}.$$
- If the Euler product
$$\left(\prod_{\mathfrak{p}\in T}\left(1-\frac{1}{N\mathfrak{p}^s}\right)^{-1}\right)^n$$
has an analytic continuation with pole of order m at $s = 1$, we say that its **polar density** is $\frac{m}{n}$.

Clearly, all of them are

- monotone where defined,
- finitely additive,
- subsets of density 0 have density 0,
- finite sets have density 0.

Proposition 25.4. *If natural density exists, then so does Dirichlet density and they are equal. If polar density exists, so does Dirichlet density and they are equal.*

There are sets like primes whose first digit of p is 1, whose Dirichlet density exists but but natural density does not exist.

Proof. Proof of natural implies Dirichlet is basically partial summation. For the proof of polar implies Dirichlet, we can use
$$\log\left(\prod_{\mathfrak{p}\in T} \frac{1}{1-N\mathfrak{p}^s}\right)^{-1} = \sum_{\mathfrak{p}\in T} (N\mathfrak{p})^s) + O(1)$$
as $s \to 1$, which is obtained by looking at the Taylor expansion. □

Proposition 25.5. *The set of all primes has density* 1*, with respect to all three definitions.*

Proof. This is obvious for natural density. For polar density, you can use that $\zeta_K(s)$ has pole of order 1 at $s = 1$. You can do this for Dirichlet density as well. □

26 March 30, 2018

Recall that we defined Dirichlet density of T as

$$\sum_{\mathfrak{p}\in T}\frac{1}{N\mathfrak{p}^s}=\delta\log\Big(\frac{1}{1-s}\Big)+O(1),$$

and we defined polar density as $\frac{m}{n}$ if

$$\bigg(\prod_{\mathfrak{p}\in T}\Big(1-\frac{1}{N\mathfrak{p}^s}\Big)^{-1}\bigg)^n$$

has a pole of order m at $s=1$.

26.1 Proof of second inequality

Proposition 26.1. *The set* $T=\{\mathfrak{p}\subseteq\mathcal{O}_K : N\mathfrak{p}=p^i$ *for* $i\geq 2\}$ *has polar density* 0*.*

Proof. Let $d=[K:\mathbb{Q}]$. Write

$$\prod_{\mathfrak{p}\in T}\Big(1-\frac{1}{N\mathfrak{p}^s}\Big)^{-1}=\prod_{j=2}^{d}\prod_{p}(1-p^{-js})^{\#\{\mathfrak{p}:N\mathfrak{p}=p^{js}\}}.$$

Then it is clear that $\#\{\mathfrak{p}:N\mathfrak{p}=p^j\}\leq d$. So in the worst case, we get

$$\prod_{j=2}^{d}\prod_{p}(1-p^{-js})^d=\zeta(2s)^d\zeta(3s)^d\cdots\zeta(ds)^d$$

which still is holomorphic on $\Re s>\frac{1}{2}$. □

Proposition 26.2. *Let* L/K *be finite Galois. Then* $\mathrm{Spl}(L/K)=\{\mathfrak{p}:\mathfrak{p}$ *splits completely in* $L\}$ *has polar density* $1/[L:K]$*.*

Proof. Let T be the set of primes of L lying above primes of $\mathrm{Spl}(L/K)$. Then if some $\mathfrak{p}_L$ lies above some $\mathfrak{p}_K$, then $N\mathfrak{p}_L=\mathfrak{p}_K^f$. So T is the set of primes $\mathfrak{p}$ such that $N\mathfrak{p}$ is prime, up to a finite number of ramified primes. This implies that the polar density $\delta(T)=1$, because the set it misses can be ignored.

Now we observe that

$$\prod_{\mathfrak{p}_L\in T}\Big(1-\frac{1}{N\mathfrak{p}_L^s}\Big)=\prod_{\mathfrak{p}_k\in\mathrm{Spl}(L/K)}\Big(1-\frac{1}{N\mathfrak{p}_K^s}\Big)^{[L:K]}.$$

This implies that $\mathrm{Spl}(L/K)$ has polar density $1/[L:K]$. □

We are working towards the second inequality. Fix $\mathfrak{m}$ a modulus. Then in $\mathrm{Cl}_\mathfrak{m}=\mathrm{Cl}_\mathfrak{m}(\mathcal{O}_K)$ fix a subgroup H of $\mathrm{Cl}_\mathfrak{m}$. Consider $L(1,\chi)$ for χ a nontrivial Dirichlet character of modulus $\mathfrak{m}$ that vanishes on H.

Theorem 26.3. *At most one character χ of H has $L(1,\chi)=0$.*

This will imply that the Dirichlet density of $\{\mathfrak{p} : [\mathfrak{p}] \in H\}$ is equal to $1/|G|$ if $L(1,\chi) \neq 0$ for all such χ, and $L(1,\chi) = 0$ for one χ.

Proof. We consider the sum

$$\begin{aligned}\frac{1}{|G|}\sum_{\chi}\log(L(s,\chi)) &= \frac{1}{|G|}\sum_{\chi}\sum_{\mathfrak{p}} -\log(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}) \\ &= \frac{1}{|G|}\sum_{\chi,\mathfrak{p}}(\chi(\mathfrak{p})N\mathfrak{p}^{-s}) + O(1) = \sum_{[\mathfrak{p}]\in H} N\mathfrak{p}^{-s} + O(1).\end{aligned}$$

But the left hand side is just

$$\frac{1}{|G|}\left(\log\left(\frac{1}{1-s}\right) - \sum_{\chi}\operatorname{ord}_{s=1} L(s,\chi)\log\left(\frac{1}{1-s}\right)\right) + O(1)$$

shows that the Dirichlet density of $\{\mathfrak{p} : [\mathfrak{p}] \in H\}$ is just

$$\frac{1}{|G|}\left(1 - \sum_{\chi}\operatorname{ord}_{s=1}(L(s,\chi))\right).$$

This shows that the sum of the orders is either 0 or 1. □

Theorem 26.4. *Let L/K be Galois and $\mathfrak{m}$ be a modulus of K. Then*

$$|C_K^\times/(N_{L/K}C_L^\times)U_{\mathfrak{m}}| \leq [L:K].$$

This implies the second inequality because we can take $\mathfrak{m}$ so that $U_{\mathfrak{m}} \subseteq N_{L/K}C_L^\times$. Then $|C_K^\times/N_{L/K}C_L^\times| \leq [L:K]$.

Proof. Consider $G = \mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)/H$ where H is the subgroup of $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$ generated by ideals that are norms from $\mathcal{O}_L$. We know that $\delta(\mathfrak{p} : [\mathfrak{p}] \in H)$ is either 0 or $1/|G|$. But if $\mathfrak{p}$ splits completely in L, then $\mathfrak{p}$ is a norm form $\mathcal{O}_L$ so $\mathfrak{p} \in H$. This shows that

$$\delta(\mathfrak{p} : [\mathfrak{p}] \in H) \geq \delta(\mathrm{Spl}(L/K)) = \frac{1}{[L:K]}.$$

So $\delta(\mathfrak{p} : [\mathfrak{p}] \in H) = 1/|G|$. This shows that $|G| \leq [L:K]$. □

Corollary 26.5. *If χ is a nontrivial character of $\mathrm{Cl}_{\mathfrak{m}}(\mathcal{O}_K)$, then $L(1,\chi) \neq 0$.*

Proof. Here, we need to be a bit careful because the previous argument only shows that $L(1,\chi) \neq 0$ only for χ that vanish on H. So we use an existence theorem. There exists a L/K Galois such that $NC_L^\times \subseteq U_{\mathfrak{m}}$, by class field theory. □

27 April 2, 2018

We want to prove the Chebotarev density theorem.

