Notes for Algebraic Number Theory
Instructor: Chao Li

Henry Liu

May 1, 2017

Abstract

These are my live-texed notes for the Spring 2017 offering of MATH GR6657 Algebraic Number Theory. Let me know when you find errors or typos. I'm sure there are plenty.

Chapter 1

Motivation

1.1 Primes $p = x^2 + ny^2$

Which primes p can be written as the sum $x^2 + y^2$ of two squares? For $p \neq 2$, it turns out $p = x^2 + y^2$ iff $p \equiv 1 \bmod 4$. Fermat discovered this phenomenon. Similarly,

$$\begin{aligned} 2 \neq p = x^2 + 2y^2 &\iff p \equiv 1, 3 \bmod 8 \\ 3 \neq p = x^2 + 3y^2 &\iff p \equiv 1 \bmod 3 \\ 2, 5 \neq p = x^2 + 5y^2 &\iff p \equiv 1, 9 \bmod 20. \end{aligned}$$

These results are really phenomena of class field theory. Let's reinterpret them in terms of number fields. Write

$$p = x^2 + y^2 = (x + iy)(x - iy) \in \mathbb{Z}[i],$$

the ring of integers of the number field $\mathbb{Q}(i)$. So $p = x^2 + y^2$ implies the ideal $(p) = \mathfrak{p}_1\mathfrak{p}_2$ decomposes in $\mathbb{Z}[i]$. In general, for the results above, we work with the number field $k \coloneqq \mathbb{Q}(\sqrt{d})$ for $d \equiv 0, 1 \bmod 4$, called the discriminant of K. These are three possibilities:

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \text{(split), } x^2 \equiv d \bmod p \text{ has solution} \\ \mathfrak{p} & \text{(inert), } x^2 \equiv d \bmod p \text{ has no solution} \\ \mathfrak{p}^2 & \text{(ramified), } p \div d. \end{cases}$$

In other words, the splitting behavior of p in $K = \mathbb{Q}(\sqrt{d})$ is controlled by solving the equation $x^2 \equiv d \bmod p$. Define the Legendre symbol

$$\left(\frac{d}{p}\right) \coloneqq \begin{cases} +1 & x^2 \equiv d \bmod p \text{ has solution} \\ -1 & x^2 \equiv d \bmod p \text{ has no solution} \\ 0 & p \mid d, \end{cases}$$

and recall Gauss's quadratic reciprocity:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \quad \forall p, q \text{ odd primes.}$$

Something miraculous is happening here. If we want to solve $x^2 \equiv q \bmod p$, this is somehow related to solving $x^2 \equiv p \bmod q$. In a real problem, q is fixed and often very small, so this second equation is much simpler. For example,

$$\left(\frac{-3}{p}\right) = +1 \iff x^2 \equiv p \bmod 3 \iff p \equiv 1 \bmod 3,$$

and this is exactly the congruence condition for $p = x^2 + 3y^2$. The motivation of **class field theory (CFT)** is to generalize this picture. Namely, given a number field K, relate the splitting behavior of p in K to some congruence condition on p. Some examples:

$$\begin{aligned} p \text{ splits in } \mathbb{Q}(\sqrt{-5}) &\iff p \equiv 1, 3, 7, 9 \bmod 20 \\ p \text{ splits in } \mathbb{Q}(\sqrt{-5}, i) &\iff p \equiv 1, 9 \bmod 20 \\ p \text{ splits in } \mathbb{Q}(\zeta_5) &\iff p \equiv 1 \bmod 5. \end{aligned}$$

However, whether there is a congruence condition for whether p splits in $\mathbb{Q}(\sqrt[3]{2})$ is unknown. One key difference between this example and the above three examples is whether $K/\mathbb{Q}$ is Galois. In addition, the Galois closure of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, which has Galois group S_3 over $\mathbb{Q}$. This is not abelian, whereas the other examples are.

Definition 1.1.1. A field extension L/K is **abelian** if L/K is Galois and has abelian Galois group $\mathrm{Gal}(L/K)$.

Class field theory studies abelian extensions, for which we can always obtain congruence relations describing the splitting of primes. It gives a vast generalization of quadratic reciprocity called Artin reciprocity.

1.2 A special case of CFT

Recall that the **class group** Cl_K of a number field K is

$$\mathrm{Cl}_K \coloneqq \{\text{fractional ideals of } K\}/K^\times.$$

Eventually we want to understand all abelian extensions of K, but for now let's look at those which are unramified, i.e. all the primes of K stay unramified.

Definition 1.2.1. A finite unramified abelian extension L/K is a **class field** for a subgroup $H \subset \mathrm{Cl}_K$ if

$$\mathfrak{p} \text{ splits in } L/K \iff [\mathfrak{p}] \in H \subset \mathrm{Cl}_K\,.$$

Theorem 1.2.2. *Given a subgroup $H \subset \mathrm{Cl}_K$, the class field for H exists and is unique. Moreover, any finite unramified abelian extension arises as a class field.*

Hence there is a bijection

$$\{\text{unramified abelian extensions } L/K\} \leftrightarrow \{\text{subgroups } H \subset \mathrm{Cl}_K\}.$$

This bijection is called the Artin reciprocity map. In particular, $\mathrm{Gal}(L/K) \cong \mathrm{Cl}_K\,/H$, and p splits in L/K iff $[p]$ is trivial in $\mathrm{Cl}_K\,/H$.

Example 1.2.3. For $K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, the class group Cl_K is trivial, so there is only the trivial unramified abelian extension. For $K = \mathbb{Q}(\sqrt{-5})$, the class group is $\mathrm{Cl}_K = \mathbb{Z}/2$. Hence there are the trivial and the maximal unramified abelian extensions. The maximal one has degree 2.

Definition 1.2.4. The maximal unramified abelian extension of K is called the **Hilbert class field** of K, denoted H_K. In particular, $\mathrm{Gal}(H_K/K) = \mathrm{Cl}_K$, i.e. H trivial.

Example 1.2.5. For $K = \mathbb{Q}(i)$, the Hilbert class group is the trivial extension, so $H_K = K$. For $K = \mathbb{Q}(\sqrt{-5})$, the Hilbert class group has degree 2, so $H_K = \mathbb{Q}(\sqrt{-5}, \sqrt{d})$ for some d. Since H_K must be unramified over K, we must have $d = -1$. So $H_K = \mathbb{Q}(\sqrt{-5}, i)$.

1.3 Back to $p = x^2 + ny^2$

We know already that

$$p = x^2 + ny^2 \implies p \text{ splits in } K = \mathbb{Q}(\sqrt{-n}).$$

Example 1.3.1. Let $n = 5$. We stated earlier that

$$p \text{ splits in } K = \mathbb{Q}(\sqrt{-5}) \iff p \equiv 1, 3, 7, 9 \bmod 20.$$

If K had class number one, then every ideal is principal, so this would be precisely the condition for $p = x^2 + ny^2$. But in this case K does not, and 3 and 7 are not valid congruence classes. The failure is that in the factorization $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$, the ideals $\mathfrak{p}_1, \mathfrak{p}_2$ may not be principal.

Theorem 1.3.2. *$\mathfrak{p}_1, \mathfrak{p}_2$ are principal iff $\mathfrak{p}_1, \mathfrak{p}_2$ split in H_K.*

So we see that $p = x^2 + 5y^2$ iff p splits in $H_K = \mathbb{Q}(\sqrt{-5}, i)$. This is again an unramified abelian extension, from which we get the congruence condition $p \equiv 1, 9 \bmod 20$.

Example 1.3.3. If we try to do the same for $p = x^2 + 14y^2$, we find that $\mathrm{Cl}_K = \mathbb{Z}/6$, and $H_K/\mathbb{Q}$ is non-abelian (even though by definition H_K/K is abelian). There is no simple congruence criterion in this case.

Chapter 2

Local Fields

Suppose we want to study the number field $\mathbb{Q}$. Then we can take a larger field, e.g. $\mathbb{R}$, such that $\mathbb{Q} \hookrightarrow \mathbb{R}$. If we want to study arithmetic problems in $\mathbb{Q}$, we can study them in $\mathbb{R}$ instead. But of course this loses a lot of information. So we construct **local fields** $\mathbb{Q}_p$ for each prime p to recover this information. We call $\mathbb{Q}$ a **global field**, so that it embeds into each of its local fields. Local fields are much simpler.

2.1 Absolute values and valued fields

Definition 2.1.1. Let K be a field. An **absolute value** or **valuation** on K is a function $|\cdot|\colon K \to \mathbb{R}$ such that:

1. $|0| = 0$ and $|\cdot|\colon K^\times \to \mathbb{R}_{>0}$ is positive;
2. $|xy| = |x||y|$ (so $|\cdot|\colon K^\times \to \mathbb{R}_{>0}$ is a group homomorphism);
3. (triangle inequality) $|x + y| \leq |x| + |y|$;

Call $(K, |\cdot|)$ a **valued field**.

Example 2.1.2. The usual absolute value on $\mathbb{R}$ induces an absolute value on $\mathbb{Q}$. In general, given a number field K, any real or complex embedding of K induces an absolute value on K:

1. for $\sigma\colon K \hookrightarrow \mathbb{R}$, define $|x|_\sigma \coloneqq |\sigma x|$;
2. for $\sigma\colon K \hookrightarrow \mathbb{C}$, define $|x|_\sigma \coloneqq |\sigma x|^2$ (called the **normalized** absolute value).

Definition 2.1.3. A valuation $|\cdot|$ on K is called **non-archimedean** if it satisfies the stronger condition

3'. (ultrametric inequality) $|x + y| \leq \max\{|x|, |y|\}$.

Otherwise, say $|\cdot|$ is **archimedean**.

Remark. Recall the **archimedean property** of $\mathbb{R}$: given $0 \neq x \in \mathbb{R}$, then $|nx| > 1$ for some $n \in \mathbb{Z}$. A non-archimedean valuation fails to satisfy the archimedean property, since $|nx| \leq |x|$ by the ultrametric inequality.

Example 2.1.4. For $0 \neq a \in \mathbb{Q}$, define $\mathrm{ord}_p(a)$ to be the power of p in the factorization of $a \in \mathbb{Z}$ (i.e. $a = \prod_p p^{\mathrm{ord}_p a}$). Then $\mathrm{ord}_p(a + b) \geq \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$. So define $|a|_p \coloneqq c^{\mathrm{ord}_p(a)}$ for some constant $0 < c < 1$. Then $|\cdot|_p$ is an absolute value on $\mathbb{Q}$, called the **p-adic valuation**. If we choose $c = 1/p$, it is the **normalized p-adic valuation**.

Remark. For a general number field K and a prime $\mathfrak{p} \subset \mathcal{O}_K$, we can define a **$\mathfrak{p}$-adic valuation**

$$|a|_{\mathfrak{p}} \coloneqq (N\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}} a}$$

where $N\mathfrak{p}$ is the **norm** of $\mathfrak{p}$, and $\operatorname{ord}_{\mathfrak{p}} a$ is the order of $\mathfrak{p}$ in the factorization of the principal ideal (a). These are all non-archimedean.

Definition 2.1.5. The valuation $|\cdot|$ is **discrete** if $|K^\times| \subset \mathbb{R}$ is a discrete subgroup (under the usual topology on $\mathbb{R}$). All these $\mathfrak{p}$-adic valuations are discrete.

Definition 2.1.6. Assume $|\cdot|$ is discrete and non-archimedean. Define

$$\begin{aligned} A &\coloneqq \{x \in K : |x| \le 1\} \subset K \text{ a subgroup} \\ U &\coloneqq \{x \in K : |x| = 1\} \subset K^\times \text{ a subgroup} \\ \mathfrak{m} &\coloneqq \{x \in K : |x| < 1\} \subset A \text{ an ideal.} \end{aligned}$$

Note that A is a DVR, and therefore a PID with only one non-zero prime ideal $\mathfrak{m} = (\pi)$ for some $\pi \in A$. The structure of A is therefore very simple.

Remark. An absolute value defines a metric $d(x, y) \coloneqq |x - y|$ and therefore a topology. A basis of open neighborhoods of $a \in K$ is given by

$$B(a, r) \coloneqq \{x \in K : d(x, a) < r\}.$$

Example 2.1.7. Let $K = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$. Then $x, y \in \mathbb{Q}$ are "closer" iff $\operatorname{ord}_p(x - y)$ is "large," i.e. $x \equiv y$ mod a "high" power of p.

Definition 2.1.8. We say two absolute values on K are **equivalent** if they define the same topology (e.g. $|\cdot| \sim |\cdot|^\alpha$ for every $\alpha \in \mathbb{R}$). An equivalence class of absolute values on a number field is called a **prime** or a **place**.

Theorem 2.1.9 (Ostrowski, 1916)**.** *There are only the following valuations on $\mathbb{Q}$:*

1. *$|\cdot|_\infty$ (the usual archimedean valuation);*
2. *$|\cdot|_p$ where p runs over primes.*

Remark. We call $|\cdot|_\infty$ the **infinite** prime/place, and $|\cdot|_p$ the **finite** prime/place.

Proof. Let $m, n > 1$ be integers. Let $N = \max\{1, |n|\}$. The claim is that $|m| \le N^{\log m / \log n}$. Then there are two cases.

1. ($|n| > 1$ for all n) In this case, $|m| \le |n|^{\log m / \log n}$. Then $|m|^{1 \log m} \le |n|^{1 / \log n}$. By symmetry, this is an equality, so let
$$c \coloneqq |m|^{1/\log m} = |n|^{1/\log n}.$$
Then $|m| = c^{\log m} = m^{\log c}$, which is just the usual archimedean valuation raised to some power $\log c$. Hence $|m| \sim |m|_\infty^{\log c}$.

2. ($|n| \le 1$ for some n) In this case, the claim shows $|m| \le 1$ for all m. Then
$$|x + y|^k \le \sum_{r=0}^{k} \left|\binom{k}{r}\right| |x|^{k-r} |y|^r \le (k+1) \max\{|x|, |y|\}^k.$$
This implies $|x + y| \le (k+1)^{1/k} \max\{|x|, |y|\}$. As $k \to \infty$, we get $|x + y| \le \max\{|x|, |y|\}$. Hence $|\cdot|$ is non-archimedean. Now consider its valuation ring A and maximal ideal $\mathfrak{m}$. Then $\mathbb{Z} \subset A$, so $\mathfrak{m} \cap \mathbb{Z} \subset A$ is a prime ideal. So $\mathfrak{m} \cap \mathbb{Z} = (p)$ for some prime p. Hence $|m| = c^{\operatorname{ord}_p(\mathfrak{m})}$, i.e. $|m| \sim |m|_p$.

To prove the claim, write $m = a_0 + a_1 n + a_2 n^2 + \cdots + a_r n^r$ where $0 \le a_i \le n-1$. The triangle inequality gives

$$|m| \le \sum_{i=0}^{r} |a_i||n|^i \le n(1 + |n| + \cdots + |n|^r) \le n(1+r)N^r.$$

But the base-n expansion of m has at most $\log m / \log n$ terms. Hence

$$|m| \le n\left(1 + \frac{\log m}{\log n}\right) N^{\log m / \log n}.$$

To eliminate the constant, replace m by m^k. Then taking the k-th root of both sides,

$$|m| \le n^{1/k}\left(1 + k\frac{\log m}{\log n}\right)^{1/k} N^{\log m / \log n}.$$

As $k \to \infty$, the constant term now goes to 1. □

Remark. A similar theorem holds for any number field K. There are three types of places:

1. $|\cdot|_\sigma$ for real embeddings $\sigma\colon K \hookrightarrow \mathbb{R}$;
2. $|\cdot|_\sigma$ for complex embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$, which are equivalent for conjugate pairs;
3. $|\cdot|_{\mathfrak{p}}$ where $\mathfrak{p}$ runs over all prime ideals of $\mathcal{O}_K$.

Theorem 2.1.10 (Product formula)**.** *Let K be a number field, and $\alpha \in K^\times$. Then using the normalized valuations,*

$$\prod_{v \text{ place of } K} |\alpha|_v = 1.$$

Proof. Suppose $K = \mathbb{Q}$. Note that $|\alpha|_v \neq 1$ iff $\mathrm{ord}_p(\alpha) \neq 0$, which happens only at finitely many primes. Hence the product is a finite product. Because $\prod_v |\cdot|_v\colon \mathbb{Q} \to \mathbb{R}^\times$ is still a group homomorphism, it suffices to check the following.

1. ($\prod_v |p|_v = 1$ for primes p) Note that $|p|_p = 1/p$, $|p|_\infty = p$, and $|p|_l = 1$ for other primes l.
2. ($\prod_v |-1|_v = 1$) $|-1|_p = 1$, and $|-1|_\infty = 1$. □

2.2 Completions

Definition 2.2.1. Say a sequence $\{a_n\}$ of elements in a valued field K is a **Cauchy sequence** if for every $\epsilon > 0$, there exists N such that for all $m, n \ge N$,

$$|a_m - a_n| < \epsilon.$$

Say K is **complete** if any Cauchy sequence has a limit in K.

Example 2.2.2. Consider the sequence

$$4, 34, 334, 3334, 33334, \ldots.$$

Under the archimedean absolute value, this does not converge. But under $|\cdot|_5$,

$$|a_m - a_n|_5 = 5^{-n} \text{ if } m \ge n.$$

So a_n is Cauchy under $|\cdot|_5$. Since we have $|3a_n - 2|_5 = 5^{-n}$, we get $3a_n - 2 \to 0$, so $a_n \to 2/3$ under $|\cdot|_5$.

Theorem 2.2.3. *Let K be a valued field. Then there exists a complete valued field $\hat{K}$ and a homomorphism $K \to \hat{K}$ such that the absolute value on $\hat{K}$ extends the absolute value on K and is universal: for every other complete L which extends the absolute value on K, the morphism $K \to L$ factors uniquely through $\hat{K}$.*

Proof. Define $\hat{K}$ to be all Cauchy sequences in K mod the equivalence $\{a_n\} \sim \{b_n\}$ if $|a_n - b_n| \to 0$. Then $\hat{K}$ has a field structure by term-wise operations, and define $|\{a_n\}| \coloneqq \lim |a_n|$. The map $K \to \hat{K}$ is given by $a \mapsto (a, a, a, \ldots)$. □

Definition 2.2.4. Define $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ under $|\cdot|_p$. The valuation ring of $\mathbb{Q}_p$ is denoted $\mathbb{Z}_p$. More generally, if K is a number field and $\mathfrak{p}$ is a prime in $\mathcal{O}_K$, define $K_\mathfrak{p}$ to be the completion of K under $|\cdot|_p$, and its valuation ring is denoted $\mathcal{O}_{K,\mathfrak{p}}$. These are all complete discrete non-archimedean fields.

