ALGEBRAIC NUMBER THEORY II

ASHWIN IYENGAR

Contents

1. Introduction

This course is a sequel to Algebraic Number Theory I, and aims to understand *class field theory*, which seeks to understand and describe of abelian extensions of a number field or a local field via what are known as *reciprocity laws*.

1.1. **Quadratic reciprocity.**

To set the stage, we begin by thinking about quadratic reciprocity.

Definition 1.1.1. Let p be an odd prime number[1]. Then for any $a \in \mathbb{Z}$ let

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } n^2 \equiv a \mod p \text{ for some } n \in \mathbb{Z} \text{ and } (a,p) = 1 \\ -1 & \text{if } n^2 \not\equiv q \mod p \text{ for all } n \in \mathbb{Z} \\ 0 & \text{if } p \mid a \end{cases}$$

Exercise 1.1.2. Show that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

and show that if $a \equiv b$ then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

Theorem 1.1.3 (Quadratic Reciprocity, Gauss)**.**

(1) If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

(2) If p is an odd prime then

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

and

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

In view of Exercise 1.1.2, this gives us an efficient algorithm to determine whether any integer is a square mod any prime; all you have to do is factor the top number and keep reducing mod p and the numbers appearing in the Legendre symbol get smaller and smaller.

Example 1.1.4. For instance,

$$\left(\frac{16,697}{331}\right) = \left(\frac{147}{331}\right) = \left(\frac{3}{331}\right)\left(\frac{7}{331}\right)\left(\frac{7}{331}\right) = -\left(\frac{331}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

There are many proofs of quadratic reciprocity, but before discussing a proof, we want to situate this in a more general context.

[1] there's also a law for $p = 2$ but I'm just going to ignore this for now

One strategy will rest on the following fact, proven by Gauss. Let ζ_p denote a primitive pth root of unity in $\overline{\mathbb{Q}}$. Then

$$\left(\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta_p^n\right)^2 = (-1)^{\frac{p-1}{2}}p. \tag{1}$$

Exercise 1.1.5. Prove the above identity. Hint: expand the sum and rearrange terms, and use properties of the Legendre symbol and the fact that the sum of all of the distinct pth roots of unity is 0. (this was one of the exam questions from last semester's final!)

In particular this implies that

$$F_p := \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) \subset \mathbb{Q}(\zeta_p)$$

Now consider the natural surjection

$$\chi : G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(F_p/\mathbb{Q}) \cong \{\pm 1\}.$$

Exercise 1.1.6. Fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_q$ for each prime q; this gives us inclusions $G_{\mathbb{Q}_q} \hookrightarrow G_{\mathbb{Q}}$, where $G_{\mathbb{Q}_q} = \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ and $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(1) Show that if $q \neq p$ is a prime number then q is unramified in F_p.

(2) Show that this implies that $\chi(I_q)$ is trivial, where $I_q \subset G_{\mathbb{Q}_q}$ is the inertia group at q. Hint: by part (a) q is unramified in F_p, so what is the image of I_q in $\mathrm{Gal}(F_p/\mathbb{Q})$? You can use the fact that the inertia group of an infinite extension is the inverse limit of the inertia groups of its finite subextensions without proof.

By the above exercise, we can meaningfully talk about $\chi(\mathrm{Frob}_q)$; note that Frob_q is only well-defined up to multiplication by an element of I_q, but χ is trivial on I_q, so $\chi(\mathrm{Frob}_q)$ is uniquely defined.

So what is $\chi(\mathrm{Frob}_q)$? It is determined by taking a lift of Frobenius $\sigma \in G_{\mathbb{Q}_q}$, restricting to $\sigma|_{F_p}$, and then seeing whether this is the trivial automorphism, or the one swapping the sign in $\pm\sqrt{(-1)^{\frac{p-1}{2}}p}$. But since $\sqrt{(-1)^{\frac{p-1}{2}}p}$ is an algebraic integer, the value of $\chi(\mathrm{Frob}_q)$ is equal to the $\pm$ sign in

$$\mathrm{Frob}_q\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) = \pm\sqrt{(-1)^{\frac{p-1}{2}}p},$$

where we now view $\sqrt{(-1)^{\frac{p-1}{2}}p}$ as living in the residue field of F_p at a prime above q, which embeds into $\overline{\mathbb{F}}_q$. This translates to

$$\sqrt{(-1)^{\frac{p-1}{2}}p}^{\,q} = \chi(\mathrm{Frob}_q)\sqrt{(-1)^{\frac{p-1}{2}}p}$$

in $\overline{\mathbb{F}}_q$. The fixed points of Frob_q are just $\mathbb{F}_q$, so the point is that you get a + sign if $\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{F}_q$, and a − sign otherwise. So in other words,

$$\chi(\mathrm{Frob}_q) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right).$$

On the other hand, χ factors through

$$\begin{tikzcd}
\chi : G_{\mathbb{Q}} \arrow[r] & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \arrow[r] \arrow[d, "\sim"] & \mathrm{Gal}(F_p/\mathbb{Q}) \arrow[d, "\sim"] \\
& (\mathbb{Z}/p)^\times \arrow[r] & \{\pm 1\}.
\end{tikzcd}$$

because of the aforementioned inclusion $F_p \subset \mathbb{Q}(\zeta_p)$.

Exercise 1.1.7.

(1) Show that there is a unique nontrivial group homomorphism $(\mathbb{Z}/p)^\times \to \{\pm 1\}$, and describe it.

(2) Show that q is unramified in $\mathbb{Q}(\zeta_p)$ for $q \neq p$, so that there is a well-defined Frob_q in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

(3) Show that the image of Frob_q in $(\mathbb{Z}/p)^\times$ is the residue class of q mod p.

(4) Conclude that $\chi(\mathrm{Frob}_q) = \left(\frac{q}{p}\right)$.

(5) Finally, prove Theorem 1.1.3(1) (you should use Theorem 1.1.3(2) for this as well).

1.2. **Class field theory.** The goal of this course is to situate this phenomenon in a more general context. The first example of this sort of generalization is the Kronecker–Weber theorem.

Definition 1.2.1. A Galois extension of fields K/F is called *abelian* if $\mathrm{Gal}(K/F)$ is an abelian group.

Theorem 1.2.2 (Kronecker–Weber)**.** *If $K/\mathbb{Q}$ is an abelian extension then there exists an n such that $K \subset \mathbb{Q}(\zeta_n)$. In other words, the maximal abelian extension of $\mathbb{Q}$ is obtained by adjoining all roots of unity.*

These extensions are called *cyclotomic extensions*, and Kronecker–Weber asserts that all abelian extensions of $\mathbb{Q}$ can be found in cyclotomic extensions; this is a massive generalization of Equation 1.

In fact, the Kronecker–Weber theorem is proven by first proving it *locally* and then using the local statement to prove the global one.

Theorem 1.2.3 (Local Kronecker–Weber)**.** *If $K/\mathbb{Q}_p$ is an abelian extension then there exists an n such that $K \subset \mathbb{Q}_p(\zeta_n)$. In other words, the maximal abelian extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity.*

Now if we replace $\mathbb{Q}$ with an arbitrary number field, things get much harder; it's not so easy (although possible in some cases, e.g. in the case of an imaginary quadratic field like $\mathbb{Q}(i)$) to describe the maximal abelian extension of $\mathbb{Q}$ explicitly. However, it turns out that the *Galois group* of the maximal abelian extension is a bit more accessible.

If K is a field let $G_K := \mathrm{Gal}(\overline{K}/K)$ denote its absolute Galois group. If G is any group let $G^{\mathrm{ab}} = G/\overline{[G,G]}$ denote the maximal abelian quotient of G. If $G = G_K$, then

$$G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

where K^{ab} is the maximal abelian extension of K.

Theorem 1.2.4 (Local Class Field Theory, version 1)**.** *If $K/\mathbb{Q}_p$ is a finite extension, then there is an isomorphism of topological groups*

$$\widehat{K}^\times \cong G_K^{\mathrm{ab}}$$

where $\widehat{K}$ denotes the profinite completion of K.

Note that I changed the setup: this is a *local statement.*

But in the global setting there is a similar statement, although it is a bit more complicated to state, and involves some terminology we have yet to introduce.

Theorem 1.2.5 (Global Class Field Theory)**.** *If $F/\mathbb{Q}$ is a finite extension, then there is an isomorphism*[2] *of topological groups*

$$\widehat{\mathbb{A}_F^\times/F^\times} \cong G_F^{\mathrm{ab}}$$

where $\mathbb{A}_F^\times$ is the topological group of F-idèles and the hat denotes profinite completion again.

The *F-idèles*, which are the units in $\mathbb{A}_F$ the ring of *F-adèles*, which we will introduce and discuss in more detail when we study global class field theory, are obtained by gluing together local information in a way that still lets you keep track of global information. The image I have in my head is that the number field F is like an unpopped bag of popcorn, and $\mathbb{A}_F$ is what happens when you put it in the microwave.

[2] note sometimes people equivalently write $F^\times\backslash\mathbb{A}_F^\times$, for reasons having to do with generalizations to the Langlands program.

1.3. Kummer theory.

1.3. Kummer theory. Let's discuss another important example of class field theory before moving onto to more generalities.

If we want to understand abelian extensions of fields, it helps to first try to understand *cyclic* extensions. Kummer studied these very early on, and his work was rephrased by Hilbert, who named it "Kummer theory".

Fix K any field, and let n denote a positive integer which is coprime to the characteristic of K. In particular we allow any characteristic 0 field.

Definition 1.3.1. A Galois extension L/K with Galois group G is called a *G-extension.*

So Kummer theory studies $\mathbb{Z}/n\mathbb{Z}$-extensions of K.

Theorem 1.3.2. *If $\zeta_n \in K$, then every $\mathbb{Z}/n\mathbb{Z}$-extension of K is of the form $K(\alpha^{1/n})$ for some $\alpha \in K^\times/(K^\times)^n$ of exact order n. Conversely, every such $K(\alpha)$ is a $\mathbb{Z}/n\mathbb{Z}$-extension.*

Remark 1.3.3. In the above theorem note that α is only well-defined mod $(K^\times)^n$ because $K((\alpha\beta)^{1/n}) = K(\alpha)$ if β is an nth power. So another way to phrase this is to say that $\mathbb{Z}/n\mathbb{Z}$-extensions of K are in bijection with the cyclic subgroups of $K^\times/(K^\times)^n$ of order n.

Exercise 1.3.4. Prove one direction of Theorem 1.3.2 by showing that $K(\alpha)$ is a $\mathbb{Z}/n\mathbb{Z}$-extension for $\alpha \in K^\times/(K^\times)^n$ of exact order n (an element $g \in G$ has *exact order* n if $n = \min\{m : g^m = 1_G\}$).

We won't prove the classification direction of Kummer's theorem yet; instead we will postpone this to after the discussion of group cohomology.

An example of a Kummer extension is $\mathbb{Q}(\zeta_3)(\sqrt[3]{2}) = \mathbb{Q}(\zeta_3)(\sqrt[3]{4})$. This is because $\mathbb{Q}(\zeta_3)^\times/(\mathbb{Q}(\zeta_3)^\times)^3$ contains the cyclic subgroup $\{1, 2, 4\}$.

Exercise 1.3.5. Using Theorem 1.3.2, figure out how many $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}_p(\zeta_p)$ there are. Hint: Hensel's lemma is useful.

Remark 1.3.6. There is a way to do Kummer theory over fields which don't contain a root ζ_n, but we will ignore this for the time being. This supplementary theory is useful when trying to prove the local Kronecker–Weber theorem.

1.4. The Hilbert class field. Before studying the maximal abelian extension of a number field, let's first try to understand the maximal *unramified* abelian extension.

First of all recall that there are no non-trivial unramified extensions of $\mathbb{Q}$. We didn't cover this last semester, but this follows from Minkowski theory; see [Neu99, p. III.2.17]. In fact, as we'll see later every field of class number one has no non-trivial unramified extensions.

But if a field does not have class number one, what happens?

Example 1.4.1. Let's take the example $K = \mathbb{Q}(\sqrt{-5})$ we studied last semester. This is only ramified at the prime 2, which becomes $(2) = (2, 1 + \sqrt{-5})^2$, which is not a principal ideal. On the other hand the Minkowski bound tells us that this field has class number 2, so $\mathfrak{p} = (2, 1 + \sqrt{-5})$ generates the class group.

Now consider the further extension $L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. Then L/K can only possibly be ramified at $\mathfrak{p}$ (use Dedekind–Kummer). But if we write $L = K(\alpha)$ with $\alpha = (1 + \sqrt{5})/2$, which has minimal polynomial $x^2 - x - 1$, then since $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_2$ and $x^2 - x - 1$ is still irreducible in $\mathbb{F}_2$, this says that $\mathfrak{p}$ is unramified in L. Therefore, L/K is unramified everywhere.

Exercise 1.4.2. Check that $(2, 1 + \sqrt{-5})\mathcal{O}_L$ is generated by $1 + \sqrt{-1}$, therefore principal.

Remark 1.4.3. Note that when we say L/K is "unramified everywhere" this also means unramified at the archimedean places, i.e. every real embedding $\tau : K \hookrightarrow \mathbb{R}$ extends to a real embedding of $L \hookrightarrow \mathbb{R}$. Since $K = \mathbb{Q}(\sqrt{-5})$ above has no real embeddings, it's automatically unramified at infinite places.

Notice that $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)$. Although this may seems superficial, this in fact generalizes.

Definition 1.4.4. If K is a number field, then the maximal unramified abelian extension L/K is called the *Hilbert class field.*

Theorem 1.4.5. *The Hilbert class field L of a number field K is a finite extension with Galois group isomorphic to* $\mathrm{Cl}(K)$*.*

We will give a proof much later using global class field theory via the adèlic formalism. The "class field" is a field with Galois group the "class group", and this is where "class field theory" gets its name from.

For now, recall that

$$\mathrm{Cl}(K) = J_K/P_K$$

where J_K is the group of fractional ideals of K and P_K is the subgroup of principal fractional ideals. Recall further the Artin reciprocity map that we introduced last semester. If L/K is a finite abelian extension and $\mathfrak{p}$ is a prime of K which is unramified in L and $\mathfrak{q}$ lies over $\mathfrak{p}$ then the decomposition group

$$G_{\mathfrak{q}} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

has trivial inertia subgroup, so it's generated by a lift of the $|\mathcal{O}_L/\mathfrak{q}|$-Frobenius which we denote by $\sigma_{\mathfrak{q}}$. But L/K is abelian so it doesn't depend on $\mathfrak{q}$, and so we can write $\sigma_{\mathfrak{p}} := \sigma_{\mathfrak{q}}$ for any $\mathfrak{q} \mid \mathfrak{p}$.

If L is the Hilbert class field, then all primes in K are unramified in K, so we get a well-defined map

$$J_K \mapsto \mathrm{Gal}(L/K)$$
$$\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$$

and the point is that, as we will show later, this map takes P_K to the identity (this is the hard part!), and thus factors through a map

$$\mathrm{Cl}(K) \to \mathrm{Gal}(L/K).$$

This is the map which will eventually turn out to be an isomorphism.

Exercise 1.4.6. If L/K is a finite extension of number fields admitting no nontrivial abelian subextension M/K which is everywhere unramified (including at the archimedean places) then show that $\#\,\mathrm{Cl}(K) \mid \#\,\mathrm{Cl}(L)$.

1.5. **Ray class fields.** Class field theory tells us about the Hilbert class field, which is the maximal unramified extension, but this is a fairly restrictive condition.

Instead, fix $\mathfrak{m}$ a formal product of places (archimedean or nonarchimedean); you can think of this as an ordinary ideal in $\mathcal{O}_K$ along with a choice of whether to include each archimedean place.

Definition 1.5.1. Let $J_K^{\mathfrak{m}}$ denote the group of fractional ideals which are coprime to $\mathfrak{m}$. Let $P_K^{\mathfrak{m}}$ denote the subgroup of principal fractional ideals generated by $\alpha \in K$ such that

- $\alpha \equiv 1 \mod \mathfrak{p}^e$ for all $\mathfrak{p}^e \mid \mathfrak{m}$ (by this I mean the finite part), and
- $\tau(\alpha) > 0$ for all real places $\tau \mid \mathfrak{m}$.

Then we define the *ray class group*

$$\mathrm{Cl}^{\mathfrak{m}}(K) := J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}.$$

A quotient of a ray class group is called a *generalized ideal class group.*

Exercise 1.5.2. If you have a real place, it matters whether or not you include it in the modulus. To see why, show that:

$$\mathrm{Cl}^{n\cdot\infty}(\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times \text{ and } \mathrm{Cl}^{n}(\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times / \{\pm 1\}\,.$$

If $\mathfrak{m}_{L/K}$ is the product of all of the places over which L ramifies, then the map

$$\begin{aligned} J_K^{\mathfrak{m}_{L/K}} &\to \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \sigma_{\mathfrak{p}} \end{aligned}$$

is called the *Artin reciprocity map*. This generalizes the Hilbert class field case above.

Theorem 1.5.3 (Artin reciprocity)**.** *There exists a formal product $\mathfrak{m}$ of places of K (including all of the places at which L/K is ramified) such that the map $J_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ sends $P_K^{\mathfrak{m}}$ to 0, and thus descends to a map*

$$\mathrm{Cl}^{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K).$$

This map is surjective.

Definition 1.5.4. Define the *(Artin) conductor* of L/K to be the smallest $\mathfrak{m}$ such that Theorem 1.5.3 holds. We say that L/K is the *ray class field* of $\mathfrak{m}$ if L/K has conductor dividing $\mathfrak{m}$ (so the Artin map exists) and

$$\mathrm{Cl}^{\mathfrak{m}}(K) \to \mathrm{Gal}(L/K)$$

is an isomorphism.

Theorem 1.5.5 (Existence of ray class fields)**.** *Every K and $\mathfrak{m}$ admits a ray class field.*

Again the proof of Artin reciprocity, as well as the existence of ray class fields, will happen much later once we study the adèlic formalism.

Example 1.5.6. Let's think about Artin reciprocity for $\mathbb{Q}$, which should be related to Kronecker-Weber. If $K/\mathbb{Q}$ is abelian with conductor m, then $K \subset \mathbb{Q}(\zeta_m)$, so there exists a surjection (restriction)

$$\pi : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

Then we want to show that we have a commuting triangle

$$\begin{tikzcd}
\mathbb{Q}^{\times,m} \arrow[rr, "\mathrm{Art}"] \arrow[rd] & & \mathrm{Gal}(K/\mathbb{Q}) \\
& \mathrm{Cl}^{m\cdot\infty}(\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times \arrow[ru, "\pi"] &
\end{tikzcd}$$

To show this, note that $r \in (\mathbb{Z}/m\mathbb{Z})^\times$ gets sent to an automorphism of K taking $\zeta_m \mapsto \zeta_m^r$. Picking some generator $p \in \mathbb{Q}^{\times,m}$, then if $p \equiv r \mod m$ then we just need to show that the image of p in $\mathrm{Gal}(K/\mathbb{Q})$ matches the image of r, i.e. $\zeta_m^r \equiv \zeta_m^p \mod \mathfrak{p}$ for any prime $\mathfrak{p} \subset \mathcal{O}_K$ dividing p. But

$$\zeta_m^r - \zeta_m^p = \zeta_m^r(1 - \zeta_m^{p-r}) = \zeta_m^r(1 - \zeta_m^{mk}) = 0$$

so we're done.

Remark 1.5.7. One of the reasons Artin reciprocity is not as easy when K is a general number field is that we don't have such an simple description of the ray class fields. So we need to take a more circuitous route to get there.

1.6. **Principal ideal theorem.** Let's use Artin reciprocity to say something interesting about the Hilbert class field.

Theorem 1.6.1 (Principal ideal theorem)**.** *If K is a number field with Hilbert class field L, then every ideal of K becomes principal in L.*

Remark 1.6.2. Note that this *does not* mean that L necessarily has class number 1; primes which become principal ideals in L may still split into non-principal primes in L.

To prove Theorem 1.6.1 we need to show that the natural map $\mathrm{Cl}(K) \to \mathrm{Cl}(L)$ (given on integral ideals $I \subset \mathcal{O}_K$ by taking $I \mapsto I\mathcal{O}_L$) is the trivial homomorphism; i.e. takes everything to the trivial ideal class in $\mathrm{Cl}(L)$. By Artin reciprocity we know that $\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}(L/K)$. But we care about $\mathrm{Cl}(L)$ as well and we know that it's the Galois group of the Hilbert class field of L, which we call M. We are led to the diagram

$$\begin{tikzcd}
\mathrm{Cl}(K) \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(L/K) \\
\mathrm{Cl}(L) \arrow[r, "\sim"] & \mathrm{Gal}(M/L)
\end{tikzcd}$$

Can we rephrase the problem in terms of Galois groups? We would need a map on the right hand side.

Lemma 1.6.3. *The maximal abelian quotient of* $\mathrm{Gal}(M/K)$ *is* $\mathrm{Gal}(L/K)$*. In particular* $\mathrm{Gal}(M/L)$ *is the commutator subgroup of* $\mathrm{Gal}(M/K)$*.*

Proof. Since M/L and L/K are both unramified, M/K is still unramified. If there were an extension $L \subset N \subset M$ such that N/K were abelian, then $N = L$ since L is the Hilbert class field. This means that L/K is the maximal abelian extension inside of M. □

Note that $M = L$ if and only if $\mathrm{Cl}(L) = 1$, so the principal ideal theorem is non-vacuous only if M is strictly larger than L, and in this case M/K is very much *not* abelian. In any case, we get a diagram

$$\begin{tikzcd}
\mathrm{Cl}(K) \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(L/K) \arrow[r, equal] & \mathrm{Gal}(M/K)^{\mathrm{ab}} \arrow[d, "V"] \\
\mathrm{Cl}(L) \arrow[r, "\sim"] & \mathrm{Gal}(M/L) \arrow[r, equal] & \mathrm{Gal}(M/L)^{\mathrm{ab}}
\end{tikzcd} \tag{2}$$

and we're now in better shape because $\mathrm{Gal}(M/L) \leq \mathrm{Gal}(M/K)$ is a normal subgroup, and because of the following construction (which explains the "V" above; we don't yet know Diagram (2) commutes).