Theorem 27.1 (Chebotarev density theorem)**.** *Let L/K be a Galois extension of fields. There is a map*

$$\{\textit{unramified primes of } K\} \to \{\textit{conjugacy classes of } \mathrm{Gal}(L/K)\}, \quad \mathfrak{p} \mapsto [\mathrm{Frob}_{\mathfrak{p}}].$$

(Note that $\mathrm{Frob}_{\mathfrak{p}}$ *is only defined up to conjugacy.) Then for any conjugacy class* $[g]$*,*

$$T_g = \{\mathfrak{p} : [\mathrm{Frob}_{\mathfrak{p}}] = [g]\}$$

has Dirichlet density $|[g]|/|\mathrm{Gal}(L/K)|$*.*

27.1 Chebotarev density theorem

Note that we have already proved this for $g = 1$. Note that we have

$$T_1 = \mathrm{Spl}(L/K)$$

because having trivial Frobenius means that you have trivial decomposition group, and then the prime splits completely. The strategy is to first do L/K abelian and then use this to do it in the general case.

Proposition 27.2. *Let C be any subset of* $\mathrm{Cl}_{\mathfrak{m}}$*. Then the density of* $\{\mathfrak{p} : [\mathfrak{p}] \in C\}$ *is* $|C|/|\mathrm{Cl}_{\mathfrak{m}}|$*.*

Proof. By additivity, assume that $C = \{\mathfrak{K}\}$. Then

$$\sum_{\mathfrak{p}\in\mathfrak{K}} \frac{1}{N\mathfrak{p}^s} = \frac{1}{|\mathrm{Cl}_{\mathfrak{m}}|} \sum_{\chi} \overline{\chi(\mathfrak{K})} \log L(s,\chi) + O(1)$$

as $s \to 1+$. But we know that all $\log L(1,\chi)$ is a number for χ nontrivial, and $L(s,\chi)$ behaves like $\log \frac{1}{1-s}$ as $s \to 1$. □

Note that for $K = \mathbb{Q}$, this is just Dirichlet's theorem for primes in arithmetic progressions.

Corollary 27.3. *L/K satisfies Chebotarev for L/K abelian.*

Proof. Choose $\mathfrak{m}$ with $L \subseteq L_{\mathfrak{m}}$. Then $\mathrm{Gal}(L/K) \cong \mathrm{Cl}_{\mathfrak{m}}/H$ for some subgroup H. Then $\mathrm{Frob}_{\mathfrak{p}} = g$ if and only if $[\mathfrak{p}] \in gH$. □

Let's now do the non-abelian case.

Proof of Chebotarev density. Ignore all ramified primes, and let $[L : K] = n$. Let $g \in \mathrm{Gal}(L/K)$ have order m and consider $M = L^{\langle g\rangle}$. Then we have a tower $L/M/K$ where L/M is cyclic of degree m. What does it mean for $\mathfrak{p} \in T_g$. This means that there exists a $\mathfrak{p}_L$ above $\mathfrak{p}$ such that $\mathrm{Frob}_{\mathfrak{p}_L} = g$. Then $\langle g\rangle = D_{\mathfrak{p}_L}$.

Here, we let $\mathfrak{p}_M$ lies below $\mathfrak{p}_L$. Then we have a surjection

$$T_{M,g} = \{\mathfrak{p}_M : f_{M/K} = 1, \mathrm{Frob}_{\mathfrak{p}_M} = g \in \mathrm{Gal}(L/M)\} \twoheadrightarrow T_g.$$

Now we can use abelian Chebotarev to compute Dirichlet density of $T_{M,g}$. Here, we can ignore $f_{M/K} = 1$ because other primes will have density 0 anyways. So we have

$$\delta(T_{M,g}) = \delta(\mathfrak{p} \text{ of } M : \mathrm{Frob}_{\mathfrak{p}_M} = g \in \mathrm{Gal}(L/M)) = \frac{1}{m}.$$

We can also understand the fiber of this surjection as well. Given $\mathfrak{p}$, how may primes $\mathfrak{p}_M \in T_{M,g}$ lie over $\mathfrak{p}$? In other words, how may $\mathfrak{p}_L$ are there above $\mathfrak{p}$ such that $\mathrm{Frob}_{\mathfrak{p}_L} = g \in \mathrm{Gal}(L/K)$? Any such $\mathfrak{p}_L$ above $\mathfrak{p}$ are going to look like

$$\mathfrak{p}_L = h\mathfrak{p}_{L,0},$$

for $h \in \mathrm{Gal}(L/K)$. Then we have

$$\mathrm{Frob}_{\mathfrak{p}_L} = h \,\mathrm{Frob}_{\mathfrak{p}_{L,0}} h^{-1} = hgh^{-1}.$$

So $hgh^{-1} = g$ if and only if h is in the centralizer. If you compute the density using orbit-stablizer and stuff, we find

$$\delta(T_g) = \sum_{\mathfrak{p} \in T_g} \frac{1}{N\mathfrak{p}^{-s}} = \frac{m|[g]|}{n} \sum_{\mathfrak{p}_M \in T_{M,g}} \frac{1}{N\mathfrak{p}_M^{-s}} = \frac{|[g]|}{|\mathrm{Gal}(L/K)|} \log(1-s) + O(1).$$

This gives the correct density. □

Here is one application. Let L/K be an arbitrary finite extension. Then we defined $\mathrm{Spl}(L/K)$ as the prime of K that split completely in L. You can show that if L' is the Galois closure of L, then $\mathrm{Spl}(L/K) = \mathrm{Spl}(L'/K)$. So

$$\delta(\mathrm{Spl}(L/K)) = \delta(\mathrm{Spl}(L'/K)) = \frac{1}{[L' : K]}.$$

Proposition 27.4. *If L and L' Galois have the same splitting set, then $L = L'$.*

Proof. Consider the compositum LL'/K. This has splitting set density equal to 1 over $[L : K]$ and of $[LL' : K]$. □

28 April 4, 2018

Now we would like to do explicit class field theory for $\mathbb{Q}$ and imaginary quadratic fields. By Kronecker–Weber, we know that $\mathbb{Q}^{\mathrm{ab}} = \bigcup_n \mathbb{Q}(\zeta_n)$. These $\mathbb{Q}(\zeta_n)$ are the ray class fields of modulus $n\infty$.

Consider the algebraic group $\mathbb{G}_m$ over $\mathbb{Q}$. Its endomorphism ring is $\mathrm{End}(\mathbb{Q}_m) \cong \mathbb{Z}$, with n corresponding to $a \mapsto a^n$, and for each n, the points of $\ker(a \to a^n)$ generate $\mathbb{Q}(\zeta_n)$. This is great for $\mathbb{Q}$, but if $K \neq \mathbb{Q}$, then $K(\zeta_\infty)$ is not the maximal abelian extension. So we need new sources of abelian extensions.

28.1 Complex multiplication

The idea is to take different 1-dimensional algebraic groups over K. For instance, we take E/K an elliptic curve for every n, consider the n-torsion points $E[n](\overline{\mathbb{Q}}) \cong (\mathbb{Z}/n\mathbb{Z})^2$, and take $K(E[n])/K$. The problem is that this is not necessarily abelian. Still there is an embedding

$$\mathrm{Gal}(K(E[n])/K) \hookrightarrow \mathrm{Aut}(E[n]) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

So we only want to look at special elliptic curves.

If E is an elliptic curve over K, then

$$\mathrm{End}_K(E) \cong \Big\{\mathbb{Z} \quad \mathcal{O} \subseteq \mathbb{Q}(\sqrt{-D}).$$

We say that E is of **complex multiplication** if it falls in the second category. Moreover, for any $\mathcal{O}$, there are only finitely many E with complex multiplication by $\mathcal{O}$. In this case, for any $a \in \mathcal{O}$ we can look at the kernel $E[a]$ of $a : E \to E$ and see that $E[a] \cong \mathcal{O}/(a)$ as $\mathcal{O}$-modules. Then we have

$$\mathrm{Gal}(K(E[a])) \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(E[a]) \cong (\mathcal{O}/(a))^\times.$$

What happens if I do this for K an imaginary quadratic field? Unless $h(K) = 1$, it turns out that there are no CM elliptic curves defined over K. So we are going to enlarge K to H so that there are CM elliptic curves defined over H with CM by $\mathcal{O}_K$. Here, we can take H to be the Hilbert class field of K.