Definition 2.2.5. Let K be a discrete nonarchimedean field. Some notation:

$$K \supset A \coloneqq \{x \in K : |x| \leq 1\} \supset \mathfrak{m}$$
$$\hat{K} \supset \hat{A} \coloneqq \{x \in \hat{K} : |x| \leq 1\} \supset \hat{\mathfrak{m}}.$$

Note that $A/\mathfrak{m} \cong \hat{A}/\hat{\mathfrak{m}}$ is always an isomorphism. We will implicitly make this identification from now on.

Theorem 2.2.6. *Let S be a set of representatives of $A/\mathfrak{m}$. Let $\mathfrak{m} = (\pi)$, where π is called the* **uniformizer**. *Then every element of $\hat{K}$ can be uniquely written as*

$$\sum_{i \geq k} a_i \pi^i, \quad k \in \mathbb{Z},\ a_i \in S.$$

Proof. Let $0 \neq x \in \hat{K}$. We can find $y \in \hat{A}^\times$ and $k \in \mathbb{Z}$ such that $x = \pi^k y$. So it suffices to write y in such a form. Since $y \in \hat{A}$, find a unique $a_0 \in S$ such that

$$y \equiv a \bmod \mathfrak{m}.$$

Then $y - a_0 \in \pi\hat{A}$. Now repeat this process with $(y - a_0)/\pi$ to get a unique $a_1 \in S$, then $a_2 \in S$, etc. □

Example 2.2.7. Let $K = \mathbb{Q}_p$. Then each element has a p-adic expansion $\sum_{i \geq k} a_i p^i$ with $0 \leq a_i \leq p - 1$, e.g. $a_{-5}p^{-5} + a_{-4}p^{-4} + \cdots$. The elements a_i are called **p-adic digits**.

Example 2.2.8. Suppose $p = 2$ and consider $1+2+2^2+2^3+\cdots$. This series converges to $\lim_{n\to\infty} 2^{n+1} - 1 = -1 \in \mathbb{Q}_2$.

Theorem 2.2.9 (Hensel's lemma)**.** *Let K be a complete discrete non-archimedean field with residue field $k \coloneqq A/\mathfrak{m}$. Suppose $f(x) \in A[x]$, and let $\bar{f}(x) = f(x) \bmod \pi \in k[x]$. Assume $\bar{f} = g_0 h_0$ in $k[x]$ where g_0, h_0 are monic and coprime. Then there exist $g, h \in K[x]$ such that $f = gh$ in $K[x]$ and $\bar{g} = g_0$ and $\bar{h} = h_0$.*

Proof. Pick an arbitrary lift of g_0, h_0 to $A[x]$. Then

$$f - g_0 h_0 \in \pi A[x],$$

i.e. they agree "up to the first digit." We will inductively increase the precision. Assume there exist g_n, h_n such that $\bar{g}_n = g_0$ and $\bar{h}_n = h_0$ and $f - g_n h_n \in \pi^{n+1} A[x]$. Write

$$g_{n+1} \coloneqq g_n + \pi^{n+1} u, \quad h_{n+1} \coloneqq h_n + \pi^{n+1} v$$

where $\deg u < \deg g_0$ and $\deg v < \deg h_0$ to preserve the property of being monic. Hence we want

$$\pi^{n+1} u h_n + \pi^{n+1} v g_n = f - g_n h_n \bmod \pi^{n+2}.$$

Rearranging, this is equivalent to wanting

$$u h_n + v g_n = \frac{f - g_n h_n}{\pi^{n+1}} \bmod \pi,$$

i.e. we want this equality in $k[x]$. By Bezout's theorem, u and v exist. □

Corollary 2.2.10. *If $\bar{f}(x)$ has a simple root $\alpha \in k$, then $f(x)$ has a root $\beta \in A$ such that $\bar{\beta} = \alpha$.*

Corollary 2.2.11. *If K is complete discrete nonarchimedean and $k = \mathbb{F}_q$, then $x^q - x$ has q distinct roots in K.*

Proof. Since $x^q - x \in \mathbb{F}_q[x]$ has q distinct roots, apply Hensel's lemma. □

Remark. In particular, $x^p - x = x(x^{p-1} - 1)$ has p distinct solutions in $\mathbb{Q}_p$. So $\mathbb{Q}_p$ contains all $(p-1)$ roots of unity. More generally, k contains all $(q-1)$ roots of unity.

2.3 Extensions of complete discrete valuation fields

Let K be a complete discrete valuation field. Recall that given a finite separable extension L/K, we have

$$N_{L/K}\beta = \prod_{\sigma\colon L \to \tilde{L}} \sigma\beta$$

where $\tilde{L}$ is the Galois closure of L/K.

Theorem 2.3.1. *Let L/K be a finite separable extension of degree n.*

1. *$|\cdot|_K$ extends uniquely to a discrete absolute value $|\cdot|_L$ on L.*
2. *L is complete under $|\cdot|_L$.*
3. *$|\beta|_L = |N_{L/K}\beta|_K^{1/n}$ for any $\beta \in L$.*

Proof. Let $A \subset K$ be the valuation ring. Define B to be the integral closure of A inside L. A general fact: A is a Dedekind domain, and B, as the integral closure, is also a Dedekind domain. Since A is a DVR, it has a unique non-zero prime ideal $\mathfrak{p}$. By unique factorization of prime ideals in Dedekind domains, write $\mathfrak{p} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, where $\mathfrak{p}_i$ are prime ideals of B.

Claim: there is exactly one non-zero prime ideal in B. Assume otherwise and let $\mathfrak{p}_1, \mathfrak{p}_2$ be two distinct non-zero prime ideals of B. Find an element $\beta \in \mathfrak{p}_1$ with $\beta \notin \mathfrak{p}_2$. Then

$$A[\beta] \cap \mathfrak{p}_1 \neq A[\beta] \cap \mathfrak{p}_2$$

are distinct prime ideals of $A[\beta]$ containing $\mathfrak{p}$. Let $f(x) \in A[x]$ be the minimal polynomial of β. Consider the reduction $\bar{f}(x) \in A/\mathfrak{p}[x] = k[x]$. By Hensel's lemma, $\bar{f}(x)$ can only have one irreducible factor; otherwise the factorization lifts to $f(x) \in A[x]$. So $\bar{f}(x) = g(x)^k$ for some $g(x) \in k[x]$ and integer k. So

$$A[\beta]/\mathfrak{p}A[\beta] = A[x]/(f(x), \mathfrak{p}) = k[x]/(\bar{f}(x)) = k[x]/(g(x)^k).$$

Hence this ring has only one non-zero prime ideal. So there can only be one prime ideal in $A[\beta]$ containing $\mathfrak{p}$. But this is a contradiction.

Let $\mathfrak{p} = \mathfrak{P}^e$, where $\mathfrak{P}$ is the non-zero prime of B. It follows that $|\cdot|_K$ extends uniquely to the $\mathfrak{P}$-adic valuation on L. The constant is determined by comparison to $|\cdot|_K$.

To show L is complete, take a basis $\{e_1, \ldots, e_n\}$ of L as a K-vector space. Suppose $\{a_k\}$ is a Cauchy sequence in L. Write $a_k = a_{k,1}e_1 + \cdots + a_{k,n}e_n$. Then by the ultrametric inequality, $\{a_{k,i}\}_k$ is a Cauchy sequence in K for each i. If $a_{k,i} \to b_i \in K$, then $a_k \to b_1e_1 + \cdots + b_ne_n$.

Finally, let $\tilde{L}$ be the Galois closure of L/K, and take $\beta \in L$. The Galois closure is a finite separable extension, so what we have proved so far applies to $\tilde{L}$ as well. So

$$|\beta|_L = |\beta|_{\tilde{L}} = |\sigma\beta|_{\tilde{L}}, \quad \sigma\colon L \to \tilde{L}$$

since Galois conjugation does not change the absolute value. In particular, by the definition of the norm $N_{L/K}$,

$$|N_{L/K}(\beta)|_K = |N_{L/K}(\beta)|_{\tilde{L}} = \prod_{\sigma\colon L \to \tilde{L}} |\sigma\beta|_{\tilde{L}} = \prod_{\sigma\colon L \to \tilde{L}} |\beta|_L = |\beta|_L^n.$$ □

Corollary 2.3.2. *Let L/K be a separable algebraic extension (of possibly infinite degree). Then $|\cdot|_K$ also extends uniquely to L.*

Proof. Note that L is the composite of all finite sub-extensions of L/K. □

Remark. A separable algebraic extension L/K may not be complete, even if K is complete.

Definition 2.3.3. Let L/K be a finite extension of degree n. Write $\mathfrak{p} = \mathfrak{P}^e$. We say this integer e is the **ramification index** of L/K. We also have an extension of residue fields $\ell = \mathcal{O}_L/\mathfrak{P} \to k = \mathcal{O}_K/\mathfrak{p}$. We call $f \coloneqq [\ell : k]$ the **residue degree** of L/K.

Lemma 2.3.4. *Some facts from Dedekind domains:*

1. *$n = ef$;*
2. *e and f are multiplicative in field extensions, i.e. for extensions $M \supset L \supset K$, we have $e(M/K) = e(M/L)e(L/K)$ and similarly for f.*

2.4 Unramified extensions

Definition 2.4.1. The finite separable extension L/K is **unramified** if $e = 1$ (i.e. $f = n$), and **totally ramified** if $e = n$ (i.e. $f = 1$). Unramified extensions are easier to understand.

Proposition 2.4.2.
1. *If L/K is unramified, then $\ell = k(\alpha_0)$. If $\alpha \in \mathcal{O}_L$ is such that $\bar{\alpha} = \alpha_0$, then $L = K(\alpha)$.*
2. *If $L = K(\alpha)$, let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α. If $\bar{f}(x) \in k[x]$ has no repeated root, then L/K is unramified.*

Proof. Let $f(x)$ be the minimal polynomial of α. Then

$$\deg \bar{f} \geq [k(\alpha_0) : k] = [\ell : k] = [L : K]$$

On the other hand,

$$\deg f = [K(\alpha) : K] \leq [L : K].$$

Hence all inequalities must be equalities. In particular, $K(\alpha) = L$.

If $\bar{f}(x)$ has no repeated roots, then by Hensel's lemma $\bar{f}(x)$ is irreducible. Then

$$[L : K] = [K(\alpha) : K] = \deg f = \deg \bar{f} = [k(\alpha) : k] \leq [\ell : k] \leq [L : K].$$

Hence all inequalities must be equalities. In particular, $[\ell : k] = [L : K]$, i.e. L/K is unramified. □

Theorem 2.4.3. *Assume k is perfect. Then there is a one-to-one correspondence*

$$\{L/K \text{ finite unramified}\} \leftrightarrow \{\ell/k \text{ finite}\}$$
$$L \mapsto \ell = \mathcal{O}_L/\mathfrak{P}.$$

Moreover, L/K is Galois iff ℓ/k is Galois. In this case, $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$.

Lemma 2.4.4.
1. *Given a tower $M \supset L \supset K$, the extension M/K is unramified iff M/L and L/K are both unramified.*
2. *Given L/K unramified and L'/K any finite extension, the composite LL'/L' is unramified.*
3. *Given L/K, L'/K unramified, then LL'/K is unramified.*

Proof. Since $e(M/K) = e(M/L)e(L/K)$, the first statement is obvious.

If L/K is unramified, then $L = K(\alpha)$ and the minimal polynomial $f \in \mathcal{O}_K[x]$ of α has $\bar{f}$ irreducible. But k is perfect, so $\bar{f}(x)$ has no repeated root. In particular, $LL'/L' = L'(\alpha)/L'$, and the minimal polynomial g of α satisfies $\bar{g} \mid \bar{f}$ so $\bar{g}$ has no repeated root. Hence LL'/L' is unramified.

Now if L'/K is unramified, then LL'/K is unramified because both LL'/L' and L'/K are. □

Proof of theorem. We first prove surjectivity. Write $\ell = k(\alpha_0)$. Let $f_0 \in k[x]$ be the minimal polynomial of α_0. Pick an arbitrary lift $f \in \mathcal{O}_K[x]$ such that $\bar{f} = f_0$. By Hensel's lemma, α_0 lifts to a root α of f. (We can do this because α_0 is a simple root, since k is perfect.) Define $L = K(\alpha)$. Then L/K is unramified and the residue field of L is ℓ.

Now we show injectivity. Suppose L, L' are two unramified extensions of K with the same residue field ℓ. Then LL'/K is also unramified, with the same residue field ℓ. But then

$$[LL' : K] = [\ell : k] = [L : K] = [L' : K].$$

This implies $LL' = L = L'$.

Assume L/K is Galois. Write $L = K(\alpha)$ and $\ell = k(\alpha_0)$ where $\alpha_0 = \bar{\alpha}$, and let $f \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Since L/K is Galois, $f(x)$ splits in L, and therefore $\bar{f}(x)$ splits in ℓ. Hence ℓ/k is also Galois. The converse follows by Hensel's lemma.

Finally, since $\mathrm{Gal}(L/K)$ stabilizes $\mathcal{O}_L$, we have $\mathfrak{p}_L \subset \mathcal{O}_L$, and since it acts trivially on $\mathcal{O}_K$, we have $\mathfrak{p}_K \subset \mathcal{O}_K$. Then automorphisms in $\mathrm{Gal}(L/K)$ descend to $\mathcal{O}_L/\mathfrak{p}_L = \ell$, and hence there is an induced map

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

The permutation of roots of $f(x)$ corresponds to that of roots of $\bar{f}(x)$, since L/K is unramified. So this is a bijection. □

Corollary 2.4.5. *If L/K is an algebraic extension, then there exists a largest unramified subset $K_0 \subset L$. Moreover, L/K_0 is totally ramified.*

Proof. Let K_0 be the composite of all unramified extensions of K. Then L/K_0 has trivial residue field extension by the theorem. By definition, L/K_0 is therefore totally ramified. □

Corollary 2.4.6. *Assume $k = \mathbb{F}_q$ is finite. Then there exists a unique degree n unramified extension K_n of K for each $n \geq 1$, and*

$$\mathrm{Gal}(K_n/K) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n.$$

Proof. $\mathbb{F}_{q^n}/\mathbb{F}_q$ is the unique degree n extension of $\mathbb{F}_q$. □

Definition 2.4.7. Let $\sigma \in \mathrm{Gal}(K_n/K)$ correspond to the automorphism $x \mapsto x^q$ in $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. We call σ the **Frobenius** in $\mathrm{Gal}(K_n/K)$. Explicitly,

$$\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{p}_{K_n} \quad \forall \alpha \in \mathcal{O}_{K_n}.$$

Corollary 2.4.8. *Assume $k = \mathbb{F}_q$. Then the maximal unramified extension of K is*

$$K^{\mathrm{ur}} \coloneqq \bigcup_{(m,p)=1} K(\zeta_m).$$

In particular, $\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{(m,p)=1} \mathbb{Q}_p(\zeta_m)$.

Proof. $\bar{\mathbb{F}}_q = \bigcup_{(m,p)=1} \mathbb{F}_q(\zeta_m)$. In fact, every element of $\mathbb{F}_{q^n}^\times$ satisfies $x^{q^n-1} - 1 = 0$. □

2.5 Totally ramified extensions

Definition 2.5.1. A polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ is **Eisenstein** if

$$|a_n| = 1, \quad |a_i| < 1 \, \forall i = 1, \ldots, n-1, \quad |a_0| = |\pi|.$$

In other words, $\pi \nmid a_n$, $\pi \mid a_i$, and $\pi \mid\mid a_0$ (exactly one factor of π goes into a_0).

Lemma 2.5.2 (Eisenstein's criterion)**.** *If $f(x)$ is Eisenstein, then $f(x)$ is irreducible.*

Remark. Given a Eisenstein polynomial $f(x)$, all of its roots are Galois conjugate and therefore have the same absolute value. In particular, because their product is $|\pi|$, it follows that this absolute value is $|\pi|^{1/n}$.

Proposition 2.5.3. *Suppose L/K is finite. Then L/K is totally ramified iff $L = K(\alpha)$ for α a root of some Eisenstein polynomial in $K[x]$.*

Proof. If $L = K(\alpha)$ for α a root of $f(x) \in K[x]$ Eisenstein, then $|\alpha|^{\deg f} = |\pi|$ by the preceding remark. Hence

$$[L : K] \geq e(L/K) \geq \deg f = [L : K],$$

and equality must hold and L/K is totally ramified. Conversely, if L/K is totally ramified, Take the uniformizer α of L, i.e. $\mathfrak{p}_L = (\alpha)$. Then $\mathfrak{p}_L^n = \mathfrak{p}_K$ and $(\alpha^n) = (\pi)$. Hence $|\alpha| = |\pi|^{1/n}$. Look at $1, \alpha, \ldots, \alpha^{n-1}$. They cannot be linearly dependent over K because they have absolute values $|\pi|^0, |\pi|^{1/n}, \ldots, |\pi|^{(n-1)/n}$, so they are exactly representatives of the cosets $|L^\times|/|K^\times|$. (In other words, if

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0, \quad \alpha_i \in K,$$

then there cannot be two $a_i\alpha^i$ with the same absolute value.) So there must be a relation

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

The cancellation in the absolute value must occur in a_0 and α^n, so $|\alpha_0| = |\alpha^n| = |\pi|$. Cancellation cannot happen in the middle terms, so $|a_i| < 1$. Hence α satisfies an Eisenstein polynomial. □

Lemma 2.5.4 (Krasner's lemma)**.** *Let $f(x) = \sum a_i x^i, g(x) = \sum b_i x^i \in K[x]$. Assume $|a_i - b_i|$ sufficiently small. Then*

$$\{k(\alpha) : \alpha \text{ a root of } f\} = \{k(\beta) : \beta \text{ a root of } g\}.$$

Proposition 2.5.5. *Assume k is finite. Then there are only finitely many totally ramified extensions of K of degree n.*

Proof. By the previous proposition, all totally ramified extensions are given by an Eisenstein polynomial of degree n. By Krasner's lemma, an Eisenstein polynomial $\sum a_i x^i$ defines a totally ramified extension, and this extension only depends on $a_i \bmod \mathfrak{p}_K^N$ for sufficiently large N. But $\mathcal{O}_K/\mathfrak{p}_K^N$ is finite. □

Corollary 2.5.6. *Assume k is finite. Then there are only finitely many extensions of K of degree n.*

Remark. This is obviously not true for other fields, e.g. $K = \mathbb{Q}$.