Definition 1.6.4. If H is a subgroup of a finite group G, then pick left coset representatives g_i so that $G = g_1H \sqcup \cdots \sqcup g_nH$. If we put $\phi(g) = g_i$ whenever $g \in g_iH$, then one can define the *transfer function*

$$V(g) := \prod_{i=1}^{n} \phi(gg_i)^{-1}(gg_i) \in H.$$

In other words, if $gg_i = g_jh_i$ then

$$V(g) = \prod_{i=1}^{n} h_i.$$

The transfer map is not necessarily a homomorphism, but:

Exercise 1.6.5. Show that the composition $G \xrightarrow{V} H \twoheadrightarrow H^{\mathrm{ab}}$ is a group homomorphism which does not depend on the choice of the coset representatives g_i. In particular, it descends to a map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

Remark 1.6.6. The transfer map looks strange, but it naturally occurs in group homology. We may or may not get to this later. There is also a way to express quadratic reciprocity using the transfer map.

Lemma 1.6.7. *Diagram (2) commutes.*

Proof. Fix $\mathfrak{p} \subset \mathcal{O}_K$ and consider $[\mathfrak{p}] \in \mathrm{Cl}(K)$.

- The image of $\mathfrak{p}$ in $\mathrm{Cl}(L)$ is $\prod_i \mathfrak{q}_i$, where $\mathfrak{q}_i$ runs over the primes of L lying over $\mathfrak{p}$. Under the Artin map, this product maps to $\prod_i \sigma_{\mathfrak{q}_i} \in \mathrm{Gal}(M/L)$.
- The image of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ is $\sigma_{\mathfrak{q}} = \sigma_{\mathfrak{p}}$ for some $\mathfrak{q}$ lying over $\mathfrak{p}$. Note that if $\mathfrak{r}$ is a prime of M lying over $\mathfrak{q}$ then $\sigma_{\mathfrak{r}} \in \mathrm{Gal}(M/K)$ lifts $\sigma_{\mathfrak{q}}$.

Therefore, it suffices to show that $V(\sigma_{\mathfrak{r}}) = \prod_i \sigma_{\mathfrak{q}_i}$. To compute $V(\sigma_{\mathfrak{r}})$ we make the following choice of cosets. First decompose $G = \mathrm{Gal}(M/K)$ into double cosets for $H = \mathrm{Gal}(M/L)$ and the decomposition group $G_{\mathfrak{r}} \subset G$:

$$G = \bigsqcup_i G_{\mathfrak{r}} \tau_i H.$$

Reorder the τ_i so that $L \cap \tau_i(\mathfrak{r}) = \mathfrak{q}_i$. Decompose further

$$G_{\mathfrak{r}} \tau_i H = \bigsqcup_j \sigma_{\mathfrak{r}}^j \tau_i H$$

and let

$$g_{ij} := \sigma_{\mathfrak{r}}^j \tau_i.$$

Then the g_{ij} give a complete set of coset representatives, and if we can show that

$$\sigma_{\mathfrak{q}_i} = \prod_j \phi(\sigma_{\mathfrak{r}} g_{ij})^{-1}(\sigma_{\mathfrak{r}} g_{ij}) \tag{3}$$

then we're done, because then

$$\prod_i \sigma_{\mathfrak{q}_i} = \prod_{i,j} \phi(\sigma_{\mathfrak{r}} g_{ij})^{-1}(\sigma_{\mathfrak{r}} g_{ij})$$

which is what we wanted. □

Exercise 1.6.8. Prove Equation 3 in the above theorem. (hint: the cosets were chosen so that most of the values in the product defining the transfer are 1. to find the nontrivial values, you need to figure out how big j is allowed to be).

The final step:

Lemma 1.6.9. *If G is a finite group and H is its commutator subgroup, then the transfer map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is trivial.*

Proof. See [Neu99, Theorem VI.7.6] for a proof involving augmentation ideals. □

This concludes the proof of Theorem 1.6.1.

1.7. Dirichlet density.

The final thing we will talk about before diving into group cohomology will be another application of Artin reciprocity, but this time a bit more analytic in nature.

Definition 1.7.1. If K is a number field, the *Dedekind zeta function* $\zeta_K(s)$ is a function $\{\mathrm{Re}(s) > 1\} \subset \mathbb{C} \to \mathbb{C}$ given by

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}.$$

Here $\mathfrak{p}$ ranges over all primes in $\mathcal{O}_K$ and $\mathfrak{a}$ ranges over all non-zero ideals in $\mathcal{O}_K$.

For instance if $K = \mathbb{Q}$, then this is the familiar Riemann zeta function. The fundamental properties of the Riemann zeta function hold for the more general Dedekind zeta function:

Theorem 1.7.2. *$\zeta_K(s)$ meromorphically continues to the entire complex plane with a pole at $s = 1$. $\zeta_K(s)$ satisfies a functional equation relating the values at s and $1-s$ in terms of discriminants and Gamma factors.*

Remark 1.7.3. The *residue* at $s = 1$ is computed by the *analytic class number formula.*

One can also define variants of this, which are useful in proving generalizations of Dirichlet's theorem on arithmetic progressions. When proving Dirichlet's theorem, one considers L-functions of Dirichlet characters. Since a Dirichlet character of conductor N are functions on $(\mathbb{Z}/N\mathbb{Z})^\times = \mathrm{Cl}^{n\cdot\infty}(\mathbb{Q})$, we look at ray class group characters in general.

Definition 1.7.4. Fix $\mathfrak{m}$ a modulus of a number field K and $\chi_\mathfrak{m} : \mathrm{Cl}^\mathfrak{m}(K) \to \mathbb{C}^\times$. Extend $\chi_\mathfrak{m}$ to all ideals of K by taking $\chi_\mathfrak{m}(\mathfrak{p}) = 0$ for $\mathfrak{p}$ dividing $\mathfrak{m}$. Then

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

Theorem 1.7.5. *$L(\chi_\mathfrak{m}, s)$ absolutely converges for $\mathrm{Re}(s) > 1$. If $\chi_\mathfrak{m} \neq 1$ then $L(\chi_\mathfrak{m}, s)$ extends to a holomorphic function on $\mathbb{C}$.*

Remark 1.7.6. On the other hand if $\chi_\mathfrak{m}$ is trivial then $L(\chi_\mathfrak{m}, s)$ is just $\zeta_K(s)$ with the factors removed for $\mathfrak{p} \mid \mathfrak{m}$, and thus still has a pole at $s = 1$.

Here's an important theorem about these L-functions.

Theorem 1.7.7. *If $\chi_\mathfrak{m} \neq 1$ then $L(\chi_\mathfrak{m}, 1) \neq 0$.*

Combined with the fact that $L(\chi_\mathfrak{m}, s)$ is holomorphic, this means that $\log L(\chi_\mathfrak{m}, s)$ is holomorphic at $s = 1$. We can use this to say something about density.

Definition 1.7.8. A set of primes S in K has *Dirichlet density* $d \in [0, 1]$ if

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} = d.$$

Exercise 1.7.9. Show that if S is the set of all primes in K then its Dirichlet density is 1. (hint: apply Möbius inversion to $\log \zeta(s)$).

It turns out that Theorem 1.7.7 implies that the Dirichlet density of primes which land in a specified ray class in $\mathrm{Cl}^\mathfrak{m}(K)$ is $1/\#\,\mathrm{Cl}^\mathfrak{m}(K)$, which generalizes Dirichlet's theorem on arithmetic progressions (saying that there are infinitely many primes in arithmetic progressions of the form $\{m + kN\}_k$ for $\gcd(m, N) = 1$).

We will give a generalization of this to number fields.

1.8. **Chebotarev density.** Now we will use Artin reciprocity to prove a general density statement, which does *not* require the extension to be abelian.

Theorem 1.8.1 (Chebotarev)**.** *Fix L/K a Galois extension of number fields. Fix a conjugacy class $C \subset G$. Then the Dirichlet density of the set of (unramified) primes $\mathfrak{p}$ of K whose corresponding Frobenius conjugacy class lands in C is $\#C/\#G$.*

Proof. If L/K is abelian, in which case $C = \{\sigma\}$, then we're done; to see this note that $L \subset K(\mathfrak{m})$ (the ray class group of $\mathfrak{m}$) where $\mathfrak{m}$ denotes the primes of K which ramify in L, so $G = \mathrm{Cl}^{\mathfrak{m}}(K)/H$ for some normal subgroup H. Now if $\mathfrak{p}$ is a prime of K, then $\sigma_{\mathfrak{p}} = \sigma$ if and only if $\mathfrak{p}$ maps to H. But the Dirichlet density of the set of primes mapping to H is $\#H/\#\,\mathrm{Cl}^{\mathfrak{m}}(K)$, so we're done.

For the general case, one takes the cyclic subgroup of G generated by an element of C, which is abelian and hence we can reduce the above argument using a group-theoretic counting argument which omit. □

2. Cohomology

One of the main tools used to express ideas and theorems in class field theory is the theory of *group cohomology.* Let's have a quick crash course in the theory.

2.1. Basic definitions.

Fix G a group. For now, G is regarded as a group with no topology, and in applications will usually be finite. Later we will consider infinite Galois groups with the profinite topology, but not for now.

Definition 2.1.1. If A is a ring, let $\mathsf{Mod}_{A,G}$ denote the category of *A-modules with a left G-action*, which we also sometimes just call *G-modules* especially if A is clear from context. In other words:

- the objects are A-modules M with an A-linear action of G; i.e. for each $g \in G$ the map $M \xrightarrow{m \mapsto g\cdot m} M$ is A-linear
- morphisms in $\mathsf{Mod}_{A,G}$ are A-linear maps which are also G-equivariant, i.e. $\phi(g \cdot m) = g \cdot \phi(m)$.

Remark 2.1.2.

- $\mathsf{Mod}_{A,G}$ is equivalent to the category $\mathsf{LMod}_{A[G]}$ of left $A[G]$-modules and is abelian.
- If $A = \mathbb{Z}$ these are just abelian groups with G-action.
- The typical example will be $G = \mathrm{Gal}(L/K)$ and $A = K$ and $M = L$.

Definition 2.1.3. If M is a G-module then its *G-invariants* are given by the A-submodule

$$M^G := \{m \in M : g \cdot m = m \text{ for all } g \in G\}$$

Any map $M \to N$ induces a map $M^G \to N^G$, and so taking G-invariants defines an endofunctor $\mathsf{Mod}_{A,G} \to \mathsf{Mod}_{A,G}$. Note that by Yoneda one also has

$$M^G \cong \mathrm{Hom}_{A[G]}(A, M).$$

Exercise 2.1.4. Show that $(\cdot)^G$ is *left-exact.* In other words, show that for any short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ the sequence

$$0 \to M_1^G \to M_2^G \to M_3^G$$

is exact.

Remark 2.1.5. On the other hand, the functor $(\cdot)^G$ is not right exact. To see this, consider $G = \mathbb{Z}/2\mathbb{Z}$ and the sequence $0 \to \mathbb{Z} \xrightarrow{x \mapsto 2x} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$, and let G act on $\mathbb{Z}$ by taking $x \mapsto -x$ and trivially on $\mathbb{Z}/2\mathbb{Z}$.

However, the above remark does mean there is no hope.

Proposition 2.1.6. *If G is a finite group and $|G|$ is invertible in A, then $(\cdot)^G$ is an exact functor on* $\mathsf{Mod}_{A,G}$.

Proof. We just need to check that if $\phi : M \to N$ is surjective then $M^G \to N^G$ is surjective. But if $n \in N^G$ then pick some $m \in M$ with $\phi(m) = n$ and note that $(1/|G|)\sum_{g\in G} g \cdot m \in M^G$ and

$$\phi\left(\frac{1}{|G|}\sum_{g\in G} g\cdot m\right) = \frac{1}{|G|}\sum_{g\in G} g\cdot\phi(m) = \frac{1}{|G|}\sum_{g\in G} g\cdot n = \frac{1}{|G|}\sum_{g\in G} n = n.$$

□

2.2. **Derived functors.** Let's use this as an opportunity to sidestep into the theory of derived functors of functors which are not exact. Before showing how we do this, what we will ultimately see is that if G is a group and $M \in \mathsf{Mod}_{A,G}$, then there are "cohomology groups" $H^i(G,M)$ for $i \geq 0$ such that $H^0(G,M) = M^G$ and such that for every short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ there is a long exact sequence

$$0 \to H^0(G,M_1) \to H^0(G,M_2) \to H^0(G,M_3) \to H^1(G,M_1) \to H^1(G,M_2) \to H^1(G,M_3) \to H^2(G,M_1) \to \cdots$$

This long exact sequence is extremely useful because in a lot of situations M_1 and M_3 are simpler than M_2, and thus their cohomology is easier to compute. Then use the exact sequence to conclude stuff about M_2.

There are two constructions. One is kind of complicated, but let's do it. The other is more explicit, we'll do it after.

Definition 2.2.1. An object X in an abelian category C is *injective* if the functor $\mathrm{Hom}_{\mathsf{C}}(-,X)$ is exact. In other words, X is injective if any map $A \to X$ extends along any monomorphism, i.e. if $A \hookrightarrow B$ is a monomorphism there's an extension $B \to X$ of $A \to X$.

Exercise 2.2.2. Show that in Ab a group is injective if and only if it is divisible (i.e. every element of the group is divisible by every positive integer). Hint: to show that a divisible group M is injective, suppose $A \subset B$ and $A \to M$ is a map and then use Zorn's lemma on the set of extensions $B' \to M$ with $A \subset B' \subset B$, and try to show that the maximal element is $B' = B$. (the converse is tricky; if you're getting stuck, just skip it for now)

By the above exercise $\mathbb{Q}/\mathbb{Z}$ is a divisible abelian group.

Corollary 2.2.3. *If R is a ring (possibly noncommutative, but always with a multiplicative unit), then LMod_R has "enough injectives", i.e. every object M embeds into an injective object.*

Proof. First regard M as a $\mathbb{Z}$-module, i.e. an abelian group. For each $m \in M$ there's a nonzero map $\mathbb{Z}\cdot m \to \mathbb{Q}/\mathbb{Z}$. To see this, note that $\mathbb{Z}\cdot m$ is either a finite cyclic group or a free group on one generator, both of which map nontrivially to $\mathbb{Q}/\mathbb{Z}$. Since $\mathbb{Q}/\mathbb{Z}$ is injective this extends to a map $M \to \mathbb{Q}/\mathbb{Z}$ of abelian groups. This gives an embedding $M \hookrightarrow I := \prod_{m\in M}\mathbb{Q}/\mathbb{Z}$, so

$$M \cong \mathrm{Hom}_R(R,M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R,M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R,I).$$

Since R is an (R,R)-bimodule, $\mathrm{Hom}_{\mathbb{Z}}(R,I)$ naturally has the structure of a left R-module. Therefore

$$\mathrm{Hom}_R(-,\mathrm{Hom}_{\mathbb{Z}}(R,I)) \cong \mathrm{Hom}_{\mathbb{Z}}(R\otimes_R -, I) = \mathrm{Hom}_{\mathbb{Z}}(-,I)$$

but I is injective (you just need to check that products of injective objects are injective), so the functor is exact hence $\mathrm{Hom}_{\mathbb{Z}}(R,I)$ is an injective R-module. □

Definition 2.2.4. If $M \in \mathsf{Mod}_R$ an *injective resolution* is an exact sequence

$$0 \to M \to I_0 \to I_1 \to \cdots$$

where each I_1 is injective.

Since $\mathsf{Mod}_{A,G}$ has enough injectives, we can always find an injective resolution. First take $M \hookrightarrow I_0$. Then take $I_0/M \hookrightarrow I_1$. Then take $I_1/I_0 \hookrightarrow I_2$, etc.

Definition 2.2.5. If we take an injective resolution $M \to I_\bullet$, then the sequence

$$0 \to I_0^G \xrightarrow{d_0} I_1^G \xrightarrow{d_1} I_2^G \xrightarrow{d_2} \cdots$$

is not necessarily exact anymore, and we define the *ith group cohomology of* M:

$$H^i(G, M) = \ker(d_i)/\operatorname{im}(d_{i-1}).$$

A priori it's not clear that this is independent of the choice of $M \to I_\bullet$.

Exercise 2.2.6. Check that $H^0(G, M)$, as defined above, is isomorphic to M^G.

Lemma 2.2.7. *If $f : M \to N$ is a map of G-modules and $M \to I_\bullet$ and $N \to J_\bullet$ are two injective resolutions, then there exists a map of complexes*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "f"] & I_0 \arrow[r] \arrow[d, "f_0"] & I_1 \arrow[r] \arrow[d, "f_1"] & \cdots \\
0 \arrow[r] & N \arrow[r] & J_0 \arrow[r] & J_1 \arrow[r] & \cdots
\end{tikzcd}$$

Proof. To construct f_0 apply injectivity of J_0 to the map $M \xrightarrow{f} N \to J_0$. To construct f_1 apply injectivity of J_1 to the map $I_0/M \xrightarrow{f_0} J_0/N \to J_1$. Repeat. □

So by Lemma 2.2.7 we naturally get maps $H^i(G, M) \to H^i(G, N)$.

Proposition 2.2.8. *The map $H^i(G, M) \to H^i(G, N)$ does not depend on $I_\bullet$ or $J_\bullet$.*

Proof. This a standard exercise in homological algebra and diagram chasing. It's worth doing once. □

Remark 2.2.9. If $M = N$ and $f = \mathrm{id}$ then this shows that $H^i(G, M)$ is independent of choice of injective resolution.

The existence of the long exact sequence follows from what we've discussed so far plus the snake lemma, but I'm not going to try to prove this in class because it's just very tedious.

Exercise 2.2.10. If M is injective, show that $H^i(G, M) = 0$ for $i > 0$. Hint: what is an injective resolution in this case?

Definition 2.2.11. An object is called *acyclic* if $H^i(G, M) = 0$ for all $i > 0$.

So injectives are acyclic. In fact it turns out that the cohomology of an *acyclic resolution* is enough to compute cohomology: in other words, if $0 \to M \to M_0 \to M_1 \to \cdots$ is exact and each M_i is acyclic then the complex

$$0 \to M_0^G \to M_1^G \to M_2^G \to \cdots$$

computes $H^i(G, M)$.

2.3. **Induction.** In the preceding discussion, we gave a construction of group cohomology by somewhat randomly constructing a complex and taking its cohomology, then showing that it's independent of the choice after the fact. But there are some canonical choices of *acyclic* complexes that give you complexes which look like they have a bit more conceptual meaning. We'll discuss how to construct one such complex.

Before doing this, we need to talk about *induction*. The idea is that if G is the trivial group then $H^i(G, M) = 0$ for any G-module M, because $I_\bullet^G = I_\bullet$. Then to construct an acyclic complex, the idea is to induce from the trivial group to some G.

Actually, we need to do something called "co-induction", which is like induction except dual somehow.

Definition 2.3.1. If $H \leq G$ is a subgroup and $N \in \mathsf{Mod}_{A,H}$ then we view $A[G]$ as a left H-module by taking the A-linear extension of $h \cdot [g] = [gh^{-1}]$. Then we define the *coinduction*

$$\operatorname{coInd}_H^G N = \operatorname{Hom}_{\mathsf{Mod}_{A,H}}(A[G], N)$$

which acquires a G-action as the dual of the right G-action on $A[G]$ given by the A-linear extension of $[g] \cdot g_0 = [g_0^{-1} g]$. One can also write

$$\operatorname{coInd}_H^G N = \{f : G \to N : f(gh^{-1}) = h \cdot f(g)\}$$

with the left G-action $(g_0 \cdot f)(g) = f(g_0^{-1} g)$.

Remark 2.3.2. The *induction* from H to G is defined as $M \mapsto M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. This is a duality in the sense that tensor and hom are sort of dual to each other.

Proposition 2.3.3 (Frobenius Reciprocity). *There are canonical isomorphisms*

$$\operatorname{Hom}_{\mathsf{Mod}_{A,G}}(M, \operatorname{coInd}_H^G N) = \operatorname{Hom}_{\mathsf{Mod}_{A,H}}(M, N)$$

and

$$\operatorname{Hom}_{\mathsf{Mod}_{A,G}}(\operatorname{Ind}_H^G N, M) = \operatorname{Hom}_{\mathsf{Mod}_{A,H}}(N, M)$$

where we view M as an H-module on the right.

Proof. Use the tensor-hom adjunction. For induction, we have

$$\operatorname{Hom}_{A[G]}(N \otimes_{A[H]} A[G], M) = \operatorname{Hom}_{A[H]}(N, \operatorname{Hom}_{A[G]}(A[G], M)) = \operatorname{Hom}_{A[H]}(N, M).$$

and for coinduction we have

$$\operatorname{Hom}_{A[G]}(M, \operatorname{Hom}_{A[H]}(A[G], N)) = \operatorname{Hom}_{A[H]}(M \otimes_{A[G]} A[G], N) = \operatorname{Hom}_{A[H]}(M, N).$$

□

In the language of adjoint functors, $\operatorname{Ind}_H^G \dashv \operatorname{Res}_H^G \dashv \operatorname{coInd}_H^G$.

Remark 2.3.4. If $[G : H] < \infty$ then one can actually show that $\operatorname{coInd}_H^G \cong \operatorname{Ind}_H^G$. This is why in finite group representation textbooks they just use "Ind" for both.

Lemma 2.3.5 (Shapiro's lemma). *If $H \leq G$ and N is an H-module, then there is a canonical isomorphism*

$$H^i(G, \operatorname{coInd}_H^G N) \xrightarrow{\sim} H^i(H, N).$$

So N is acyclic if and only if $\operatorname{Ind}_H^G N$ is acyclic.

Proof. For $i = 0$ note that

$$(\operatorname{coInd}_H^G N)^G = \operatorname{Hom}_{A[G]}(A, \operatorname{coInd}_H^G N) = \operatorname{Hom}_{A[H]}(A, N) = N^H.$$

For $i > 0$, we take an injective resolution $0 \to N \to I_\bullet$. Then $0 \to \operatorname{coInd}_H^G N \to \operatorname{coInd}_H^G I_\bullet$ is in fact still an injective resolution. To see that it is exact, note that coInd_H^G is an exact functor because $A[G]$ is a free $A[H]$-module (e.g. spanned by coset representatives). To see that $\operatorname{coInd}_H^G I_\bullet$ consists of injectives, just note that

$$\operatorname{Hom}_{A[G]}(-, \operatorname{coInd}_H^G I_n) = \operatorname{Hom}_{A[H]}(-, I_n)$$

is exact since I_n is injective. So then we're done because $(\operatorname{coInd}_H^G I_n)^G = I_n^H$. □

Definition 2.3.6. If $M \in \mathsf{Mod}_{A,G}$ is such that $M \cong \operatorname{coInd}_{\{1\}}^G N$ for some A-module N, then we say that M is *coinduced.*

Corollary 2.3.7. *Coinduced modules are acyclic.*

Exercise 2.3.8. If L/K is finite Galois, show that $L \in \mathsf{Mod}_{K,G}$ is coinduced. Conclude that $H^i(\operatorname{Gal}(L/K), L) = 0$ for $i > 0$.