Note that there is a bijection

$$\{E \text{ elliptic curve over } \mathbb{C} \text{ with CM over } K\} \quad \longleftrightarrow \quad \mathrm{Cl}(K),$$

because for any ideal $\mathfrak{a}$ we can take $\mathbb{C}/\mathfrak{a}$ as an elliptic curve. Then we can look at the j-invariants $j(E) \in H$. This is going to have minimal polynomial

$$\prod_{E \text{ CM by } K} (X - j(E))$$

over K and then $j(E)$ generates the Hilbert class field.

Let $\mathfrak{m}$ be a modulus of K. (There are no infinity parts, because K has only a complex place.) Then we can define

$$E[\mathfrak{m}] = \{P \in E : aP = 0 \text{ for all } a \in \mathfrak{m}\} \cong \mathcal{O}_K/\mathfrak{m}.$$

Then $L_{\mathfrak{m}} = H(E[\mathfrak{m}])$ is the ray class field corresponding to $\mathfrak{m}$.

28.2 Elliptic curves

Let $L \subseteq \mathbb{C}$, and consider $\mathbb{C}/L$. This is a Riemann surface of genus 1, so it should correspond to a curve over $\mathbb{C}$. We want to make this isomorphism $\mathbb{C}/L \to E$ explicit.

Definition 28.1. An **elliptic function** is a meromorphic function f_n on $\mathbb{C}/L$.

There is the **Weierstrass $\wp$-function** defined by

$$\wp(z, L) = \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \Big(\frac{1}{(z-w)^2} - \frac{1}{w^2} \Big).$$

Then $\wp$ is an elliptic function, with double poles at points of L.

29 April 6, 2018

Let $L \subseteq \mathbb{C}$ be a lattice. Recall that we defined an elliptic function as a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ that is L-periodic. We know that $\mathbb{C}/L$ is an elliptic curve. We are interested in what elliptic function this is. Last time we defined

$$\wp(z, L) = \frac{1}{z^2} + \sum_{w \in L \setminus \{0\}} \Big(\frac{1}{(z-w)^2} - \frac{1}{w^2} \Big).$$

We showed that this as double poles at L and elsewhere holomorphic.

29.1 Properties of the Weierstrass function

Let us fix L and write $\wp(z) = \wp(z, L)$. We first note that $\wp(-z) = \wp(z)$. Now we observe that $\wp(z) - \wp(z+w)$ is a bounded entire function, and hence constant. But for $z = -w/2$, we have $\wp(z) = \wp(z+w)$. This shows that this holds for all z.

Now note that we can just differentiate and get

$$\wp'(z) = -2 \sum_{w \in L} \frac{1}{(z-w)^3}.$$

This is again an elliptic function, and it now has triple poles at points of L. But because I am on a curve, there should be an algebraic relation between these two functions. It is useful to have a power series for $\wp$.

Lemma 29.1. $\wp(z) = \dfrac{1}{z^2} + \sum_{n \geq 1} (2n+1) G_{2n+2} z^{2n}$ *where* $G_{2n+2}(L) = \sum_{w \in L \setminus \{0\}} \frac{1}{w^{2n+2}}$.

Proof. I just expand

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \sum_{m \geq 1} (m+1) w^{-m-2} z^m.$$

Here, note that if m is odd, then $G_{m+2} = 0$. □

We can now use this to find a polynomial P in $\wp$ and $\wp'$ such that $P(\wp, \wp') = \sum_{z \geq 1} c_n z^n$. This would imply that $P(\wp, \wp') = 0$. If you work this out, you get

$$(\wp'(z))^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3, \quad g_2 = 60 G_4, \quad g_3 = 120 G_6.$$

This is called the **Weierstrass form** of the elliptic curve. Then we get a map

$$\mathbb{C}/L \to E : 4y^2 = x^3 - g_2 x - g_3; \quad z \mapsto (\wp(z), \wp'(z)).$$

In fact, this implies that for all n, G_{2n} is a polynomial in g_2 and g_3 of degree n, where we consider g_2 as having degree 2 and g_3 as having degree 3. We want to show that this map is an isomorphism.

Proposition 29.2. *$\wp(z) = \wp(w)$ if and only if $z \cong \pm w \bmod L$.*

Proof. Let's take the difference $\wp(z) - \wp(w)$ as a function of z on $\mathbb{C}/L$. We know that the function has double poles at $z = 0$, and zeros at $\pm w$ (unless w is 2-torsion). So there can't be any other zeros. If w is 2-torsion, it is going to have a double zero because it is going to be even. □

Using this, we see that $(\wp(z), \wp'(z)) = (\wp(w), \wp'(w))$ can only happen when $w = -z$ or $w = z$. In the first case, we see that $\wp'(z) = \wp'(w)$. But $\wp'(z)$ has zeros as 3 nonzero point of $\frac{1}{2}L/L$. So we have an isomorphism

$$\mathbb{C}/L \cong E$$

of Riemann surfaces. If you know enough theory, it follows that this is also an isomorphism of complex Lie groups. But we can do this explicitly.

Theorem 29.3 (Addition theorem)**.** $\wp(z+w) = -\wp(z) - \wp(w) + \Big(\dfrac{1}{4}\dfrac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\Big)^2.$

Proof. Differentiate both sides in z. It is elliptic, entire and 0 at $z = 0$. □

This shows that $\mathbb{C}/L \cong E$ is indeed an isomorphism of complex Lie groups.

29.2 j-invariant

Define the **discriminant** of an elliptic curve by

$$\Delta(L) = g_2^3 - 27g_3^2$$

which is the discriminant of the polynomial $4x^3 - g_2^3x - g_3$. Then define the **j-invariant** as

$$j(L) = \frac{1728g_2^3}{\Delta}.$$

Theorem 29.4. *For two lattices $L, L' \subseteq \mathbb{C}$, $j(L) = j(L')$ if and only if L' is homothetic to L.*

Proof. If $L' = \lambda L$ then $g_2(L') = \lambda^{-4}g_2(L)$ and $g_3(L') = \lambda^{-6}g_3(L)$. If $j(L) = j(L')$, then there exist λ such that $g_2(L) = \lambda^{-2}g_2(L')$ and $g_3(L) = \lambda^{-3}g_3(L')$. Because G_{2n} are polynomials in g_2 and g_3, we get $G_{2n}(L) = \lambda^{-2n}G_{2n}(L')$. So

$$\wp(z, L) = \wp(\lambda^{-1}z, L').$$

Comparing poles, we recover L and L'. □

Now which L give E that have complex multiplication? If we have an isogeny (a nonzero homomorphism of complex Lie groups) $\varphi : E \to E$, on $\mathbb{C}/L \to \mathbb{C}/L$, it is going to look like multiplication by some complex number.

Theorem 29.5. *Let L be a lattice and consider $\wp(z) = \wp(z, L)$. Take $\alpha \in \mathbb{C}\backslash\mathbb{Z}$. The following are equivalent:*

(1) *multiplication by* $\alpha : \mathbb{C} \to \mathbb{C}$ *induces an isogeny of* $\mathbb{C}/L$

(2) $\alpha L \subseteq L$

(3) $\wp(\alpha z)$ *is a rational function in* $\wp(z)$

(4) *there exists a* $\mathcal{O}$ *the ring of integers of some imaginary quadratic field* K *such that* $\alpha \in \mathcal{O}$ *and* $\mathfrak{a} \subseteq \mathcal{O}$ *is homothetic to* $\mathfrak{a}$*.*

30 April 9, 2018

I missed 40 minutes of class.