2.6 Local class field theory

Definition 2.6.1. A **local field** is a field K with an absolute value such that K is locally compact (under the induced topology of $|\cdot|$).

Remark. Recall that a topological space is compact iff any open cover has a finite subcover. It is locally compact iff every open neighborhood of every point contains a compact neighborhood. For example, $\mathbb{R}$ and $\mathbb{C}$ are locally compact. A metric space is compact iff it is complete and totally bounded (i.e. for any $r \in \mathbb{R}_+$, there exists a finite cover by balls of radius r). Similarly, a metric space is locally compact iff all closed balls are compact. In particular, local fields are complete.

Lemma 2.6.2. *Let K be a complete discrete valued field. Then K is locally compact iff K has finite residue field.*

Proof. Assume K is locally compact. Then $\mathcal{O}_K = \{x \in K : |x| \leq 1\}$ is a closed ball, and therefore is compact. It contains an open ball $\mathfrak{m}_K = \{x \in K : |x| < 1\}$. By compactness, $\mathcal{O}_K = \bigcup_{x \in \mathcal{O}_K/\mathfrak{m}_K} (x + \mathfrak{m}_K)$ has a finite subcover, i.e. $\mathcal{O}_K/\mathfrak{m}_K$ is finite.

Conversely, suppose K has finite residue field. Then $\mathcal{O}_K/\mathfrak{m}_K^n$ is finite, by inductively using the short exact sequence

$$0 \to \mathfrak{m}_K^{n-1}/\mathfrak{m}_K^n = \mathcal{O}_K/\mathfrak{m}_K \to \mathcal{O}_K/\mathfrak{m}_K^n \to \mathcal{O}_K/\mathfrak{m}_K^{n-1} \to 0.$$

Then the balls $B_{a,r} \coloneqq \{x \in K : |x - a| < r\}$ cover $\mathcal{O}_K$ where a runs over all representatives of $\mathcal{O}_K/\mathfrak{m}_K^n$ for sufficiently large n. But $\mathcal{O}_K/\mathfrak{m}_K^n$ is finite, so $\mathcal{O}_K$ is totally bounded and therefore compact. Hence K is locally compact. □

Theorem 2.6.3. *Every local field is one of the following:*

1. *$\mathbb{R}$ or $\mathbb{C}$;*
2. *a finite extension of $\mathbb{Q}_p$ for some prime p;*
3. *the field $\mathbb{F}_{p^n}((T))$ of Laurent series over $\mathbb{F}_{p^n}$, for some prime p and some $n \geq 1$.*

Proof. Suppose the local field K is archimedean. There is an injection $\mathbb{Q} \hookrightarrow K$. Since K is complete, $\mathbb{R} \hookrightarrow K$. By local compactness, $K/\mathbb{R}$ must be a finite extension. Hence K is either $\mathbb{R}$ or $\mathbb{C}$.

Suppose the local field K is non-archimedean. If $\operatorname{char} K = 0$, then $\mathbb{Q} \hookrightarrow K$. Since K is complete, $\mathbb{Q}_p \hookrightarrow K$. By local compactness, $K/\mathbb{Q}_p$ must be a finite extension. Otherwise if $\operatorname{char} K = p$, then $\mathbb{F}_p \hookrightarrow K$. Write the residue field as $\mathbb{F}_{p^n}$ for some n, since it must be finite. Then

$$K = \{\sum_{n \geq k} a_n \pi^n : k \in \mathbb{Z},\, a_n \in S \text{ a representative of } \mathcal{O}_K/\mathfrak{m}_K\}.$$

Observe that $\mathbb{F}_{p^n} \hookrightarrow K$ by Hensel's lemma. So actually,

$$K = \{\sum_{n \geq k} a_n \pi^n : k \in \mathbb{Z},\, a_n \in \mathbb{F}_{p^n}\} \cong \mathbb{F}_p((T))$$

under the isomorphism $\pi \leftrightarrow T$. □

Remark. The **goal** of local class field theory is to classify all finite abelian extensions of K for K a non-archimedean local field. (Recall that a field extension L/K is abelian iff L/K is Galois and $\operatorname{Gal}(L/K)$ is abelian.)

Lemma 2.6.4. *If L_1/K and L_2/K are both abelian, then L_1L_2/K is also abelian.*

Definition 2.6.5. Let K^{ab} be the union of all finite abelian extensions of K. It is the maximal abelian extension of K. We want to understand $\operatorname{Gal}(K^{\mathrm{ab}}/K)$ in terms of $K^\times$ itself.

Theorem 2.6.6 (Part I of local CFT, local reciprocity)**.** *Assume K is a non-archimedean local field. Then there exists a unique homomorphism $\phi_K \colon K^\times \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ such that:*

1. *for any uniformizer π of K and any finite unramified extension L/K, the image of $\phi_K(\pi)$ in the quotient $\operatorname{Gal}(K^{\mathrm{ab}}/K) \to \operatorname{Gal}(L/K)$ is given by the Frobenius in $\operatorname{Gal}(L/K)$;*
2. *for any finite abelian extension L/K, the map ϕ_K factors as*

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_K} & \operatorname{Gal}(K^{\mathrm{ab}}/K) \\ \downarrow & & \downarrow \\ K^\times/\operatorname{Nm}(L^\times) & \xrightarrow{\phi_{L/K}} & \operatorname{Gal}(L/K) \end{array}$$

where $\phi_{L/K}$ is an isomorphism. Here $\operatorname{Nm} \colon L^\times \to K^\times$ is the norm map.

Remark. This map ϕ_K is called the **local Artin reciprocity map**.

2.7 Norm groups

Definition 2.7.1. A subgroup of $K^\times$ of the form $\mathrm{Nm}(L^\times)$ for some finite abelian L/K is called a **norm group** of $K^\times$.

Remark. We recall some Galois theory before continuing. Suppose Ω/K is a possibly infinite extension. We say Ω/K is Galois if it is algebraic, separable, and normal. Note that Ω/K is Galois iff Ω is the union of finite Galois extensions. We have

$$\mathrm{Gal}(\Omega/K) = \{\sigma\colon \Omega \to \Omega : \sigma|_K = \mathrm{id}\} = \varprojlim_{L/K \text{ finite Galois}} \mathrm{Gal}(L/K).$$

So $\mathrm{Gal}(\Omega/K)$ is an example of a profinite group, i.e. an inverse limit of finite groups. There is a profinite topology on $\mathrm{Gal}(\Omega/K)$ making it a topological group. A basis of open neighborhoods of 1 in $\mathrm{Gal}(\Omega/K)$ is given by $\mathrm{Gal}(\Omega/L)$ where L/K is finite.

Theorem 2.7.2 (Galois theory for infinite extensions)**.** *Fix Ω/K Galois. Then there is a bijection*

$$\begin{aligned} \{L/K \textit{ sub-extension}\} &\leftrightarrow \{\textit{closed subgroups of } \mathrm{Gal}(\Omega/K)\} \\ L &\mapsto \mathrm{Gal}(\Omega/L) \\ \Omega^H &\hookleftarrow H. \end{aligned}$$

Moreover,

$$\{L/K \textit{ Galois}\} \leftrightarrow \{\textit{normal closed subgroups of } \mathrm{Gal}(\Omega/L)\}.$$

Remark. Note that if L/K is finite, then $\mathrm{Gal}(\Omega/L)$ is open. In a topological group, open subgroups are always closed, so $\mathrm{Gal}(\Omega/L)$ is closed.

Proposition 2.7.3. *1.* $\mathrm{Nm}(L_1) \cap \mathrm{Nm}(L_2) = \mathrm{Nm}(L_1L_2)$.

2. $L_1 \subset L_2$ *iff* $\mathrm{Nm}(L_1) \supset \mathrm{Nm}(L_2)$.

3. $\mathrm{Nm}(L_1)\,\mathrm{Nm}(L_2) = \mathrm{Nm}(L_1 \cap L_2)$.

4. Every subgroup of $K^\times$ containing a norm group is also a norm group.

Proof. Clearly $\mathrm{Nm}(L_1L_2) \subset \mathrm{Nm}(L_1)$ by transitivity (take the norm in the extension L_1L_2/L_1 first) and similarly for $\mathrm{Nm}(L_2)$, so $\mathrm{Nm}(L_1L_2) \subset \mathrm{Nm}(L_1) \cap \mathrm{Nm}(L_2)$. Now suppose $a \in \mathrm{Nm}(L_1) \cap \mathrm{Nm}(L_2)$. Using the local Artin map, $a \in \ker(\phi_{L_1/K}) \cap \ker(\phi_{L_2/K})$. In other words, $\phi_K(a)|_{L_1} = \phi_K(a)|_{L_2} = 1$, so $\phi_K(a)|_{L_1L_2} = 1$. Then $a \in \mathrm{Nm}(L_1L_2) = \ker(\phi_{L_1L_2/K})$. So $\mathrm{Nm}(L_1L_2) \supset \mathrm{Nm}(L_1) \cap \mathrm{Nm}(L_2)$.

Clearly if $L_1 \subset L_2$, then $\mathrm{Nm}(L_1) \supset \mathrm{Nm}(L_2)$. Conversely, $\mathrm{Nm}(L_1) \cap \mathrm{Nm}(L_2) = \mathrm{Nm}(L_2)$, and by part (1), this intersection is $\mathrm{Nm}(L_1L_2)$. Using the local Artin map, $[K^\times : \mathrm{Nm}(L^\times)] = [L : K]$, so $[L_1L_2 : K] = [L_2 : K]$. Hence $[L_1L_2 : L_2] = 1$, i.e. $L_1L_2 = L_2$, so $L_1 \subset L_2$.

Assume $H \supset \mathrm{Nm}(L)$. Let M be the fixed field $L^{\phi_{L/K}(H)}$. (Note that $\phi_{L/K}(H) \subset \mathrm{Gal}(L/K)$.) By Galois theory, $H/\mathrm{Nm}(L^\times) = \mathrm{Gal}(L/M)$. Using the Artin map, $\mathrm{Nm}(M^\times) = \ker(\phi_{M/K}) = \phi_{L/K}(\mathrm{Gal}(L/M)) = H$.

Finally, $\mathrm{Nm}(L_1)\,\mathrm{Nm}(L_2)$ is the smallest norm group containing $\mathrm{Nm}(L_1)$ and $\mathrm{Nm}(L_2)$. On the field side, we therefore want the largest field contained in L_1 and L_2. This is $L_1 \cap L_2$. Hence $\mathrm{Nm}(L_1 \cap L_2) = \mathrm{Nm}(L_1)\,\mathrm{Nm}(L_2)$. □

Proposition 2.7.4. *Let L/K be any finite extension. If $\mathrm{Nm}(L^\times)$ is finite index in $K^\times$, then $\mathrm{Nm}(L^\times)$ is open in $K^\times$.*

Remark. In general, a finite index closed subgroup is open. Also, in general, every open subgroup is closed.

Proof. It suffices to show that $\mathrm{Nm}(L^\times)$ contains an open subgroup $\mathrm{Nm}(\mathcal{O}_L^\times)$. We know $\mathcal{O}_L^\times$ is a closed subspace of $\mathcal{O}_L$. But $\mathcal{O}_L$ is compact, so $\mathcal{O}_L^\times$ is also compact. Now note that $\mathrm{Nm}(\mathcal{O}_L^\times) = \mathrm{Nm}(L^\times) \cap \mathcal{O}_K^\times$ (since the norms must have valuation 1). Hence $\mathcal{O}_K^\times / \mathrm{Nm}(\mathcal{O}_L^\times) \to K^\times / \mathrm{Nm}(L^\times)$ is an injection. By assumption, the rhs is finite. So the lhs is also finite, and $\mathrm{Nm}(\mathcal{O}_L^\times)$ is finite index in $\mathcal{O}_K^\times$. But $\mathcal{O}_L^\times$ is compact, so $\mathrm{Nm}(\mathcal{O}_L^\times)$ is also compact and closed. Therefore $\mathrm{Nm}(\mathcal{O}_L^\times)$ is open in $\mathcal{O}_K^\times$. □

Theorem 2.7.5 (Part II of local CFT, local existence)**.** *Every finite index open subgroup of $K^\times$ is a norm group.*

Corollary 2.7.6. *There is a one-to-one correspondence*

$$\{L/K \textit{ finite abelian}\} \Leftrightarrow \{\textit{finite index open subgroup of } K^\times\}$$
$$L \mapsto \mathrm{Nm}(L^\times),$$

and $\mathrm{Gal}(L/K) \cong K^\times / \mathrm{Nm}(L^\times)$.

Remark. The corollary also holds for K archimedean, i.e. $\mathbb{R}$ or $\mathbb{C}$. This is easily checked, because $\mathbb{R}/\mathbb{R}$ corresponds to $\mathbb{R}^\times \subset \mathbb{R}^\times$, and $\mathbb{C}/\mathbb{R}$ corresponds to $\mathbb{R}_{>0} \subset \mathbb{R}^\times$. Finally, $\mathbb{C}/\mathbb{C}$ corresponds to $\mathbb{C}^\times \subset \mathbb{C}^\times$, and there are no non-trivial finite index subgroups of $\mathbb{C}^\times$.

Remark. If $\mathrm{char}\, K = 0$, i.e. K is a finite extension of $\mathbb{Q}_p$, then any finite index subgroup of $K^\times$ is automatically open. In particular, the bijection becomes

$$\{L/K \text{ abelian of degree } n\} \Leftrightarrow \{\text{index } n \text{ subgroup of } K^\times/(K^\times)^n\}.$$

The reason for this is as follows. Given $H \subset K$ finite index, $H \supset (K^\times)^n$. So to show H is open, it suffices to show $(K^\times)^n$ contains an open subgroup. But $(K^\times)^n \supset 1 + \mathfrak{m}^k$ for some k, because $x^n - a = 0$ has a solution when $a \in 1 + \mathfrak{m}^k$ for sufficiently large k (by Hensel's lemma when $p \nmid n$, and by the stronger version of Hensel's lemma otherwise).

Remark. If $\mathrm{char}\, K = p > 0$, then finite index does not necessarily imply open.

Chapter 3

Galois cohomology

3.1 Group cohomology

Definition 3.1.1. Let G be a group. A **G-module** is an abelian group M together with a G-action $G \times M \to M$ given by $(g, m) \mapsto gm$ such that:

1. $g(x + y) = gx + gy$ for $g \in G$ and $x, y \in M$;
2. $(gh)(x) = g(hx)$ for $g, h \in G$ and $x \in M$;
3. $1(x) = x$ for $x \in M$, where $1 \in G$ is the identity.

We say the G-action is **trivial** if $gx = x$ for all $g \in G$ and $x \in M$.

Remark. The G-action defines a homomorphism $G \to \mathrm{Aut}(M)$.

Example 3.1.2. If L/K is a Galois extension, let $G = \mathrm{Gal}(L/K)$. Then $M = L^\times$ (or L) is a G-module, via the usual Galois action.

Definition 3.1.3. The **group algebra** $\mathbb{Z}[G]$ is the free abelian group with basis given by the elements in G and multiplication given by

$$\left(\sum n_i g_i\right) \cdot \left(\sum m_j h_j\right) \coloneqq \sum n_i m_j (g_i h_j).$$

Then a G-module is the same as a $\mathbb{Z}[G]$-module. In other words, $\mathsf{Mod}_G = \mathsf{Mod}_{\mathbb{Z}[G]}$. Write the homomorphisms in Mod_G as

$$\mathrm{Hom}_G(M, N) \coloneqq \{\varphi \colon M \to N \text{ group homomorphism} : \varphi(gx) = g\varphi(x)\}.$$

Definition 3.1.4. The motivation for group cohomology is to study the **G-invariants**

$$M^G \coloneqq \{x \in M : gx = x \, \forall g \in G\}.$$

Example 3.1.5. Let $G = \mathrm{Gal}(L/K)$ and $M = L^\times$. Then $M^G = K^\times$, by the definition of the Galois group G.

Remark. Note that we can identify $M^G \coloneqq \mathrm{Hom}_G(\mathbb{Z}, M)$ where $\mathbb{Z}$ is regarded as the trivial G-module. Hence $(-)^G = \mathrm{Hom}_G(\mathbb{Z}, -)$ as functors. We therefore see that $(-)^G$ is left-exact, by the left-exactness of Hom.

Definition 3.1.6. For every $i \geq 0$, define the **r-th group cohomology** $H^r(G, M) \coloneqq \mathrm{Ext}^r_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. (Here $\mathrm{Ext}^r_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ is the right derived functor of $\mathrm{Hom}_G(\mathbb{Z}, -)$.)

Remark. Concretely, the following three properties characterize $H^r(G, -)$:

1. $H^0(G, M) = M^G$, by construction;
2. if I is an injective G-module, then $\mathrm{Hom}_G(-, I)$ is exact and therefore $H^r(G, I) = 0$ for all $r \geq 1$;
3. to every short exact sequence $0 \to A \to B \to C \to 0$, there is a long exact sequence in cohomology

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots.$$

Remark (Computing using injective resolutions). We can compute $H^r(G, -)$ using injective resolutions. Given a G-module M, take an exact sequence

$$0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$$

where all the I^k are injectives. Then apply $(-)^G$ to get

$$0 \to (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \to \cdots$$

Then $H^r(G, M) = \ker d^r / \operatorname{im} d^{r-1}$.