Exercise 2.3.9. Show that $H^i(G, M \oplus N) = H^i(G, M) \oplus H^i(G, N)$. Conclude that direct summands of acyclic modules are acyclic.

2.4. **Explicit complex.** There are a few different ways to compute $H^i(G, M)$ explicitly. For the first way, note that

$$(-)^G = \mathrm{Hom}_{A[G]}(A, -)$$

so after taking right derived functors, $H^i(G, -) \cong \mathrm{Ext}^i_{A[G]}(A, -)$. Ext groups can be computed using something called the *bar complex*, which is a *projective* resolution of A as an $A[G]$-module.

The above approach is probably the right way conceptually to develop the theory. But we'll take a different and more elementary approach, which is a bit faster.

Definition 2.4.1. If G is a group and M is a G-module define a G-module N_i for $i \geq 0$ to be the set of functions $\phi : G^{i+1} \to M$, with the G-action

$$(g \cdot \phi)(g_0, \ldots, g_i) = g\phi(g^{-1}g_0, \ldots, g^{-1}g_i)$$

Equivalently $N_i = \mathrm{Hom}_A(A[G^{i+1}], M)$ which acquires a left G-action by viewing $A[G^{i+1}]$ as a right G-module (by acting on the left via the inverse).

Lemma 2.4.2. *Each N_i is coinduced.*

Proof. I will leave the details as an exercise, but note that

$$\phi(g_0, \ldots, g_i) = g_0(g_0^{-1} \cdot \phi)(e, g_0g_1, \ldots, g_0g_i),$$

so the lemma follows essentially because there's a unique way to translate a tuple $(g_0, \ldots, g_i)$ to a tuple where the first item is the identity. □

We can define a differential $d : N_i \to N_{i+1}$ by taking

$$(d\phi)(g_0, \ldots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j \phi(g_0, \ldots, \widehat{g_j}, \ldots, g_{i+1}).$$

Exercise 2.4.3. Check that d is a map of G-modules.

Proposition 2.4.4. *The complex $0 \to M \to N_0 \to N_1 \to \cdots$ is exact.*

Proof. Omitted. This is a tedious exercise, worth doing once. □

So since each N_i is coinduced, the exact sequence $0 \to M \to N_0 \to N_1 \to \cdots$ is an acyclic resolution of M and thus

$$0 \to N_0^G \xrightarrow{d_0} N_1^G \xrightarrow{d_1} N_2^G \to \cdots$$

computes $H^i(G, M)$, i.e. $H^i(G, M) = \ker d_i / \operatorname{im} d_{i+1}$.

Remark 2.4.5. In analogy with the case of singular cohomology of topological spaces,

- elements of N_i^G are called *i-cochains*,
- elements of $\ker d_i$ are called *i-cocycles*, and
- elements of $\operatorname{im} d_{i-1}$ are called *i-coboundaries*

and thus $H^i(G, M)$ is i-cocycles mod i-coboundaries. In fact there exists a topological space BG called the "classifying space of G" admitting a functorial isomorphism

$$H^i_{\mathrm{sing}}(BG, \widetilde{M}) \cong H^i(G, M)$$

where $\widetilde{M}$ is a certain local system on BG constructed using M.

2.5. **H^1.** Let's unpack this for $i = 1$. A 1-cochain $\phi : G^2 \to M$ is determined by the function $\rho(g) = \phi(e, g)$ and is a cocycle iff $d\phi(g, h, k) = 0$ for all $g, h, k \in G$. But we can assume $g = e$ by G-invariance and thus for any $g, h \in G$ this is equivalent to

$$\begin{aligned} 0 &= (d\phi)(e, g, gh) \\ &= \phi(g, gh) - \phi(e, gh) + \phi(e, g) \\ &= g \cdot (g^{-1} \cdot \phi)(e, h) - \phi(e, gh) + \phi(e, g) \\ &= g \cdot \rho(h) - \rho(gh) + \rho(g). \end{aligned}$$

So $\ker(N_1^G \to N_2^G)$ consists of so-called *crossed homomorphisms*

$$\{\rho : G \to M : \rho(gh) = g \cdot \rho(h) + \rho(g)\}.$$

A map ρ is the image of a 0-cocycle $\psi : G \to M$ if and only if

$$\rho(g) = \phi(e, g) = \psi(g) - \psi(e) = g \cdot \psi(e) - \psi(e),$$

i.e. if ρ is a *principal crossed homomorphism*, i.e. one of the form $g \mapsto g \cdot m - m$ for some $m \in M$.

Remark 2.5.1. If G acts trivially on M then $H^1(G, M) = \mathrm{Hom}_{\mathsf{Grp}}(G, M) = \mathrm{Hom}_{\mathsf{Ab}}(G^{\mathrm{ab}}, M)$.

Now that we have an explicit description of $H^1(G, M)$ let's show that it vanishes in a special case which is relevant to Kummer theory.

Theorem 2.5.2 (Hilbert Theorem 90)**.** *If L/K is a finite Galois extension with Galois group G, then $H^1(G, L^\times) = 0$.*

Proof. First note that the automorphisms in G are linearly independent. So if $\rho : G \to L^\times$ is a crossed homomorphism there must exist $x \in L^\times$ such that

$$t = \sum_{\sigma \in G} \rho(\sigma)\sigma(x) \neq 0.$$

But then if $\tau \in G$

$$\tau(t) = \sum_{\sigma \in G} (\tau \cdot \rho(\sigma))(\tau\sigma(x)) = \sum_{\sigma \in G} \rho(\tau\sigma)\rho(\tau)^{-1}(\tau\sigma(x)) = \rho(\tau)^{-1}t$$

So $\rho(\tau) = (\tau \cdot t)/t$, as desired. □

Once we discuss infinite Galois theory, we will use this to prove Kummer theory.

We saw that a map $M \to M'$ of G-modules induces a map $H^i(G, M) \to H^i(G, M')$ of A-modules, i.e. cohomology is covariantly functorial in the second argument. But we can slightly extend this functoriality. Pick a map $\alpha : G' \to G$ of groups and fix $M \in \mathsf{Mod}_{A,G}$ and $M' \in \mathsf{Mod}_{A,G'}$ and suppose there is a map $\varphi : M \to M'$ of A-modules. We want to say that φ is equivariant, but since the groups are different we need to use α.

Definition 2.5.3. We say that φ is *equivariant* if $\varphi(\alpha(g') \cdot m) = g' \cdot \varphi(m)$ for all $g' \in G'$ and $m \in M$.

Example 2.5.4. For instance if $H \leq G$ and $G' = H$, then the inclusion is equivariant whenever $M = M'$.

Lemma 2.5.5. *Given α, M, M', φ as above, there is a canonical induced map*

$$H^i(G, M) \to H^i(G', M').$$

Proof. For $i = 0$, this is $M^G \to (M')^{G'}$. But this is just the map $m \mapsto \varphi(m)$, since

$$g' \cdot \varphi(m) = \varphi(\alpha(g') \cdot m) = \varphi(m).$$

For $i > 0$, one takes two injective resolutions and reasons similarly; the proof is omitted. □

Exercise 2.5.6. Show that if $\alpha : G \to G$ is conjugation by $h \in G$ then $H^i(G, M) \to H^i(G, M)$ is the identity.

If $G' = H \leq G$ and the map $H \to G$ is the natural inclusion, then the map

$$\mathrm{Res} : H^i(G, M) \to H^i(H, M)$$

is called the *restriction* map.

Exercise 2.5.7. Note that since $\mathrm{Hom}_H(M, M) = \mathrm{Hom}_G(M, \mathrm{coInd}_H^G M)$, there is a map $M \to \mathrm{Ind}_H^G M$ corresponding to the identity map $M \to M$. Show that this induces a map

$$H^i(G, M) \to H^i(G, \mathrm{coInd}_H^G M) \xrightarrow{\sim} H^i(H, M)$$

which is the same as Res (the second isomorphism is by Lemma 2.3.5).

Finally, I want to mention the inflation-restriction sequence.

Lemma 2.5.8. *If $H \leq G$ is normal, then there is an exact sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\textit{inflation}} H^1(G, A) \xrightarrow{\textit{restriction}} H^1(H, A)^{G/H} \to H^2(G/H, A^H) \to H^2(G, A)$$

Proof. One can show this directly, or alternatively you can use the fact that $(\cdot)^G = (\cdot)^{G/H} \circ (\cdot)^H$ where $(\cdot)^H : \mathsf{Mod}_{A,G} \to \mathsf{Mod}_{A,G/H}$ and $(\cdot)^{G/H} : \mathsf{Mod}_{A,G/H} \to \mathsf{Mod}_A$, and then use the five-term exact sequence from the Grothendieck spectral sequence of the composition. If you're not comfortable with spectral sequences don't linger on this, just take it on faith for now. □

2.6. **Group homology.** It probably won't surprise you that (just like for topological spaces) there is a dual theory to group cohomology, called group homology. We just basically dualize everything.

Definition 2.6.1. If $M \in \mathsf{Mod}_{A,G}$, then let M_G denote the largest quotient of M on which G acts trivially. In other words,

$$M_G = M / \langle g \cdot m - m : g \in G \text{ and } m \in M \rangle .$$

Exercise 2.6.2. Show that if $A[G] \to A$ is the map given by $\sum_g a_g[g] \mapsto \sum_g a_g$ with kernel I_G then

$$M_G \cong M \otimes_{A[G]} A \cong M/I_G M.$$

In fact, the tensor-hom adjunction implies that there are adjunctions

$$(\cdot)_G \dashv (\cdot)_{\mathrm{triv}} \dashv (\cdot)^G$$

where $(\cdot)_{\mathrm{triv}} : \mathsf{Mod}_A \to \mathsf{Mod}_{A,G}$ takes N to N with the trivial action of G. This shows that M_G is *right exact* but not left-exact. So just as we defined cohomology groups to fix failure of exactness of M^G by taking injective resolutions, one can fix failure of exactness of M_G by taking *projective resolutions.*

Definition 2.6.3.

- An object P in an abelian category C is *projective* if $\mathrm{Hom}_{\mathsf{C}}(P, -)$ is exact.
- A projective resolution of $M \in \mathsf{Mod}_{A,G}$ is an exact sequence

  $$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

  with P_i all projective.
- The *group homology* $H_i(G, M)$ is defined by taking the kernels-mod-images of

  $$\cdots \to (P_2)_G \to (P_1)_G \to (P_0)_G \to 0.$$

Again the definition of homology is well-defined and doesn't depend on choices, and enjoys the same sort of functoriality. If $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact, there is a long exact sequence

$$\cdots \to H_1(G, M_3) \to H_0(G, M_1) \to H_0(G, M_2) \to H_0(G, M_3) \to 0.$$

Remark 2.6.4. Even though these notions look completely dual to one another, it's much easier to find projective objects than injectives: indeed any free $A[G]$-module is projective. This apparent "failure" of duality is really a reflection of the fact that $\mathsf{Mod}_{A[G]}$ is very much *not* a self-dual category.

Lemma 2.6.5 (Shapiro's lemma for homology)**.** *If $H \leq G$ and $N \in \mathsf{Mod}_{A,H}$ then there are canonical isomorphisms*

$$H_i(G, \operatorname{Ind}_H^G N) \cong H_i(H, N).$$

Proof. For $i = 0$ this is

$$\operatorname{Ind}_H^G N \otimes_{A[G]} A = N \otimes_{A[H]} A[G] \otimes_{A[G]} A = N \otimes_{A[H]} A$$

and the proof for $i > 0$ is same as in Lemma 2.3.5. □

This means that an *induced* module is acyclic for homology.

Remark 2.6.6. Note that by using the sequence

$$0 \to I_G \to A[G] \to A \to 0$$

one can do some explicit computations: the long exact sequence gives

$$0 = H_1(G, A[G]) \to H_1(G, A) \to H_0(G, I_G) \to H_0(G, A[G])$$

i.e. $0 \to H_1(G, A) \to I_G/I_G^2 \to A[G]/I_G$. But the last map is zero so

$$H_1(G, A) \cong I_G/I_G^2$$

2.7. **Tate cohomology.** Now we restrict to the case where G is a finite group. Note $\operatorname{Ind} \cong \operatorname{coInd}$ in this setting, and Tate cohomology which gives a way of gluing together homology and cohomology. You might expect that there's a way to do this, because taking cohomology and homology involves taking injective and projective resolutions, which look like

$$\begin{tikzcd} & & & M \arrow[r] & I_0 \arrow[r] & I_1 \arrow[r] & I_2 \arrow[r] & \cdots \\ \cdots \arrow[r] & P_2 \arrow[r] & P_1 \arrow[r] & P_0 \arrow[r] & M & & & \end{tikzcd}$$

So if you want to connect them, you need to do something near degree $i = 0$. This turns out to be *very* useful.

The key observation is that there is a map connecting H_0 and H^0:

Definition 2.7.1. If $G \in \mathsf{Mod}_{A,G}$ the *norm* map $N_G : M \to M$ is

$$N_G(m) = \sum_{g \in G} g \cdot m.$$

Exercise 2.7.2. Check that $N_G(m) \in M^G$ and $N_G(I_G M) = 0$, so that N_G descends to a map

$$N_G^\star : H_0(G, M) \to H^0(G, M).$$

Definition 2.7.3. *Tate cohomology* is

$$H_T^i(G, M) = \begin{cases} H^i(G, M) & i > 0 \\ \operatorname{coker} N_G^\star = H^0(G, M)/N_G(M) & i = 0 \\ \ker N_G^\star & i = -1 \\ H_{-(i+1)}(G, M) & i < -1. \end{cases}$$

Proposition 2.7.4. *With the definition as above, we get long exact sequences*

$$\cdots \to H_T^{i-1}(G, M_3) \to H_T^i(G, M_1) \to H_T^i(G, M_2) \to H_T^i(G, M_3) \to H_T^{i+1}(G, M_1) \to \cdots .$$

Proof. For $i > 0$ and $i < -1$ there's nothing to do. For $i = -1, 0$, chase the commutative diagram

$$\begin{tikzcd}
H_1(G, M_3) \arrow[r] \arrow[d] & H_0(G, M_1) \arrow[r] \arrow[d, "N_G"] & H_0(G, M_2) \arrow[r] \arrow[d, "N_G"] & H_0(G, M_3) \arrow[r] \arrow[d, "N_G"] & 0 \arrow[d] \\
0 \arrow[r] & H^0(G, M_1) \arrow[r] & H^0(G, M_2) \arrow[r] & H^0(G, M_3) \arrow[r] & H^1(G, M_1)
\end{tikzcd}$$

□

Exercise 2.7.5. Show that if M is induced (equivalently, coinduced) then $H_T^i(G, M) = 0$ for all i (hint: think about $N_G^\star$).

2.8. **Tate cohomology of cyclic groups.** In general Tate cohomology, although computable, is not really that intuitive of an object. However:

Theorem 2.8.1. *If G is a finite cyclic group and $M \in \mathsf{Mod}_{A,G}$ then there is a functorial isomorphism*

$$H_T^i(G, M) \xrightarrow{\sim} H_T^{i+2}(G, M)$$

which only depend on the choice of a generator $g \in G$.

Proof. We have an exact sequence

$$0 \to A \xrightarrow{1 \mapsto \sum_{h \in G}[h]} A[G] \xrightarrow{h \mapsto [hg]-[h]} A[G] \xrightarrow{[h] \mapsto 1} A \to 0.$$

Since everything in the sequence is a free A-module, and the kernels and cokernels of the maps are as well, it turns out that tensoring with M makes this sequence remain exact so we get

$$0 \to M \to M \otimes_A A[G] \to M \otimes_A A[G] \to M \to 0.$$

This is a sequence of A-modules, and we regard these as G-modules by considering M with its given G-action, and $M \otimes_A A[G]$ with the tensor product action $g \cdot m \otimes x = (g \cdot m) \otimes (g \cdot x)$. Now we use Exercise 2.8.2 below to show that there is an isomorphism of G-modules $M \otimes_A A[G] \cong M_0 \otimes_A A[G]$ (where M_0 is the same underlying A-module as M, but with trivial G-action). So then $M \otimes_A A[G] \cong \operatorname{Ind}_1^G M_0$, and thus the middle two terms in our new exact sequence therefore have trivial Tate cohomology.

Now, given any sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to D \to 0$ with B, C having trivial Tate cohomology, then the sequences

$$0 \to A \xrightarrow{f} B \to B/\operatorname{im}(f) \to 0$$

and

$$0 \to B/\ker(g) \xrightarrow{g} C \to D \to 0$$

allow us to do a bit of "degree-shifting" (since the middle terms have trivial cohomology) and so we get

$$H_T^{i+2}(G, A) = H_T^{i+1}(G, B/\operatorname{im}(f)) = H_T^{i+1}(G, B/\ker(g)) = H_T^i(G, D).$$

In our situation we have $A = D = M$. □

In the proof above we used the following lemma.

Exercise 2.8.2. If $M \in \mathsf{Mod}_{A,G}$ and $M_0 \in \mathsf{Mod}_{A,G}$ has underlying A-module M with trivial G-action, show that the map

$$M_0 \otimes_A A[G] \xrightarrow{\sim} M \otimes_A A[G]$$

sending $m \otimes [g] \mapsto (g \cdot m) \otimes [g]$ is an isomorphism.

In conclusion, instead of long exact sequences we get an exact hexagon

$$\begin{tikzcd}
 & H^{\mathrm{odd}}(G,M_2) \arrow[r] & H^{\mathrm{odd}}(G,M_3) \arrow[dr] & \\
H^{\mathrm{odd}}(G,M_1) \arrow[ur] & & & H^{\mathrm{even}}(G,M_1) \arrow[dl] \\
 & H^{\mathrm{even}}(G,M_3) \arrow[ul] & H^{\mathrm{even}}(G,M_2) \arrow[l] &
\end{tikzcd}$$

Exercise 2.8.3. Depending on a choice of generator $g \in G$, there is a canonical isomorphism

$$\ker N_G^\star = H_T^{-1}(G,M) \to H_T^1(G,M)$$

onto the space of 1-cocycles. Given an element of $\ker N_G^\star$, write out the cocycle it corresponds to.

Definition 2.8.4. The *Herbrand quotient* of $M \in \mathsf{Mod}_{A,G}$ for G finite cyclic is

$$h(M) = \frac{|H^{\mathrm{even}}(G,M)|}{|H^{\mathrm{odd}}(G,M)|}$$

(provided the groups are finite).

The Herbrand quotient can actually be computable, because you only need to look at $i = 0$ and $i = -1$, both of which are relatively explicit compared with the higher or lower Tate cohomology groups.

One nice feature of the Herbrand quotient is that it is multiplicative in exact sequences. In other words if $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact and the Herbrand quotients exist (in fact, if two of them exist then so does the third!) then $h(M_2) = h(M_1)h(M_3)$. This follows from exactness of the above hexagon.

The Herbrand quotient will be an important invariant, because what will end up happening is that when we prove class field theory we will often try to reduce ourselves to the case where G is cyclic, even if we start with an abelian extension that isn't cyclic.

Lemma 2.8.5. *If M is finite (i.e. its underlying set is finite) then $h(M) = 1$.*

Proof. For this, fix a generator $g \in G$ and note that

$$0 \to M^G \to M \xrightarrow{g \cdot m - m} M \to M_G \to 0$$

and

$$0 \to H_T^{-1}(G,M) \to M_G \xrightarrow{N_G} M^G \to H_T^0(G,M) \to 0$$

are both exact. But by exactness this implies that $|M_G| = |M^G|$ and thus $H_T^{-1}(G,M) = H_T^0(G,M)$. □

So the Herbrand quotient is really only interesting in the case where M is infinite, which will often be the case that we're interested in. For instance, if L/K is a finite cyclic extension then Hilbert 90 tells us that $H_T^1(G,L^\times) = H^1(G,L^\times) = 0$, but $H_T^0(G,L^\times) = K^\times/N(L^\times)$, which as we will later see is finite, so $h(L^\times) = |K^\times/N(L^\times)|$.

2.9. **Infinite Galois theory.** Recall the main theorem of usual Galois theory:

Theorem 2.9.1. *If L/K is a finite Galois extension of fields with Galois group G, then there is an inclusion-reversing bijection*

$$\{\textit{subgroups of } G\} \xrightarrow{\sim} \{\textit{intermediate field extensions of } L/K\}$$
$$H \mapsto L^H$$
$$\mathrm{Gal}(L/M) \leftarrow\!\shortmid L/M/K.$$

By restricting, this also induces a bijection

$$\{\textit{normal subgroups of } G\} \xrightarrow{\sim} \{\textit{intermediate Galois extensions of } L/K\}$$

Definition 2.9.2. An algebraic extension L/K of fields (possibly of infinite degree) is *Galois* if any of the following equivalent conditions are satisfied:

(1) L is normal and separable

(2) $L^{\mathrm{Aut}(L/K)} = K$

(3) L is the composite field of a collection of finite Galois extensions of K.

On the other hand, if L/K is infinite, this doesn't quite work.

Example 2.9.3. Consider the extension $\overline{\mathbb{F}}_p/\mathbb{F}_p$. This contains the Frobenius element $\sigma : x \mapsto x^p$. Note that $(\overline{\mathbb{F}}_p)^{\sigma=1} = \mathbb{F}_p$, so you might expect that $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is generated by σ. But this is *not true*! The point is that

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

where the inverse limit is taken over the positive integers ordered by divisibility, since $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ iff $n \mid m$. This is much bigger than $\mathbb{Z}$, and is in particular not isomorphic to $\mathbb{Z}$. The point is that a sequence $\{s_n\}_n$ satisfying $s_n \equiv s_m \mod n$ whenever $n \mid m$ defines a Galois element by acting on $\mathbb{F}_{p^n}$ as σ^{s_n}.

So $\overline{\mathbb{F}}_p^{\langle\sigma\rangle} = \mathbb{F}_p$, but $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is much bigger than $\langle\sigma\rangle$. This is because $\langle\sigma\rangle$ is not a *closed subgroup* for the profinite topology.

In general if L/K is an infinite algebraic extension, then it is the union of finite extensions, and it's Galois if each of the finite extensions is Galois; equivalently, $L^{\mathrm{Gal}(L/K)} = K$. In fact, it's always true that

$$\mathrm{Gal}(L/K) = \varprojlim_M \mathrm{Gal}(M/K)$$

where M runs over all of the finite Galois extensions of K in L. If we give each of the $\mathrm{Gal}(M/K)$ the discrete topology, then $\mathrm{Gal}(L/K)$ acquires the structure of a topological group by taking the inverse limit topology, which is called the *profinite topology.*

Definition 2.9.4. A topological group is *profinite* if it is the inverse limit of finite discrete groups, or equivalently it's compact Hausdorff and admits a neighborhood basis of the identity consisting of normal subgroups.