30.1 j-invariants of CM elliptic curves

Theorem 30.1. *Let $\mathcal{O}$ be the order in an imaginary quadratic field, and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a}) = j(\mathbb{C}/\mathfrak{a})$ is an algebraic number of degree at most $h(\mathcal{O})$.*

Proof. We consider $\{j(E) : \operatorname{End}(E) \cong \mathcal{O}\} \subseteq \mathbb{C}$. This is the same as $\{j(\mathfrak{a})\}$ where $\mathfrak{a}$ runs over invertible fractional ideals of $\mathcal{O}$. This is a union of Galois orbits, which is set of size $h(\mathcal{O})$. □

We will be showing that actually

$$[\mathbb{Q}(j(\mathfrak{a})) : \mathbb{Q}] = h(\mathcal{O})$$

and also that $j([\mathfrak{a}])$ is an algebraic integer. When $\mathcal{O} = \mathcal{O}_K$, an $K(j[\mathfrak{a}]) = H$, in general we can describe $K(j[\mathfrak{a}])$ as follows. We define

$$\operatorname{Gal}(L_{\mathcal{O}}/K) \cong C_K / \prod_{v \text{ fin}} U_v^\times$$

where $\mathcal{U}_v$ is the closure of $\mathcal{O}$ in $\mathcal{O}_v$. (Then if $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ then $U_v = (\mathbb{Z}_p + f\mathcal{O}_v)^\times$. This means that $L_{\mathcal{O}} \subseteq L_f$.)

31 April 11, 2018

Let $L \subseteq \mathbb{C}$ be a lattice and let $E = \mathbb{C}/L$ have complex multiplication. Then $\operatorname{End}(E) = \mathcal{O} \supsetneq \mathbb{Z}$, and we say that L has complex multiplication by $\mathcal{O}$. In that case, $L \sim \mathfrak{a}$ for some invertible fraction ideal $\mathcal{O}$. We saw that $j(L)$ is an algebraic number of degree at most $h(L)$.

Theorem 31.1 (main theorem of complex multiplication)**.** *The j-invariant $j(L)$ is an algebraic integer of degree $h(L)$ and $K(j(L)) = L_{\mathcal{O}}$ (which is the ring class field of $\mathcal{O}$).*

Definition 31.2. A **cyclic sublattice** of index m is a sublattice $L' \subseteq L$ such that $L/L' \cong \mathbb{Z}/m\mathbb{Z}$.

Proposition 31.3. *If L has complex multiplication, then there exists a cyclic sublattice $L' \subseteq L$ such that L' is homothetic to L.*

Proof. Without loss of generality, let $\mathfrak{a}$ be an invertible ideal of $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. Choose $m = p$ such that p is relatively prime to $\mathfrak{a}, f$, and p completely splits in $\mathcal{O}_K$ as $p = \pi\bar{\pi}$. Take $L' = \pi L$ so that

$$L/\pi L = \mathfrak{a}/p\mathfrak{a} \cong \mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}.$$

□

31.1 Modular forms and functions

We defined the j-invariant as a function for a lattice invariant under homothety, but the classical way of looking at it is as a function on the upper half plane H. For $\tau \in H$, the free abelian group $[1, \tau] \subseteq \mathbb{C}$ is a lattice. So we can define

$$g_2(\tau) = g_2[1,\tau], \quad g_3(\tau) = g_3[1,\tau], \quad \Delta(\tau) = \Delta[1,\tau], \quad j(\tau) = j[1,\tau].$$

Here, there is an action of $\mathrm{SL}_2(\mathbb{Z})$ on H, and the action on τ only does a homothety on the lattice by taking L to $\frac{1}{c\tau+d}L$. So we get

$$g_2(\gamma\tau) = (c\tau+d)^4 g_2(\tau), \quad g_3(\gamma\tau) = (c\tau+d)^6 g_3(\tau).$$

This is saying that g_2 is a modular form of weight 4 and g_3 is a modular form of weight 4. For the j-invariant, we will have

$$j(\gamma\tau) = j(\tau)$$

for all $j \in \mathrm{SL}_2(\mathbb{Z})$. This means that j descends to a function on $Y(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus H$. There is a fundamental domain

$$\{\tau \in H : -\tfrac{1}{2} < \Re(\tau) < \tfrac{1}{2}, |\tau| > 1\}$$

and then you can see that this is a sphere minus one point, but with one order 2 orbifold point and one 3 orbifold point. This is not compact, so we compactify it to get a Riemann surface $X(1) = Y(1) \cup \{\infty\}$. Around infinity, the local coordinates are going to be given by $q = e^{2\pi i z}$.

Definition 31.4. A **modular function** for $\mathrm{SL}_2(\mathbb{Z}$ (a meromorphic modular form of weight 0) is a meromorphic function f on H such that $f(\gamma\tau) = f(\tau)$ for all $\tau \in H$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and f can be written as $\sum_{n\geq -k} c_n q^n$ converging for $\Im\tau \gg 0$.

For example $j(\tau)$ is a modular function. Next time we are going to try and get a q-series for the j function.

32 April 13, 2018

Last time we saw that a modular function for $\mathrm{SL}_2(\mathbb{Z})$ is just a meromorphic function on $X(1) = \mathrm{SL}_2(\mathbb{Z}) \setminus H \cup \{\infty\}$. This is a compact Riemann surface of genus 0. An alternative description of a modular function is a meromorphic function f on H such that

$$f(\gamma\tau) = f(\tau)$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $f = \sum_{n\geq -k} c_n q^n$.

We now check that $j(\tau)$ actually has a q-expansion. We have

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2^k}}{(2k-1)!}\sum_{n\geq 1}\sigma_{2k-1}(n)q^n, \quad \sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}.$$

So

$$\begin{aligned} g_2(\tau) &= 60G_4(\pi) = \frac{4}{3}\pi^4\biggl(1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\biggr), \\ g_3(\tau) &= 120G_6(\pi) = \frac{8}{27}\pi^6\biggl(1 + 504\sum_{n\geq 1}\sigma_5(n)q^n\biggr), \\ \Delta(\tau) &= (2\pi)^{12}\sum_{n\geq 1}\tau(n)q^n, \\ j(\tau) &= \frac{1}{q} + \sum_{n\geq 0} c(n)q^n = \frac{1}{q} + 744 + 196884q + \cdots. \end{aligned}$$

The important thing here is that the coefficients $c(n)$ are all integers. This shows that $j(\tau)$ is indeed a modular function. It has a simple pole at ∞ and no other poles. It has the only 0 at $\tau = \omega$ where $\omega^3 = 1$. It follows that the field of modular functions for $\mathrm{SL}_2(\mathbb{Z})$ is $\mathbb{C}(j(z))$ and the subring of modular functions that are holomorphic away from ∞ is $\mathbb{C}[j(z)]$.

32.1 Congruence subgroups

Recall that $\mathrm{SL}_2(\mathbb{Z}) \setminus H$ corresponds to lattices $L \subseteq \mathbb{C}$ up to homothety. We want to look at a finer group, so that $\Gamma_0(m) \setminus H$ parametrizes pairs (L, L') up to homothety, where $L \subseteq \mathbb{C}$ is a lattice and $L' \subseteq L$ is cyclic of index m.

Definition 32.1. For $m \geq 1$, we define

$$\Gamma_0(m) = \biggl\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{m}\biggr\}.$$

So if $[\tau] \in \Gamma_0(m) \setminus H$, we look at the corresponding $[1, \tau]$ and $[1, m\tau]$. Up to homothety, the lattice acted by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is $[c\tau + d, m(a\tau + b)]$, and this is equal to $[1, m\tau]$ because c is a multiple of m. Then we can look at the modular curve

$$Y_0 = \Gamma(m) \setminus H.$$

This is going to be a non-compact Riemann surface, and we compactify it by adding cusps. This can be compactified to a modular curve $X_0(m)$.