Remark (Computing using projective resolutions). $\mathrm{Ext}^r_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ can be computed as the cohomology $H^r(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, I^\bullet))$ where $I^\bullet$ is an injective resolution of M. However, we can also use a projective resolution $P_\bullet$ of $\mathbb{Z}$ to compute

$$\mathrm{Ext}^r_{\mathbb{Z}[G]}(\mathbb{Z}, M) = H^r(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, M)).$$

Definition 3.1.7. Take a particular free resolution of $\mathbb{Z}$:

$$P_r = \mathbb{Z}[\overbrace{G \times \cdots \times G}^{r+1 \text{ copies}}], \quad g(g_0, \ldots, g_r) \coloneqq (gg_0, \ldots, gg_r).$$

We see that P_r is a free $\mathbb{Z}[G]$-module. Define the differential

$$d_r \colon P_r \to P_{r-1}, \quad (g_0, \ldots, g_r) \mapsto \sum_{i=0}^{r} (-1)^r (g_0, \ldots, \widehat{g_i}, \ldots, g_r).$$

Then $P_r \to P_{r-1} \to \cdots \to P_1 \to P_0 \to \mathbb{Z}$ is a free resolution of $\mathbb{Z}$ as $\mathbb{Z}[G]$-modules. Then $H^r(G, M) = H^r(\mathrm{Hom}_G(P_\bullet, M))$. Explicitly,

$$\mathrm{Hom}_G(P_r, M) = \{\varphi \colon G^{r+1} \to M : \varphi((gg_0, \ldots, gg_r)) = g\varphi(g_0, \ldots, g_r)\}.$$

We write $\tilde{C}^r(G, M) \coloneqq \mathrm{Hom}_G(P_r, M)$, and call its elements **homogeneous cochains of G valued in M**. The differential is

$$d^r \colon \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M), \quad \varphi \mapsto d^r(\varphi) \coloneqq \left((g_0, \ldots, g_{r+1}) \mapsto \sum_{i=0}^{r+1} (-1)^i \varphi(g_0, \ldots, \widehat{g_i}, \ldots, g_{r+1}) \right).$$

Definition 3.1.8. Note that a homogeneous cochain $\varphi \colon G^{r+1} \to M$ is determined by its value on elements $(1, g_1, g_1g_2, g_1g_2g_3, \ldots, g_1 \cdots g_r)$. Define the **inhomogeneous cochains** $C^r(G, M) \coloneqq \{\varphi \colon G^r \to M\}$. Under the identification $\tilde{C}^r(G, M) \cong C^r(G, M)$, the differential becomes $d^r \colon C^r \to C^{r+1}$, given by

$$\begin{aligned} d^r(\varphi)(g_1, \ldots, g_{r+1}) = g_1\varphi(g_2, \ldots, g_{r+1}) &+ \sum_{i=1}^{r} (-1)^i \varphi(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{r+1}) \\ &+ (-1)^{r+1} \varphi(g_1, \ldots, g_r). \end{aligned}$$

We call $Z^r(G, M) \coloneqq \ker d^r$ the **cocycles**, and $B^r(G, M) \coloneqq \operatorname{im} d^{r-1}$ the **coboundaries**. Then $H^r(G, M) = Z^r(G, M)/B^r(G, M)$.

Example 3.1.9. We can explicitly compute some low-degree groups. For example,

$$\begin{aligned} Z^1(G,M) &= \{\varphi\colon G \to M : d^1\varphi = 0\} \\ &= \{\varphi\colon G \to M : g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1) = 0\} \\ &= \{\varphi\colon G \to M : \varphi(g_1g_2) = g_1\varphi(g_2) + \varphi(g_1)\}. \end{aligned}$$

Such homomorphisms $\varphi\colon G \to M$ are called **crossed homomorphisms**. Similarly, we can compute

$$B^0(G,M) = \{d^0\varphi : \varphi\colon G^0 \to M\} = \{\varphi\colon G \to M : \varphi(g) = gm - m \text{ for some } m \in M\}.$$

Such homomorphisms $\varphi\colon G \to M$ are called **principal crossed homomorphisms**. Hence

$$H^1(G,M) = \{\text{crossed homomorphisms}\}/\{\text{principal crossed homomorphisms}\}.$$

Example 3.1.10. If M is a trivial G-module, then the crossed homomorphisms from $G \to M$ are precisely the usual homomorphisms $G \to M$, since $g_1\varphi(g_2) = \varphi(g_2)$. Similarly, since $gm = m$ for every $m \in M$, the only principal crossed homomorphism is the zero map. Hence $H^1(G,M) = \operatorname{Hom}(G,M)$.

3.2 Induction and restriction

Definition 3.2.1. Let $H \le G$ be a subgroup, and $M \in \mathsf{Mod}(H)$. The **induced G-module** is

$$\operatorname{Ind}_H^G M \coloneqq \operatorname{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M) = \{\varphi\colon G \to M : \varphi(hg) = h\varphi(g)\ \forall h \in H,\ g \in G\}.$$

Then $\operatorname{Ind}_H^G M \in \mathsf{Mod}(G)$, where G acts on $\operatorname{Ind}_H^G M$ by $(g \cdot \varphi)(x) = \varphi(xg)$, i.e. via the right action.

Remark. Note that $\varphi \in \operatorname{Ind}_H^G(M)$ is determined by its value on coset representatives S of $H\backslash G$. So as an abelian group, $\operatorname{Ind}_H^G M = \prod_{g\in S} gM$.

Proposition 3.2.2. *Consider $\operatorname{Ind}_H^G\colon \mathsf{Mod}(H) \to \mathsf{Mod}(G)$ as a functor.*

1. *(Frobenius reciprocity) For $M \in \mathsf{Mod}(G)$ and $N \in \mathsf{Mod}(H)$,*

$$\operatorname{Hom}_G(M, \operatorname{Ind}_H^G N) = \operatorname{Hom}_H(\operatorname{Res}_H^G M, N),$$

   where $\operatorname{Res}_H^G M$ is M regarded as an H-module (i.e. Ind_H^G is the right adjoint of Res_H^G).

2. *Ind_H^G is exact.*

3. *Ind_H^G preserves injective modules.*

Proof. Given $\alpha \in \operatorname{Hom}_G(M, \operatorname{Ind}_H^G N)$, define $\beta\colon \operatorname{Res}_H^G M \to N$ by $m \mapsto \alpha(m)(1_G)$. We must check β is H-equivariant. But clearly $\beta(hm) = (h\alpha(m))(1_G) = \alpha(m)(h) = h(\alpha(m)(1_G)) = h\beta(m)$, since α is G-equivariant. Conversely, given $\beta \in \operatorname{Hom}_H(\operatorname{Res}_H^G M, N)$, define $\alpha\colon M \to \operatorname{Ind}_H^G N$ by $m \mapsto (g \mapsto \beta(gm))$. These two maps $\alpha \mapsto \beta$ and $\beta \mapsto \alpha$ are inverse to each other.

Since Ind_H^G is a right adjoint, it is left exact by abstract nonsense. So it suffices to show it preserves surjections. Suppose $M \twoheadrightarrow N$ is a surjection of H-modules. Take $S = H\backslash G$ to be the coset representatives. Maps $\varphi \in \operatorname{Ind}_H^G N$ are defined by the values $\varphi(s) \in N$ for $s \in S$. Take $\tilde\varphi(s) \in M$ to be lifts of $\varphi(s) \in N$, using the surjection $M \twoheadrightarrow N$. Then $\tilde\varphi \in \operatorname{Ind}_H^G M$ and $\tilde\varphi \mapsto \varphi$, so $\operatorname{Ind}_H^G M \twoheadrightarrow \operatorname{Ind}_H^G N$ is a surjection.

Take $I \in \mathsf{Mod}(H)$ injective, so that $\operatorname{Hom}_H(-, I)$ is exact. By Frobenius reciprocity, $\operatorname{Hom}_H(-, I) = \operatorname{Hom}_G(-, \operatorname{Ind}_H^G I)$. Hence $\operatorname{Ind}_H^G I$ is also injective. □

Proposition 3.2.3 (Shapiro's lemma)**.** *For any $r \ge 0$, we have $H^r(G, \operatorname{Ind}_H^G N) = H^r(H, N)$.*

Proof. Take an injective resolution $N \to I^\bullet$. Then by the previous proposition, this gives an injective resolution $\mathrm{Ind}_H^G N \to \mathrm{Ind}_H^G I^\bullet$. So

$$H^r(G, \mathrm{Ind}_H^G N) = H^r(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \mathrm{Ind}_H^G I^\bullet)) = H^r(\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I^\bullet)) = H^r(H, N). \qquad \square$$

Definition 3.2.4. A G-module $M \in \mathsf{Mod}(G)$ is called **induced** if $M = \mathrm{Ind}_1^G M_0$ for some abelian group M_0.

Remark. If G is a finite group, then $\mathrm{Ind}_1^G M_0 \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$, which as an abelian group is $\bigoplus_{g \in G} gM_0$. Concretely, the map is $\varphi \mapsto \sum_{g \in G} g \otimes \varphi(g^{-1})$.

Corollary 3.2.5. *If M is an induced module, then $H^r(G, M) = 0$ for $r > 0$.*

Proof. By Shapiro's lemma, $H^r(G, \mathrm{Ind}_1^G M_0) = H^r(1, M_0)$. If $r = 0$, then $H^0(1, M_0) = (M_0)^1 = M_0$ where here $(-)^1$ denotes invariants under the trivial group. But this functor is exact, because it is the identity functor. Hence higher cohomologies vanish. $\square$

3.3 Functorial properties

Definition 3.3.1. Let $M \in \mathsf{Mod}(G)$ and $M' \in \mathsf{Mod}(G')$. Given $\alpha\colon G' \to G$ and $\beta\colon M \to M'$ such that they are **compatible**, i.e. $\beta(\alpha(g')m) = g'\beta(m)$, we get a homomorphism of cochain complexes

$$C^\bullet(G, M) \to C^\bullet(G', M'), \quad \varphi \mapsto \beta \circ \varphi \circ \alpha.$$

This induces a homomorphism $H^r(G, M) \to H^r(G', M')$. We will define three specific cases:

1. the **restriction** map $H^r(G, M) \xrightarrow{\mathrm{res}} H^r(H, M)$, given by $\alpha\colon H \hookrightarrow G$ and $\beta = \mathrm{id}$;
2. the **co-restriction** map $H^r(H, M) \xrightarrow{\mathrm{cor}} H^r(G, M)$, defined when $[G : H] < \infty$, given by $\alpha = \mathrm{id}_G$ and $\beta\colon \mathrm{Ind}_H^G(\mathrm{Res}_H^G M) \to M$ where $\varphi \mapsto \sum_{g \in H\backslash G} g\varphi(g^{-1})$;
3. the **inflation** map $H^r(G/H, M^H) \xrightarrow{\mathrm{inf}} H^r(G, M)$, defined when H is normal in G, given by $\alpha\colon G \twoheadrightarrow G/H$ and $\beta\colon M^H \hookrightarrow M$.

Proposition 3.3.2. *The composition* $\mathrm{cor} \circ \mathrm{res}\colon H^r(G, M) \to H^r(G, M)$ *is multiplication by* $[G : H]$.

Proof. By construction, $\mathrm{cor} \circ \mathrm{res}$ arises from $\alpha = \mathrm{id}_G$ and $\beta\colon M \to \mathrm{Ind}_H^G M \to M$. We can compute β explicitly:

$$m \mapsto (\varphi\colon g \mapsto gm) \mapsto \sum_{g \in H\backslash G} g\varphi(g^{-1}) = \sum_{g \in H\backslash G} m = [G : H]m.$$

(So in fact this is multiplication by $[G : H]$ at the level of the cochain complexes.) $\square$

Corollary 3.3.3. *If G is finite, then $H^r(G, M)$ is killed by $|G|$ for $r > 0$.*

Proof. Use $\mathrm{cor} \circ \mathrm{res}$ for the trivial group, to get the composition $H^r(G, M) \xrightarrow{\mathrm{res}} H^r(1, M) \xrightarrow{cor} H^r(G, M)$. We know $H^r(1, M) = 0$ for $r > 0$, so this composition is the zero map. But by the proposition, this composition is multiplication by $[G : 1] = |G|$. $\square$

Corollary 3.3.4. *If G is finite and M is finitely generated as an abelian group, then $H^r(G, M)$ is a finite group for $r > 0$.*

Proof. Since M is finitely generated, $H^r(G, M)$ is a finitely generated abelian group. (The cochain groups are finitely generated.) By the previous corollary, $H^r(G, M)$ is torsion, i.e. it has no free part. Hence it is actually a finite group. $\square$

Theorem 3.3.5 (Inflation-restriction exact sequence)**.** *Let $H \triangleleft G$ be a normal subgroup and $M \in \mathsf{Mod}(G)$. Let $r \geq 1$ and assume $H^i(H, M) = 0$ for $0 < i < r$. Then there is an exact sequence*

$$0 \to H^r(G/H, M^H) \xrightarrow{\inf} H^r(G, M) \xrightarrow{\mathrm{res}} H^r(H, M).$$

Proof. Consider $r = 1$. We check explicitly that the sequence is exact.

1. (Injectivity) Let $\varphi\colon G/H \to M^H$ be a cocycle such that $\inf(\varphi)$ is a coboundary. The inflation is the composition $\inf(\varphi)\colon G \to G/H \xrightarrow{\varphi} M^H \hookrightarrow M$, and $\inf(\varphi)(g) = gm - m$ for some $m \in M$ because we assume it is a coboundary. Then $\inf(\varphi)(g)$ depends only on $\bar{g} \in G/H$. In particular, $\inf(\varphi)(h) = 0$ for all $h \in H$. So $hm = m$ for all $h \in H$, i.e. $m \in M^H$. Hence $\varphi(\bar{g}) = \bar{g}m - m$ for some $m \in M^H$, i.e. φ itself is a coboundary.

2. ($\mathrm{res} \circ \inf = 0$) Let φ be a 1-cocycle representing some element in $H^1(G/H, M^H)$. Its image under the composition is $(\mathrm{res} \circ \inf)(\varphi)\colon H \hookrightarrow G \to G/H \xrightarrow{\varphi} M^H \hookrightarrow M$, which is clearly 0.

3. ($\ker \mathrm{res} \subset \mathrm{im}\inf$) Let $\varphi\colon G \to M$ be such that $\mathrm{res}(\varphi) = 0$. Then $\varphi(h) = hm - m$ for all $h \in H$. Define another cocycle $\varphi'\colon G \to M$ such that $\varphi'(g) \coloneqq \varphi(g) - (gm - m)$ for the same $m \in M$. Clearly φ' is cohomologous to φ, since we only added a coboundary, and $\varphi'(h) = 0$ for all $h \in H$. So φ' factors through G/H, i.e. $\varphi' \in \mathrm{im}(\inf)$.

Now induct on r. Recall we have $M \hookrightarrow \mathrm{Ind}_1^G M$. Write the quotient as M', so that we have an exact sequence $0 \to M \to \mathrm{Ind}_1^G M \to M' \to 0$. The long exact sequence of cohomology is

$$\cdots \to H^{r-1}(G, \mathrm{Ind}_1^G M) \to H^{r-1}(G, M') \to H^r(G, M) \to H^r(G, \mathrm{Ind}_1^G M) \to \cdots.$$

If $r \geq 2$, then both terms involving $\mathrm{Ind}_1^G M$ are zero. So $H^{r-1}(G, M') \cong H^r(G, M)$. By assumption, $H^i(H, M) = 0$ for all $0 < i < r$. Then $H^i(H, M') = 0$ for all $0 < i < r - 1$. So by the induction hypothesis, there is an exact sequence

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^{r-1}(G/H, (M')^H) & \xrightarrow{\inf} & H^{r-1}(G, M') & \xrightarrow{\mathrm{res}} & H^{r-1}(H, M') & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & H^r(G/H, M^H) & \xrightarrow{\inf} & H^r(G, M) & \xrightarrow{\mathrm{res}} & H^r(H, M) & \longrightarrow & 0.
\end{array}$$

where the isomorphisms arise from dimension shifting. □

Remark. More generally, given an exact sequence of G-modules $0 \to M \to A^1 \to \cdots \to A^k \to N \to 0$ such that A^i are induced, there are isomorphisms $H^r(G, N) \xrightarrow{\sim} H^{r+k}(G, M)$ for all $r \geq 1$.

3.4 Group homology

Recall that $H^r(G, -)$ is the right derived functor of $(-)^G$, the invariants functor. View M^G as the largest G-submodule with trivial G-action. By analogy, $H_r(G, -)$ is the left derived functor of $(-)_G$, the **coinvariants functor**. View M_G as the largest quotient with trivial G-action.

Definition 3.4.1. The **coinvariants** M_G of M is defined by

$$M_G \coloneqq M/\langle gm - m : g \in G, m \in M \rangle.$$

Let $\mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z}$ be induced by $g \mapsto 1$, and let $I_G \coloneqq \ker(\deg)$, called the **augmentation ideal**. This is a free $\mathbb{Z}[G]$-submodule with basis $\{g - 1 : g \neq 1\}$. Then

$$M_G = M/I_G M \cong M \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]/I_G$$

by definition. Hence $(-)_G$ is right exact.

Remark. We can compute $H_r(G, M)$ using a projective resolution $P_\bullet \to M$. Then $H_r(G, M) = H^r(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]/I_G)$. Concretely, the following properties characterize $H_r(G, -)$:

1. $H_0(G, M) = M_G$, by construction;
2. if P is a projective G-module, then $H_r(G, P) = 0$ for all $r \geq 1$;
3. to every short exact sequence $0 \to A \to B \to C \to 0$, there is a long exact sequence in homology

$$\cdots \to H_2(G, C) \to H_1(G, A) \to H_1(G, B) \to H_1(G, C) \to A_G \to B_G \to C_G \to 0.$$

Proposition 3.4.2. *$H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}} := G/[G, G]$ (with trivial G-action on $\mathbb{Z}$).*

Proof. Use the short exact sequence $0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z} \to 0$. This gives a long exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_1(G,\mathbb{Z}) & \longrightarrow & H_0(G, I_G) & \longrightarrow & H_0(G,\mathbb{Z}[G]) & \longrightarrow & H_0(G,\mathbb{Z}) & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \| & & \\ 0 & \longrightarrow & H_1(G,\mathbb{Z}) & \longrightarrow & I_G/I_G^2 & \longrightarrow & \mathbb{Z}[G]/I_G\mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

where we used that $\mathbb{Z}[G]$ is a free G-module, so its H_1 vanishes. So the map $H_0(G, I_G) \to H_0(G, \mathbb{Z}[G])$ is the zero map. It follows that $H_1(G, \mathbb{Z}) \cong I_G/I_G^2$. Define the map

$$G \to I_G/I_G^2, \quad g \mapsto g - 1.$$

This is a group homomorphism by checking

$$I_G^2 \ni (g_1 - 1)(g_2 - 1) = -(g_1 - 1) - (g_2 - 1) + (g_1 g_2 - 1),$$

so that $g_1 g_2 - 1 = (g_1 - 1) + (g_2 - 1)$ in I_G/I_G^2. But I_G/I_G^2 is abelian, so this map necessarily factors through $G^{\mathrm{ab}} \to I_G/I_G^2$. Now define the map

$$I_G \mapsto G^{\mathrm{ab}}, \quad g - 1 \mapsto g.$$

Using the same identity, we can check I_G^2 lies in the kernel, and the induced $I_G/I_G^2 \to G^{\mathrm{ab}}$ is the inverse map. □

Remark. We can identify $H^r(G, \mathbb{Z}) \cong H^r_{\mathrm{sing}}(BG, \mathbb{Z})$, where BG is the classifying space of G (recall that $\pi_1(BG) = G$), and H^r_{sing} denotes singular cohomology. Similarly, $H_r(G, \mathbb{Z}) \cong H_r^{\mathrm{sing}}(BG, \mathbb{Z})$. In particular, the proposition reflects that $H_1(G, \mathbb{Z}) \cong H_1^{\mathrm{sing}}(BG, \mathbb{Z}) = \pi_1(BG)^{\mathrm{ab}} = G^{\mathrm{ab}}$.