Exercise 2.9.5.

(1) Show the equivalence in the above definition.

(2) Show that the topology on $\mathrm{Gal}(L/K)$ can alternatively be defined by declaring that the open subgroups of $\mathrm{Gal}(L/K)$ are exactly the $\mathrm{Gal}(L/M)$ for M/K a finite extension contained in L.

Lemma 2.9.6. *A subgroup $H \leq G$ of a profinite group is open if and only if it is closed and has finite index.*

Proof. If H is closed of finite index, then each of its left cosets is closed, so $\cup_{gH \neq H} gH$ is closed, hence H is open. Conversely if H is open then the set $\{gH\}$ of left coset is an open cover, but G is compact so it has a finite subcover, i.e. there are only finitely many cosets. □

Theorem 2.9.7. *If L/K is any Galois extension of fields with Galois group G, then*

$$\{\textit{closed subgroups of } G\} \xrightarrow{\sim} \{\textit{intermediate field extensions of } L/K\}$$

$$H \mapsto L^H$$

$$\mathrm{Gal}(L/M) \leftarrow\!\shortmid L/M/K.$$

This restricts to bijections

$$\{\textit{closed normal subgroups of } G\} \xrightarrow{\sim} \{\textit{intermediate Galois extensions of } L/K\}$$
$$\{\textit{open subgroups of } G\} \xrightarrow{\sim} \{\textit{intermediate finite extensions of } L/K\}$$
$$\{\textit{open normal subgroups of } G\} \xrightarrow{\sim} \{\textit{intermediate finite Galois extensions of } L/K\}$$

By the exercise above, if H is a closed normal subgroup of G then $\mathrm{Gal}(L^H/K) = G/H$, so L^H/K is a finite extension if and only if H has finite index, i.e. if and only if H is open. So in the above example $\langle\sigma\rangle$ is not closed, but its closure in the profinite topology is $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, which is to say that even though σ is not a generator of $G_{\mathbb{F}_p}$, it is a *topological generator.*

2.10. **Infinite Galois cohomology.** So now we can talk about cohomology of these groups.

Definition 2.10.1. If G is profinite, then the category $\mathsf{Mod}_{A,G}$ is the category of A-modules with a *continuous* left G-action. In other words if M is an A-module then

$$G \times M \to M$$

has to be continuous, where we give M the discrete topology.

Lemma 2.10.2. *The stabilizer of every $m \in M$ is an open subgroup in G. In particular, $M = \bigcup_H M^H$ where H runs over open subgroups.*

Proof. The action map restricts to a continuous map $G \to M$ given by $g \mapsto g \cdot m$. The preimage of m is the stabilizer, and thus it must be open. □

There are two ways of defining the cohomology of G:

- The first way is to prove that the category $\mathsf{Mod}_{A,G}$ is still abelian, has enough injectives, and then use the usual homological algebra machinery. One can then prove that
$$H^i(G, M) = \varinjlim_H H^i(G/H, M^H)$$
via the inflation maps $H^i(G/H, M^H) \to H^i(G, M)$.
- The second way is to use the explicit complex of cochains as we did before, but now use *continuous cochains* instead of regular ones. In other words, there is a resolution
$$0 \to M \to N_0 \to N_1 \to N_2 \to \cdots$$
where $N_i = \mathrm{Fun}_{\mathrm{cts}}(G^{i+1}, M)$.

But in any case, it's not so important that we discuss this in detail. All you need to know and remember is that you can take the group cohomology of profinite groups, and it behaves in basically the same way as for finite groups. In other words, we get long exact sequences as before.

Let's briefly state how to get Kummer theory from this.

Corollary 2.10.3. *If K is a field of characteristic coprime to n containing μ_n (the nth roots of unity), then the $\mathbb{Z}/n\mathbb{Z}$-extensions of K are in bijection with the elements of $K^\times/(K^\times)^n$ of exact order n.*

Proof. Let $G_K = \mathrm{Gal}(\overline{K}/K)$.

$$H^1(G_K, \overline{K}^\times) = \varinjlim_{L/K \text{ finite}} H^1(G_{L/K}, L^\times) = \varinjlim_{L/K \text{ finite}} 0 = 0$$

so in the long exact sequence associated with $0 \to \mu_n(\overline{K}) \to \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times \to 0$ gives

$$0 \to \mu_n(K) \to K^\times \xrightarrow{x \mapsto x^n} K^\times \to H^1(G_K, \mu_n(\overline{K})) \to 0$$

and so

$$K^\times/(K^\times)^n \cong H^1(G_K, \mu_n(\overline{K})) = \mathrm{Hom}_{\mathrm{cts}}(G_K, \mu_n)$$

since G_K acts trivially on $\mu_n(\overline{K}) = \mu_n(K)$. But now any (cts) group homomorphism $G_K \to \mu_n$ has open kernel and the quotient by this kernel gives $\mathrm{Gal}(L/K) \hookrightarrow \mu_n$ for some n. Now one simply needs to check that the elements of exact order n map to the homomorphisms with kernel of index n, which is left as an exercise. □

3. Local class field theory

Today we'll start talking about our first main goal, which is *local class field theory*, or in other words the classification of abelian extensions of F for $F/\mathbb{Q}_p$ finite.

3.1. **Overview.**

Let's review the goal. In this section K will be a fixed p-adic local field.

Theorem 3.1.1 (Local reciprocity)**.** *If K is a local field, then there exists a unique map*

$$\mathrm{Art}_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

inducing an isomorphism $\widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that

(1) for any uniformizer $\varpi \in K$ and any finite unramified L/K, $\mathrm{Art}_K(\varpi_K)$ acts on L as the Frobenius automorphism,

(2) and if L/K is any finite abelian extension then $\mathrm{Art}_K(N_{L/K}L^\times) = 0$ and the induced map $K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$ is an isomorphism.

In fact, we'll basically construct Art_K by constructing the induced maps in part (2) and then gluing them together along an inverse limit.

Remark 3.1.2 (Local and global relationship)**.** The local Artin reciprocity map is compatible with the global Artin reciprocity map. We will discus what this means later, but for now let's consider the case $K = \mathbb{Q}$ and consider the Kronecker–Weber theorem. Global Kronecker–Weber (Theorem 1.2.2) tells us that

$$G_{\mathbb{Q}}^{\mathrm{ab}} \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \widehat{\mathbb{Z}}^\times \cong \mathbb{Z}_p^\times \times \prod_{\ell \neq p} \mathbb{Z}_\ell^\times .$$

We want to relate this to local Kronecker–Weber (Theorem 1.2.3). First note that we can write $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}_1\mathbb{Q}_2$ where $\mathbb{Q}_1 = \bigcup_n \mathbb{Q}(\zeta_{p^n})$ is the maximal abelian ramified extension of $\mathbb{Q}$ and $\mathbb{Q}_2 = \bigcup_n \mathbb{Q}(\zeta_{p^n-1})$ is the maximal abelian unramified extension. These are linearly disjoint, so

$$G_{\mathbb{Q}_p}^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_2/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \times \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \mathbb{Z}_p^\times \times \widehat{\mathbb{Z}}.$$

Note that there is a map $G_{\mathbb{Q}_p}^{\mathrm{ab}} \to G_{\mathbb{Q}}^{\mathrm{ab}}$ and it turns out that Artin reciprocity map in this case is

$$\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times \mathbb{Z} \to \mathbb{Z}_p^\times \times \widehat{\mathbb{Z}} = G_{\mathbb{Q}_p}^{\mathrm{ab}}$$

and there is a commutative diagram

$$\begin{tikzcd}
G_{\mathbb{Q}_p}^{\mathrm{ab}} \arrow[r] \arrow[d] & \mathbb{Z}_p^\times \times \widehat{\mathbb{Z}} \arrow[d, "\mathrm{id}_{\mathbb{Z}_p^\times} \times (1 \mapsto (p)_\ell)"] \\
G_{\mathbb{Q}}^{\mathrm{ab}} \arrow[r] & \mathbb{Z}_p^\times \times \prod_{\ell \neq p} \mathbb{Z}_\ell^\times
\end{tikzcd}$$

As we'll see later, this map satisfies both (1) and (2) in Theorem 3.1.1.

Exercise 3.1.3. In the above diagram there is a map $\mathbb{Z} \xrightarrow{1 \mapsto (p)_\ell} \prod_{\ell \neq p} \mathbb{Z}_\ell^\times$. This is constructed by first defining a map of abelian groups

$$\mathbb{Z} \to \prod_{\ell \neq p} \mathbb{Z}_\ell^\times$$

by taking the generator 1 to the tuple $(\dots, p, p, p, \dots)$, noting that p is a unit in $\mathbb{Z}_\ell$ for all $\ell \neq p$. Show that this then extends uniquely to a continuous map

$$\widehat{\mathbb{Z}} \to \prod_{\ell \neq p} \mathbb{Z}_\ell^\times.$$

We also get a correspondence between open subgroups of $K^\times$ and finite abelian extensions:

Theorem 3.1.4 (Local existence theorem)**.** *If K is a local field and L/K is a finite extension, then $N_{L/K}L^\times$ is an open subgroup of $K^\times$. Conversely if $U \subset K^\times$ is any open subgroup then $U = N_{L/K}L^\times$ for some finite abelian L/K. Furthermore if L/K is finite and M/K denotes the maximal abelian extension of K contained in L, then $N_{L/K}L^\times = N_{M/K}M^\times$.*

This gives the precise sense in which the Artin map classifies abelian extensions of K.

3.2. **Unramified H^2.** Now let's get to the proof. The rough idea of the proof is to find both sides of the Artin reciprocity map in Galois cohomology, then study long exact sequences, so we need to understand cohomology of the units. From now on write $H^i(L/K) := H^i(\mathrm{Gal}(L/K), L^\times)$ for L/K Galois. We know that $H^0(L/K) = K^\times$ and by Hilbert 90 (Theorem 2.5.2) we have already shown that $H^1(L/K) = 0$, so let's study $H^2(L/K)$. Let's start with the unramified case.

Proposition 3.2.1. *If L/K is a finite extension of finite fields, then $N_{L/K} : L^\times \to K^\times$ is surjective.*

Proof. Since $L^\times$ is a finite set, $h(L^\times) = 1$ by Lemma 2.8.5. But $H^1_T(L/K) = H^1(L/K) = 0$, so

$$K^\times / N_{L/K}L^\times = H^0_T(L/K) = 0$$

as well. □

Now we'll upgrade this to cohomology of the units.

Definition 3.2.2. The m-units in $\mathcal{O}_K$ are by definition $\mathcal{O}_K^{(m)} = 1 + \varpi_K^m \mathcal{O}_K$, i.e. the kernel of the map

$$\mathcal{O}_K^\times \to (\mathcal{O}_K/\varpi_K^m)^\times.$$

Note that $\mathcal{O}_K^\times = \varprojlim_n (\mathcal{O}_K/\varpi_K^n)^\times$.

Exercise 3.2.3.

(1) Show that $\mathcal{O}_K^\times/\mathcal{O}_K^{(1)} = k^\times$ and $\mathcal{O}_K^{(m)}/\mathcal{O}_K^{(m+1)} \cong k$ for $m \geq 1$.

(2) If L/K is unramified, show that there are commutative diagrams

$$\begin{tikzcd} \mathcal{O}_L^\times \arrow[r] \arrow[d, "N_{L/K}"] & k_L^\times \arrow[d, "N_{k_L/k_K}"] \\ \mathcal{O}_K^\times \arrow[r] & k_K^\times \end{tikzcd}$$

and

$$\begin{tikzcd} \mathcal{O}_L^{(m)} \arrow[r] \arrow[d, "N_{L/K}"] & k_L \arrow[d, "\mathrm{tr}"] \\ \mathcal{O}_K^{(m)} \arrow[r] & k_K \end{tikzcd}$$

Lemma 3.2.4. *The trace map $k_L \to k_K$ is surjective.*

Proof. Note that if we view k_L as a $\mathrm{Gal}(k_L/k_K)$-module then the trace map is the same as N_G in the context of Tate cohomology. We saw in Exercise 2.3.8 that $H^i(\mathrm{Gal}(k_L/k_K), k_L) = 0$ for all $i > 0$, so by periodicity $H^i_T(\mathrm{Gal}(k_L/k_K), k_L) = 0$ for all i, in particular when $i = 0$. □

Proposition 3.2.5. *If L/K is finite unramified, then $N_{L/K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective.*

Proof. If $u \in \mathcal{O}_K^\times$ then pick $v_0 \in \mathcal{O}_L^\times$ such that $Nv_0 \equiv u \mod \varpi_K$. Now the point is to correct v_0 bit by bit by going down the m-units. For example, we can write $u = N_{L/K}(v_0)c_1$ with $c_1 \in \mathcal{O}_K^{(1)}$. But then we can find $v_1 \in \mathcal{O}_L^{(1)}$ such that $N_{L/K}v_1 \cong c_1 \mod \mathcal{O}_K^{(2)}$. Then we can write $u = N_{L/K}(v_0v_1)c_2$ with $c_2 \in \mathcal{O}_K^{(2)}$ and find $v_2 \in \mathcal{O}_L^{(2)}$ such that $N_{L/K}(v_2) \equiv c_2 \mod \mathcal{O}_K^{(3)}$, so $u = N_{L/K}(v_0v_1v_2)c_3$ with $c_3 \in \mathcal{O}_K^{(3)}$. Rinse and repeat. Finally let $v = v_0v_1v_2\cdots$ and $N_{L/K}(v) = u$. □

Exercise 3.2.6. Show that the expression for v in Proposition 3.2.5 converges.

Corollary 3.2.7. *If L/K is finite unramified then $H^i_T(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = 1$ for all $i \in \mathbb{Z}$.*

Proof. The previous proposition shows that $H^0_T = 0$. For $H^1_T = H^1$, note that $L^\times = \mathcal{O}_L^\times \times \mathbb{Z}$, so $H^1(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)$ is a direct summand of $H^1(L/K) = 0$. Then 2-periodicity yields the result. □

As a G-module the exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$ is split, and $\mathrm{Gal}(L/K)$ acts trivially on the quotient $\mathbb{Z}$ (think of this as $\{\varpi_K^n : n \in \mathbb{Z}\}$ and note that the Galois group acts by isometries).

Proposition 3.2.8. *If L/K is finite unramified then $H^2(L/K)$ is cyclic of order $[L : K]$.*

Proof. If we take the long exact sequence for $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$ then by Corollary 3.2.7

$$H^2(G, \mathcal{O}_L^\times) = 0 \to H^2(L/K) \to H^2(G, \mathbb{Z}) \to 0 = H^3(G, \mathcal{O}_L^\times)$$

is exact, so by periodicity

$$H^2(L/K) \cong H^2(G, \mathbb{Z}) \cong H^0_T(G, \mathbb{Z}) \cong \mathbb{Z}/[L : K]\mathbb{Z}.$$ □

Here is another interpretation of $H^2(L/K)$. Note there is an exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and since $\mathbb{Q}$ is always injective, we get an isomorphism

$$H^2(G, \mathbb{Z}) \xrightarrow{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Since $\mathrm{Gal}(L/K)$ is generated by Frobenius, we get a canonical map $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ by evaluation at Frobenius. But then we get

$$\mathrm{inv} : H^2(L/K) \xrightarrow{\sim} H^2(G, \mathbb{Z}) \xrightarrow{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$$

and the image is $1/[L : K]\mathbb{Z}$. This is called the *invariant map* and comes from the theory of relative Brauer groups, which we won't discuss.

It's worth pointing out now that we already have enough ingredients to define the local reciprocity map for unramified extensions, at least on the finite level. To see this, note that one can show that if G is a group then

$$H_1(G, \mathbb{Z}) = I_G/I_G^2 \cong G^{\mathrm{ab}}.$$

So then if L/K is unramified you can just take

$$K^\times/N_{L/K}L^\times = H^0_T(L/K) \cong H^{-2}_T(L/K) = H^{-2}_T(\mathrm{Gal}(L/K), \mathbb{Z}) = H_1(G, \mathbb{Z}) = \mathrm{Gal}(L/K)$$

where, when using the 2-periodicity maps, we fix the generator of $\mathrm{Gal}(L/K)$ to be the Frobenius element (or its inverse, depending on how you like to normalize things).

On the other hand, to get the Theorem 3.1.4 in general, we need to do a bit more; we won't be able to run exactly the same method, but we can get away with a proof if we can show that $H^2(L/K)$ is always cyclic, so let's prove this first.

3.3. **Cyclic H^2.** Now suppose L/K is a finite cyclic extension, not necessarily unramified. Hilbert 90 still tells us that $H^1(L/K) = 0$. We'll show that $H^0_T(L/K)$ has size $[L : K]$, and then later show that it's cyclic.

The strategy we used before to understand the $H^0_T(L/K)$ was to reduce to $\mathbb{Z}$ by showing that $H^i_T(G, \mathcal{O}_L^\times) = 0$. But this is no longer necessarily true if L/K is ramified, so we will need a slightly modified statement. This modified statement is motivated by the fact that the Herbrand quotient (measuring the difference between H^0_T and H^1_T) is insensitive to finite pieces.

Lemma 3.3.1. *There exists an open and* $\mathrm{Gal}(L/K)$*-stable subgroup $W \subset \mathcal{O}_L^\times$ such that for all $i \in \mathbb{Z}$*

$$H^i_T(\mathrm{Gal}(L/K), W) = 0.$$

Proof. First note that there exists an open Galois-stable subgroup $V \subset \mathcal{O}_L$ such that $H^i_T(\mathrm{Gal}(L/K), V) = 0$ for all i. By the normal basis theorem in Galois theory, there exists an $\alpha \in L$ such that $\{g(\alpha) : g \in G\}$ forms a basis for L over K. Without loss of generality we can assume $\alpha \in \mathcal{O}_L$ so we can define

$$V = \sum \mathcal{O}_K \cdot g(\alpha)$$

which has finite index, and furthermore is a coinduced G-module, and thus acyclic by Shapiro's lemma.

But we're interested in $\mathcal{O}_L^\times$! And normally the way to get from something additive to something multiplicative is to exponentiate. Note that the power series

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

has a positive radius of convergence, so (by replacing α with something p-adically closer to 0) we can scale V so that e^V is defined. But $W := e^V$ is an open subgroup of $\mathcal{O}_L^\times$ and furthermore e^x is G-equivariant, so W is Galois stable. □

Exercise 3.3.2. Check that e^x converges on $|x| < p^{-1/(p-1)}$ in $\mathcal{O}_L$. Check further that e^x is a homeomorphism onto its image (hint: there is also a logarithm! use the usual power series).

Corollary 3.3.3. $|H^0_T(\mathrm{Gal}(L/K), L^\times)| = [L : K]$.

Proof. Since W as above has finite index in $\mathcal{O}_L^\times$, note that

$$h(L^\times) = h(\mathcal{O}_L^\times)h(\mathbb{Z}) = h(W)h(\mathbb{Z}) = h(\mathbb{Z}) = [L : K].$$ □

Note that this *doesn't* allow us to conclude that $H^2(G, L^\times)$ is cyclic because $\mathcal{O}_L^\times$ is not necessarily acyclic, but we will show this later.

3.4. **General H^2.** For this we use the *inflation-restriction sequence.*

Lemma 3.4.1. *If $H^i(H, M) = 0$ for $i = 1, \ldots, r-1$, then*

$$0 \to H^r(G/H, M^H) \to H^r(G, M) \to H^r(H, M)$$

is exact

Proof. The proof is by dimension shifting using the exact sequence

$$0 \to M \to \mathrm{coInd}_1^G \mathrm{Res}_1^G M \to N \to 0,$$

but I'll skip the details. There's also a spectral sequence which this falls out of, but I won't discuss this either. □

Now suppose L/K is any finite Galois extension. Maybe L is not cyclic or abelian, but $\mathrm{Gal}(L/K)$ is at least *solvable*. That means that there exists a sequence

$$0 \subset G_1 \subset \cdots \subset G_n = \mathrm{Gal}(L/K)$$

with each G_i/G_{i-1} cyclic. In particular, there exists some tower of Galois extensions $K \subsetneq M \subsetneq L$, and using inflation-restriction along with Hilbert 90 we get an exact sequence

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

which implies

$$|H^2(L/K)| \leq |H^2(M/K)||H^2(L/M)|$$

Lemma 3.4.2. $|H^2(L/K)| \leq [L : K]$

Proof. We can argue by induction on $[L : K]$. In the base case we assume L/K is cyclic, and then we already know that $|H^2(L/K) = [L : K]$. In general we know that L/K is solvable so there exists an intermediate extension $L/M/K$ with L/M cyclic, so by the inductive step,

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

□

Finally we show cyclicity by comparison to the unramified case.

Proposition 3.4.3. *$H^2(L/K)$ is cyclic of order $[L : K]$.*

Proof. Take M/K (the unique) unramified extension of degree $[M : K] = [L : K]$, let U denote the maximal unramified subextension of L containing K, and form the diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & H^2(U/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{Inf}"] & H^2(L/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{Inf}"] & H^2(L/U) \\
0 \arrow[r] & H^2(M/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{Res}"] \arrow[dr] & H^2(ML/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{Res}"] & H^2(ML/M) \\
 & H^2(M/U) \arrow[r, dashed] & H^2(ML/L) &
\end{tikzcd}$$

The rows and columns are inflation-restriction, and the dashed line is induced by the map (which is actually an isomorphism) $\mathrm{Gal}(ML/L) \xrightarrow{\sigma \mapsto \sigma|_M} \mathrm{Gal}(M/U)$ and $M^\times \hookrightarrow (ML)^\times$; one can check that the dashed line makes the square commute.

If we show that the diagonal map $H^2(M/K) \to H^2(ML/L)$ is zero, then we're done because then by exactness $H^2(M/K) \subset H^2(L/K)$ and $H^2(M/K)$ is cyclic of order $[L : K]$.