Definition 32.2. A **modular function** for $\Gamma_0(m)$ is a

- meromorphic function on $X_0(m)$,
- a meromorphic function f on H such that $f(\gamma\tau) = f(\tau)$ for all $\gamma \in \Gamma_0(m)$, and the q-series such that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the function $f(\gamma(\tau))$ is a Laurent series in $q^{1/m}$.

Examples include $j(\tau)$ or even $j(m\tau)$. Note that the projection map $X_0(m) \to X(1)$ has degree

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(m)] = m \prod_{p|m} \Big(1 + \frac{1}{p}\Big) = d_m,$$

where d_m counts the number of cyclic index m sublattices of $\mathbb{Z}^2$. Then we are going to have a field extension

$$(\text{modular functions for } \Gamma_0(m))/(\text{modular functions for } \mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}(j(\tau))$$

of degree d_m. But this is not Galois because $\Gamma_0(m)$ is not a normal subgroup of SL_2.

Theorem 32.3. *The modular functions for $\Gamma_0(m)$ are $\mathbb{C}(j(z), j(mz))$.*

Proof. We will show that $[\mathbb{C}(j(z), j(mz)) : \mathbb{C}(j(z))]$ is at least d_m. To show that $[L : K] \geq k$, we exhibit a field $K \hookrightarrow E$ with k distinct extensions $L \hookrightarrow E$. For every $\gamma \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_0(m)$, we embed

$$C(j(z), j(mz)) \hookrightarrow E; \quad j(z) \mapsto j(\gamma z) = j(z), \quad j(mz) \mapsto j(m\gamma z).$$

This shows that $j(z)$ and $j(mz)$ exhaust the field of modular functions. □

This tells us that there exists some algebraic relation between $j(\tau)$ and $j(m\tau)$. We are going to leverage this to prove stuff about the j-invariant. In particular, we are going to explicitly construct Φ_m such that $\Phi_m(j(\tau), j(m\tau)) = 0$.

33 April 16, 2018

Last time we looked at $X_0(m)$ over $X(1)$, which has degree d_m. The rational functions on $X_0(m)$ is $\mathbb{C}(j(\tau), j(m\tau))$ and the rational functions on $X(1)$ is $\mathbb{C}(j(\tau))$. So we have a field extension, and there is going to be an algebraic relation between the two.

33.1 Modular polynomial

The goal today is to find a polynomial $\Phi_m(x, y)$ such that $\Phi(j(m\tau), j(\tau)) = 0$. Then we will have $\Phi_m(j(m\gamma\tau), j(\gamma\tau)) = 0$. The strategy is to look at

$$f_m(X, \tau) = \prod_{\gamma\in\Gamma_0(m)\backslash\mathrm{SL}_2(\mathbb{Z})} (X - j(m\gamma\tau)) = \prod_{L'\subseteq[1,\tau] \text{ cyclic}} (X - j(L')).$$

Note that coefficients of $f_m(X, \tau)$ are holomorphic functions of $\tau \in H$. It is also $\mathrm{SL}_2(\mathbb{Z})$-invariant. So once we check that they have q-expansions, we will get that they are modular functions for $\mathrm{SL}_2(\mathbb{Z})$. Then the coefficients lie in $\mathbb{C}[j(\tau)]$ and so we can write

$$f_m(X, \tau) = \Phi_m(X, j(\tau)).$$

This will be our Φ_m.

We first study cyclic index m sublattice of $L = [1, \tau]$. For $L' \subseteq L$, take $d \in \mathbb{Z}_{>0}$ be minimal with $d \in L$. Then $d \mid m$ and so we can take $a = \frac{m}{d}$. Then there is some b with $0 \le b < d$ and $a\tau + b \in L$. In this case, $L' = [d, a\tau + b]$ with $ad = m$, $0 \le b < d$, $\gcd(a, b, d) = 1$. So the cyclic index m sublattices of $[1, \tau]$ are (up to homothety) the lattices $[1, \sigma\tau]$ for

$$\sigma \in C_m = \biggl\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \text{ as before} \biggr\}.$$

One can equivalently classify cosets $\Gamma_0(m) \setminus \mathrm{SL}_2(\mathbb{Z})$ as

$$\mathrm{SL}_2(\mathbb{Z}) \cap \sigma^{-1} \mathrm{SL}_2(\mathbb{Z})\sigma$$

for $\sigma \in C_m$. For instance, if we consider $\sigma_0 = \left(\begin{smallmatrix} m & 0 \\ 0 & 1 \end{smallmatrix}\right)$ then $\sigma_0^{-1} \mathrm{SL}_2(\mathbb{Z})\sigma_0 = \left(\begin{smallmatrix} a & b/m \\ cm & d \end{smallmatrix}\right)$ and so the intersection is $\Gamma_0(m)$. Then

$$f_m(X, \tau) = \prod_{\sigma\in C_m} (X - j(\sigma\tau)),$$

with the coefficients of X^i being symmetric functions in $j(\sigma\tau)$.

We know that each $j(\sigma\tau)$ is

$$j(\sigma\tau) = j\Bigl(\frac{a\tau + b}{d}\Bigr),$$

which is a Laurent series in

$$e^{2\pi i(a\tau+b)/d} = Q^{a^2}\zeta_m^{ab}$$

where $Q = q^{1/m}$ and $Q = 2\pi i\tau$. Then it is a Laurent series in $Q = q^{1/m}$ and invariant in $\tau \mapsto \tau + 1$. So it is a power series in $q = e^{2\pi i\tau}$. This now shows that the coefficients of $f_m(\tau)$ actually line in $\mathbb{C}[j(\tau)]$. So $f_m(\tau) = \Phi_m(X, j(\tau))$ for $\Phi_m \in \mathbb{C}[X, \tau]$.

To show that the coefficients of Φ_m are integers, we show that the coefficients of $\Phi_m(X, j(\tau))$ are in $\mathbb{Z}((q))$.

Proposition 33.1. *If $p \in \mathbb{C}[x]$ and $p(j(\tau)) \in \mathbb{Z}((q))$ then $p \in \mathbb{Z}[x]$.*

Proof. Exercise. □

Now it is obvious that the coefficients of $\Phi_m(X, j(\tau))$ are algebraic integers, because we are multiplying algebraic integer coefficient power series together. But we also note that the set

$$\left\{Q^{-a^2}\zeta_m^{-ab} + \sum_{k\geq 0} c_k Q^{a^2k}\zeta_m^{abk} : \sigma \in C_m\right\}$$

is invariant under $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. This shows that the coefficients are in $\mathbb{Z}$.

34 April 18, 2018

We constructed $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$. By construction, this has the property that $\Phi_m(j(L'),j(L)) = 0$ if and only if L' is a cyclic index m sublattice of L. So $\Phi_m(j(E'),j(E)) = 0$ if and only if there exists a cyclic m-isogeny $\phi : E' \to E$ (isogeny with $\ker(\phi)$ cyclic of order m). This is true even in characteristic p.

34.1 Coefficients of the modular polynomial

Proposition 34.1. *(a)* $\Phi_m(X,Y) = \Phi_m(Y,X)$.

(b) If m is not a square, then $\Phi_m(X,X)$ has leading coefficient ± 1.

(c) (Kronecker congruence) $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \bmod p$.

Proof. For (a), we show first that the zero locus is symmetric. So we show that L' is similar to a cyclic index m sublattice of L if and only if L is similar to a cyclic index m sublattice of L'. But if $L' \subseteq L$ is cyclic of index m, then $mL \subseteq L'$ is cyclic of index m. This shows that $\Phi_m(X,Y) = c\Phi_m(Y,X)$, where $c = \pm 1$, but $c = 1$ implies $\Phi_m(X,X) = 0$, which is not true.