Example 3.4.3. If $G = \mathbb{Z}$, then $BG = S^1$. Hence $H^r(\mathbb{Z}, M) = 0$ for $r \geq 2$. Similarly, if $G = \mathbb{Z} * \cdots * \mathbb{Z}$, then $BG = S^1 \vee \cdots \vee S^1$, and $H^r(\mathbb{Z}, M) = 0$ again for $r \geq 2$.

3.5 Tate cohomology

Let G be a finite group. In this special case, we can "patch together" group cohomology and homology.

Definition 3.5.1. Let $M \in \mathsf{Mod}(G)$. Define the **norm map**

$$\mathrm{Nm}_G \colon M \to M, \quad m \mapsto \sum_{g \in G} gm.$$

Then $g \,\mathrm{Nm}_G(m) = \mathrm{Nm}_G(m)$, so that $\mathrm{im}(\mathrm{Nm}_G) \subset M^G$. Also, $\mathrm{Nm}_G(gm) = \mathrm{Nm}_G(m)$, so that $\ker(\mathrm{Nm}_G) \supset I_G M$. Hence Nm_G induces a map

$$\mathrm{Nm}_G \colon (H_0(G, M) = M_G = M/I_G M) \to (M^G = H^0(G, M)).$$

Using this, we connect the two long exact sequences $H^\bullet$ and $H_\bullet$:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H_1(C) & \longrightarrow & H_0(A) & \longrightarrow & H_0(B) & \longrightarrow & H_0(C) & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \\
0 & \longrightarrow & H^0(A) & \longrightarrow & H^0(B) & \longrightarrow & H^0(C) & \longrightarrow & H^1(A) & \longrightarrow & \cdots.
\end{array}$$

We can apply the snake lemma to this diagram to get the **Tate cohomology groups**

$$\widehat{H}^r(G,M) \coloneqq \begin{cases} H^r(G,M) & r > 0 \\ H^0(G,M)/\operatorname{im}(\mathrm{Nm}_G) & r = 0 \\ \ker(\mathrm{Nm}_G)/I_G M & r = -1 \\ H_{-(r+1)}(G,M) & r < -1, \end{cases}$$

which therefore form a **very long exact sequence** in both directions.

Remark. If M is an induced G-module, then $\widehat{H}^r(G,M) = 0$ for all $r \in \mathbb{Z}$. (See homework.) More strongly, Shapiro's lemma holds in general for $\widehat{H}^r(G,M)$. Hence we can dimension shift for $\widehat{H}^r$ in both directions:

1. using $0 \to M \hookrightarrow \mathrm{Ind}_1^G M \to M' \to 0$, we get $\widehat{H}^{r+1}(M) = \widehat{H}^r(M')$;
2. using $0 \to M' \to (\mathrm{Ind}_1^G M = \mathbb{Z}[G] \otimes_{\mathbb{Z}} M) \to M \to 0$, we get $\widehat{H}^r M = \widehat{H}^{r+1}(M')$.

Remark. There are also functorial maps

$$\mathrm{res}\colon \widehat{H}^r(G,M) \to \widehat{H}^r(H,M), \quad \mathrm{cor}\colon \widehat{H}^r(H,M) \to \widehat{H}^r(G,M),$$

and $\mathrm{cor} \circ \mathrm{res} = [G:H]$.

Remark. Let $P_\bullet \to \mathbb{Z}$ be a free $\mathbb{Z}[G]$-resolution of $\mathbb{Z}$. Taking duals gives another $\mathbb{Z}[G]$-resolution $\mathbb{Z} \to P_\bullet^*$. Then we get a very long exact sequence

$$\to P_2 \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to \cdots$$

where $P_{-i} \coloneqq P_i^*$. Then $\widehat{H}^r(G,M) = H^r(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, M))$, using $P_n \otimes_{\mathbb{Z}[G]} M = \mathrm{Hom}_{\mathbb{Z}[G]}(P_n^*, M)$.

3.6 Tate cohomology of finite cyclic groups

Example 3.6.1. Let $G = \langle \sigma \rangle$ be a finite cyclic group. Then

$$\begin{aligned} \widehat{H}^0(G,M) &= H^0(G,M)/\operatorname{im}(\mathrm{Nm}_G) = \ker(\sigma - 1)/\operatorname{im}(\mathrm{Nm}_G) \\ \widehat{H}^{-1}(G,M) &= \ker(\mathrm{Nm}_G)/I_G M = \ker(\mathrm{Nm}_G)/\operatorname{im}(\sigma - 1). \end{aligned}$$

Proposition 3.6.2. *Let $G = \langle \sigma \rangle$ be a finite cyclic group. Then*

$$\widehat{H}^r(G,M) \cong \widehat{H}^{r+2}(G,M) \quad \forall r \in \mathbb{Z}.$$

Proof. Since $\mathrm{Nm}_G = 1 + \sigma + \cdots + \sigma^{n-1}$, there is a free resolution

$$\cdots \xrightarrow{\mathrm{Nm}_G} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\mathrm{Nm}_G} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z}.$$

Hence this gives a very long exact sequence which is periodic of period 2. So Tate cohomology is also periodic of period 2, i.e. $\widehat{H}^r(G,M) \cong \widehat{H}^{r+2}(G,M)$. □

Definition 3.6.3. Let G be finite cyclic. Define the **Herbrand quotient** of M as

$$h(M) \coloneqq |\widehat{H}^0(G,M)|/|\widehat{H}^1(G,M)|$$

if both $\widehat{H}^0$ and $\widehat{H}^1$ are finite.

Proposition 3.6.4. *If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules and two of the three Herbrand quotients $h(A)$, $h(B)$, $h(C)$ are defined, so is the third, and $h(B) = h(A)h(C)$.*

Proof. Write the long exact sequence and truncate it:

$$0 \to K \to \widehat{H}^0(A) \to \widehat{H}^0(B) \to \widehat{H}^0(C) \to \widehat{H}^1(A) \to \widehat{H}^1(B) \to \widehat{H}^1(C) \to Q \to 0.$$

For long exact sequences, cardinality is multiplicative, so

$$1 = \frac{|K| \cdot |\widehat{H}^0(B)| \cdot |\widehat{H}^1(A)| \cdot |\widehat{H}^1(C)|}{|\widehat{H}^0(A)| \cdot |\widehat{H}^0(C)| \cdot |\widehat{H}^1(B)| \cdot |Q|} = \frac{h(B)}{h(A)h(C)} \frac{|K|}{|Q|}.$$

So it suffices to show $|K| = |Q|$. From the previous proposition,

$$K = \ker(\widehat{H}^0(A) \to \widehat{H}^0(B)) = \operatorname{coker}(\widehat{H}^{-1}(B) \to \widehat{H}^{-1}(C)) = \operatorname{coker}(\widehat{H}^1(B) \to \widehat{H}^1(C)) = Q. \qquad \square$$

Proposition 3.6.5. *If M is a finite-order G-module, then $h(M) = 1$.*

Proof. There is an exact sequence $0 \to \widehat{H}^{-1}(G,M) \to M_G \xrightarrow{\mathrm{Nm}_G} M^G \to \widehat{H}^0(G,M) \to 0$. We want to show $|\widehat{H}^1| = |\widehat{H}^0|$, so it suffices to show $|M_G| = |M^G|$. But if $G = \langle\sigma\rangle$, there is another exact sequence $0 \to M^G \to M \xrightarrow{\sigma-1} M \to M_G \to 0$. Hence $|M^G| = |M_G|$. $\square$

Corollary 3.6.6. *If $\alpha\colon M \to N$ has finite-order kernel and cokernel, then $h(M) = h(N)$.*

Proof. There is an exact sequence $0 \to \ker(\alpha) \to M \xrightarrow{\alpha} N \to \operatorname{coker}(\alpha) \to 0$. By the proposition, $h(\ker\alpha) = h(\operatorname{coker}\alpha) = 1$. Splitting this into two short exact sequences, we get $h(M) = h(N)$. $\square$

Chapter 4

Local class field theory

4.1 Tate's theorem

Theorem 4.1.1 (Tate)**.** *Let G be a finite group and $C \in \mathsf{Mod}(G)$. Assume that for any subgroup $H \subset G$,*

1. *$H^1(H, C) = 0$, and*
2. *$H^2(H, C)$ is a cyclic group of order $|H|$.*

Then for any $r \in \mathbb{Z}$, there is an isomorphism $\widehat{H}^r(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{r+2}(G, C)$.

Example 4.1.2. Take L/K a Galois extension of local fields and $G \coloneqq \mathrm{Gal}(L/K)$. Let $C = L^\times$. Take $r = -2$. Then $H_1(G, \mathbb{Z}) \cong \widehat{H}^0(G, L^\times)$. But $H_1(G, \mathbb{Z}) = G^{\mathrm{ab}}$, and $\widehat{H}^0(G, L^\times) = K^\times / \mathrm{Nm}(L^\times)$. Hence

$$G^{\mathrm{ab}} \xrightarrow{\sim} K^\times / \mathrm{Nm}(L^\times),$$

which is precisely the local Artin map.

Remark. The proof strategy: we will construct an exact sequence of G-modules $0 \to C \to C(\varphi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ such that $\widehat{H}^r(G, C(\varphi)) = \widehat{H}^r(G, \mathbb{Z}[G]) = 0$. To do so, we need to discuss H^2. Recall that:

1. a 2-cocycle is a map $\varphi\colon G^2 \to M$ such that
$$0 = d\varphi = g_1\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) + \varphi(g_1, g_2);$$
2. a 2-coboundary is a map $\varphi\colon G^2 \to M$ such that
$$\varphi(g_1, g_2) = (d\psi)(g_1, g_2) = g_1\psi(g_2) - \psi(g_1g_2) + \psi(g_1).$$

Fact (we will show part of it): an interpretation of $H^2(G, M)$ is

$$H^2(G, M) \xrightarrow{\sim} \left\{ \begin{array}{c} \text{group extensions of } G \text{ by } M \\ 1 \to M \to E \to G \to 1 \\ \text{s.t. conjugation of } G \text{ on } M \text{ is the } G\text{-module structure} \end{array} \right\}$$

For example, if M is a trivial G-module, then we are looking at all extensions such that $M \subset Z(E)$, the center of E. Such extensions are called **central extensions**. Given an extension $1 \to M \to E \to G \to 1$, we want to get a 2-cocycle. Choose an arbitrary (set-theoretic) section $s\colon G \to E$. For any $g_1, g_2 \in G$, the images $s(g_1)s(g_2)$ and $s(g_1g_2)$ map to the same element in g, and therefore must differ by an element

$\varphi(g_1, g_2) \in M$, i.e. $s(g_1)s(g_2) = \varphi(g_1, g_2)s(g_1g_2)$. By associativity and the requirement that conjugation is the G-module structure,

$$\begin{aligned}\varphi(g_1, g_2)\varphi(g_1g_2, g_3)s(g_1g_2g_3) &= \varphi(g_1, g_2)s(g_1g_2)s(g_3) = (s(g_1)s(g_2))s(g_3)\\ &= s(g_1)((s(g_2)s(g_3)) = s(g_1)\varphi(g_2, g_3)s(g_2g_3)\\ &= g_1\varphi(g_2, g_3)s(g_1)s(g_2g_3) = g_1\varphi(g_2, g_3)\varphi(g_1, g_2g_3)s(g_1g_2g_3).\end{aligned}$$

So φ is a 2-cocycle. We can check that different choices of the section s gives φ up to 2-coboundaries.

Definition 4.1.3. Let φ be a 2-cocycle representing $\gamma \in H^2(G, C)$. Define $C(\varphi) \coloneqq C \oplus \bigoplus_{1\neq g\in G} \mathbb{Z}x_g$ as an abelian group, where x_g is just a formal symbol, with G-action given by

$$g_1 \cdot x_{g_2} \coloneqq x_{g_1g_2} - x_{g_1} + \varphi(g_1, g_2).$$

Convention: $x_1 \coloneqq \varphi(1, 1) \in C$. The 2-cocycle condition ensures this is indeed a G-action. We have an exact sequence of G-modules

$$1 \to C \to C(\varphi) \xrightarrow{\varphi\colon x_g\mapsto g-1} I_G \to 1.$$

Because $\varphi(g_1, g_2) = g_1x_{g_2} - x_{g_1g_2} + x_{g_1} = d(g \mapsto x_g)$, we get a natural map $H^2(G, C) \to H^2(G, C(\varphi))$ where $\varphi \mapsto 0$. Therefore $C(\varphi)$ is called the **splitting module of** φ.

Proof of Tate's theorem. The exact sequence $0 \to C \to C(\varphi) \to I_G \to 0$ gives a long exact sequence

$$\cdots \to H^1(H, C) \to H^1(H, C(\varphi)) \to H^1(H, I_G) \to H^2(H, C) \xrightarrow{0} H^2(H, C(\varphi)) \to H^2(H, I_G) \to \cdots,$$

where the middle map is 0 by the construction of $C(\varphi)$ and that $H^2(H, C)$ is cyclic. Exercise: if G is finite and $H \leq G$ is normal, then

$$\widehat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}, \quad H^1(G, \mathbb{Z}) = 0, \quad H^2(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$
$$H^1(H, I_G) = \mathbb{Z}/|H|\mathbb{Z}, \quad H^2(H, I_G) = 0.$$

By assumption, $H^1(H, C) = 0$ and $H^2(H, C) = \mathbb{Z}/|H|\mathbb{Z}$ is cyclic. It follows that $H^1(H, I_G) \to H^2(H, C)$ is an isomorphism, and its kernel and cokernel are zero: $H^1(H, C(\varphi)) = H^2(H, C(\varphi)) = 0$. Now Tate's theorem follows from the following more general theorem. It gives $\widehat{H}^r(G, C(\varphi)) = 0$ for all $r \in \mathbb{Z}$. Then the result follows from the exact sequence $0 \to C \to C(\varphi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ (since all Tate cohomologies vanishes for the induced module $\mathbb{Z}[G]$ as well). □

Theorem 4.1.4. *Let G be a finite group. If $H^1(H, M) = H^2(H, M) = 0$ for any subgroup $H \leq G$, then $\widehat{H}^r(G, M) = 0$ for every $r \in \mathbb{Z}$.*

Proof. If G is cyclic, we are done by the 2-periodicity of Tate cohomology for finite cyclic groups. If G is solvable, induct on $|G|$. Pick $H \leq G$ such that G/H is cyclic. By the inductive hypothesis, $H^r(H, M) = 0$ for all $r \geq 0$. So by the inflation-restriction exact sequence, $H^r(G/H, M^H) \xrightarrow{\sim} H^r(G, M)$ is an isomorphism for $r \geq 1$. Since $H^r(G, M) = 0$ for $r = 1, 2$, this implies $H^1(G/H, M^H) = H^2(G/H, M^H) = 0$. Hence $\widehat{H}^r(G/H, M^H) = 0$ for all $r \in \mathbb{Z}$, and so $H^r(G, M) = 0$ for all $r \geq 1$. We can manually check $\widehat{H}^0(G, M) = 0$, because $\widehat{H}^0(G/M, M^H) = 0$ implies $M^G = \mathrm{im}(\mathrm{Nm}_{G/H} M^H)$ and $\widehat{H}^0(H, M) = 0$ implies $M^H = \mathrm{im}(\mathrm{Nm}_H M)$, so $M^G = \mathrm{im}(\mathrm{Nm}_G M)$.

Now dimension shift: given $0 \to M^1 \to \mathrm{Ind}_1^G M \to M \to 0$, we have $\widehat{H}^r(H, M) \xrightarrow{\sim} \widehat{H}^{r+1}(H, M')$ for all $r \in \mathbb{Z}$. By the inductive hypothesis, $\widehat{H}^r(H, M') = 0$ implies $\widehat{H}^r(G, M') = 0$ for all $r \geq 0$. But then $\widehat{H}^r(G, M) = 0$ for all $r \geq -1$. Repeating, we get $\widehat{H}^r(G, M) = 0$ for all $r \in \mathbb{Z}$. Finally, for an arbitrary finite group G, apply the solvable case to all p-Sylow subgroups $G_p \leq G$. This implies $\widehat{H}^r(G_p, M) = 0$ for all $r \in \mathbb{Z}$ and all p, which implies $\widehat{H}^r(G, M) = 0$ for all $r \in \mathbb{Z}$. □

4.2 Vanishing of H^1

Theorem 4.2.1 (Hilbert's theorem 90)**.** *If L/K is a finite Galois extension of arbitrary fields, then*

$$H^1(\mathrm{Gal}(L/K), L^\times) = 0.$$

Proof. Let φ be a 1-cocycle. We want to show $\varphi(g) = gm/m$ for some $m \in L^\times$. To construct m, pick $a \in L^\times$ and define $m \coloneqq \sum_{g\in G} \varphi(g)ga$ such that $m \neq 0$. We can always arrange for $m \neq 0$ because $g\colon L^\times \to L^\times$ as characters of $L^\times$ are linearly independent. Then $\sum \varphi(g)g\colon L^\times \to L^\times$ is a non-zero map, so such an a exists. Since $g\varphi(h) = \varphi(gh)\varphi(g)^{-1}$,

$$gm = g\sum_{h\in G} \varphi(h)ha = \sum_{h\in G} \frac{\varphi(hg)}{\varphi(g)} gha = \frac{1}{\varphi(g)} \sum_{h\in G} \varphi(h)ha = \frac{m}{\varphi(g)}.$$

Hence $\varphi(g) = m/gm$. (Fix this by inverting m.) □

Example 4.2.2. If L/K is a cyclic Galois extension, then $0 = H^1(G, L^\times) = \widehat{H}^{-1}(G, L^\times)$ by the 2-periodicity of Tate cohomology for cyclic groups. Write $G = \langle\sigma\rangle$, so that

$$\widehat{H}^{-1}(G, L^\times) = \ker(\mathrm{Nm}_G)/\operatorname{im}(\sigma - 1).$$

In other words, if $a \in L^\times$ with $\mathrm{Nm}_{L/K}(a) = 1$, then $a = \sigma b/b$ for some $b \in L^\times$.