Note M/K, M/U, and ML/L are all unramified, so by 2-periodicity we want to show that

$$H^0_T(M/K) \xrightarrow{\mathrm{Res}} H^0_T(M/U) \to H^0_T(ML/L)$$

is the zero map, but this is

$$K^\times/N^M_K(M^\times) \to U^\times/N^M_U(M^\times) \to L^\times/N^{ML}_L((ML)^\times)$$

induced by the natural inclusions $K^\times \to U^\times \to L^\times$. Now note that the first group is cyclic of order $[L : K]$ generated by π_K, and the third group is cyclic of order $[ML : L]$ generated by π_L, but

$$[ML : L] = [M : U] = \frac{[M : K]}{[U : K]} = \frac{[L : K]}{[U : K]} = [L : U] = e(L/K)$$

where the last equality follows because U/K is the maximal unramified extension in L. Finally $\pi_K = u\pi_L^{e(L/K)}$ for some $u \in \mathcal{O}_L^\times$, so the map is zero. □

Note that there's a unique unramified extension K_n/K of degree n for all n, and $K_n \subset K_m$ if and only if $n \mid m$. The inflation maps

$$H^2(K_n/K) \to H^2(K_m/K)$$

are the inclusions $\mathbb{Z}/n \to \mathbb{Z}/m$, so

$$H^2(K^{\mathrm{unr}}/K) \cong \varinjlim_n H^2(K_n/N) = \varinjlim_n \mathbb{Z}/n\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

Proposition 3.4.4. *The inflation map*

$$H^2(K^{\mathrm{unr}}/K) \to H^2(\overline{K}/K)$$

is an isomorphism.

Proof. Inflation is injective so we just need to check surjectivity. But note that $H^2(\overline{K}/K)$ is the union of the $H^2(L/K)$ and if we take M/K unramified of degree $[L:K]$ then

$$\mathrm{im}(H^2(M/K) \to H^2(ML/K) \to H^2(\overline{K}/K)) = \mathrm{im}(H^2(L/K) \to H^2(ML/K) \to H^2(\overline{K}/K))$$

so in particular every element in $H^2(L/K)$ is hit by something coming from an unramified extension. Finally, note that $H^2(K^{\mathrm{unr}}/K)$ is the union of the $H^2(M/K)$ over M unramified. □

Exercise 3.4.5. If $L/M/K$ is a tower of finite Galois extensions, then the diagram

$$\begin{tikzcd}
H^2(M/K) \arrow[r, "\sim"] \arrow[d, "\mathrm{Inf}"] & \mathbb{Z}/[M:K]\mathbb{Z} \arrow[d, hook] \\
H^2(L/K) \arrow[r, "\sim"] & \mathbb{Z}/[L:K]\mathbb{Z}
\end{tikzcd}$$

commutes.

Finally, we mention what happens if you change the base field.

Proposition 3.4.6. *If L/K is a finite extension, then the restriction map $H^2(K^{\mathrm{unr}}/K) \to H^2(L^{\mathrm{unr}}/L)$ is the same as the map $\mathbb{Q}/\mathbb{Z} \xrightarrow{x \mapsto [L:K]x} \mathbb{Q}/\mathbb{Z}$.*

Proof. Note that the identification with $\mathbb{Q}/\mathbb{Z}$ can be expressed in the diagram

$$\begin{tikzcd}
H^2(K^{\mathrm{unr}}/K) \arrow[r, "v_K"] \arrow[d, "\mathrm{Res}"] & H^2(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Z}) \arrow[d, "e\,\mathrm{Res}"] & H^1(\mathrm{Gal}(K^{\mathrm{unr}}/K), \mathbb{Q}/\mathbb{Z}) \arrow[l, "\sim"'] \arrow[r, "\mathrm{ev}_{\mathrm{Frob}_K}"] \arrow[d, "e\,\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "ef"] \\
H^2(L^{\mathrm{unr}}/L) \arrow[r, "v_L"] & H^2(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Z}) & H^1(\mathrm{Gal}(L^{\mathrm{unr}}/L), \mathbb{Q}/\mathbb{Z}) \arrow[l, "\sim"'] \arrow[r, "\mathrm{ev}_{\mathrm{Frob}_L}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

□

3.5. **Artin reciprocity.** We now prove a fairly general homological algebra statement, due to Tate, which is then immediately applied to our scenario to define the local Artin reciprocity map.

See https://www.jstor.org/stable/1969801 or page 84 of https://www.jmilne.org/math/CourseNotes/CFT.pdf for a full proof of the following.

Theorem 3.5.1. *If G is a finite group and M is an $A[G]$-module, then suppose that $H^1(H, M) = 0$ for all subgroups $H \leq G$ and $H^2(H, M)$ is cyclic of order $|H|$. Then there are isomorphisms*

$$H^i_T(G, A) \xrightarrow{\sim} H^{i+2}(G, M)$$

which are canonical up to the choice of a generator $\gamma \in H^2(G, M)$. These are in fact the cup products with γ.

Proof. This is a bit dry, so I won't prove the whole thing. Instead I'll give a sketch of a proof. Pick a generator $\gamma \in H^2(G, M)$. Then one can construct a module $M[\gamma]$ admitting an injection $M \to M[\gamma]$ such that the image of γ under the map $H^2(G, M) \to H^2(G, M[\gamma])$ is zero (so the map is 0); in fact $M[\gamma]$ is basically the minimal possible thing you can construct to make γ vanish, and is essentially a way of formally turning a cocycle representing γ into a coboundary. By construction, we have that $M[\gamma]$ fits into an exact sequence

$$0 \to M \to M[\gamma] \to I_G \to 0$$

and in the long exact sequence we get

$$0 = H^1(H, M) \to H^1(H, M[\gamma]) \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M[\gamma]) \to H^2(H, I_G)$$

But then $H^1(H, I_G) = H^0_T(H, \mathbb{Z})$, which has size $|H|$. Note $H^2(H, I_G) = H^1(H, \mathbb{Z}) = \mathrm{Hom}(H, \mathbb{Z}) = 0$, and the map $H^2(H, M) \to H^2(H, M[\gamma])$ is zero by construction, so $H^2(H, M[\gamma]) = 0$. But then $H^1(H, I_G) \to H^2(H, M)$ is surjective map of finite groups of the same order, so $H^1(H, M[\gamma]) = 0$. Then one shows that $H^1(H, M[\gamma]) = H^2(H, M[\gamma]) = 0$ for all H actually implies $H^i_T(G, M[\gamma]) = 0$.

But now note that we have two exact sequences

$$0 \to M \to M[\gamma] \to I_G \to 0$$

and

$$0 \to I_G \to A[G] \to A \to 0$$

where the middle terms are acyclic, so the connecting homomorphisms give us isomorphisms

$$H^i_T(G, A) \xrightarrow{\sim} H^{i+1}_T(G, I_G) \xrightarrow{\sim} H^{i+2}_T(G, M).$$

The dependence on γ and nothing else is clear, since the two maps are just connecting maps which are completely canonical. □

Exercise 3.5.2. If G is a finite group, then $I_G/I_G^2 \cong G^{\mathrm{ab}}$. Hint: the map is $G^{\mathrm{ab}} \to I_G/I_G^2$ taking $g \mapsto [g] - 1$.

As a consequence, we get the Artin reciprocity map. To see this, note that we can apply Theorem 3.5.1 to $G = \mathrm{Gal}(L/K)$ for L/K finite Galois, and $M = L^\times$, and we get:

Definition 3.5.3. The *local Artin map*, or *local reciprocity map*, is the isomorphism

$$\begin{aligned}\mathrm{Art}_{L/K} : K^\times / N^L_K L^\times &= H^0_T(L/K) \\ &\xrightarrow{\sim} H^{-2}_T(\mathrm{Gal}(L/K), \mathbb{Z}) \\ &= H_1(\mathrm{Gal}(L/K), \mathbb{Z}) \\ &= I_G/I_G^2 \\ &\xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}.\end{aligned}$$

The first line is by definition, the second is from Tate's theorem, and rest is basically by definition.

Remark 3.5.4. What about the dependence of the Artin map on the choice of generator of $H^2(L/K)$?

Here we see that it ends up being extremely useful that we reduced to the unramified case first, because it allows you to make the choice completely canonical. To see why, note that in Proposition 3.4.3 we showed that if M/K is the unique unramified extension with $[M:K]=[L:K]$ then $H^2(L/K)$ and $H^2(M/K)$ have the same image in $H^2(ML/K)$, and $H^2(M/K)$ has a canonical generator given by the inverse image of $1/[L:K]$ under the invariant map

$$H^2(L/K) \xrightarrow{\sim} H^2(G,\mathbb{Z}) \to H^1(G,\mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}.$$

So we can look at the image of $1/[L:K]$ in $H^2(ML/L)$ and take its preimage in $H^2(L/K)$ to get the canonical generator. It will be important that we make this choice in the next lemma.

Also, note that there are two different normalizations that are used in the literature, either you can choose to take the inverse image of $1/[L:K]$, or you can choose its inverse $([L:K]-1)/[L:K]$. This amounts to a choice between the arithmetic and geometric Frobenius.

Proposition 3.5.5. *If $M/L/K$ is a tower of fields with both L and M Galois over K then there is a commuting square*

$$\begin{tikzcd}
K^\times/N_K^M M^\times \arrow[r, "\mathrm{Art}_{M/K}"] \arrow[d] & \mathrm{Gal}(M/K)^{\mathrm{ab}} \arrow[d, two heads] \\
K^\times/N_K^L L^\times \arrow[r, "\mathrm{Art}_{L/K}"] & \mathrm{Gal}(L/K)^{\mathrm{ab}}
\end{tikzcd}$$

where the map on the right is the natural surjection and the map on the left is the natural projection (noting that $N_K^M = N_K^L \circ N_L^M$, so $N_K^M M^\times \subset N_K^L L^\times$.

Proof. The compatibility of choice of generator of H^2 implies that the Artin maps are really induced by the diagram:

$$\begin{tikzcd}
0 \arrow[r] & M^\times \arrow[r] \arrow[d, "N_L^M"] & M[\gamma_M] \arrow[r] \arrow[d] & I_{\mathrm{Gal}(M/K)} \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & L^\times \arrow[r] & L[\gamma_L] \arrow[r] & I_{\mathrm{Gal}(L/K)} \arrow[r] & 0.
\end{tikzcd}$$

The right vertical map is the natural surjection and the middle vertical map is a combination of the norm map on $M^\times$ with a map on the extra data in $M[\gamma_M]$ (we've been a bit vague about what this module is, so details are omitted). □

Corollary 3.5.6 (Norm Limitation Theorem)**.** *If L/K is Galois and L^{ab} is its maximal abelian subextension then*

$$N_K^L L^\times = N_K^{L^{\mathrm{ab}}}(L^{\mathrm{ab}})^\times.$$

Proof. Take $L = L^{\mathrm{ab}}$ and $M = L$ in Proposition 3.5.5. □

We also deduce the following compatibility property for norm groups which matches the similar statement for Galois groups.

Corollary 3.5.7. *If L/K is a finite abelian extension and $K \subseteq L_1, L_2 \subseteq L$ are sub-extensions satisfying $L_1L_2 = L$, then*

$$N_K^{L_1}L_1^\times \cap N_K^{L_2}L_2^\times = N_K^L L^\times$$

Proof. Note that $N_K^L = N_{L_1}^L \circ N_K^{L_1} = N_{L_2}^L \circ N_K^{L_2}$, which gives $N_K^L L^\times \subseteq N_K^{L_1} L_1^\times \cap N_K^{L_2} L_2^\times$. For the other direction, consider the diagram

$$\begin{tikzcd}
K^\times \arrow[r, "\mathrm{Art}_{L/K}"] \arrow[dr, swap, "\mathrm{Art}_{L_1/K} \times \mathrm{Art}_{L_2/K}"] & \mathrm{Gal}(L/K) \arrow[d, hook, "\mathrm{res} \times \mathrm{res}"] \\
& \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)
\end{tikzcd}$$

and note that the kernel of the top map is $N_K^L L^\times$, and the kernel of the diagonal map is $N_K^{L_1} L_1^\times \cap N_K^{L_2} L_2^\times$. □

This compatibility allows us to construct a map

$$\mathrm{Art}_K : K^\times \to \varprojlim_M \mathrm{Gal}(M/K)^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K) = \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}.$$

where M/K runs over all finite Galois extensions.

Note that we've supplied the map in Theorem 3.1.1, and showed that it satisfies property (2). To show that it satisfies (1) note that if L/K is unramified then $K^\times / N_K^L L^\times$ is a cyclic group of order $[L : K]$ generated by ϖ_K, and it maps to Frobenius by the calculations we did in Section 3.2.

It remains to show that Art_K induces an isomorphism on profinite completions:

$$\widehat{K^\times} = \varprojlim_U K^\times / U \to G_K^{\mathrm{ab}}.$$

But this will follow if we can show that every open and finite index subgroup $U \subset K^\times$ is actually equal to $N_K^L L^\times$ for some finite Galois extension L/K; we show this now.

3.6. The local existence theorem.

Showing that $U = N_K^L L^\times$ needs more than just Galois cohomology. Given a U, we need to construct actual Galois extensions. We will do this using Kummer theory.

Lemma 3.6.1. *If K contains the ℓ-th roots of unity for a prime number ℓ then $x \in (K^\times)^\ell$ if and only if $x \in N_K^L L^\times$ for all ℓ-extensions L/K.*

Proof. Kummer theory tells us that if M is the compositum of all of the ℓ-extensions of K then $\mathrm{Gal}(M/K) = K^\times/(K^\times)^\ell$. Local reciprocity tells us that $\mathrm{Gal}(M/K) \cong K^\times / N_K^M M^\times$.

By Exercise 3.6.2 there are only finitely many ℓ-extensions of K, so M/K is a finite extension. Moreover, the distinct ℓ-extensions are pairwise linearly disjoint, so we actually obtain that

$$K^\times / N_K^M M^\times \cong K^\times / (K^\times)^\ell \cong (\mathbb{Z}/\ell\mathbb{Z})^n$$

where n is the number of distinct ℓ-extensions of K. But this means that $K^\times / N_K^M M^\times$ is killed by ℓ (as a $\mathbb{Z}$-module) and it immediately follows that $(K^\times)^\ell \subseteq N_K^M M^\times$. But these subgroups are both of finite index and have isomorphic quotients, so they must be equal.

Finally, since M/K is finite (also by the exercise below), Corollary 3.5.7 implies that $N_K^M M^\times = \bigcap N_K^L L^\times$ where L runs over all ℓ-extensions of K. □

Exercise 3.6.2. Show that $K^\times/(K^\times)^n$ is a finite group for any n.

Lemma 3.6.1 is useful because it allows us to prove:

Proposition 3.6.3.

$$\bigcap_L N_K^L L^\times = 1.$$

Before proving this, we first show how this implies the local existence theorem.

Proof of Theorem 3.1.4. First note that it is enough to construct L such that $N_K^L L^\times \subset U$, because $K^\times/N_K^L L^\times = \mathrm{Gal}(L/K)$, so $K^\times/U$ will be a quotient of $\mathrm{Gal}(L/K)$ and thus equal to $\mathrm{Gal}(M/K)$ for some intermediate extension M, and thus $U = N_K^M M^\times$.

Note U is of finite index in $K^\times$, so its image in $K^\times/\mathcal{O}_K^\times \cong \mathbb{Z}$ must be $m\mathbb{Z}$ for some integer m. So whichever L we construct should contain an unramified extension of degree at least m. Then we are reduced to finding L a finite extension of the unramified extension satisfying

$$N_K^L L^\times \cap \mathcal{O}_K^\times \subset U \cap \mathcal{O}_K^\times. \tag{4}$$

For each L, $N_K^L L^\times \cap \mathcal{O}_K^\times = N_K^L \mathcal{O}_L^\times \subseteq \mathcal{O}_K^\times$ is compact since the norm is continuous. Proposition 3.6.3 implies that $\bigcap_L N_K^L L^\times \cap \mathcal{O}_K^\times = 1$. But then

$$\bigcap_L [(N_K^L L^\times \cap \mathcal{O}_K^\times) - (U \cap \mathcal{O}_K^\times)] = \varnothing$$

But then terms in the intersection are all closed, since $U \cap \mathcal{O}_K^\times$ is open (since it's finite index and $\mathcal{O}_K^\times$ is topologically finitely generated and profinite). By compactness of $\mathcal{O}_K^\times$ we can intersect finitely many of the terms to get something empty, but then

$$[(N_K^{L_1} L_1^\times \cap \mathcal{O}_K) - (U \cap \mathcal{O}_K^\times)] \cap \cdots \cap [(N_K^{L_n} L_n^\times \cap \mathcal{O}_K) - (U \cap \mathcal{O}_K^\times)] = (N_K^{L_1 \cdots L_n}(L_1 \cdots L_n)^\times \cap \mathcal{O}_K) - (U \cap \mathcal{O}_K^\times) = \varnothing$$

and thus we get the desired containment. □

Now we fill in the missing detail.

Proof of Proposition 3.6.3. Let $D_K = \bigcap_L N_K^L L^\times$ varying over all finite Galois extensions L/K. Since the unramified extensions K_m/K are included in this intersection and $v(N_K^{K_m} K_m^\times) = m\mathbb{Z}$, we see that $D_K \subset \mathcal{O}_K^\times$.

Then one shows that D_K is n-divisible for all n, so by Exercise 3.6.4 D_K is trivial. It suffices to show that D_K is ℓ-divisible for all ℓ. The point is that this *almost* follows from Kummer theory, but not quite, so one has to pass to a finite extension containing the ℓth roots of unity. We omit the details, but see III.5 in Milne's book. □

Exercise 3.6.4. Show that $\bigcap_n (K^\times)^n = 1$.

In any event, in conclusion we get that the Artin map induces an isomorphism

$$\widehat{K^\times} \xrightarrow{\sim} G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

3.7. **Ramification: a word.** If we write $K^\times = \varpi_K^{\mathbb{Z}} \times \mathcal{O}_K^\times$, we have already seen that the copy of $\mathbb{Z}$ corresponds to Frobenius acting on the maximal unramified extension of K. So how do we understand $\mathcal{O}_K^\times$ on the Galois side?

Recall that the *inertia subgroup* is

$$I_K = \left\{ g \in G_K : v(g(x) - x) \geq 1 \text{ for all } x \in \mathcal{O}_{\overline{K}} \right\}.$$

Note that the inertia group fits into the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\sim"] & K^\times \arrow[r] \arrow[d, "\mathrm{Art}_K"] & \mathbb{Z} \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & I_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{unr}}) \arrow[r] & G_K^{\mathrm{ab}} \arrow[r] & \mathrm{Gal}(K^{\mathrm{unr}}/K) \arrow[r] & 0
\end{tikzcd}$$

We already showed that there exists a distinguished filtration

$$\cdots \subset \mathcal{O}_K^{(2)} \subset \mathcal{O}_K^{(1)} \subset \mathcal{O}_K^\times$$

where $\mathcal{O}_K^{(i)} = 1 + \varpi_K^i \mathcal{O}_K$ for all $i > 0$. So for instance, what is the image of $\mathcal{O}_K^{(1)}$ under the Artin map?

Recall that last semester we said that a finite Galois extension L/K is *tamely ramified* if $p \nmid e(L/K)$, and *wildly ramified* otherwise. We proved, basically using Hensel's lemma, that $L = K(\varpi_K^{1/n})$ where

$n = [L : K]$ for some uniformizer $\varpi_K \in K$. Therefore, the maximal tamely ramified extension of K is $K^{\mathrm{unr}}(\left\{\varpi_K^{1/n}, (n,p) = 1\right\})$. So we get a tower of extensions $K \subset K^{\mathrm{unr}} \subset K^{\mathrm{tame}} \subset \overline{K}$ and a tower of Galois groups $0 \subset P_K \subset I_K \subset G_K$, and we called P_K the *wild inertia subgroup*.

It turns out that wild inertia is the most complicated part of the Galois group. This is because the explicit description of the ramified and unramified Galois groups plus a bit more actually gives us that

$$G_K/P_K \cong \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \rtimes \mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \widehat{\mathbb{Z}}^{(p)} \rtimes \widehat{\mathbb{Z}}$$

where the map $\widehat{\mathbb{Z}} \to \mathrm{Aut}(\widehat{\mathbb{Z}}^{(p)})$ is defined using the cyclotomic characters; in other words, lift $g \in \mathrm{Gal}(K^{\mathrm{unr}}/K)$ to something in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and conjugate $\sigma \in \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$; this is independent of the lift.

Definition 3.7.1. Let

$$G_{K,i} = \left\{g \in G_K : v(g(x) - x) \geq i + 1 \text{ for all } x \in \mathcal{O}_{\overline{K}}\right\}.$$

Then $G_K = G_{K,-1}$ and $I_K = G_{K,0}$. What about $G_{K,1}$?

Proposition 3.7.2. $P_K = G_{K,1}$.

Proof. First we check that $G_{K,1} \subset P_K$. Since $P_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{tame}})$ it suffices to check that if you take any $\sigma \in G_{K,1}$ then $\sigma|_{K^{\mathrm{tame}}}$ is the identity. Note K^{tame} is generated by the $\pi_K^{1/n}$ for $(n,p) = 1$ and σ takes $\pi_K^{1/n}$ to $\zeta\pi_K^{1/n}$ for ζ an nth root of unity in K. So we must have $v(\pi_K^{1/n}(1-\zeta)) \geq 2$. But $v(\pi_K^{1/n}) < 1$ and $v(1-\zeta) = 0$ if $\zeta \neq 1$, so $\zeta = 1$. □

Exercise 3.7.3. Show the converse; i.e. that $P_K \subseteq G_{K,1}$.

So you might wonder whether $\mathrm{Art}(1 + \pi^i\mathcal{O}_K) = G_{K,i}$. Even though this is true when $i = 0$, it turns out *not* to be true in general, unfortunately, even for $i = 1$. There is another filtration on the Galois group G_K which makes this work, but the definition is a bit complicated, so we'll skip this for now.

3.8. **Lubin-Tate theory.** Recall that by Kronecker-Weber we can write $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}_1\mathbb{Q}_2$ where $\mathbb{Q}_1 = \bigcup_n \mathbb{Q}(\zeta_{p^n})$ is a maximal abelian ramified extension of $\mathbb{Q}$ and $\mathbb{Q}_2 = \bigcup_n \mathbb{Q}(\zeta_{p^n-1})$ is the maximal abelian unramified extension.

In general, local class field theory gave us a bijective correspondence between maximally totally ramified subextensions $K \subset L \subset K^{\mathrm{ab}}$ and $\langle\pi\rangle \leq K^\times$ for π a uniformizer (remember that these are only unique up to multiplication by $\mathcal{O}_K^\times$!). Since $K^\times \cong \langle\pi\rangle \times \mathcal{O}_K^\times$, we may write $K^{\mathrm{ab}} = K^{\mathrm{unr}}K_\pi$ where $K_\pi = \overline{K}^{\pi=1}$.

We know how to explicitly construct K^{unr}, and if $K = \mathbb{Q}_p$ then we know how to explicitly construct $(\mathbb{Q}_p)_p = \mathbb{Q}_1$. But then is there an explicit way to construct K_π in general?

Lubin-Tate theory provides us with a way of doing this, in a relatively explicit way.