For (b), we look at

$$\Phi_m(j(\tau),j(\tau)) = c_m q^{-m} \sum_{k>-m} c_k q^{-k}.$$

We want to show that c_m is ± 1. But we see that

$$\Phi_m(j(\tau),j(\tau)) = \prod_{\sigma \in C_m} (j(\tau) - j(\sigma\tau))$$

where $j(\tau) - j(\sigma\tau) = (Q^{-m} + \text{holomorphic}) + (\zeta^{-ab}Q^{-a^2} + \text{holomorphic})$. But if m is not a square, whatever the leading term is, it is going to have coefficient a root of unity. So c_m should be a product of roots of unity, which is also a integer.

For (c), we need the explicit description of C_p. It is going to be

$$C_p = \{\sigma_i = \left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right) : 0 \le i < p\} \cup \{\sigma_\infty = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\}.$$

Then we have

$$j(\sigma_\infty \tau) = j(p\tau) = q^{-p} + \sum_{k \ge 0} c_k q^{pk} \equiv (j(\tau))^p \pmod{p}.$$

For $j(\sigma_i\tau)$, the coefficients are going to be in $\mathbb{Z}[\zeta_p]$. So we work at the prime $(1-\zeta_p)$ that lies over p. Then

$$j(\sigma_i\tau) = j\Big(\frac{\tau+i}{p}\Big) = \zeta_p^{-i} Q^{-1} + \sum_{k\ge 0} c_k \zeta^{ik} Q^k \equiv Q^{-1} + \sum_{k \ge 0} c_k Q^k \pmod{1-\zeta_p}.$$

Then we can compute

$$\Phi_m(X, j(\tau)) \equiv (X - j(\tau)^p)(X - j(\tau/p))^p \equiv (X - j(\tau)^p)(X^p - j(\tau)) \pmod{1 - \zeta_p}$$

and so $\Phi_m(X, Y) \equiv (X - Y^p)(X^p - Y)$ modulo p. □

Theorem 34.2. *If L is a lattice with complex multiplication by $\mathcal{O}$, then $j(L)$ is an algebraic integer.*

Proof. We have previously seen that there exists an $L' \subseteq L$ cyclic of index m such that $\Phi_m(j(L), j(L)) = 0$. Here, we were able to choose $L' = \pi L$ for some principal prime $\pi\bar{\pi} = p$. So $\Phi_m(j(L), j(L)) = 0$ and so $j(L)$ is a root of a monic polynomial. □

Recall that $L_{\mathcal{O}}$ the ring class field of $\mathcal{O}$ was defined as $L_{\mathcal{O}}/K = \mathrm{Frac}(\mathcal{O})$ of degree $\mathrm{Cl}(\mathcal{O})$. We want to prove that if $\mathfrak{a}$ is an invertible ideal of $\mathcal{O}$ then $M = K(j(\mathfrak{a})) = L_{\mathcal{O}}$.

Next time, we will show $M \subseteq L_{\mathcal{O}}$ by looking at splitting behavior of primes. First we will show that $\mathrm{Spl}(L/\mathbb{Q}) \subseteq \mathrm{Spl}(M/\mathbb{Q})$ so that the Galois closure of M is contained in L. For the other half, we will show that $\mathrm{Spl}'(M/\mathbb{Q})$ (which has at least one completely split factor in M) is contained in $\mathrm{Spl}(L/\mathbb{Q})$. That implies that $L \subseteq M$.

35 April 20, 2018

Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and write $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ where f is called the conductor.

35.1 Main theorem of complex multiplication

Theorem 35.1 (main theorem of complex multiplication). *If $\mathfrak{a}$ is any invertible ideal of $\mathcal{O}$, then $M = K(j(\mathfrak{a}))$ is the ring class field $L = L_{\mathcal{O}}$.*

The first step is to show that $\mathrm{Spl}(L/\mathbb{Q}) \subseteq \mathrm{Spl}(M/\mathbb{Q})$ up to finitely many exceptions. Take $p \in \mathrm{Spl}(L/\mathbb{Q})$ and assume $p \nmid f$ and $p \nmid \mathfrak{a}$ and $p \nmid [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$. You are going to show in the homework that the hypothesis for p implies that $p = N\pi = \pi\bar{\pi}$ for some $\pi \in \mathcal{O}$. Then we have $\pi\mathfrak{a} \subseteq \mathfrak{a}$ a cyclic sublattice of index p. This implies that

$$\Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = 0$$

and so $j(\mathfrak{a})$ is a root of $\Phi_p(x,x)$. Observe that $\Phi_p(x,x) \equiv (x^p - x)(x - x^p)$ modulo p.

Choose an arbitrary prime $\mathfrak{p}_M$ of $M = K(j(\mathfrak{a}))$ above p. Module $\mathfrak{p}_M$, we have

$$(j(\mathfrak{a})^p - j(\mathfrak{a}))(j(\mathfrak{a}) - j(\mathfrak{a})^p) \equiv 0 \pmod{\mathfrak{p}_M}.$$

So $j(\mathfrak{a})$ is in $\mathfrak{p}_M$. But the hypothesis that $p \nmid [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a}\mathfrak{j})]]$ implies that $\mathcal{O}_K[j(\mathfrak{a})]$ surjects to $\mathcal{O}_M/\mathfrak{p}_M$. Then

$$\mathcal{O}_M/\mathfrak{p}_M \cong (\mathcal{O}_K/\mathfrak{p}_K)[j(\mathfrak{a})] \cong \mathbb{F}_p,$$

so this means that p splits completely in $M/\mathbb{Q}$. This shows that $M \subseteq L$.

The next step is to show $\mathrm{Spl}'(M/\mathbb{Q}) \subseteq \mathrm{Spl}(L/\mathbb{Q})$ again up to finitely many primes p. Here, Spl' is the set of primes with at least one prime with no interia. Consider $p \in \mathrm{Spl}'(M/\mathbb{Q})$ and exclude $p \mid f$ and p sharing a factor with $\prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j)) \in \mathcal{O}_L$. (Here, $\mathfrak{a}_1, \dots, \mathfrak{a}_{H(\mathcal{O})}$ are the representatives for all ideal classes of $\mathcal{O}$.

By assumptions, there exists a $\mathfrak{p}_M$ above p such that $p = N\mathfrak{p}_M$. Let $\mathfrak{p}$ be the prime in K below $\mathfrak{p}_M$. Our goal is to show $\mathfrak{p} \cap \mathcal{O} = \pi\mathcal{O}$ for some π. This will imply

$$p = [\mathcal{O}_K : \mathfrak{p}] = [\mathcal{O} : \mathfrak{p} \cap \mathcal{O}] = [\mathcal{O} : \pi\mathcal{O}] = N\pi$$

and so $p \in \mathrm{Spl}(L/\mathbb{Q})$. Let $\mathfrak{a}' = \mathfrak{p} \cap \mathcal{O}$. Then $\mathfrak{a}'$ is a cyclic sublattice of $\mathfrak{a}$ of index p. Then we have

$$\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0.$$

If we pick $\mathfrak{p}_L$ over $\mathfrak{p}_M$ and work in $\mathcal{O}_L/\mathfrak{p}_L$, we get

$$0 = (\overline{j(\mathfrak{a}')}^p - \overline{j(\mathfrak{a})})(\overline{j(\mathfrak{a})}^p - \overline{j(\mathfrak{a}')})$$

inside $\mathcal{O}_L/\mathfrak{p}_L$. But $\overline{j(\mathfrak{a})}$ is actually in $\mathcal{O}_M/\mathfrak{p}_M = \mathbb{F}_p$. So we get $\overline{j(\mathfrak{a}')} = \overline{j(\mathfrak{a})}$ modulo $\mathfrak{p}_L$. Because we have set our p so that $\mathfrak{p}_L$ does not divide $\prod_{i<j}(j(\mathfrak{a}_i) -$

$j(\mathfrak{a}_j))$, this implies that $j(\mathfrak{a}) = j(\mathfrak{a}')$. This shows that there is some π such that $p \cap \mathcal{O} = \pi\mathcal{O}$.