Example 4.2.3. Explicitly, take $L/K = \mathbb{Q}(i)/\mathbb{Q}$. If $a \coloneqq x + iy$ and $b \coloneqq m + in$ are in $\mathbb{Q}(i)^\times$, then

$$\mathrm{Nm}_{L/K}(a) = x^2 + y^2, \quad \frac{\sigma b}{b} = \frac{m - in}{m + in} = \frac{m^2 - n^2}{m^2 + n^2} + \frac{2mn}{m^2 + n^2} i.$$

Hilbert's theorem 90 therefore implies that if $x^2 + y^2 = 1$, then there exist $m, n \in \mathbb{Q}$ such that

$$x = \frac{m^2 - n^2}{m^2 + n^2}, \quad y = \frac{2mn}{m^2 + n^2}.$$

Clearing denominators, this is the complete family of solutions to the Pythagorean triples problem.

Remark. Hilbert's theorem 90 implies $H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times) = 0$. In general, if $G = \varprojlim_H G/H$ is a profinite group, then we define $H^r(G, M) \coloneqq \varinjlim_H H^r(G/H, M^H)$. This is the same as $H^r(G, M) = Z^r_{\mathrm{cts}}(G, M)/B^r_{\mathrm{cts}}(G, M)$ using continuous cochains, i.e. we require that any cochains factors through some finite quotient G/H. So we interpret Hilbert's theorem 90 in this case as

$$0 = H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times) = H^1_{\text{ét}}(\operatorname{Spec} K, \mathbb{G}_m) = \mathrm{Pic}(\operatorname{Spec} K).$$

4.3 H^2 of unramified extensions

Theorem 4.3.1. *Let L/K be a finite Galois unramified extension of non-archimedean local fields, and write $G \coloneqq \mathrm{Gal}(L/K)$. Then $H^2(G, L^\times)$ is a cyclic group of order $|G|$.*

Remark. Recall that in the setting of the theorem, $G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k) = \langle\mathrm{Frob}_{L/K}\rangle$ where ℓ, k are the residue fields of L and K respectively, and the Frobenius map is $x \mapsto x^q$ where $q \coloneqq \#k$.

Remark. The strategy of proof is as follows. We have a G-module decomposition $L^\times \cong \mathcal{O}_L^\times \times \pi^{\mathbb{Z}}$, where π is a uniformizer. We can choose $\pi \in K^\times$ because L/K is unramified. In particular, G acts trivially on $\pi^{\mathbb{Z}}$. We will put a filtration on $\mathcal{O}_L^\times$ so that we can compute its cohomology. The cohomology of $\pi^{\mathbb{Z}}$ is easy.

Definition 4.3.2. Let $U_L \coloneqq \mathcal{O}_L^\times$, and define $U_L^{(i)} \coloneqq 1 + \mathfrak{m}_L^i$. Then there is a **filtration** $U_L \supset U_L^{(1)} \supset U_L^{(2)} \supset \cdots$. The inclusions give short exact sequences

$$1 \to U_L^{(1)} \to U_L \xrightarrow{a \mapsto a \bmod \pi} \ell^\times \to 1$$
$$1 \to U_L^{(i+1)} \to U_L^{(i)} \xrightarrow{1 + a\pi^i \mapsto a \bmod \pi} \ell \to 1.$$

We will use these short exact sequences to compute the cohomology of the units $\mathcal{O}_L^\times$.

Proposition 4.3.3. *$\widehat{H}^r(G, \ell^\times) = 0$ for all $r \in \mathbb{Z}$.*

Proof. By Hilbert's theorem 90, $H^1(G, \ell^\times) = 0$. Recall that the Herbrand quotient $h(M) = 1$ for M finite order. So in particular, $h(\ell^\times) = 1$. Hence $\widehat{H}^0(G, \ell^\times) = 0$ as well. By the 2-periodicity of Tate cohomology, we are done. □

Corollary 4.3.4. *The norm map $\mathrm{Nm}\colon \ell^\times \to k^\times$ is surjective, since $\widehat{H}^0(G, \ell^\times) = k^\times / \mathrm{Nm}(\ell^\times)$.*

Proposition 4.3.5. *$\widehat{H}^r(G, \ell) = 0$ for all $r \in \mathbb{Z}$.*

Proof. We showed (in the homework) that $H^r(G, \ell) = 0$ for all $r \geq 1$ because by Galois theory, ℓ is an induced module. By the 2-periodicity of Tate cohomology, we are done. □

Corollary 4.3.6. *$\mathrm{Tr}\colon \ell \to k$ is surjective, since $\widehat{H}^0(G, \ell) = k / \mathrm{Tr}(\ell)$.*

Proposition 4.3.7. *$\mathrm{Nm}\colon \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective.*

Proof. There are commutative diagrams

$$\begin{array}{ccc} U_L & \longrightarrow & \ell^\times \\ {\scriptstyle \mathrm{Nm}}\downarrow & & {\scriptstyle \mathrm{Nm}}\downarrow \\ U_K & \longrightarrow & k^\times \end{array} \qquad \begin{array}{ccc} U_L^{(i)} & \longrightarrow & \ell \\ {\scriptstyle \mathrm{Nm}}\downarrow & & {\scriptstyle \mathrm{Tr}}\downarrow \\ U_K^{(i)} & \longrightarrow & k. \end{array}$$

If $a \in U_K$, then there exists $a_0 \in U_L$ such that $a / \mathrm{Nm}(a_0) \in U_K^{(1)}$ by the surjectivity of $\mathrm{Nm}\colon \ell^\times \to k^\times$. Similarly, there exists $a_1 \in U_L^{(1)}$ such that $(a / \mathrm{Nm}(a_0))(1 / \mathrm{Nm}(a_1)) \in U_K^{(2)}$ by the surjectivity of $\mathrm{Tr}\colon \ell \to k$. Repeating, we get $a_0, \ldots, a_n$ such that

$$\frac{a}{\mathrm{Nm}(a_0 \cdots a_n)} \in U_K^{(n+1)}.$$

Define $b \coloneqq \prod_{i=1}^\infty a_i$. Then $a / \mathrm{Nm}(b) \in \bigcap_{i=1}^\infty U_K^{(i)} = \{1\}$, i.e. $a = \mathrm{Nm}(b)$. □

Corollary 4.3.8. *$\widehat{H}^0(G, U_L) = 0$*

Proposition 4.3.9. *$\widehat{H}^r(G, U_L) = 0$ for all $r \in \mathbb{Z}$.*

Proof. It suffices by the 2-periodicity of Tate cohomology to check $H^1(G, U_L) = 0$. But $U_L \times \pi^{\mathbb{Z}} \cong L^\times$ as G-modules, so by Hilbert's theorem 90

$$0 = H^1(G, L^\times) = H^1(G, U_L) \oplus H^1(G, \pi^{\mathbb{Z}}) \qquad \square.$$

Proposition 4.3.10. *$H^2(G, L^\times) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$.*

Proof. Write $L^\times = U_L \times \pi^{\mathbb{Z}}$. Then $H^2(G, L^\times) \cong H^2(G, \pi^{\mathbb{Z}}) = H^2(G, \mathbb{Z})$. By a homework exercise, this is $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. □

4.4 H^2 of ramified extensions

Definition 4.4.1. Define the **invariant map** $\mathrm{inv}_{L/K}\colon H^2(\mathrm{Gal}(L/K), L^\times) \to \mathbb{Q}/\mathbb{Z}$ to be the composition

$$H^2(G, L^\times) \xrightarrow{\sim} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} (1/|G|)\mathbb{Z}/\mathbb{Z}$$

where $G = \langle \sigma \rangle$ (i.e. $\sigma = \mathrm{Frob}_L$). Patch these together to get

$$\mathrm{inv}_K\colon (H^2(\mathrm{Gal}(K^{\mathrm{un}}/K), (K^{\mathrm{un}})^\times) = \varinjlim_{L/K \text{ unramified}} H^2(\mathrm{Gal}(L/K), L^\times)) \to \mathbb{Q}/\mathbb{Z}.$$

(Here K^{un} is the maximal unramified extension of K inside a fixed algebraic closure.)

Remark. Shorthand notation: write $H^2(L/K) \coloneqq H^2(\mathrm{Gal}(L/K), L^\times)$. The invariant map gives an isomorphism $H^2(K^{\mathrm{un}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$.

Proposition 4.4.2. *Let L/K be a finite extension of degree n. Then there is a commutative diagram*

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{un}/L) \\ {\scriptstyle \mathrm{inv}_K}\downarrow & & {\scriptstyle \mathrm{inv}_L}\downarrow \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Proof. Decompose the invariant map so that we can wee what the base change to L does at each step:

$$\begin{array}{ccccccc} H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{ord}_K} & H^2(K^{\mathrm{un}}/K, \mathbb{Z}) & = & H^1(K^{\mathrm{un}}/K, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & {\scriptstyle ?}\downarrow & & {\scriptstyle ?}\downarrow & & {\scriptstyle ?}\downarrow \\ H^2(L^{\mathrm{un}}/L) & \xrightarrow{\mathrm{ord}_L} & H^2(L^{\mathrm{un}}/L, \mathbb{Z}) & = & H^1(L^{\mathrm{un}}/L, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}. \end{array}$$

To understand the first square, note that we have a commutative diagram

$$\begin{array}{ccc} (K^{\mathrm{un}})^\times & \xrightarrow{\mathrm{ord}_K} & \mathbb{Z} \\ \downarrow & & {\scriptstyle e(L/K)}\downarrow \\ (L^{\mathrm{un}})^\times & \xrightarrow{\mathrm{ord}_L} & \mathbb{Z} \end{array}$$

because the uniformizer in K and the uniformizer in L get sent to 1 in $\mathbb{Z}$, but the ratio of their degrees is by definition $e(L/K)$, the ramification index. The second square is trivial and does nothing to the vertical maps. To understand the third square, note that the generator Frob_K is $x \mapsto x^q$ where $q = \#k$, and the generator Frob_L is $x \mapsto x^{q^f}$ where $q^f = \#\ell$. Hence $\mathrm{Frob}_L = (\mathrm{Frob}_K)^f$. Hence the last vertical arrow is multiplication by $ef = n$. □

Theorem 4.4.3. *There exists a canonical isomorphism*

$$\mathrm{inv}_K\colon H^2(K^{al}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

If L/K is finite Galois of degree n, then we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\mathrm{inf}} & H^2(K^{al}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{al}/L) \\ & & \downarrow & & {\scriptstyle \mathrm{inv}_K}\downarrow & & {\scriptstyle \mathrm{inv}_L}\downarrow \\ 0 & \longrightarrow & (1/n)\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Lemma 4.4.4. *For any finite Galois extension L/K, the group $H^2(L/K)$ contains a subgroup isomorphic to $(1/n)\mathbb{Z}/\mathbb{Z}$.*

Proof. Recall that the restriction map for the unramified part is just multiplication by n, so using the inflation-restriction sequence, there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & (1/n)\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L) \\ & & & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} \\ 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\inf} & H^2(K^{\mathrm{al}}/K) & \longrightarrow & H^2(L^{\mathrm{al}}/L). \end{array}$$

The two vertical arrows are injections. So there is an injection of the kernel as well, i.e. $(1/n)\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(L/K)$. □

Lemma 4.4.5. $|H^2(L/K)| = n$.

Proof. First assume L/K is cyclic of order n. By a homework exercise, $h(L^\times) = n$. By Hilbert 90, $H^1(\mathrm{Gal}(L/K), L^\times) = 0$, so $|H^2(L/K)| = n$.

In general, $\mathrm{Gal}(L/K)$ is always solvable (by another homework exercise). So induct on $|\mathrm{Gal}(L/K)|$. Choose a cyclic sub-extension L'/K inside L/K. The inflation-restriction sequence is

$$0 \to H^2(L'/K) \xrightarrow{\inf} H^2(L/K) \xrightarrow{\mathrm{Res}} H^2(L/L').$$

By the induction hypothesis, $|H^2(L/K)| \le |H^2(L'/K)||H^2(L/L')|$. Both of these groups have smaller order, so we are done by the previous lemma. □

Proof of theorem. By the previous two lemmas,

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\inf} & H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{Res}} & H^2(K^{\mathrm{al}}/L) \\ & & \| & & \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \inf} \\ 0 & \longrightarrow & (1/n)\mathbb{Z}/\mathbb{Z} & \xrightarrow{\inf} & H^2(K^{\mathrm{un}}/K) & \xrightarrow{\mathrm{Res}} & H^2(L^{\mathrm{un}}/L). \end{array}$$

Hence $H^2(K^{\mathrm{un}}/K) \xrightarrow{\inf} H^2(K^{\mathrm{al}}/K) = \varinjlim H^2(L/K)$ is an injection. This implies the map inf here must actually be an isomorphism. So the invariant map is defined on $H^2(K^{\mathrm{al}}/K)$ using this isomorphism. □

Remark. There are actually two commutative diagrams:

$$\begin{array}{ccc} H^2(K^{\mathrm{al}}/K) & \xrightarrow{\mathrm{res}} & H^2(L^{\mathrm{al}}/L) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_K} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array} \qquad \begin{array}{ccc} H^2(K^{\mathrm{al}}/K) & \xleftarrow{\mathrm{cor}} & H^2(L^{\mathrm{al}}/L) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_K} \\ \mathbb{Q}/\mathbb{Z} & = & \mathbb{Q}/\mathbb{Z}. \end{array}$$

This comes from the fact that $\mathrm{cor} \circ \mathrm{res} = n$.

Remark. $H^2(K^{\mathrm{al}}/K) \cong \mathrm{Br}(K)$, the **Brauer group of** K. Local class field theory is essentially the computation $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$ when K is a local field.

Definition 4.4.6. The **fundamental class** $u_{L/K} \in H^2(L/K) \xrightarrow{\sim} (1/n)\mathbb{Z}/\mathbb{Z}$ is the inverse image of $1/n$, the canonical generator of the cyclic group.

4.5 Proof of local class field theory

Theorem 4.5.1 (Local class field theory)**.** *1. (Local Artin reciprocity) There exists a homomorphism*

$$\phi_K \colon K^\times \to \mathrm{Gal}(K^{al}/K)^{\mathrm{ab}}$$

such that:

(a) for any finite Galois extension L/K, the restriction $\phi_{L/K} \colon K^\times/\operatorname{Nm}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}$ of ϕ_K is an isomorphism;

(b) for any L/K finite unramified and any uniformizer π of K, we have $\phi_{L/K}(\pi) = \mathrm{Frob}_{L/K} \in \mathrm{Gal}(L/K)$.

2. (Local existence) The norm subgroups of $K^\times$ (i.e. of the form $\operatorname{Nm}(L^\times)$) are exactly the open subgroups of $K^\times$ of finite index.

Remark. Recall that if $\operatorname{char} K = 0$, then all finite index subgroups are open.

Proof. Recall that we have a map

$$\mathrm{inv}_K \colon H^2(K^{\mathrm{al}}/K, (K^{\mathrm{al}})^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

which induces $\mathrm{inv}_{L/K} \colon H^2(L/K, L^\times) \xrightarrow{\sim} (1/n)\mathbb{Z}/\mathbb{Z}$ for a finite extension L/K of degree n. By Tate's theorem, we have an isomorphism $\widehat{H}^r(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{r+2}(\mathrm{Gal}(L/K), L^\times)$ for every $r \in \mathbb{Z}$. Taking $r = -2$, we get

$$\begin{array}{ccc} \widehat{H}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) & \xrightarrow{\sim} & \widehat{H}^0(\mathrm{Gal}(L/K), L^\times) \\ \| & & \| \\ \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{\sim} & K^\times/\operatorname{Nm}(L^\times), \end{array}$$

which is precisely the inverse of the local Artin isomorphism $\phi_{L/K}$. Moreover, we have compatibility, i.e. given a tower $E \supset L \supset K$ of extensions, the natural quotient map commutes:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ \| & & \uparrow \\ K^\times & \xrightarrow{\phi_{E/K}} & \mathrm{Gal}(E/K)^{\mathrm{ab}}. \end{array}$$

Taking an inverse limit, we get the desired local Artin reciprocity map $\phi_K \colon K^\times \to \mathrm{Gal}(K^{\mathrm{al}}/K)^{\mathrm{ab}}$.

Let L/K be a finite unramified extension with $G \coloneqq \mathrm{Gal}(L/K)$. We need to check that $\mathrm{Frob}_{L/K} \in \widehat{H}^{-2}(G, \mathbb{Z}) \cong G$ is mapped to $\pi \in \widehat{H}^0(G, L^\times) = K^\times/\operatorname{Nm}(L^\times)$ by this construction of the local Artin isomorphism. Note that the class of π is independent of the choice of π, because L/K is unramified and therefore $\mathrm{Nm} \colon \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective. Recall that the isomorphism $\widehat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^0(G, L^\times)$ is constructed by following the short exact sequence

$$0 \to L^\times \to L^\times(\varphi) \to \mathbb{Z}[G] \xrightarrow{\deg} \mathbb{Z} \to 0$$

where $L^\times(\varphi)$ is the splitting module of the generator $\varphi \coloneqq u_{L/K} \in H^2(G, L^|times) \cong (1/n)\mathbb{Z}/\mathbb{Z}$, defined as $L^\times(\varphi) = L^\times \oplus \bigoplus_{1 \neq g \in G} x_g$ with the G-action given by $g_1 x_{g_2} \coloneqq x_{g_1 g_2} - x_{g_1} + \varphi(g_1, g_2)$. Compute explicitly that

$$\widehat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{-1}(G, I_G) = I_G/I_G^2 \to \widehat{H}^0(G, L^\times), \quad \sigma \mapsto \sigma - 1 \mapsto ?$$

where the second map is the connecting homomorphism for the short exact sequence $0 \to L^\times \to L^\times(\varphi) \to I_G \to 0$. We compute the connecting homomorphism. First pick the pre-image $x_\sigma \in \widehat{H}^0(L^\times(\varphi))$ of $\sigma - 1$. Then compute its norm

$$\begin{aligned}\mathrm{Nm}(x_\sigma) &= (1 + \sigma + \cdots + \sigma^{n-1})x_\sigma \\ &= x_\sigma + \sum_{k=1}^{n-1}(x_{\sigma^{k+1}} - x_{\sigma^k} + \varphi(\sigma^k, \sigma)) \\ &= x_1 + \varphi(\sigma, \sigma) + \cdots + \varphi(\sigma^{n-1}, \sigma) \\ &= \varphi(1,1) + \varphi(\sigma, \sigma) + \cdots + \varphi(\sigma^{n-1}, \sigma).\end{aligned}$$

Now we construct an explicit 2-cocycle representing φ using the isomorphism

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

Take the generator $f\colon \sigma \mapsto 1/n$ in $G \to \mathbb{Q}/\mathbb{Z}$ and lift it to $\tilde{f}\colon \sigma \mapsto 1/n$ in $G \to \mathbb{Q}$. Then a 2-cocycle representing φ is given by

$$\begin{aligned}\varphi(\sigma^i, \sigma^j) &= \sigma^i \tilde{f}(\sigma^j) - \tilde{f}(\sigma^{i+j}) + \tilde{f}(\sigma^i) \\ &= \tilde{f}(\sigma^j) - \tilde{f}(\sigma^{i+j}) + \tilde{f}(\sigma^i) = \frac{j}{n} - \frac{(i+j) \bmod n}{n} + \frac{i}{n} = \begin{cases} 0 & i + j < n \\ 1 & i + j \geq n. \end{cases}\end{aligned}$$

So now we can finish the computation of $\mathrm{Nm}(x_\sigma)$: it is

$$\mathrm{Nm}(x_\sigma) = \varphi(1,1) + \varphi(\sigma, \sigma) + \cdots + \varphi(\sigma^{n-1}, \sigma) = 0 + 0 + \cdots + 0 + 1 = 1.$$

Hence the image of $\widehat{H}^{-2}(G, \mathbb{Z}) \to \widehat{H}^0(G, L^\times)$ is $\sigma \mapsto \pi^1 = \pi$.