Remark 3.8.1. To see how you might come up with Lubin-Tate theory, consider the multiplicative group scheme $\mathbb{G}_m$ (defined over K), which we can view as a functor $\mathbb{G}_m : \mathsf{Alg}_K \to \mathsf{Grp}$ taking $A \mapsto A^\times$. Then notice that $\{\zeta_{p^n}\}$ is the p-power torsion part of $\mathbb{G}_m(\overline{K})$.

In fact, we can really replace $\mathbb{G}_m$ with its *formal completion at the identity* to obtain what is called a *formal group scheme*, and you can consider its torsion points again, which are the same. This is what we will generalize, although we'll do it in the language of formal group laws.

Definition 3.8.2. If R is a commutative ring, then a power series $F \in R[[X,Y]]$ is a *(commutative) formal group law* if

(1) $F(F(X,Y),Z) = F(X,F(Y,Z))$,

(2) $F(X,Y) = X + Y +$ higher order terms.

(3) $F(X,0) = F(0,X) = X$.

(4) There exists a unique power series $i_F(X)$ such that $F(X, i_F(X)) = 0$.

and it is commutative if $F(X,Y) = F(Y,X)$.

It can be helpful to write $X *_F Y := F(X,Y)$ to aid the intuition that this is supposed to define a kind of group operation.

Remark 3.8.3. Some of these are actually redundant. For instance, if you know (1) and (2) you can deduce (3). If you know (1) and (3) you can deduce (2). If you know (1) and (2) you can deduce (4) and if you know (1)-(4) and you know that R has no nilpotents, then you can deduce that F is commutative.

For example, if you write $F(X,Y) = a+bX+cY$ then if you assume $F(X,0) = F(0,X) = X$ you immediately get that $a = 0$ and $b = c = 1$.

Exercise 3.8.4. Slightly harder: prove that (1) and (2) imply (3) (you can do this inductively on the degrees of $F(X,0)$ and $F(0,X)$).

Remark 3.8.5. These can also be interpreted as certain group objects in the category of formal schemes with a choice of coordinate. Namely, if you pick G to be a formal scheme over R which is smooth and one dimensional, then you will have $G \cong \operatorname{Spf} R[[T]]$ abstractly. Picking a specific isomorphism $G \cong \operatorname{Spf} R[[T]]$ then gives you the maps defining a formal group law: namely, the maps

$$\operatorname{Spf}(R[[X,Y]]) = \operatorname{Spf}(R[[X]]\widehat{\otimes}_R R[[Y]]) = \operatorname{Spf}(R[[X]]) \times_R \operatorname{Spf}(R[[Y]]) \xrightarrow{\sim} G \times G \xrightarrow{m} G \xrightarrow{\sim} \operatorname{Spf}(R[[T]])$$

which yields a map $R[[T]] \to R[[X,Y]]$ in the other direction. The image of T under this map is a formal group law. All of the formal group law axioms follow from the group object axioms.

Exercise 3.8.6. Show that if K is a field of characteristic p and $R = K[t]/t^2$ then show that $F(X,Y) = X + Y + tXY^p$ is a formal group law, which is visibly *not* commutative.

Example 3.8.7.

- The additive group law $F_a(X,Y) = X + Y$
- The multiplicative group law $F_m(X,Y) = (1+X)(1+Y) - 1 = X + Y + XY$.

Just as groups have homomorphisms, formal group laws have them too.

Definition 3.8.8.

- If F and G are two formal group laws, then a homomorphism $\varphi : F \to G$ is a power series $\varphi(x) \in XR[[X]]$ such that
$$F(\varphi(X), \varphi(Y)) = \varphi(G(X,Y)).$$
This can also be written as $\varphi(X +_G Y) = \varphi(X) +_H \varphi(Y)$.
- If G is commutative, then two homomorphisms $\varphi, \psi : F \to G$ can be added by taking $(\varphi + \psi)(X) = G(\varphi(X), \psi(X))$. Note this is still a homomorphism:
$$F((\varphi+\psi)(X), (\varphi+\psi)(Y)) = F(G(\varphi(X), \psi(X)), G(\varphi(Y), \psi(Y)))$$
- An endomorphism is a homomorphism $F \to F$, and the set of such things is $\operatorname{End}(F)$. There is a unique ring homomorphism $\mathbb{Z} \to \operatorname{End}(F)$, and we denote the image of n by $[n]_F$.

Exercise 3.8.9. Show that $\operatorname{End}(F)$ becomes a (possibly non-commutative) ring with respect to addition and multiplication given by composition. Show that $\varphi(X) = X$ is the multiplicative identity and that $\varphi(X) = 0$ is the additive identity.

Example 3.8.10.

- An endomorphism of F_a is a power series $f \in XR[[X]]$ satisfying $f(X+Y) = f(X) + f(Y)$. If R has characteristic 0 (i.e. contains $\mathbb{Q}$) then the only way this can hold is if $f(X) = rX$ for some $r \in R$. In this way, $\operatorname{End}(F_a) = R$. The natural map $\mathbb{Z} \to \operatorname{End}(F_a)$ is just the structure map $\mathbb{Z} \to R$.
- An endomorphism of F_m is a power series $f \in XR[[X]]$ satisfying $(1 + f(X))(1 + f(Y)) - 1 = f((1 + X)(1 + Y) - 1)$. This contains everything of the form $(1 + X)^n - 1$, and the natural map $\mathbb{Z} \to \operatorname{End}(F_m)$ sends $n \mapsto [n]_{F_m} = (1 + X)^n - 1$.

So how can we use this definition to construct K_π?

Remark 3.8.11. If you take $R = \mathcal{O}_K$, then a formal group law $F \in \mathcal{O}_K[[X, Y]]$ gives a group structure on $\mathfrak{m}_{\overline{K}}$ by sending $x, y \in \mathfrak{m}_{\overline{K}}$ to $F(x, y)$. Note this converges since $|x|, |y| < 1$. For $n > 0$ let

$$F[p^n] = \left\{x \in \mathfrak{m}_{\overline{K}} : [p]_F(x) = 0\right\}.$$

For example if $F = F_m$, then $F[p^n]$ consists of elements satisfying $(1+x)^{p^n} = 1$, which in other words means that

$$F_m[p^n] = \left\{x - 1 : x^{p^n} = 1\right\}.$$

Thus we see that the extension $(\mathbb{Q}_p)_p$ is obtained by adjoining $F_m[p^n]$ for all $n > 0$.

The goal of Lubin-Tate theory is to generalize this. First note that the linear term of the power series $[p]_{F_m}$ is just pX and the mod p reduction is just X^p.

Now let $K/\mathbb{Q}_p$ be finite again. Let $q = |k_K|$.

Definition 3.8.12. If $\pi \in \mathcal{O}_K$ is a uniformizer, then a π-*Lubin-Tate power series* is a power series $f(X) \in \mathcal{O}_K[[X]]$ satisfying

- the linear term of $f(X)$ is πX,
- $f(X) \equiv X^q \mod \pi$.

For instance one can take $f = \pi X + X^q$, but there are many other choices.

Proposition 3.8.13. *If f is a π-Lubin-Tate power series, then there exists a unique formal group law $F_f \in \mathcal{O}_K[[X, Y]]$ with $f \in \operatorname{End}(F_f)$. Furthermore, the map $\mathbb{Z} \to \operatorname{End}(F_f)$ extends to a ring homomorphism*

$$\begin{aligned} \mathcal{O}_K &\to \operatorname{End}(F_f) \\ a &\mapsto [a] \end{aligned}$$

such that the linear term of $[a]$ is aX and $[\pi] = f$.

Remark 3.8.14. Note that if $K = \mathbb{Q}_p$ then the choice $f = pX + X^p$ does *not* give the multiplicative formal group $F_m \in \mathbb{Z}_p[[X, Y]]$ on the nose; instead you have to take $(1 + X)^p - 1$. However, it is true that if f, f' are two p-Lubin-Tate power series, then $F_f \cong F_{f'}$ (although they may not literally be equal).

Theorem 3.8.15 (Lubin-Tate). *The field generated by $F[\pi^n]$ for all n over K is K_π. More specifically,*

1. *$F[\pi^n]$ is (non-canonically) isomorphic to $\mathcal{O}_K/\pi^n$ as an $\mathcal{O}_K$-module.*
2. *The action of G_K on $\overline{K}$ preserves $F[\pi^n]$, and the natural map*

   $$G_K \to \operatorname{Aut}_{\mathcal{O}_K} F[\pi^n] = (\mathcal{O}_K/\pi^n)^\times$$

   is surjective.
3. *If you let K_n denote the fixed field of the above map then*

   $$K_\pi = \bigcup_{n>0} K_n$$

Lubin-Tate theory thus gives a completely explicit way to do local class field theory.

4. Adèles

Now let's talk about the adeles. The name is a bit bizarre and has nothing to do with the singer Adèle; it's a portmanteau of "additive", "ideal", and "element", for reasons that will hopefully become more clear as we dig into the material.

4.1. **Definition.** Part of the reason that the adeles are defined in the way they are is so that we can do Fourier analysis on them. This is something we'll talk about later, but just note for now that when you do Fourier theory for $\mathbb{R}$ you use the lattice $\mathbb{Z} \subset \mathbb{R}$. Ultimately the adeles give us a way to "do analysis on a number field" by combining all of the valuations together into a huge object which contain the original number field discretely.

Remark 4.1.1. Recall first of all that if $F/\mathbb{Q}$ is a number field, then when we did Minkowski theory we considered the subspace

$$F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \subset F \otimes_{\mathbb{Q}} \mathbb{C}$$

Recall that $F \otimes_{\mathbb{Q}} \mathbb{C} \cong \prod_{\tau : F \hookrightarrow \mathbb{C}} \mathbb{C}$ indexed by the distinct embeddings, and that $F \otimes_{\mathbb{Q}} \mathbb{R}$ identifies with the subspace fixed under the automorphism

$$(z_\tau) \mapsto (\overline{z}_{\overline{\tau}})$$

so that $F \otimes_{\mathbb{Q}} \mathbb{R}$ identifies with $\mathbb{R}^r \times \mathbb{C}^s$ where r is the number of real embeddings and s is the number of complex-conjugate pairs of complex embeddings. We have

$$\dim_{\mathbb{R}} F_{\mathbb{R}} = [F : \mathbb{Q}].$$

Then $\mathcal{O}_F \subset F_{\mathbb{R}}$ sits is a discrete and cocompact lattice, and furthermore that any fractional ideal satisfies the same property.

Exercise 4.1.2. Show that $\mathcal{O}_=F$ is discrete and cocompact. In other words, show that the subspace topology on $\mathcal{O}_F \subset F_{\mathbb{R}}$ is the discrete topology, and show that the (Hausdorff) space $F_{\mathbb{R}}/\mathcal{O}_F$ is compact.

But since our goal is to find a space in which F itself sits compactly, we need to somehow enlarge $F_{\mathbb{R}}$ in such a way that passing from $\mathcal{O}_F$ to F preserves discreteness. One way of viewing this shift is to invert primes in the ring, so to proceed we will consider p-adic completions and see what we get.

Recall that we can write the profinite completion of the integers as

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \prod_p (\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}) = \prod_p \mathbb{Z}_p.$$

But we need to work rationally, so we make the following definition.

Definition 4.1.3. The ring of *finite adeles over* $\mathbb{Q}$ is

$$\mathbb{A}_{\mathbb{Q}}^{\text{fin}} := \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

On the other hand, one can view this as

$$\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q} = (\prod_p \mathbb{Z}_p) \otimes_{\mathbb{Z}} \mathbb{Q}$$

which is emphatically *not* isomorphic to $\prod_p \mathbb{Q}_p$ because infinite products do not always commute with the tensor product. On the other hand, $(\prod_p \mathbb{Z}_p) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ is a subspace of $\prod_p \mathbb{Q}_p$, via the following construction.

Definition 4.1.4. If $(X_i)_{i \in I}$ is a collection of sets and $Y_i \subset X_i$ is a collection of subsets, then the *restricted product* of the X_i with respect to the Y_i is

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

Here "almost all" means "all but finitely many". Alternatively,

$$\prod_{i\in I}{}' X_i := \bigcup_{S\subset I \text{ finite}} X_S$$

where $X_S = \prod_{i\in S} X_i \times \prod_{i\notin S} Y_i \subset \prod_{i\in I} X_i$.

Exercise 4.1.5. Show that if I is finite then the restricted product is the usual product. Show further that if you change finitely many of the Y_i, the restricted product does not change.

Remark 4.1.6. You can vary the category in this definition:

- If the X_i are topological spaces, then $\prod'_{i\in I} X_i$ obtains a natural topology by saying that $U \subset \prod'_{i\in I} X_i$ is open if and only if $U \cap X_S$ is open for all finite subsets $S \subset I$.

  This can alternatively be defined as the topology generated by sets of the form

  $$\prod_{i\in S} U_i \times \prod_{i\notin S} Y_i$$

  where $U_i \subset X_i$ are open. This description immediately implies (by Tychonoff's theorem) that if each X_i is locally compact and each Y_i is compact then $\prod'_{i\in I} X_i$ is locally compact as well.

- If the $X_i = G_i$ are groups and $Y_i = H_i$ are subgroups, then $\prod'_i G_i$ obtains a group structure. If the $X_i = R_i$ are rings and $Y_i = S_i$ are subrings, then $\prod'_i R_i$ obtains a natural ring structure. If the G_i or R_i are locally compact topological groups/rings and the H_i or S_i are compact subgroups/subrings, then $\prod'_i G_i$ is a locally compact topological group and $\prod'_i R_i$ is a locally compact topological ring.

Exercise 4.1.7. Show that there is an identification of rings $\mathbb{A}_{\mathbb{Q}}^{\text{fin}} = \prod'_p \mathbb{Q}_p$ with respect to the subrings $\mathbb{Z}_p$ for all p.

Definition 4.1.8. The *ring of* $\mathbb{Q}$*-adeles* is

$$\mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \mathbb{A}_{\mathbb{Q}}^{\text{fin}}$$

or alternatively the restricted product of $(\mathbb{R}, \{0\}), (\mathbb{Q}_2, \mathbb{Z}_2), (\mathbb{Q}_3, \mathbb{Z}_3), \ldots$ Since $\mathbb{R}$ and $\mathbb{Q}_p$ is locally compact, and $\{0\}$ and $\mathbb{Z}_p$ are compact, $\mathbb{A}_{\mathbb{Q}}$ is a locally compact topological ring.

Note there is a natural (injective) map

$$\begin{aligned} \mathbb{Q} &\mapsto \mathbb{A}_{\mathbb{Q}} \\ x &\mapsto (x \in \mathbb{R}, x \in \mathbb{Q}_2, x \in \mathbb{Q}_3, \ldots) \end{aligned}$$

which indeed lands in $\mathbb{A}_{\mathbb{Q}}$ because $x \in \mathbb{Z}_p$ for every p except for those dividing the denominator. Even more interestingly,

Proposition 4.1.9. *$\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q}}$ is discrete and cocompact.*

Proof. To show that $\mathbb{Q}$ sits discretely inside, we can translate to 0 and then we just need to find $U \subset \mathbb{A}_{\mathbb{Q}}$ open such that $U \cap \mathbb{Q} = \{0\}$. For this, consider the open subset

$$U = \{x \in \mathbb{R} : |x|_\infty < 1\} \times \prod_p \mathbb{Z}_p.$$

If $x \neq 0$ then note $|x|_p \leq 1$ for all p, hence $x \in \mathbb{Z}$. But $|x|_\infty < 1$, so $x = 0$, and clearly $0 \in U$. We conclude that $\mathbb{Q}$ is discrete.

We sketch the proof that $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact as an exercise. Note that

$$W := \{(a_v) \in \mathbb{A}_{\mathbb{Q}} : |a|_v \leq 1 \text{ for all } v \leq \infty\}$$

is the Cartesian product of compact sets, and is therefore compact. One needs to show that it contains a complete set of coset representatives for $\mathbb{Q}$ in $\mathbb{A}_\mathbb{Q}$, and then its image in $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ is compact, and is equal to $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$, so we're done.

To show that it contains a complete set of coset representatives, you need to show that given any $(x_v)_v \in \mathbb{A}_\mathbb{Q}$, you can add an element of $\mathbb{Q}$ and land in W. Note that for almost all prime numbers p, the element x_p is contained in $\mathbb{Z}_p$ already. Let $m = p_1^{a_1} \cdots p_r^{a_r}$ denote the minimal integer such that $mx_p \in \mathbb{Z}_p$ for *all* primes p. By the Chinese Remainder Theorem there exists some $n \in \mathbb{Z}$ such that

$$mx_{p_i} \equiv n \mod p_i^{a_i} \text{ for } i = 1, \cdots, r$$

Then define $y' = n/m \in \mathbb{Q}$. Note that if $(p, n) = 1$ then $x_p - y' \in \mathbb{Z}_p$ still. On the other hand, we also have

$$x_{p_i} - y' = x_{p_i} - \frac{n}{m} = \frac{1}{m}(mx_{p_i} - n) = \prod_{j \neq i} p_j^{a_j}.$$

So for each prime number p, the p-component of $(x_v)_v + y'$ is contained in $\mathbb{Z}_p$. Note that this doesn't change if we add an integer, and there exists some integer $z \in \mathbb{Z}$ such that $|x_\infty - y' - z|_\infty \leq 1$. So if we set $y = y' + z \in \mathbb{Q}$ then $(x_v)_v - y \in W$. □

This will be useful later; the fact that this quotient is compact means that we can do harmonic analysis on it.

So far we've treated the case $F = \mathbb{Q}$. In general, one has a very similar construction. First note that the profinite completion of the group of $\mathcal{O}_F$ is

$$\widehat{\mathcal{O}}_F = \varprojlim_{\mathfrak{p}} \mathcal{O}_F/\mathfrak{p} = \varprojlim_{n>0} \mathcal{O}_F/n\mathcal{O}_F$$

Definition 4.1.10. The *ring of finite F-adeles* is

$$\mathbb{A}_F^{\text{fin}} := \widehat{\mathcal{O}}_F \otimes_{\mathcal{O}_F} F = \prod_{\mathfrak{p}}{}' F_\mathfrak{p}$$

(taken with respect to $\mathcal{O}_{F_\mathfrak{p}}$) and the *ring of F-adeles* is

$$\mathbb{A}_F := F_\mathbb{R} \otimes \mathbb{A}_F^{\text{fin}} = \prod_v{}' F_v$$

where v now runs over *all* places of F, both finite and infinite.

Exercise 4.1.11. Adapt the proof of Proposition 4.1.9 to show that $F \subseteq \mathbb{A}_F$ is discrete and cocompact. (hint: you'll want to replace $[0, 1]$ with a fundamental domain for the full lattice $\mathcal{O}_F \subseteq F_\mathbb{R}$.

4.2. Idéles and class groups.

The adèles will let us do a certain type of Fourier analysis, which is useful when studying ζ-functions. On the other hand, there is a connection between the adèles and class groups that lets us state class field theory in a succinct way. For this we need to introduce the idèles.

Definition 4.2.1. If F is a number field, then the *group of idèles* is $\mathbb{I}_F = \mathbb{A}_F^\times$. In other words

$$\mathbb{I}_F = \left\{(x_v)_v : x_v \in \mathcal{O}_F^\times \text{ for almost all finite } v\right\}$$

In other words, $\mathbb{I}_F$ is the restricted direct product of $(F_v, \{1\})$ when v is an infinite place and $(F_v, \mathcal{O}_{F_v})$ when v is a finite place. We equip $\mathbb{I}_F$ with the restricted product topology.

Remark 4.2.2. Warning: the topology on $\mathbb{I}_F$ is *not* the same as the subspace topology on $\mathbb{A}_F^\times$! To see this note that we may write

$$\mathbb{I}_F = \varinjlim_S \mathbb{I}_{F,S}$$

where $\mathbb{I}_{F,S} = \prod_{v \in S} F_v^\times \times \prod_{v \notin S \text{ finite}} \mathcal{O}_{F_v}^\times$ where S is a finite set of places. Then $\mathbb{I}_{F,S}$ is by definition open in $\mathbb{I}_F$ but it is not the intersection of $\mathbb{I}_F$ with an open subset of $\mathbb{A}_F$. This is because any open subset of $\mathbb{A}_F$

must contain a basic open set $U = \prod_{v \in S'} U_v \times \prod_{v \notin S'} \mathcal{O}_{F_v}$ for some other finite set S' of places. But now construct an element $(x_v) \in U$ such that $x_v \neq 0$ for all v and $x_v \in \mathcal{O}_{F_v}^\times$ for almost all v. Then x_v is invertible in $\mathbb{A}_F$ (note that its inverse will *not* necessarily lie in U again!). Now further require that $x_v \in \mathfrak{m}_{F_v}$ for some $v \notin S$. Then $(x_v) \notin \mathbb{I}_{F,S}$.

Exercise 4.2.3. Show that the embedding

$$\begin{aligned} \mathbb{I}_F &\to \mathbb{A}_F \times \mathbb{A}_F \\ x &\mapsto (x, x^{-1}) \end{aligned}$$

is a topological isomorphism onto its image equipped with the subspace topology on $\mathbb{A}_F \times \mathbb{A}_F$.

Remark 4.2.4. Note that as a group, $\mathbb{I}_F = \mathrm{GL}_1(\mathbb{A}_F)$. The topology can then be described as follows. Suppose A is a topological ring and X is an affine scheme. Then we define a topology on $X(A)$ by forcing $f(A) : X(A) \to A$ to be continuous for all morphisms $f : X \to \mathbb{A}^1$.

Since each $F_v^\times$ is locally compact and each $\mathcal{O}_{F_v}^\times$ is compact, $\mathbb{I}_F$ is a locally compact topological group. One of its main features is that it recovers class groups via the following construction.

Note that for any $\alpha \in F^\times$ the image $\alpha \in \mathbb{A}_F$ is invertible, since it factors into finitely many prime ideals. So the embedding $F \hookrightarrow \mathbb{A}_F$ induces an embedding $F^\times \hookrightarrow \mathbb{I}_F$.

Definition 4.2.5. The image of $F^\times \to \mathbb{I}_F$ is called the *principal idèles*. The *idèle class group* is

$$C_F := \mathbb{I}_F / F^\times.$$

Exercise 4.2.6. Show that $F^\times$ is discrete inside $\mathbb{I}_F$. (hint: it's similar to the reason F is discrete in $\mathbb{A}_F$)

To justify this definition, note that there is a map

$$\begin{aligned} \mathbb{I}_F &\to J_F \\ x &\mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})} \end{aligned}$$

where J_F denotes the group of fractional ideals. This is well-defined because all but finitely many $x_\mathfrak{p}$ land in $\mathcal{O}_{F_\mathfrak{p}}^\times$ and thus have $\mathfrak{p}$-adic valuation 0.