The conclusion is that

$$K(j(\mathfrak{a})) = L_{\mathcal{O}}.$$

Then we have

$$h(\mathcal{O}) \geq [\mathbb{Q}(j(\mathfrak{a})) : \mathbb{Q}] \geq [K(j(\mathfrak{a})) : K] = [L_{\mathcal{O}} : K] = h(\mathcal{O})$$

and so

$$\begin{tikzcd}
 & L_{\mathcal{O}} = K(j(\mathfrak{a})) \arrow[dl, dash, "h(\mathcal{O})"'] \arrow[dr, dash, "2"] \arrow[dd, dash, "\mathrm{Gal}"'] & \\
K \arrow[dr, dash, "2"'] & & \mathbb{Q}(j(\mathfrak{a})) \arrow[dl, dash, "h(\mathcal{O})"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

We can talk about Shimura reciprocity which says that if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ and $(\mathfrak{p}, f) = 1$ with no ramification, then

$$\mathrm{Frob}_{\mathfrak{p}}(j(\mathfrak{a})) = j((\mathfrak{p} \cap \mathcal{O})\mathfrak{a}).$$

Another thing we can talk about is Gross–Zagier, which gives a formula for $j(\mathfrak{a}) - j(\mathfrak{a}')$. We can also talk about the class number 1 problem. If $h(\mathcal{O}) = 1$ then $j(\mathcal{O}) \in \mathbb{Z}$ and actually $j(\mathcal{O})$ is always a cube. Then the problem comes down to showing finitely many rational points on elliptic curves.

36 April 23, 2018

Today we will look at Heegner's proof of the class number 1 problem.

36.1 Cube root of j

For $j = g_2^3/\Delta$, we define $\gamma_2 = \sqrt[3]{j}$ in the q-expansion, so that

$$\gamma_2(\tau) = q^{1/3} + \sum_k a_k q^k + \cdots$$

where a_k are rational. This is no longer going to be SL_2-invariant, but we will have

$$r_2(\gamma\tau) = \zeta r_2(\tau)$$

for some $\zeta^3 = 1$. It turns out that $r_2(\gamma\psi) = r_2(\psi)$ if and only if $a \equiv d \equiv 0 \bmod 3$ or $b \equiv c \equiv 0 \bmod 3$. So $\gamma_2(3\tau)$ is a modular function for $\Gamma_0(9)$. So $r_2(3\tau) \in \mathbb{Q}(j(\tau), j(3\tau))$.)

Theorem 36.1. *If $\mathcal{O}$ is an order in an imaginary quadratic field, and* 3 *does not divide* $\mathrm{Disc}(\mathcal{O})$*, define $\tau_0 = \sqrt{-m}$ if* $\mathrm{Disc}(\mathcal{O}) = -4m$ *and $\tau_0 = \frac{3+\sqrt{-m}}{2}$ otherwise (so that τ_0 is relatively prime to* 3*). Then $\mathbb{Q}(r_2(\tau_0)) = \mathbb{Q}(j(\tau_0))$ and $K(r_2(\tau_0)) = K(j(\tau_0)) = L_{\mathcal{O}}$.*

Proof. We have seen that $r_2(\tau_0) \in \mathbb{Q}(j(\frac{\tau_0}{3}), j(3\tau_0))$. But both lattices $[1, \frac{\tau_0}{3}]$ and $[1, 3\tau_0]$ has complex multiplication by exactly $\mathcal{O}' = \mathbb{Z}[3\tau_0]$, by the coprimality conditions. This immediately shows that $r_2(\tau_0) \in L_{\mathcal{O}'}$. So we need to know how passing to a smaller order affects.

In general, let $\mathcal{O}$ be an order in an imaginary quadratic field, and let $p \nmid \mathrm{Disc}(\mathcal{O})$. Suppose $\mathcal{O}' \subseteq \mathcal{O}$ is the unique index p suborder, which is $\mathcal{O}' = \mathbb{Z} + p\mathcal{O}$. In this case, we have the Galois group of $L_{\mathcal{O}'}/L_{\mathcal{O}}$ is going to be $(\mathcal{O}/p\mathcal{O})^\times/(\mathbb{Z}/p\mathbb{Z})^\times$ which is a cyclic group of order either $p-1$ or $p+1$, depending on whether $\mathcal{O}/p\mathcal{O}$ is $\mathbb{F}_{p^2}$ or $\mathbb{F}_p^2$.

So we have $L_{\mathcal{O}'}/L_{\mathcal{O}}$ of degree either 2 or 4 (assuming $\mathcal{O}^\times = \pm 1$). So the degree of the minimal polynomial of $r_2(\tau_0)$ over $L_{\mathcal{O}}$ divides 4. But we know that $r_2(\tau_0)^3 \in L_{\mathcal{O}}$. This shows that $r_2(\tau_0) \in L_{\mathcal{O}}$. □

There are **Weber functions** $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Q}((q^{1/48}))$ and $\mathrm{SL}_2(\mathbb{Z})$ fixes the set $\{\mathfrak{f}^{48}, \mathfrak{f}_1^{48}, \mathfrak{f}_2^{48}\}$. Here, we have that

$$\mathfrak{f}(\tau)\mathfrak{f}_1(\tau)\mathfrak{f}_2(\tau) = \mathfrak{f}_1(2\tau)\mathfrak{f}_2(\tau) = \sqrt{2}.$$

It is also true that $\mathfrak{f}^8, -\mathfrak{f}_1^8, -\mathfrak{f}_2^8$ are roots of $X^3 - \gamma_2 X - 16$.

Proposition 36.2. *If $m \equiv -3 \bmod 8$ then*

$$K(\mathfrak{f}(\sqrt{-m})^2) = L_{\mathbb{Z}[-\sqrt{m}]},$$

where $\mathbb{Z}[\sqrt{-m}]$ is of index 2 *in $\mathcal{O}_{\sqrt{-m}}$.*

Proof. Use the fact that $\mathfrak{f}(84)^6$ is a modular function for $\Gamma_0(64)$. □

36.2 Class number one problem

Theorem 36.3. *Let K be an imaginary quadratic field, and let $d_K = \mathrm{disc}(K)$. Then $h(\mathcal{O}_K) = 1$ if and only if $d_K \in \{-3, -5, -7, -8, -11, -19, -43, -67, -163\}$.*

Proof. First, consider the case when 2 is split or ramified in $\mathcal{O}_K$. Then there is some prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ with $N\mathfrak{p} = 2$. Because $\mathfrak{p}$ has to be a prime, this can happen only for $d = -4, -7, -8$. So assume that d is odd.

By one of the homework, we have $\mathrm{Cl}(K)[2] = (\mathbb{Z}/2\mathbb{Z})^k$ where k is the number of prime factors of d minus 1. This shows that $d = -2$, and 2 being inert in $\mathbb{Q}(-\sqrt{d})$ shows that $p \equiv 3 \pmod 8$.

Setting aside the case $3 = p$, we may assume that $3 \nmid p$. Consider $\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{-p})}$ and $\mathcal{O}' = \mathbb{Z}[\sqrt{-p}]$. Then $[\mathcal{O} : \mathcal{O}'] = 2$ and because 2 is inert, we have that $L_{\mathcal{O}'}/L_{\mathcal{O}}$ is of degree $2 + 1 = 3$. Then we have the following.

$$\begin{tikzcd}
L_{\mathcal{O}'} = \mathbb{Q}(\sqrt{-p})(\mathfrak{f}(\sqrt{-p})^2) \arrow[d, dash, "3"'] & \mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2) \arrow[l, hook] \arrow[d, dash, "3"'] \\
L_{\mathcal{O}} = \mathbb{Q}(\sqrt{-p}) & \mathbb{Q} \arrow[l, hook, "2"']
\end{tikzcd}$$

You can check that $\mathfrak{f}(\sqrt{-p})$ is some real number.