Finally, we prove the local existence theorem. Assume for simplicity that $\mathrm{char}\, K = 0$. Note that if L/K is a finite extension and E/K is the maximal abelian sub-extension, then $\mathrm{Nm}(L^\times) = \mathrm{Nm}(E^\times)$. For example, if L/K is Galois, local Artin reciprocity gives a diagram

$$\begin{array}{ccc} K^\times/\mathrm{Nm}(E^\times) & \xrightarrow{\phi_{E/K}} & \mathrm{Gal}(E/K) \\ \uparrow & & \| \\ K^\times/\mathrm{Nm}(L^\times) & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}}. \end{array}$$

Recall that any subgroup of $K^\times$ containing a norm subgroup is also a norm subgroup. Because any finite index subgroup of $K^\times$ contains $(K^\times)^n$ for some n, it suffices to prove that $(K^\times)^n$, for every n, contains a norm subgroup. Consider the **Kummer sequence** of $\mathrm{Gal}(K^{\mathrm{al}}/K)$-modules

$$1 \to \mu_n \to (K^{\mathrm{al}})^\times \xrightarrow{a \mapsto a^n} (K^{\mathrm{al}})^\times \to 1$$

where μ_n is the subgroup of n-th roots of unity. It gives a long exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(\mu_n) & \longrightarrow & H^0((K^{\mathrm{al}})^\times) & \longrightarrow & H^0((K^{\mathrm{al}})^\times) & \longrightarrow & H^1(\mu_n) & \longrightarrow & H^1((K^{\mathrm{al}})^\times) \\ & & & & \| & & \| & & & & \| \\ & & & & K^\times & \xrightarrow{(\cdot)^n} & K^\times & & & & 0, \end{array}$$

so we get the **Kummer isomorphism** $K^\times/(K^\times)^n \cong H^1(\mathrm{Gal}(K^{\mathrm{al}}/K), \mu_n)$. If $\mu_n \subset K$, then $\mu_n \subset \mathbb{Z}/n$ as a $\mathrm{Gal}(K^{\mathrm{al}}/K)$-module, and

$$H^1(\mathrm{Gal}(K^{\mathrm{al}}/K), \mu_n) \cong \mathrm{Hom}(\mathrm{Gal}(K^{\mathrm{al}}/K), \mathbb{Z}/n) \cong \mathrm{Gal}(L/K)$$

where L is the maximal abelian extension of degree n. By local Artin reciprocity, $K^\times/\operatorname{Nm}(L^\times) = \operatorname{Gal}(L/K)$, so $\operatorname{Nm}(L^\times) = (K^\times)^n$. If $\mu_n \not\subset K$, then consider $K_1 \coloneqq K(\mu_n)$ and apply the preceding case to K_1 to get an abelian extension L_1/K_1 such that $\operatorname{Nm}(L_1^\times) = (K_1^\times)^n$. Pick $L \supset L_1$ Galois over K, so that by the transitivity of norm,

$$\operatorname{Nm}_{L/K}(L^\times) = \operatorname{Nm}_{K_1/K}(\operatorname{Nm}_{L/K_1}(L^\times)) \subset \operatorname{Nm}_{K_1/K}(\operatorname{Nm}_{L_1/K_1}(L_1^\times) = \operatorname{Nm}_{K_1/K}((K_1^\times)^n) \subset (K^\times)^n.$$

Hence in general, $(K^\times)^n$ contains a norm subgroup. □

Chapter 5

Global class field theory

Now that we have proved local class field theory, we can focus on more interesting things. Let K be a number field (i.e. a finite extension of $\mathbb{Q}$). The goal is to study abelian extensions of K and to understand $\mathrm{Gal}(K^{\mathrm{al}}/K)^{\mathrm{ab}}$ in terms of the arithmetic of K itself. (Note that even $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ is not understood, so we look only at the abelian part.) To do so, we will construct a group C_K and the global Artin reciprocity map

$$\phi_K \colon C_K \to \mathrm{Gal}(K^{\mathrm{al}}/K)^{\mathrm{ab}} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

where K^{ab} is the maximal abelian extension of K. Moreover, there are norm maps $\mathrm{Nm}_{L/K} \colon C_L \to C_K$, for a finite abelian extension L/K, such that the induced map

$$\phi_{L/K} \colon C_K / \mathrm{Nm}_{L/K}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

is an isomorphism. Note that if K is a local field, we know the Artin map exists from local class field theory, and $C_K = K^\times$. However, C_K cannot be $K^\times$ in the global situation. For example, if $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, then $\mathrm{Nm}_{L/K}(L^\times) = \{a^2 + b^2 : a, b \in \mathbb{Q},\ (a,b) \neq (0,0)\}$ is not of index 2 inside $K^\times$, and so there cannot be an isomorphism $K^\times / \mathrm{Nm}_{L/K}(L^\times) \cong \mathrm{Gal}(L/K)$. Instead, we will construct a locally compact group C_K as a generalization of the ideal class group Cl_K of K. (Recall that $\mathrm{Cl}_K \coloneqq I_K/K^\times$, where I_K is the group of fractional ideals of K, and $K^\times$ is the group of principal ideals). In particular, $C_K \coloneqq \mathbb{I}_K/K^\times$, where $\mathbb{I}_K$ is the group of idèles ("ideal element"), and $K^\times$ is the group of principal ideles. This is called the idèle class group.

5.1 Idèle class group

Let K be a number field. Let v denote a (finite or infinite) prime of K. Associated to the prime v, there is a (normalized) absolute value $|\cdot|_v$ such that the product formula $\prod_v |x|_v = 1$ holds for every $x \in K^\times$. Let K_v denote the completion of K at v, so that K_v is a local field. If v is a finite prime, let $\mathcal{O}_v \subset K_v$ denote the ring of integers and $\hat{\mathfrak{p}}_v \subset \mathcal{O}_v$ denote the maximal ideal. Let $\mathfrak{p}_v \subset \mathcal{O}_K$ denote the (global) maximal ideal associated to v.

Definition 5.1.1. We will construct $\mathbb{I}_K$ from $K_v^\times$. The naive construction $\prod_v K_v^\times$ fails because it is "too big": not locally compact. To make it locally compact, impose the condition that only finitely many entries have denominators. The **group of idèles** is

$$\mathbb{I}_K \coloneqq \{(a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\}.$$

We say $\mathbb{I}_K$ is the **restricted product** $\prod_v' K_v^\times$ of the $K_v^\times$ with respect to $\mathcal{O}_v^\times$.

Remark. For any finite set of primes $S \supset S_\infty \coloneqq \{\text{infinite primes}\}$, define

$$\mathbb{I}_{K,S} \coloneqq \{(a_v) \in \mathbb{I}_K : a_v \in \mathcal{O}_v^\times \text{ if } v \notin S\} = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times.$$

By definition, $\mathbb{I}_K = \bigcup_S \mathbb{I}_{K,S}$.

Definition 5.1.2. Define a **topology** on $\mathbb{I}_K$ (to make each $\mathbb{I}_{K,S}$ open): a basis of neighborhoods of 1 consists of

$$U(S,\epsilon) \coloneqq \{(a_v) : |a-1|_v < \epsilon \, \forall v \in S, \ |a_v|_v = 1 \, \forall v \notin S\}.$$

The $\mathbb{I}_K$ becomes a topological group under this topology.

Remark. We have a natural injection $K_v^\times \hookrightarrow \mathbb{I}_K$ given by $a \mapsto (\ldots, 1, \ldots, a, \ldots, 1, \ldots)$, i.e. put a at the v-th entry and 1's everywhere else. This is continuous in the induced topology of $\mathbb{I}_K$.

Remark. There is a natural surjection $\mathbb{I}_K \twoheadrightarrow I_K$ given by $(a_v) \mapsto \prod_v \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}$. Note that this is a finite product, because at all but finitely many places we have $\mathrm{ord}_v(a_v) = 0$. The kernel is $\prod_{v \in S_\infty} K_v^\times \times \prod_{v \notin S_\infty} \mathcal{O}_v^\times = \mathbb{I}_{K,S_\infty}$. So we can think of $\mathbb{I}_K$ as an enlargement of I_K by $\mathbb{I}_{K,S_\infty}$.

Proposition 5.1.3. *The natural injection $K^\times \hookrightarrow \mathbb{I}_K$ given by $a \mapsto (a, a, a, \ldots)$ has discrete image.*

Proof. We show that if $S \supset S_\infty$ and $\epsilon < 1$, then $K^\times \cap U(S,\epsilon) = \{1\}$. By the definition of $U(S,\epsilon)$, if $a \in K^\times \cap U(S,\epsilon)$, then $|a-1|_v < \epsilon$ for $v \in S$ and $|a|_v = 1$ for $v \notin S$. But then for $v \notin S$, the ultrametric inequality says $|a-1|_v \leq \max\{|a|_v, |-1|_v\} = 1$. Hence $\prod_v |a-1|_v < 1$. This contradicts the product formula unless $a = 1$. □

Remark. The product formula, as we used it in the proof above, shows that the different places "repel" each other for a global element. Consider a more elementary example: $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}$ is dense, but

$$\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R} \times \mathbb{R}, \quad a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2})$$

is discrete. The phenomenon of the previous proposition is an infinite-dimensional generalization of this phenomenon.

Definition 5.1.4. The **idèle class group** is $C_K \coloneqq \mathbb{I}_K / K^\times$, endowed with the quotient topology.

Remark. The surjection $\mathbb{I}_K \twoheadrightarrow I_K$ we saw earlier induces a surjection $C_k \twoheadrightarrow \mathrm{Cl}_K$.

Definition 5.1.5. Let L/K be a finite extension. Define the **norm map**

$$\mathrm{Nm}_{L/K} \colon \mathbb{I}_L \to \mathbb{I}_K, \quad (a_w) \mapsto (b_v)$$

where $b_v \coloneqq \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a_w)$.

Remark. For any $a \in L^\times$, we have $\mathrm{Nm}_{L/K}(a) = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a)$. This is because of the isomorphism $L \otimes_K K_v \cong \prod_{w|v} L_w$. Hence the norm map induces a map $\mathrm{Nm}_{L/K} \colon C_L \to C_K$ of idèle class groups.

5.2 Global class field theory

Definition 5.2.1. Let L/K be a finite Galois extension and v be a prime of K. Let $w \mid v$ be a prime of L. Define the **decomposition group**

$$D(w) \coloneqq \{\sigma \in \mathrm{Gal}(L/K) : \sigma w = w\} \cong \mathrm{Gal}(L_w/K_v).$$

Moreover, for a different choice $w' \mid v$, there exists $\tau \in \mathrm{Gal}(L/K)$ such that $w' = \tau w$. So $D(w') = \tau D(w) \tau^{-1}$.

Remark. If $\mathrm{Gal}(L/K)$ is abelian, then $D(w)$ and the local Artin map $\phi_v \colon K_v^* \to \mathrm{Gal}(L_w/K_v) = D(w) \subset \mathrm{Gal}(L/K)$ are independent of the choice of $w \mid v$

Proposition 5.2.2. *There exists a unique continuous homomorphism $\phi_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ such that for every L/K finite abelian extension and any choice of $w \mid v$, the following diagram commutes:*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K). \end{array}$$

Proof. If $a \in \mathbb{I}_K$, then define $\phi_K(a) \coloneqq \prod_v \phi_v(a_v)$. Note that $a_v \in \mathcal{O}_v^\times$ and L_w/K_v is unramified for all but finitely many v. So in this case, by local class field theory, $\phi_v(a_v) = 1$. Hence the product is actually finite and well-defined. This uniquely defines ϕ_K. It remains to check ϕ_K is continuous, i.e. check that $\ker(\phi_K)$ is open. By global class field theory, we have the functorial property

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{\phi_{L/L}} & \mathrm{Gal}(L/L) \\ {\scriptstyle \mathrm{Nm}_{L/K}}\downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Hence $\phi_{L/K} \circ \mathrm{Nm}_{L/K} = 0$. So $\ker(\phi_{L/K})$ contains $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$, which is open by local CFT. □

Theorem 5.2.3 (Global class field theory)**.** *1. (Global Artin reciprocity) The map*

$$\phi_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

satisfies $\phi_K(K^\times) = 1$, and therefore induces the global Artin map

$$\phi_K \colon C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Moreover, for any L/K finite abelian, ϕ_K induces an isomorphism $\phi_{L/K} \colon C_K/\operatorname{Nm} C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$.

2. (Global existence) For any open subgroup $N \subset C_K$ of finite index, there exists a finite abelian L/K such that $N = \mathrm{Nm}_{L/K}(C_L)$.

Remark. From the statement of global class field theory, we get a bijection

$$\begin{aligned} \{L/K \text{ finite abelian extension}\} &\Leftrightarrow \{\text{finite index open subgroup } N \subset C_K\} \\ L &\mapsto \mathrm{Nm}(C_L). \end{aligned}$$

Remark. Note that if $L_1 \subset L_2$, then $\mathrm{Nm}(C_{L_1}) \supset \mathrm{Nm}(C_{L_2})$. Also, $\mathrm{Nm}(C_{L_1 L_2}) = \mathrm{Nm}(C_{L_1}) \cap \mathrm{Nm}(C_{L_2})$, and $\mathrm{Nm}(C_{L_1} \cap C_{L_2}) = \mathrm{Nm}(C_{L_1}) \mathrm{Nm}(C_{L_2})$.

Definition 5.2.4. A **modulus** of K is a function $m \colon \{\text{primes of } K\} \to \mathbb{Z}_{\geq 0}$ such that:

1. $m(\mathfrak{p}) = 0$ for all but finitely many primes $\mathfrak{p}$;
2. $m(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is a real prime;
3. $m(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is a complex prime.

Shorthand notation: $\mathfrak{m} \coloneqq \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})} = \mathfrak{m}_0 \mathfrak{m}_\infty$ where $\mathfrak{m}_\infty$ is a product of real primes.

Definition 5.2.5. Given a modulus $\mathfrak{m}$, define

$$\mathbb{I}_K^{\mathfrak{m}} \coloneqq \prod_{\mathfrak{p}|\mathfrak{m}_0} (1+\mathfrak{p}^{m(\mathfrak{p})}) \prod_{\mathfrak{p}|\mathfrak{m}_\infty} (K_{\mathfrak{p}})_{\geq 0}^{\times} \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \mathcal{O}_{\mathfrak{p}}^{\times} \prod_{\mathfrak{p}\nmid\mathfrak{m}_\infty} K_{\mathfrak{p}}^{\times}$$

Define $C_K^{\mathfrak{m}} \coloneqq \mathbb{I}_K^{\mathfrak{m}} K^\times / K^\times$, called the **congruence subgroup**. Define the **ray class group** $\mathrm{Cl}_{\mathfrak{m}} \coloneqq C_K / C_K^{\mathfrak{m}}$.

Definition 5.2.6. By global class field theory, there exists an abelian extension $L_{\mathfrak{m}}$ corresponding to $C_K^{\mathfrak{m}}$, and $\mathrm{Cl}_{\mathfrak{m}} \cong \mathrm{Gal}(L_{\mathfrak{m}}/K)$. In particular, when $\mathfrak{m} = 1$, then $\mathrm{Cl}_1 = \mathrm{Cl}_K$, and L_1 is called the **Hilbert class field**. In particular, $\mathrm{Gal}(L_1/K) \cong \mathrm{Cl}_K$. The Hilbert class field is the maximal abelian extension of K which is unramified at all finite places and stays real at all real places.

Example 5.2.7. If $K = \mathbb{Q}$, then $\mathrm{Cl}_{\mathbb{Q}} = \{1\}$ by unique factorization, and the Hilbert class field is $\mathbb{Q}$ itself.

Example 5.2.8. If $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$ for some $m \in \mathbb{Z}$, then $\mathrm{Cl}_{\mathfrak{m}} \coloneqq (\mathbb{Z}/m)^\times / \{\pm 1\}$. Similarly, if $\mathfrak{m} = (m) \cdot \infty$, then $\mathrm{Cl}_{\mathfrak{m}} \cong \{\pm 1\} \times (\mathbb{Z}/m)^\times / \{\pm 1\} = (\mathbb{Z}/m)^\times$. Global CFT says $\mathrm{Cl}_{(m)} \cong \mathrm{Gal}(L_{(m)}/\mathbb{Q})$ and $\mathrm{Cl}_{(m)\cdot\infty} \mathrm{Gal}(L_{(m)\cdot\infty}/\mathbb{Q})$. Clearly the cyclotomic extension $\mathbb{Q}(\zeta_m)$ has Galois group $(\mathbb{Z}/m)^\times$. Hence it is $L_{(m)\cdot\infty}$. The sub-extension $L_{(m)}$ of index 2 is precisely the sub-extension fixed by complex conjugation. We have recovered the classical Kronecker–Weber theorem.

Theorem 5.2.9 (Kronecker–Weber)**.** $\mathbb{Q}^{\mathrm{ab}} = \bigcup_{m\geq 1} \mathbb{Q}(\zeta_m)$.

5.3 Cohomology of idèles

Theorem 5.3.1 (First inequality)**.** $[C_K : \mathrm{Nm}\, C_L] \geq [L : K]$.

Remark. The proof of the first inequality will establish global class field theory for cyclic extensions L/K. In fact, for cyclic extensions, we will show that the Herbrand quotient $h(C_L) = [L : K]$. This will imply the first inequality, since $h(C_L) = [C_K : \mathrm{Nm}\, C_L]/|H^1(G, C_L)|$.