Exercise 4.2.7. Show that the above map is continuous for the discrete topology on the target.

Moreover, this map is clearly surjective; its kernel is $\mathbb{I}_{F,S_\infty}$ where S_∞ is the set of all infinite places. Note further that the image of $\alpha \in F^\times$ under the above map is the principal fractional ideal $(\alpha) \in J_F$, and thus we get a surjection

$$C_F \to J_F / P_F =: \mathrm{Cl}(F).$$

Remark 4.2.8. The kernel of the map $\mathbb{I}_F \to \mathrm{Cl}(F)$ is $\mathbb{I}_{F,S_\infty} F^\times$, which is an open subgroup. But what about the other kinds of class groups? The Hilbert class field had no ramification, but the ray class groups had some restricted ramification. It turns out that $\mathbb{I}_F$ can handle these as well. If $\mathfrak{m}$ is a finite formal product of places and the finite part of $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_f$ is $\mathfrak{m}_f = \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$, then let

$$U_\mathfrak{m} = \left(\prod_{v \mid \mathfrak{m} \text{ real}} \mathbb{R}_{>0}^\times \right) \times \left(\prod_{\text{other infinite } v} F_v^\times \right) \times \left(\prod_{\mathfrak{p} \mid \mathfrak{m} \text{ finite}} 1 + \mathfrak{p}_\mathfrak{p}^e \mathcal{O}_{F_\mathfrak{p}} \right) \times \left(\prod_{\mathfrak{p} \notin S \text{ finite}} \mathcal{O}_{F_\mathfrak{p}}^\times \right)$$

This is an open subgroup of $\mathbb{I}_F$ by definition and induces an isomorphism

$$\mathbb{I}_F / F^\times U_\mathfrak{m} \xrightarrow{\sim} J_F^\mathfrak{m} / P_F^\mathfrak{m} = \mathrm{Cl}^\mathfrak{m}(F).$$

Proof. Note

$$\mathbb{I}_F/U_{\mathfrak{m}} = J_F^{\mathfrak{m}} \times \prod_{v|\mathfrak{m}\text{ real}} \mathbb{R}^\times/\mathbb{R}^\times_{>0} \times \prod_{\mathfrak{p}|\mathfrak{m}_f} F_v^\times/(1+\mathfrak{p}^{e_\mathfrak{p}}\mathcal{O}_{F_\mathfrak{p}})$$

with S the union of the places dividing $\mathfrak{m}$ and the infinite places. To see this, note that $F_v^\times$ is killed for all complex v and real $v \nmid \mathfrak{m}$, and for finite $\mathfrak{p} \nmid \mathfrak{m}_f$ we get a copy of $F_\mathfrak{p}^\times/\mathcal{O}_{F_\mathfrak{p}}^\times \cong \mathbb{Z}$, so we get a copy of $\mathbb{Z}$ for each prime $\mathfrak{p} \nmid \mathfrak{m}_f$. But note that $J_F^{\mathfrak{m}}$ is by definition the free abelian group on the finite $\mathfrak{p} \nmid \mathfrak{m}_f$. There is an exact sequence

$$0 \to F^{\times,\mathfrak{m}} \to F^\times \to \prod_{v|\mathfrak{m}\text{ real}} \mathbb{R}^\times/\mathbb{R}^\times_{>0} \times \prod_{\mathfrak{p}|\mathfrak{m}_f} F_\mathfrak{p}^\times/(1+\mathfrak{p}^{e_\mathfrak{p}}\mathcal{O}_{F_\mathfrak{p}}) \to 0$$

with $F^{\times,\mathfrak{m}} = \{\alpha \in F^\times : \alpha \equiv 1 \mod \mathfrak{m}_f \text{ and } \tau(\alpha) > 0 \text{ for } \tau \in \mathfrak{m}_\infty \text{ real}\}$. So

$$\begin{aligned}\mathbb{I}_F/U_{\mathfrak{m}}F^\times &\xrightarrow{\sim} \left(J_F^{\mathfrak{m}} \times \prod_{v|\mathfrak{m}\text{ real}} \mathbb{R}^\times/\mathbb{R}^\times_{>0} \times \prod_{\mathfrak{p}|\mathfrak{m}_f} F_v^\times/(1+\mathfrak{p}^{e_\mathfrak{p}}\mathcal{O}_{F_\mathfrak{p}})\right)/\operatorname{im}(F^\times) \\ &= (J_F^{\mathfrak{m}} \times 1)/\operatorname{im}(F^{\times,\mathfrak{m}}) \\ &= J_F^{\mathfrak{m}}/P_F^{\mathfrak{m}} = \mathrm{Cl}^{\mathfrak{m}}(F).\end{aligned}$$

□

So as the above remark indicates, the idèle class group C_F gives us a way to glue together all of the ray class groups into one object, which will greatly simplify the formulation of class field theory.

Note that even though $\mathbb{A}_F/F$ is compact, its idèlic counterpart $\mathbb{I}_F/F^\times$ is not; it's still locally compact though. However, we can remedy this as follows.

There is a norm map

$$\begin{aligned}|\cdot|_{\mathbb{A}_F} : \mathbb{I}_F &\to \mathbb{R}_{>0} \\ (x_v)_v &\mapsto \prod_v |x_v|_v\end{aligned}$$

The product formula implies that $|x|_{\mathbb{A}_F} = 1$ for all $x \in F$.

Definition 4.2.9. The group of *norm-1 idèles* $\mathbb{I}_F^0$ is the kernel of the map $|\cdot|_{\mathbb{A}_F} : \mathbb{I}_F \to \mathbb{R}_{>0}$. By the product formula we have $F^\times \subset \mathbb{I}_F^0$ and thus we can define

$$C_F^0 = \mathbb{I}_F^0/F^\times.$$

Proposition 4.2.10. *C_F^0 is compact.*

We omit the proof, which involves rephrasing Minkowski theory in an adelic way.

Corollary 4.2.11. *$\mathrm{Cl}(F)$ is finite.*

Proof. The point is that C_F^0 still surjects onto $\mathrm{Cl}(F)$. This is because C_F surjects onto $\mathrm{Cl}(F)$ and ignores the archimedean components, so if you pick a lift of a fractional ideal class to C_F you can adjust at the archimedean places to get norm 1. But then $C_F^0 \to \mathrm{Cl}(F)$ is a continuous surjection (by Exercise 4.2.7) from a compact set and $\mathrm{Cl}(F)$ has the discrete topology. □

We also get the following corollary, whose proof we omit.

Corollary 4.2.12 (Dirichlet's Unit Theorem)**.** *There is an exact sequence*

$$0 \to \mu_F \to \mathcal{O}_F^\times \to \mathbb{Z}^{r+s-1} \to 0$$

4.3. **Changing fields.** Before stating the main theorems of class field theory, we need to discuss what happens when you change the field of definition of the adèles. If E/F is an extension of number fields, then how does $\mathbb{A}_E$ relate to $\mathbb{A}_F$?

There are a few things to say. First of all, there is a natural map $\mathbb{A}_F \to \mathbb{A}_E$. To construct it, pick $(x_v)_v \in \mathbb{A}_F$. Then its image is $(y_w)_w$ where w ranges over all of the places of E and $y_w = x_v$ if w restricts to v.

Exercise 4.3.1.

(1) Show that with the map described above, the following diagram commutes:

$$\begin{tikzcd}
F \arrow[r] \arrow[d] & E \arrow[d] \\
\mathbb{A}_F \arrow[r] & \mathbb{A}_E
\end{tikzcd}$$

(2) Show that the natural map
$$\mathbb{A}_F \otimes_F E \to \mathbb{A}_E$$
is an isomorphism. To do this, first show that a basis $\alpha_1, \ldots, \alpha_n$ of E over F makes $\mathbb{A}_E$ into a free $\mathbb{A}_F$-module of rank n (hint: focus on a single place v of F at a time and consider $\prod_{w|v} E_v$ as a F_v-vector space).

In particular we get an induced map $\mathbb{I}_F \to \mathbb{I}_E$ and $C_F \to C_E$.

So that gives a way to get from F to E, so to speak. What about the other way? Let's try to get from E back down to F using a Galois action.

Any element $g \in \mathrm{Aut}(E/F)$ acts on $\mathbb{A}_E$. To see this, note firstly that if v is a place of F then g permutes the places w of E lying over v and naturally defines an isomorphism $g : E_w \to E_{g\cdot w}$, and $g \cdot w$ also restricts to v. This is essentially because $|x|_w = |g(x)|_{g\cdot w}$ for any $x \in E$. But since $\mathbb{A}_E$ consists of elements of E_w for every w, g naturally acts (from the left) on $\mathbb{A}_E$ (and $\mathbb{I}_E$) by
$$g((x_w)_w) = (g(x_{g^{-1}\cdot w}))_w$$
and fixes $\mathbb{A}_F$ because if $(x_w)_w \in \mathrm{im}(\mathbb{A}_F \to \mathbb{A}_E)$ then $x_w \in F_v$ for $w \mid v$ and $x_w = x_{w'}$ for all $w, w' \mid v$. Furthermore since $C_E = \mathbb{I}_E/E^\times$, g acts on C_E as well. More generally if $g \in \mathrm{Gal}(\overline{F}/F)$ then you get isomorphisms
$$\mathbb{A}_E \to \mathbb{A}_{g(E)}, \quad \mathbb{I}_E \to \mathbb{I}_{g(E)}, \quad C_E \to C_{g(E)}.$$

Proposition 4.3.2. *If E/F is Galois with Galois group G then $\mathbb{A}_E^G = \mathbb{A}_F$ and $\mathbb{I}_E^G = \mathbb{I}_F$.*

Proof. Pick an adele $(x_w)_w \in \mathbb{A}_E$. Pick a place v of F and w lying over it. Note that the decomposition group $G_w = \{g \in G : g \cdot w = w\}$ is isomorphic to $\mathrm{Gal}(E_w/F_v)$ and this isomorphism preserves the action on E_w. So since x_w is fixed by every $g \in G_w$ it is also fixed by every $g \in \mathrm{Gal}(E_w/F_v)$ and thus $x_w \in F_v$. But G also permutes the w lying over v, so $x_w = x_{w'}$ for all w, w' lying over v. But this is exactly the image of $\mathbb{A}_F$ in $\mathbb{A}_E$. The same proof works for $\mathbb{I}_E$. □

In fact the map $C_F \to C_E$ is injective because $E^\times \cap \mathbb{I}_F = F^\times$, which follows from the fact that $E \cap \mathbb{A}_F = F$.

Exercise 4.3.3. Show that $E \cap \mathbb{A}_F = F$. This basically amounts to unraveling the definitions.

Corollary 4.3.4. *If E/F is Galois with Galois group G then $C_E^G = C_F$.*

Proof. The short exact sequence $0 \to E^\times \to \mathbb{I}_E \to C_E \to 0$ of G-modules yields the long exact sequence
$$0 \to F^\times \to \mathbb{I}_F \to C_E^G \to H^1(\mathrm{Gal}(E/F), E^\times) = 0$$
by Hilbert 90 so $C_E^G = \mathbb{I}_F/F^\times = C_F$. □

Remark 4.3.5. Corollary 4.3.4 is something specific to the adèlic formalism because in general if E/F is Galois then the map

$$\mathrm{Cl}(F) \to \mathrm{Cl}(E)^G$$

is neither injective nor surjective. For instance, if you take F to be a field with $h_F > 0$ then the map $\mathrm{Cl}(F) \to \mathrm{Cl}(E)$ is trivial if E is the Hilbert class field.

4.4. **Norm and trace.** Recall that in local class field theory we classified finite extension via norm subgroups. We want to do something similar in the global setting, so we need to introduce norms and traces on adèles.

First let E/F be a Galois extension of number fields.

Definition 4.4.1. The *trace map* $\mathrm{tr}_{E/F} : \mathbb{A}_E \to \mathbb{A}_F$ and *norm map* $N_{E/F} : \mathbb{I}_E \to \mathbb{I}_F$ are

$$\mathrm{tr}_{E/F}(x) = \sum_{g \in \mathrm{Gal}(E/F)} g(x) \text{ and } N_{L/F}(x) = \prod_{g \in \mathrm{Gal}(EE/F)} g(x).$$

More generally if E/F is not Galois you can make the same definition by indexing over coset representatives of $\mathrm{Gal}(\overline{F}/E)$ inside $\mathrm{Gal}(\overline{F}/F)$.

On the level of components these maps are as follows:

$$(\mathrm{tr}_{E/F}(x))_v = \sum_{w|v} \mathrm{tr}_{E_w/F_v}(x_w) \text{ and } (N_{E/F}(x))_v = \prod_{w|v} N_{E_w/F_v}(x_w).$$

Remark 4.4.2. If you view $\mathbb{A}_E$ as a free $\mathbb{A}_F$-module of rank $[E : F]$ then one can check that the trace of $\alpha \in \mathbb{A}_E$ is the trace of the endomorphism $\mathbb{A}_E \xrightarrow{\times\alpha} \mathbb{A}_E$, and if $\beta \in \mathbb{I}_E$ then the norm is the determinant of the endomorphism $\mathbb{A}_E \xrightarrow{\times\beta} \mathbb{A}_E$.

Exercise 4.4.3. Check that the norm induces a map $N_{E/F} : C_E \to C_F$.

4.5. **Statement of adélic class field theory.** With this machinery developed, we can state the main theorems of adèlic class field theory.

Theorem 4.5.1 (Reciprocity). *There is a canonical map $r_F : C_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ which induces, for each E/F Galois, an isomorphism*

$$r_{E/F} : C_F/N_{E/F}C_E \to \mathrm{Gal}(E/F)^{\mathrm{ab}}.$$

Moreover, $N_{E/F}C_E$ is an open subgroup of C_F.

Theorem 4.5.2 (Existence). *If $H \leq C_F$ is open of finite index then there is a finite extension E/F such that $H = N_{E/F}C_E$.*

Theorem 4.5.3 (Norm limitation). *If E/F is finite Galois then $N_{E/F}C_E = N_{F'/E}C_{F'}$ where F' is the maximal abelian extension of F in E.*

4.6. **Abstract class field theory.** We won't give all of the details of the proof of global class field theory, but we at least want to give a sketch of how it goes. In fact, the way we'll do it will use the formalism of "abstract class field theory", which abstracts away some of the machinery from the local and global settings.

To run the machine you need the following data:

- G a profinite group.
- A G-module A.

If $K \leq H \leq G$ are two open subgroups, there is a *norm map*

$$\begin{aligned} N_{K/H} : A^K &\to A^H \\ a &\mapsto \sum_g a^g \end{aligned}$$

where g runs over a set of coset representatives of K in H.

Then you need more data:

- A continuous surjection $d : G \to \widehat{\mathbb{Z}}$.
- A *valuation* map $v : A^G \to \widehat{\mathbb{Z}}$ satisfying
  - the image Z of v contains $\mathbb{Z}$ and $Z/nZ = \mathbb{Z}/n\mathbb{Z}$ for all $n > 0$
  - for every open subgroup $H \leq G$, $v(N_{H/G}(A^H)) = [d(G) : d(H)]Z$.

Definition 4.6.1. We say that (G, A) satisfies the *class field axiom* if for every tower of open subgroups $K \leq H \leq G$ such that K is normal in H and H/K is cyclic, we have

$$\#H^i_T(H/K, A^K) = \begin{cases} [H : K] & i \text{ even} \\ 1 & i \text{ odd} \end{cases}$$

Remark 4.6.2. This should look familiar, because it directly abstracts local class field theory. Let $K/\mathbb{Q}_p$ be a finite extension.

- Let $G = G_K = \mathrm{Gal}(\overline{K}/K)$.
- Let $A = \overline{K}^\times$
- Let $d : G_K \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \widehat{\mathbb{Z}}$.
- Let $v : K^\times \xrightarrow{v_K} \mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$.

Our Tate cohomology computations from earlier in the course showed that (G, A) satisfies the class field axiom. Also $Z = \mathbb{Z}$ and $N_{L/K}(L) = f_{L/K}\mathbb{Z}$ by considering uniformizers, so the axioms are all satisfied.

Remember that when we proved local class field theory we performed a reduction to the unramified case, and then the cyclic case; in general, one abstracts the notion of "unramified" using the map d, and one abstracts valuation theory using the map v. For example, one can define an abstract "inertia group" $I = \ker(d)$.

It turns out that just with this data, you can get all the statements of class field theory that you would want.

Theorem 4.6.3 (Abstract class field theory)**.** *Suppose we have (G, A, d, v) as above. Then for any open subgroup $H \leq G$ there exists a canonical map*

$$r : A^H \to H^{\mathrm{ab}}$$

called the abstract reciprocity map such that the composition $A^H \xrightarrow{r} H^{\mathrm{ab}} \to (H/K)^{\mathrm{ab}}$ maps $N_{H/K} \mapsto 0$ and induces an isomorphism

$$A^H/N_{K/H}A^K \xrightarrow{\sim} (H/K)^{\mathrm{ab}}.$$

The proof is an abstraction of the proofs that we gave in the local case. There is an analogous norm limitation and existence theorem as well.

Remark 4.6.4. Note that if you input $G = G_{\mathbb{Q}_p}$ and $A = \overline{\mathbb{Q}}_p^\times$ then you get local class field theory for *every finite extension $K/\mathbb{Q}_p$ at once*! That's one advantage of this machinery.

Exercise 4.6.5. Show that if k is a finite field and if $G = \mathrm{Gal}(\overline{k}/k)$, $A = \mathbb{Z}$ with the trivial action, $d : \mathrm{Gal}(\overline{k}/k) \to \widehat{\mathbb{Z}}$ is the usual isomorphism, and $v : \mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$ is the usual inclusion, then all of the axioms above are satisfied.

4.7. **Abstract to global.** So how do global fields fit into the abstract class field theory developed above? We need to specify (G, A, d, v), but the trickiest part is proving the class field axiom.

- Since we care about finite Galois extensions of number fields, a sensible choice is
$$G = G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$
- In the local case we had $A = \overline{K}^{\times}$ and got a map $A^{G_K} = K^{\times} \to G_K^{\mathrm{ab}}$. But in the global setting we ultimately want a map $C_F \to G_{\mathbb{Q}}^{\mathrm{ab}}$, so we need to find some huge module A such that $A^{G_F} = C_F$ for any finite extension $F/\mathbb{Q}$. But remember that we have natural inclusions $C_F \to C_E$ whenever E/F is a finite extension, so we let
$$A = \bigcup_{F/\mathbb{Q}\text{ finite}} C_F.$$
- For d we use the cyclotomic extensions. There is a surjective map
$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) = \mathrm{Gal}(\bigcup_n \mathbb{Q}(\zeta_n)/\mathbb{Q})$$
and the target is isomorphic to $\widehat{\mathbb{Z}}^{\times}$. But
$$\widehat{\mathbb{Z}}^{\times} = \prod_p \mathbb{Z}_p^{\times} \cong (\mu_2 \times \mathbb{Z}_2) \times \prod_{p>2} \mu_{p-1} \times \mathbb{Z}_p$$
(non-canonically). So if we kill all of the torsion parts we are left with $\prod_p \mathbb{Z}_p = \widehat{\mathbb{Z}}$. So d is the map
$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^{\times} \twoheadrightarrow \widehat{\mathbb{Z}} = \mathrm{Gal}(\mathbb{Q}_0^{\mathrm{cyc}}/\mathbb{Q})$$
where $\mathbb{Q}_0^{\mathrm{cyc}}$ is the extension cut out by the quotient, sometimes called the "small cyclotomic extension".
- One can show (exercise) that $I_{\mathbb{Q}} = \mathbb{Q}^{\times} \times \mathbb{R}_{>0}^{\times} \times \widehat{\mathbb{Z}}^{\times}$, so $C_{\mathbb{Q}} = \mathbb{R}_{>0}^{\times} \times \widehat{\mathbb{Z}}^{\times}$, and thus we can define
$$v : C_{\mathbb{Q}} \twoheadrightarrow \widehat{\mathbb{Z}}^{\times} = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_0^{\mathrm{cyc}}/\mathbb{Q}) = \widehat{\mathbb{Z}}.$$
Note here that we are using the *same* extension $\mathbb{Q}_0^{\mathrm{cyc}}$ when defining v and d.

The two things to check are the class field axiom, which is pretty subtle, and the compatibility between d and v, which is more straightforward.

To prove the class field axiom, we first show that if E/F is a cyclic extension of number fields, the Herbrand quotient $h(C_E)$ (as a $\mathrm{Gal}(E/F)$ module) is $[E : F]$. Since $h(C_E) = h^{\mathrm{even}}(C_E)/h^{\mathrm{odd}}(C_E)$, this implies the **First Inequality**
$$h^{\mathrm{even}}(C_E) \geq [E : F]$$
It then remains to show the **Second Inequality**.
$$h^{\mathrm{even}}(C_E) \leq [E : F]$$
and hence
$$h^{\mathrm{even}}(C_E) = [E : F]$$
and thus
$$h^{\mathrm{odd}}(C_E) = 1$$
Note that in local class field theory the last equality follows immediately from Hilbert 90, but this is much more complicated in the global case, and requires an actual argument.

4.8. **The first inequality.** Now let's show the first inequality. We just need to show that if E/F is cyclic, then we have $h(C_E) = [E : F]$; here $G_{E/F}$ is acting on C_E and $h(C_E)$ is the Herbrand quotient. So how do we compute this?

First we need a lemma.

Lemma 4.8.1. *There exists a finite set of places S of F such that*

$$\mathbb{I}_E = \mathbb{I}_{E,S} E^\times$$

where $\mathbb{I}_{E,S} = \mathbb{I}_{E,T}$ where T is the places of E lying over S.

Proof. Remember that $\mathbb{I}_E/\mathbb{I}_{E,T_\infty}E^\times \xrightarrow{\sim} \mathrm{Cl}(E)$ where T_∞ denotes the set of infinite places of E. Since $\mathrm{Cl}(E)$ is finite, it is generated by the image of finitely many elements $x_1, \dots, x_k$ of $\mathbb{I}_E$ under the above isomorphism. But $T_i = \left\{w : (x_i)_w \notin \mathcal{O}_{E_w}^\times\right\}$ is finite for each i, so we can take $T = T_\infty \cup \bigcup_{i=1,\dots,k} T_i$. Then by construction $\mathbb{I}_E/\mathbb{I}_{E,T}E^\times = 0$, and so we can take S to denote the places lying under T. □

By the isomorphism theorems,

$$C_E = \mathbb{I}_E/E^\times = \mathbb{I}_{E,S}E^\times/E^\times = \mathbb{I}_{E,S}/(\mathbb{I}_{E,S} \cap E^\times) = \mathbb{I}_{E,S}/\mathcal{O}_{E,S}^\times$$

so the exact sequence $0 \to \mathcal{O}_{E,S}^\times \to \mathbb{I}_{E,S} \to C_E \to 0$ yields $h(C_E) = h(\mathbb{I}_{E,S})/h(\mathcal{O}_{E,S}^\times)$.