Let $\tau_0 = \frac{3+\sqrt{-p}}{2}$ and let $\alpha = \zeta_8^{-2}\mathfrak{f}_2(\tau_0)^2 = 2/\mathfrak{f}(\sqrt{-p})^2$. (This is from some Weber function identity.) Because α generates $\mathbb{Q}(\mathfrak{f}(\sqrt{-p})^2)$, α^4 generates that field. What is the minimal polynomial of α^4 over $\mathbb{Q}$? Because $\alpha^4 = -\mathfrak{f}_2(\tau_0)^8$, its minimal polynomial must be $X^3 - \gamma_2(\tau)X - 16$.

On the other hand, this is very restrictive, because we have an algebraic integer that is a fourth power in a cubic field. α is an algebraic integer of degree 3 and take $X^3 + aX^2 + bX + c$ the minimal polynomial of α. You can show that α^2 has minimal polynomial $X^3 + eX^2 + fX + g$ for

$$e = 2b - a^2, \quad f = b^2 - ac, \quad g = c^2,$$

and so α^4 has minimal polynomial

$$X^3 + (2f - e^2)X^2 + (f^2 - eg)X - g^2.$$

This shows that $2f = e^2$, $g^2 = 16$. So $g = -4$ and (assuming $c = 2$) $2f = e^2$ becomes $2(b^2 - 4a)^2 = (2b - a^2)^2$. Change of variables gives $Y^2 = 2X(X^3 + 1)$ and you end up getting a finite number of integral points. These gives the list of possible j-invariants. $\square$

37 April 25, 2018

Let $\mathfrak{a}$ be an invertible ideal in $\mathcal{O} \subseteq K$, and let $\mathfrak{p}$ be any prime of $\mathcal{O}_K$. Assume that $\mathfrak{p} \nmid \operatorname{Disc}(\mathcal{O}) = f^2 \operatorname{Disc}(\mathcal{O}_K)$. The thing we want to show is that

$$\operatorname{Frob}_{\mathfrak{p}}(j(\mathfrak{a})) = j((\bar{\mathfrak{p}} \cap \mathcal{O})\mathfrak{a}) = j((\mathfrak{p} \cap \mathcal{O})^{-1}\mathfrak{a}).$$

37.1 Shimura reciprocity

Here is the elliptic curve perspective. For $\mathcal{O} \subseteq K$ an order in an imaginary quadratic field, we have

$$\operatorname{Ell}(\mathcal{O}) = \{\text{isomorphism classes of } E/\overline{\mathbb{Q}} \text{ with } \operatorname{End}(E) \cong \mathcal{O}\}.$$

Then we have a bijection $\operatorname{Ell}(\mathcal{O})$ with $\operatorname{Cl}(\mathcal{O})$, by sending $\mathfrak{a}$ to $\mathbb{C}/\mathfrak{a}$.

Let $\operatorname{Cl}(\mathcal{O})$ act on $\operatorname{Ell}(\mathcal{O})$, define analytically by

$$\mathfrak{a} * (\mathbb{C}/L) = \mathbb{C}/(\mathfrak{a}^{-1}L).$$

The claim is that $\mathfrak{a} * E = \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, E)$ as $\mathcal{O}$-modules. The reason is that if $E = \mathbb{C}/\mathfrak{b}$ then $0 \to \mathfrak{b} \to \mathbb{C} \to E \to 0$. Because $\mathfrak{a}$ is a projective $\mathcal{O}$-module, we get

$$0 \to \mathfrak{a}^{-1}\mathfrak{b} = \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathfrak{b}) \to \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathbb{C}) \cong \mathbb{C} \to \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, E) \to 0.$$

This shows that $\mathfrak{a} * E = \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, E)$.

But this is analytic. How do you make $\mathfrak{a} * E$ into a group variety? For any finitely generated $\mathcal{O}$-module M, we can put a group variety structure on $\operatorname{Hom}_{\mathcal{O}}(M, E)$. If M is free, this is clear. If not, take a finite presentation $\mathcal{O}^b \to \mathcal{O}^a \to M \to 0$ and define

$$\operatorname{Hom}_{\mathcal{O}}(M, E) = \ker(E^a \to E^b)$$

given by the matrix. If $M = \mathfrak{a}$, we are going to get another elliptic curve $E' = \mathfrak{a} * E$.

For any elliptic curve E over a number field L, such that $\mathcal{O} \hookrightarrow \operatorname{End}_L(E)$, we define $\mathfrak{a} * E = \operatorname{Hom}_{\mathcal{O}}(\mathfrak{a}, E)$. For any invertible ideal $\mathfrak{a}$ of $\mathcal{O}$, we get another elliptic curve

$$\mathcal{O} \hookrightarrow \operatorname{End}_L(\mathfrak{a} * E).$$

Now $\operatorname{Gal}(L_{\mathcal{O}}/K)$ acts on $\operatorname{Ell}(\mathcal{O})$, and also the class group $\operatorname{Cl}(\mathcal{O})$ acts on $\operatorname{Ell}(\mathcal{O})$.

Proposition 37.1. *We have $g(\mathfrak{a} * E) = \mathfrak{a} * g(E)$ for all $g \in \operatorname{Gal}(L_{\mathcal{O}}/K)$.*

So we are going to get a map $\phi : \operatorname{Gal}(L_{\mathcal{O}}/K) \to \operatorname{Cl}(\mathcal{O})$, defined so that $g(E) = \phi(g) * E$. We will show that ϕ is inverse to the map

$$\theta : \operatorname{Cl}(\mathcal{O}) \to \operatorname{Gal}(L_{\mathcal{O}}/K).$$

Proof. We check this for $[\mathfrak{p}] \in \mathrm{Cl}(\mathcal{O})$. Take $\mathfrak{p} \subseteq \mathcal{O}_K$ and look at $\mathfrak{p}_{\mathcal{O}} = \mathfrak{p} \cap \mathcal{O}$, which we are going to refer to as $\mathfrak{p}$ as well. Take $E \in \mathrm{Ell}(\mathcal{O})$ such that E has good reduction at $\mathfrak{p}_L$, where $\mathfrak{p}_L$ is the prime of L above $\mathfrak{p}$. Write $\tilde{E}$ the reduction of E over L.

Let $\tilde{E}^p$ be the elliptic curve given by $y^2 = x^3 a^p x + b^p$. Then we have $j(\tilde{E}^p) = j(\tilde{E})^p$. Now the claim is that

$$\tilde{E}^{N\mathfrak{p}} \cong \mathfrak{p} * \tilde{E} = \widetilde{\mathfrak{p} * E}.$$

(The second equality follows from the definition of $*$.) If we have this, then

$$j(\mathfrak{p} * E) = j(\widetilde{\mathfrak{p} * E}) = j(\tilde{E})^{N\mathfrak{p}} = j(E)^{N\mathfrak{p}} \pmod{\mathfrak{p}_L}$$

shows that $\mathrm{Frob}_{\mathfrak{p}}(j(E)) = j(\mathfrak{p} * E)$.

First suppose that $N\mathfrak{p} = p$. Then restriction $\mathrm{Hom}(\mathcal{O}, E) \to \mathrm{Hom}(\mathfrak{p}, E)$ is an isogeny

$$\tilde{E} \xrightarrow{p} \mathfrak{p} * \tilde{E}$$

of degree p. We also have an isogeny $\tilde{E} \to \tilde{E}^p$ given by Frobinius. We can show that both maps are inseparable isogenies of degree p. Then there is a unique such isogeny, so we get that the target are isomorphic.

Now suppose that $N\mathfrak{p} = p^2$, which means that $\mathfrak{p} = (p)$. Then the reduction $\tilde{E}$ has no p-torsion and they are called supersingular. Then there exists a unique isogeny from $\tilde{E} \to \tilde{E}'$ of degree p^2. Then again I can there are both the Frobenius and restriction are degree p^2 isogenies. □

Index