So now it remains to compute these two Herbrand quotients separately:

- *Cohomology of the idèles*: we can write $\mathbb{I}_E = \varinjlim_S \mathbb{I}_{E,S}$ with S required to contain all infinite places and all places of F which are ramified in E. Tate cohomology commutes with direct limits, so $H_T^i(E/F, \mathbb{I}_E) = \varinjlim_S H_T^i(E/F, \mathbb{I}_{E,S})$. But

$$\begin{aligned} H_T^i(E/F, \mathbb{I}_{E,S}) &= \prod_{v\in S} H_T^i(E/F, \prod_{w|v} E_w^\times) \times \prod_{v\notin S} H_T^i(E/F, \prod_{w|v} \mathcal{O}_{E_w}^\times) \\ &\xrightarrow{\sim \text{ (Shapiro's Lemma)}} \prod_{v\in S} H_T^i(E_w/F_v, E_w^\times) \times \prod_{v\notin S} H_T^i(E_w/F_v, \mathcal{O}_{E_w}^\times) \\ &= \prod_{v\in S} H_T^i(E_w/F_v, E_w^\times) \end{aligned}$$

  where the last term vanishes by Corollary 3.2.7 because E_w/F_v is unramified for $v \notin S$. We also used the fact that for any place w lying over v we can identify

$$\mathrm{Ind}_{\mathrm{Gal}(E_w/F_v)}^{\mathrm{Gal}(E/F)} E_w^\times \cong \prod_{w|v} E_w^\times.$$

  (I'll leave this as an exercise, but the idea is that the decomposition group at w consists of exactly the Galois elements which fix the place w, But now finally note that by the analysis we did in the nonarchimedean local case we can conclude that

$$h^{\text{even}}(\mathbb{I}_{E,S}) = \prod_{v\in S}[E_w : F_v] \text{ and } h^{\text{odd}}(\mathbb{I}_{E,S}) = 1$$

  In the archimedean local case, just note that

$$H_T^0(\mathbb{C}/\mathbb{R}, \mathbb{C}^\times) \cong \mathbb{R}^\times/\mathbb{R}_{>0}^\times \cong \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad H_T^0(\mathbb{C}/\mathbb{C}, \mathbb{C}^\times) = 0.$$

- *Cohomology of the units*: We need to study $h(\mathcal{O}_{E,S}^\times)$ where

$$\mathcal{O}_{E,S}^\times = \left\{x \in E^\times : |x|_w = 1 \text{ for } w \notin T\right\}$$

  Let $V = \prod_{w\in T} \mathbb{R}$, and consider the map

$$\begin{aligned} \varphi : \mathcal{O}_{E,S}^\times &\to V \\ x &\mapsto (\log|\alpha|_w)_{w\in T} \end{aligned}$$

whose kernel is (by Dirichlet's unit theorem) exactly the group of roots of unity in E, which is finite. Furthermore, if we let $\mathrm{Gal}(E/F)$ act on V by permuting the $w \in T$, then φ is $\mathrm{Gal}(E/F)$-equivariant, so if M denotes the image of φ then $h(\mathcal{O}_{E,S}^\times) = h(M)$.

There are two natural full lattices in V. One is given by $N = \prod_{w \in T} \mathbb{Z}$. The other is the lattice generated by M and the vector $(1, \ldots, 1)$! Note M is contained in $V_0 = \{v \in V : \sum v_i = 0\}$. But Dirichlet's unit theorem says that $0 \to \mu_F \to \mathcal{O}_{E,S}^\times \to \mathbb{Z}^{\#S-1} \to 0$, and thus M is a full lattice in V_0, so $\langle M, (1, \ldots, 1)\rangle$ is a full lattice in V. Both lattices are $\mathrm{Gal}(E/F)$-stable. The statement thus boils down to the following lemma:

Lemma 4.8.2. *If V is a real vector space on which a finite cyclic group G acts linearly and L_1, L_2 are two G-stable lattices then $h(L_1) = h(L_2)$ whenever either number is defined.*

Proof. Omitted. A sketch of the proof; L_1 and L_2 become isomorphic after tensoring with $\mathbb{R}$, and you can use finiteness of G and G-stability to descend this isomorphism to $\mathbb{Q}$. This implies that some rational multiple of L_1 is isomorphic to some rational multiple of L_2. One can then show that this implies they differ by a chain of finite index inclusions, so they have the same Herbrand quotient. □

But $(1, \ldots, 1)$ is G-stable, so

$$h(N) = h(\langle M, (1, \ldots, 1)\rangle) = h(M \times \mathbb{Z}) = h(M)h(\mathbb{Z}) = [E : F]h(M)$$

and

$$h(N) = h(\mathrm{Hom}(T, \mathbb{Z})) = \prod_{v \in S} h(\mathrm{Hom}(G/G_w, \mathbb{Z})) = \prod_{v \in S} h(\mathrm{Ind}_{G_w}^G \mathbb{Z}) = \prod_{v \in S} h_{G_w}(\mathbb{Z}) = \prod_{v \in S} [E_w : F_v].$$

So finally we see that

$$h(\mathcal{O}_{E,S}^\times) = h(M) = \frac{h(N)}{[E : F]} = \frac{1}{[E : F]} \prod_{v \in S} [E_w : F_v].$$

In conclusion,

$$h(C_E) = \frac{h(\mathbb{I}_{E,S})}{h(\mathcal{O}_{E,S}^\times)} = [E : F].$$

4.9. **The second inequality.** We skip this, but note that one can reduce this to a statement about Dirichlet density of prime ideals — see https://kskedlaya.org/cft/sec_ideles-cohom2.html for the details.

4.10. **Local-global compatibility.** Now let's formulate a compatibility between local and global class field theory.

Theorem 4.10.1 (Local-global compatibility)**.** *If F is a number field and v is a place of F, then the diagram*

$$\begin{tikzcd} F_v^\times \arrow[r] \arrow[d] & C_F \arrow[d] \\ G_{F_v}^{\mathrm{ab}} \arrow[r] & G_F^{\mathrm{ab}} \end{tikzcd}$$

commutes.

Note that at the infinite places the map $\mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is just the sign map $x \mapsto x/|x|$, and $\mathbb{C}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{C})$ is just the unique trivial map. The map $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to G_F^{\mathrm{ab}}$ sends the non-trivial element to complex conjugation in $\overline{F}$.

This is proven by first showing the following.

Theorem 4.10.2. *Fix E/F a finite abelian extension of number fields. If $r_{E/F} : \mathbb{I}_F \to C_F \to \mathrm{Gal}(E/F)$ denotes the global reciprocity map from abstract class field theory and $r_{E_w/F_v} : F_v^\times \to \mathrm{Gal}(E_w/F_v)$ denotes the local reciprocity map for some (equivalently, any) choice of $w \mid v$ (for each v), then*

$$r_{E/F} = \prod_v r_{E_w/F_v}$$

Let's break this down. First of all, note that if v is a place of F then there is an embedding

$$\mathrm{Gal}(E_w/F_v) \hookrightarrow \mathrm{Gal}(E/F)$$

as the decomposition group for (any) w. Then since any $x \in \mathbb{I}_F$ satisfies $x_v \in \mathcal{O}_{F_v}^\times$ for almost all v and almost all $w \mid v$ is unramified, it follows that the product is well-defined.

Proof of Theorem 4.10.2. We will just prove local-global compatibility when $E \subseteq F_0^{\mathrm{cyc}}$. In this case, the setup of abstract class field theory gives us that $r_{E/F}$ is just

$$\mathbb{I}_F \to C_F \xrightarrow{v} \widehat{\mathbb{Z}} \xrightarrow{d^{-1}} \mathrm{Gal}(F_0^{\mathrm{cyc}}/F) \twoheadrightarrow \mathrm{Gal}(E/F)$$

But then you can just check "by hand" that these are the same, since you know what the Artin map is explicitly in the local case for cyclotomic extensions.

From here there is a way to reduce to the previous case, but for lack of time I will skip this for now. □

5. Langlands

Class field theory is supposed to be a 1-dimensional case of the Langlands program for GL_n. What does this mean?

Conjecture 5.0.1 (Langlands reciprocity for GL_n over F, rough form)**.** *For any irreducible continuous representation $\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\mathbb{C})$ there exists a cuspidal automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_F)$ such that $L(\pi, s) = L(\rho, s)$.*

Here $L(\rho, s)$ and $L(\pi, s)$ are the *L-functions* associated with ρ and π, which we'll discuss further. Moreover, there is a compatiblity with the "local Langlands correspondence", which we will discuss later.

5.1. Langlands for GL_1.

Let's first study 1-dimensional representations $G_F \to \mathbb{C}^\times$.

Lemma 5.1.1. *Any continuous map $\rho : G_F \to \mathbb{C}^\times$ factors through $G_F \to \mathrm{Gal}(E/F)$ for E/F a finite abelian extension.*

Proof. Since G_F is compact the image $\rho(G_F) \subset \mathbb{C}^\times$ is compact, and thus has to land in the circle $S^1 = e^{i\mathbb{R}}$. If we pick a tiny open neighborhood U of $1 \in \mathbb{C}^\times$ then the preimage of U is an open subset of G_F containing the identity, and thus must contain an open subgroup N. But if U is small enough, then U contains no nontrivial subgroups, so $\rho(N) = 1$ and thus $\ker \rho$ contains an open subgroup and is thus open. But $\ker \rho$ is normal, so $G_F / \ker \rho = \mathrm{Gal}(E/F)$ for some finite extension E/F. Furthermore $\mathrm{Gal}(E/F)$ embeds as a finite subgroup of S^1 and is therefore abelian, so E/F is abelian. □

Remark 5.1.2. In fact, roughly the same argument (one needs to show that small enough neighborhoods of 1 in $\mathrm{GL}_n(\mathbb{C})$ contain no nontrivial subgroups) shows that any continuous $\rho : G_F \to \mathrm{GL}_n(\mathbb{C})$ factors through $\mathrm{Gal}(E/F)$ for E/F finite, but not necessarily abelian in general.

By global class field theory, $C_F/N_F^E(C_E) \xrightarrow{\sim} \mathrm{Gal}(E/F)$, and thus we get a representation

$$\omega : \mathrm{GL}_1(\mathbb{A}_F) = \mathbb{A}_F^\times \twoheadrightarrow C_F \twoheadrightarrow C_F/N_F^E(C_E) \to \mathbb{C}^\times.$$

In fact this representation is *automorphic* in some precise sense, which we won't get into now.

The L-functions they define are constructed by taking

$$L(\rho, s) = \prod_{\mathfrak{p} \text{ unramified in } E} \frac{1}{1 - \rho(\mathrm{Frob}_{\mathfrak{p}})|\mathcal{O}_F/\mathfrak{p}|^{-s}}$$

and

$$L(\omega, s) = \prod_{\mathfrak{p} \text{ unramified for } \omega} \frac{1}{1 - \omega(\varpi_{\mathfrak{p}})|\mathcal{O}_F/\mathfrak{p}|^{-s}}$$

But remember that we have a commutative diagram

$$\begin{tikzcd} F_{\mathfrak{p}}^{\times} \arrow[r] \arrow[d] & C_F \arrow[d] \\ G_{F_{\mathfrak{p}}}^{\mathrm{ab}} \arrow[r] & G_F^{\mathrm{ab}} \end{tikzcd}$$

So if $\mathfrak{p}$ is unramified then $\omega(\varpi_{\mathfrak{p}}) = \rho(\mathrm{Frob}_{\mathfrak{p}})$ and thus the L-functions are equal.

There's far more to the story than what I just said; for example, there are other 1-dimensional representations of C_F which don't factor through a norm subgroup (and thus don't correspond to a Galois representation). But for now let's think a bit about GL_2.

5.2. **Two-dimensional case.** In the 2-dimensional case, we need to think about the relationship between $\rho : G_F \to \mathrm{GL}_2(\mathbb{C})$ and "automorphic representations of $\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A}_F)$". Without saying too much more for now, let me just mention that "automorphic representations" in this context are a generalization of *modular forms*, which we will define and discuss in more detail.

Then the 2-dimensional Galois representations are things that come from elliptic curves. But let's first talk about modular forms.

Let $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, the *complex upper half plane.* This space admits an action of the group $\mathrm{SL}_2(\mathbb{Z}) = \left\{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}) : ad - bc = 1\right\}$ by taking

$$\gamma \cdot z = \frac{az + b}{cz + d}.$$

Exercise 5.2.1. Check that this map is well-defined and gives a group action; in other words check that $\mathrm{Im}(\gamma \cdot z) > 0$ and that $(\gamma_1\gamma_2) \cdot z = \gamma_1 \cdot (\gamma_2 \cdot z)$.

Remark 5.2.2. One could also act by the group $\mathrm{SL}_2(\mathbb{R})$, or even $\mathrm{GL}_2^+(\mathbb{R}) = \{M \in \mathrm{GL}_2(\mathbb{R}) : \det M > 0\}$. There is not much difference between the GL_2^+ and SL_2-actions really, because every matrix in $\mathrm{GL}_2^+(\mathbb{R})$ can be written $\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)M$ for some $r \in \mathbb{R}_{>0}$ and $M \in \mathrm{SL}_2(\mathbb{R})$, but

$$\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \cdot z = z.$$

Why is it interesting to note this? Well, $\mathrm{SL}_2(\mathbb{R})$ acts transitively on $\mathcal{H}$ because $\left(\begin{smallmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{smallmatrix}\right) \cdot i = x + iy$. So $\mathrm{Stab}_i \backslash \mathrm{SL}_2(\mathbb{R}) \cong \mathcal{H}$, and one can check that $\mathrm{Stab}_i = \mathrm{SO}_2(\mathbb{R})$.

Exercise 5.2.3. Check that $\mathrm{Stab}_i = \mathrm{SO}_2(\mathbb{R})$, i.e. the circle group. Check that

$$\mathcal{H} = \mathrm{SO}_2(\mathbb{R})\backslash \mathrm{SL}_2(\mathbb{R}) = Z^+(\mathbb{R})\,\mathrm{SO}_2(\mathbb{R})\backslash \mathrm{GL}_2^+(\mathbb{R}) = Z(\mathbb{R})O_2(\mathbb{R})\backslash \mathrm{GL}_2(\mathbb{R})$$

where $Z(\mathbb{R})$ denotes the center of $\mathrm{GL}_2(\mathbb{R})$. This will be important to note when we talk about the connection between modular forms and the adelic group; one can also express $\mathcal{H}$ as a certain coset space of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$.

How can one visualize this action?

Exercise 5.2.4. Show that $\mathrm{SL}_2(\mathbb{Z})$ is generated by $T = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$. Hint: use the division algorithm and the fact that

$$\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a+cn & b+dn\\ c & d\end{pmatrix}$$

to reduce to the case of an upper triangular matrix.

(draw upper half plane model)

Here's a hallucination to motivate the definition of modular forms: if G is a group and S is a set, then G acts (from the left) on the space of functions $G \to S$ by taking

$$(g \cdot f)(h) = f(hg).$$

Now if $S = K$ is a field then $\mathsf{Fun}(G, K) = \{f : G \to K\}$ forms a K-vector space, usually not finite dimensional, and G acts K-linearly. We can thus hope to find interesting representations of G on K-vector spaces by considering interesting subsets $V \subset \mathsf{Fun}(G, K)$ which are G-stable. In fact this a completely natural thing to do because if V is an irreducible representation of G then

$$0 \neq \mathrm{Hom}_K(V, K) = \mathrm{Hom}_1(V|_1, 1) = \mathrm{Hom}_G(V, \mathrm{coInd}_1^G 1) = \mathrm{Hom}_G(V, \mathsf{Fun}(G, K))$$

(here 1 denotes the trivial group) and thus there is a nonzero map $V \to \mathsf{Fun}(G, K)$, which must be injective since V is irreducible. So any representation can be considered as a subspace of the space of functions.

Now if we apply this setup to $G = \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ and $K = \mathbb{C}$, we can (roughly) recover the definition of an automorphic representation, as long as we put a huge list of conditions on the functions $f : \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) \to \mathbb{C}$ that appear in a given V, and a huge list of conditions on the G-action on V as well.

But that means that we probably care about functions $f : \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) \to \mathbb{C}$. I've already told you that $\mathcal{H}$ can appear as a coset space for $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$, and it turns out that some of the interesting functions we'll want to consider factor through this quotient. So in conclusion, we are led to consider functions

$$f : \mathcal{H} \to \mathbb{C}$$

subject to some conditions. One of the conditions is that f is *almost* invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, but not quite; instead it satisfies a transformation property with respect to this action.

Definition 5.2.5. A *modular form* of level 1 and weight $k > 0$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ satisfying:

(1) $f(\gamma \cdot z) = (cz + d)^k f(z)$

(2) f is bounded as $z \to i\infty$.

Remark 5.2.6.

- There are modular forms of higher level; for this, we replace $\mathrm{SL}_2(\mathbb{Z})$ with certain well-chosen finite index subgroups.
- If you consider $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$ you get that $f(z) = (-1)^k f(z)$, so if k is odd then $f = 0$. Note that if you pick a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ then this doesn't always happen.
- If you consider $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ you get that $f(-1/z) = z^k f(z)$.
- If you consider $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ then you get that $f(z+1) = f(z)$. This means that $f(z)$ is periodic of period 1 and thus admit a Fourier series, so we can write

$$f(z) = \sum_{i=0}^{\infty} a_n q^n$$

where $q = e^{2\pi i z}$. Note further that the holomorphic map $z \mapsto e^{2\pi i z}$ takes $\mathcal{H} \to D^\star = \{q \in \mathbb{C}^\times : |q| < 1\}$ so f can be regarded as a holomorphic function on D^*. The fact that f is bounded as $z \to i\infty$ means that f actually extends to the whole disk $D = \{q \in \mathbb{C} : |q| < 1\}$. We say that f is a *cusp form* if f vanishes at the center of the disk. This is equivalent to $a_0 = 0$.

Example 5.2.7. Generally speaking, examples of modular forms are hard to write down. Here is the simplest one:

$$E_k(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m+nz)^k}$$

This is called an *Eisenstein series of weight* k, and it is *not* a cusp form. The first nonzero cusp form of level 1 is of weight 12 and is equal to

$$\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n).$$

5.3. **Modular forms of other levels.** Above we defined a modular form for the group $\mathrm{SL}_2(\mathbb{Z})$. But if you take certain finite index subgroups, then you can make the same definition.

Definition 5.3.1. The *principal congruence subgroup* of level $N \geq 1$ is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod N \text{ and } b \equiv c \equiv 0 \mod N \right\}.$$

We define two other groups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod N \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod N \text{ and } c \equiv 0 \mod N \right\}.$$

Clearly $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \mathrm{SL}_2(\mathbb{Z})$. Each of these inclusions is a finite index subgroup. For instance, the $\Gamma_0(N)$ is the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$.

Definition 5.3.2. A modular form of weight k and level Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

(1)

We denote by $M_k(\Gamma)$ and $S_k(\Gamma)$ the space of modular forms and cusp forms respectively.

The groups $\Gamma_0(N)$ and $\Gamma_1(N)$ are examples of *congruence subgroups*, i.e. subgroups of $\mathrm{SL}_2(\mathbb{Z})$ which contain a $\Gamma(N)$ for some N. If you take $\mathcal{H}$ and you quotient by the action of Γ for some congruence subgroup you get the *modular curve of level* Γ, denoted $Y_\Gamma = \mathcal{H}/\Gamma$. These are Hausdorff topological spaces, and actually naturally form Riemann surfaces. They are not themselves compact, but they admit natural compactifications by taking $\mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ and topologizing this in a rather natural way.

In any case, this picture is set up in such a way that

$$H^i(\Gamma, M) = H^i_{\mathrm{sing}}(Y_\Gamma, \widetilde{M}).$$

Here M is a (discrete) Γ-module, and the left hand side is group cohomology, and the right hand side is singular cohomology of the topological space Y_Γ. The local system $\widetilde{M}$ is defined as $\widetilde{M} = (\mathcal{H} \times M)/\Gamma$, and there is a notion of *singular cohomology with coefficients in a local system.*

Why am I mentioning this? Well, remember that modular forms are functions on $\mathcal{H}$ which satisfy a transformation property. It turns out that you can interpret modular forms as cohomology classes! More precisely, there is an isomorphism called the *Eichler-Shimura isomorphism*

$$H^i(Y_\Gamma, V_k) \xrightarrow{\sim} S_k(\Gamma) \oplus M_k(\Gamma)$$

This gives a kind of hint about how you would compute the dimension of spaces of modular forms; these dimensions are intimately related to the geometry of modular curves.

5.4. **Elliptic curves.** Now let's talk a bit about the phenomenon known as "modularity" of elliptic curves.

Definition 5.4.1. Over a field K of characteristic 0, an *elliptic curve* is the algebraic variety defined by an equation of the form

$$y^2 = f(x)$$

where $f(x)$ is a degree 3 polynomial with no repeated roots (i.e. with non-zero discriminant).

Equivalently, it turns out that these can be defined as smooth projective curves of genus 1 with a marked point.

Take the example of $y^2 + y = x^3 - x^2$ considered over $\mathbb{Q}$. There exists a change of coordinates into something of the form $y^2 = f(x)$ which is nonsingular. The $f(x)$ that you get has discriminant -11.

Let's consider what happens if you try to solve this equation mod p for all prime numbers p. If $p \mid \Delta$ then the equation $f(x)$ reduces to something which has repeated roots, so you no longer get an elliptic curve. But if not, then $\Delta \neq 0 \mod p$ so you get an elliptic curve defined over $\mathbb{F}_p$. Since $\mathbb{F}_p$ is a finite field, you can just count the number of solutions to this equation!

Let $a_p(E) = p + 1 - N_p$ where N_p denotes 1 plus the number of solutions to the equation $y^2 - y = x^3 - x^2$ mod p (you also have to include the point at infinity which is where the 1 comes from). This is something you can compute on a computer!

$-2, -1, 1, -2, 1, 4, -2, 0, -17(2017), 284(100003)$.

On the other hand, one can consider the modular form

$$\eta(z)^2(\eta)\eta(11z)^2 = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2.$$

This is a modular form of level $\Gamma_0(11)$. Its q-expansion coefficients are exactly the $a_p(E)$!

5.5. **Modular curves and Jacobians.**

References

[Neu99] Neukirch, Jürgen. *Algebraic number theory.* Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. URL: https://doi.org/10.1007/978-3-662-03983-0 (cit. on pp. 5, 9).