Recall that if v is a prime of K and L/K is a finite Galois extension, then v decomposes into multiple primes $w_1 \cdots w_g$ in L. Moreover, $L \otimes KK_v = \prod_{w|v} L_w$. The Galois group $G \coloneqq \mathrm{Gal}(L/K)$ acts on the lhs on the factor L, and induces a G-action on the rhs by permuting the factors in the product. Specifically, if $\alpha = (\alpha_w) \in \prod_{w|v}$ and $\sigma \in G$, then $(\sigma\alpha)_{\sigma w} = \sigma\alpha_w$.

Proposition 5.3.2. *As G-modules, there is an isomorphism $\prod_{w|v} L_w = \mathrm{Ind}_{G_{w_0}}^G L_{w_0}$ for any fixed $w_0 \mid v$.*

Proof. Recall that by definition,

$$\mathrm{Ind}_{G_{w_0}}^G L_{w_0} = \{f \colon G \to L_{w_0} : f(\tau\sigma) = \tau f(\sigma)\ \forall \tau \in G_{w_0},\ \sigma \in G\}.$$

For any $\alpha \in \prod_{w|v} L_w$, define such a function $f_\alpha \colon G \to L_{w_0}$ by $\sigma \mapsto \sigma\alpha_{\sigma^{-1}w_0}$. We verify that

$$f_\alpha(\tau\sigma) = (\tau\sigma)\alpha_{(\tau\sigma)^{-1}w_0} = \tau(\sigma\alpha_{\sigma^{-1}w_0}) = \tau f_\alpha(\sigma).$$

Conversely, given $f \in \mathrm{Ind}_{G_{w_0}}^G L_{w_0}$, define $\alpha_f \in \prod_{w|v} L_w$ by $(\alpha f)_{\sigma w_0} \coloneqq \sigma f(\sigma^{-1})$. We can check that $\alpha \mapsto f_\alpha$ and $f \mapsto \alpha_f$ are mutually inverse and respect the G-action. □

Corollary 5.3.3. *For all r, we have $\widehat{H}^r(G, \prod_{w|v} L_w) = \widehat{H}^r(G_{w_0}, L_{w_0})$.*

Proof. Apply Shapiro's lemma to the proposition. □

Remark. Since we know $\widehat{H}^r(G_{w_0}, L_{w_0})$ is independent of the choice of $w_0 \mid v$, we often write it as $\widehat{H}^r(G^v, L^v)$.

Corollary 5.3.4. *For all r, $\widehat{H}^r(G, \prod_{w|v} L_w^\times) = \widehat{H}^r(G_{w_0}, L_{w_0}^\times)$ and $\widehat{H}^r(G, \prod_{w|v} U_w) = \widehat{H}^r(G_{w_0}, U_{w_0})$*

Proposition 5.3.5. *$H^0(G, \mathbb{I}_L) = \mathbb{I}_K$, and for any r, we have*

$$\widehat{H}^r(G, \mathbb{I}_L) = \bigoplus_v \widehat{H}^r(G^v, (L^v)^\times).$$

Proof. $\alpha = (\alpha_w) \in \mathbb{I}_L$ is fixed by G iff $(\alpha_w)_{w|v}$ is fixed by G for every v of K, iff $\alpha_w \in K_v^\times$ and is independent of $w \mid v$. This data is equivalent to an element of $\mathbb{I}_K$.

Let S be a finite set of primes of K containing all infinite primes and all the primes ramified in L. Let T be the finite set of primes of L lying over the primes v in S. Let $\mathbb{I}_{L,T} \coloneqq \prod_{w \in T} L_w^\times \times \prod_{w \notin T} U_w^\times$. Then $\mathbb{I}_L = \bigcup_T \mathbb{I}_{L,T}$, and by Shapiro's lemma,

$$\widehat{H}^r(G, \mathbb{I}_L) = \varinjlim_T \widehat{H}^r(G, \mathbb{I}_{L,T}) = \varinjlim_S \prod_{v \in S} \widehat{H}^r(G^v, (L^v)^\times) \times \prod_{v \notin S} \widehat{H}^r(G^v, U^v).$$

By assumption, all $v \notin S$ are unramified, so $\widehat{H}^r(G^v, U^v) = 0$. Hence we are left with

$$\varinjlim_S \prod_{v \in S} \widehat{H}^r(G^v, (L^v)^\times) = \bigoplus_v \widehat{H}^r(G^v, (L^v)^\times). \qquad \square$$

Corollary 5.3.6. *$\widehat{H}^1(G, \mathbb{I}_L) = 0$, and $\widehat{H}^2(G, \mathbb{I}_L) = \bigoplus_v (\frac{1}{n_v}\mathbb{Z}/\mathbb{Z})$ where $n_v \coloneqq [L^v : K_v]$.*

Proof. We know $H^1(G^v, (L^v)^\times) = 0$ by Hilbert 90, and $H^2(G^v, (L^v)^\times) = (1/n_v)\mathbb{Z}/\mathbb{Z}$ by local class field theory. $\square$

Proposition 5.3.7. *Let S be a finite set of primes of K, and $T \coloneqq \{w \mid v : v \in S\}$. Assume L/K is finite cyclic. Then the Herbrand quotient $h(\mathbb{I}_{L,T}) = \prod_{v \in S} n_v$, where $n_v \coloneqq [L^v : K_v]$.*

Proof. $h(\mathbb{I}_{L,T}) = h(\prod_{v \in S}(L^v)^\times \times \prod_{v \notin S} U^v) = h(\prod_{v \in S}(L^v)^\times) = \prod_{v \in S} n_v$. $\square$

5.4 Cohomology of units

Let L/K be a finite Galois extension of number fields.

Definition 5.4.1. Let T be a finite set of primes in L. The **group of T-units** is

$$U(T) \coloneqq \{\alpha \in L^\times : \mathrm{ord}_w(\alpha) = 0 \ \forall w \notin T\} = L^\times \cap \mathbb{I}_{L,T}.$$

For example, if T is the set of infinite primes of L, then $U(T) = U_L$.

Lemma 5.4.2. *Let G be a finite cyclic group and V be a finite $\mathbb{R}[G]$-module, i.e. a finite-dimensional real vector space with a G-action. Let M, N be G-stable lattices in V. Then $h(M) = h(N)$, if either is defined.*

Proof. Since M, N are lattices, $M \otimes_{\mathbb{Z}} \mathbb{R} = N \otimes_{\mathbb{Z}} \mathbb{R}$ as G-modules. In the homework, we showed this implies $\alpha\colon M \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} N \otimes_{\mathbb{Z}} \mathbb{Q}$ as G-modules. By scaling by the common denominator of α, we get $\alpha(M) \subset N$. These are two free $\mathbb{Z}$-modules of the same rank, so their quotient $N/\alpha(M)$ is torsion and therefore finite. Hence $h(N/\alpha(M)) = 1$, and $h(\alpha(M)) = h(N)$. $\square$

Proposition 5.4.3. *Assume L/K is cyclic. Then $h(U(T)) = \frac{1}{n}\prod_{v \in S} n_v$ where $n \coloneqq [L : K]$.*

Proof. Apply the lemma to the $\mathbb{R}$-vector space $V \coloneqq \mathrm{Fun}(T, \mathbb{R})$ consisting of functions from T to $\mathbb{R}$. It has a G-action given by $(g \cdot f)(w) = f(g^{-1}w)$, where $f \in V$, $w \in T$ and $g \in G$. In other words, as a G-module, $V = \bigoplus_{v \in S} \mathrm{Ind}_{G^v}^G \mathbb{R}$ where $\mathbb{R}$ is the trivial G-module. By this description, we have two lattices.

1. Consider the lattice
$$N \coloneqq \bigoplus_{v \in S} \mathrm{Ind}_{G^v}^G \mathbb{Z} \subset V.$$
The Herbrand quotient is $h(G, N) = \prod_{v \in S} h(G, \mathrm{Ind}_{G^v}^G \mathbb{Z})$. By Shapiro's lemma, this is $\prod_{v \in S} h(G^v, \mathbb{Z}) = \prod_{v \in S} n_v$.

2. Define a map $\lambda \colon U(T) \to V$ given by $a \mapsto (\log |a|_w)_{w \in T}$ (cf. proof of Dirichlet's unit theorem). Then $\mathrm{im}(\lambda)$ has a single non-trivial relation coming from the product formula $\prod_w |a|_w = 1$, so $\mathrm{im}(\lambda)$ is a lattice in $V^0 \coloneqq \{\sum_{w \in T} x_w = 0\} \subset V$. Note that
$$\ker(\lambda) = \{a \in L^\times : |a|_w = 1 \, \forall w \notin T, \ |a|_w = 1 \, \forall w \in T\}.$$
This is precisely the roots of unity in $L^\times$, so in particular it is finite. Hence $h(U(T)) = h(\mathrm{im}(U(T)))$. Define $M \coloneqq \mathrm{im}(U(T)) \oplus \mathbb{Z}(1, \dots, 1)$. Then M is a G-stable lattice in V, and $h(\mathrm{im}(U(T))) = h(M)/h(\mathbb{Z})$. Clearly $h(\mathbb{Z}) = n$.

By the lemma, $\prod_{v \in S} n_v = h(N) = h(M) = nh(U(T))$. □

5.5 The first inequality

Lemma 5.5.1. *Let $S \supset S_\infty$ be a finite set of primes containing the generating set of primes of the class group Cl_K. Then $\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$. Then*
$$\mathbb{I}_K / K^\times = \mathbb{I}_{K,S} / (\mathbb{I}_{K,S} \cap K^\times) = \mathbb{I}_{K,S} / U(S).$$

Proof. Recall that we have a surjection
$$\mathbb{I}_K \twoheadrightarrow I_K = \{\text{fractional ideals}\}, \quad (a_v) \mapsto \mathfrak{p}_v^{\mathrm{ord}_v(a_v)}$$
with kernel $\mathbb{I}_{K,S_\infty}$. This implies $\mathbb{I}_K / (K^\times \cdot \mathbb{I}_{K,S_\infty}) = \mathrm{Cl}_K$. By enlarging ∞ to S, we get $\mathbb{I}_K / (K^\times \cdot \mathbb{I}_{K,S}) = 0$. Hence $\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$. □

Theorem 5.5.2 (First inequality)**.** $[C_K : \mathrm{Nm}\, C_L] \geq [L : K]$.

Proof. Recall that for cyclic extensions, it suffices to show that the Herbrand quotient is $h(C_L) = [L : K]$. This will imply the first inequality, since $h(C_L) = [C_K : \mathrm{Nm}\, C_L] / |H^1(G, C_L)|$. Take S to be the finite set of primes of K such that:

1. $S \supset S_\infty$;
2. $S \supset \{\text{primes ramified in } L\}$;
3. $S \supset \{\mathfrak{p}_L \cap \mathcal{O}_K : \mathfrak{p}_L \text{ runs over a generating set of } \mathrm{Cl}_L\}$.

Take $T \coloneqq \{w : w \mid v, \ v \in S\}$. Then by previous lemmas, $C_L = \mathbb{I}_{L,T} / U(T)$, and hence $h(C_L) = n = [L : K]$. □

Lemma 5.5.3. *If L/K is finite Galois with solvable $G \coloneqq \mathrm{Gal}(L/K)$, and there exists a subgroup $D \subset \mathbb{I}_K$ such that*

1. *$D \subset \mathrm{Nm}_{L/K}(\mathbb{I}_L)$, and*
2. *$K^\times \cdot D$ is dense in $\mathbb{I}_K$,*

then $L = K$.

Proof. Suppose otherwise. Choose a cyclic sub-extension K'/K (since L/K is solvable). By condition (1), $D \subset \mathrm{Nm}_{K'/K}(\mathbb{I}_{K'})$. By local CFT, $\mathrm{Nm}_{K'/K}(\mathbb{I}_{K'}) \subset \mathbb{I}_{K'}$ is open. Hence $K^\times \cdot \mathrm{Nm}_{K'/K}(\mathbb{I}_{K'}) \subset \mathbb{I}_K$ is closed. By condition (2), this is actually an equality. Hence $[C_K : \mathrm{Nm}_{K'/K} C_{K'}] = 1$. By the first inequality, $[K' : K] = 1$. It follows that $[L : K] = 1$, so $L = K$. □

Definition 5.5.4. A prime v of K **splits completely** in L if the primes $w_1, \dots, w_g$ above a prime v satisfy $g = [L : K]$ and $e, f, = 1$, i.e. no ramification or non-trivial residue field.

Corollary 5.5.5 (Weak version of Chebotarev density theorem)**.** *If L/K is solvable and $L \neq K$, then there exists infinitely many primes of K that do not split completely in L.*

Proof. Let $D \coloneqq \{(a_v) : a_v = 1 \, \forall v \in S\} \subset \mathbb{I}_K$ where $S = S_\infty \cup \{\text{all primes that don't split completely in } L\}$. If there are only finitely many such primes, then S is finite. For any $v \notin S$, by definition $L_w = K_v$. Hence $D \subset \mathrm{Nm}_{L/K}(\mathbb{I}_L)$. Moreover, $K^\times \cdot D$ is dense in $\mathbb{I}_K$ by the following weak approximation (Milne ANT theorem 7.20): if $|\cdot|_1, \dots, |\cdot|_n$ are inequivalent absolute values on a field K, and $a_1, \dots, a_n \in K$, then for every $\epsilon > 0$ there exists $a \in K$ such that $|a_i - a|_i < \epsilon$. Specifically, using weak approximation, given $a = (a_v) \in \mathbb{I}_K$, we can choose $b \in K$ close to a_v for all $v \in S$, and choose $c \in D$ such that $c_v = 1$ for all $v \in S$ and $c_v = a_v$ for all $v \notin S$, so that bc is close to a. Hence $K^\times \cdot D$ is dense. But then by the lemma, $L = K$, a contradiction. □

Example 5.5.6. Take $K \coloneqq \mathbb{Q}$ and $L \coloneqq \mathbb{Q}(i)$. If p is an odd prime, then p splits in $\mathbb{Q}(i)$ iff $p \equiv 1 \bmod 4$. In other words, p doesn't split in L iff $p \equiv 3 \bmod 4$. Hence there are infinitely many primes $p \equiv 3 \bmod 4$. (In fact, the "density" of each of these two classes is $1/2$.)

5.6 Density and L-functions

Definition 5.6.1. Let P be a set of primes in $\mathbb{Z}$. Its **natural density** is

$$\mu(P) \coloneqq \lim_{x \to \infty} \frac{\#\{p \in P : p < x\}}{\#\{p \text{ prime} : p < x\}}$$

if the limit exists.

Remark. This is quite a natural definition, but depends on the existence of an ordering of primes in $\mathbb{Z}$. So it does not work for general number fields.

Definition 5.6.2. Let P be a set of finite primes of a number field K. Its **natural density** is

$$\mu(P) \coloneqq \lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in P : N\mathfrak{p} < x\}}{\#\{\mathfrak{p} \text{ prime} : N\mathfrak{p} < x\}}$$

if the limit exists.

Definition 5.6.3. We have an alternative notion of density which is useful in analytic arguments. Let P be a set of finite primes of a number field K. Its **Dirichlet density** is

$$\delta(P) \coloneqq \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in P} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}} N\mathfrak{p}^{-s}}$$

if the limit exists.

Proposition 5.6.4. *If $\mu(p)$ exists, then $\delta(p)$ also exists and $\mu(p) = \delta(p)$.*

Remark. We will not prove this fact. It shows that in some sense, the natural density is the "strongest" notion of density.

Definition 5.6.5. Recall the **Riemann zeta function**

$$\zeta(s) \coloneqq \sum_{n\geq 1} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

Dedekind then introduced the **Dedekind zeta function** for arbitrary number fields

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

where $\mathfrak{a}$ ranges over all (integral) ideals, and $\mathfrak{p}$ over (integral) prime ideals. Now fix a character $\chi\colon (\mathbb{Z}/m)^\times \to \mathbb{C}^\times$, and define the **Dirichlet L-function**

$$L(s,\chi) \coloneqq \sum_{n\geq 1} \chi(n) n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}}$$

where χ is extended by 0 to all integers. Finally, note that $(\mathbb{Z}/m)^\times$ is a ray class group, so fix a character $\chi\colon \mathrm{Cl}_\mathfrak{m} \to \mathbb{C}^\times$ and define the **Weber L-function**

$$L(s,\chi) \coloneqq \sum_{\substack{\mathfrak{a}\in\mathcal{O}_K \\ \gcd(\mathfrak{a},\mathfrak{m})=1}} \chi(\mathfrak{a})(N\mathfrak{a})^{-s} = \prod_{\substack{\mathfrak{p}\subset\mathcal{O}_K \\ \gcd(\mathfrak{p},\mathfrak{m})=1}} \frac{1}{1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}}$$

where to evaluate $\chi(\mathfrak{a})$ we implicitly embed $\mathfrak{a}$ into $\mathrm{Cl}_\mathfrak{m}$.

Example 5.6.6. If $K=\mathbb{Q}$ and $\mathfrak{m} \coloneqq (m)\cdot\infty$, then $\mathrm{Cl}_\mathfrak{m} = (\mathbb{Z}/m)^\times$. So we recover the Dirichlet L-function from the Weber L-function.

Remark. In general, an **L-function** of the form $\sum_{n\geq 0} a_n n^{-s}$ with an Euler product $\prod_p 1/(1-\alpha_p p^{-s})$.

Theorem 5.6.7. *If χ is not trivial, then $L(s,\chi)$ has an analytic continuation to $s\in\mathbb{C}$, and $L(1,\chi)\neq 0$. Otherwise if χ is trivial, then $L(s,\chi)=\zeta_K(s)$ has an analytic continuation to $s\in\mathbb{C}-\{1\}$, and has a simple pole at $s=1$ (with residue given by the class number formula).*

Remark. There is a relationship between $\sum_\mathfrak{p} N\mathfrak{p}^{-s}$ and $\zeta_K(s)$ as follows. Compute

$$\log\zeta_K(s) = \log\prod_\mathfrak{p} \frac{1}{1-N\mathfrak{p}^{-s}} = -\sum_\mathfrak{p} \log(1-N\mathfrak{p}^{-s}) = \sum_\mathfrak{p}\sum_{m\geq 1} \frac{N\mathfrak{p}^{-ms}}{m} = \sum_\mathfrak{p} N\mathfrak{p}^{-s} + \sum_\mathfrak{p}\sum_{m\geq 2}\frac{N\mathfrak{p}^{-ms}}{m}.$$

The second term is analytic when $\Re(s) > 1/2$. In particular, it is analytic at $s=1$. Hence we write

$$\log\zeta_K(s) \sim \sum_\mathfrak{p} N\mathfrak{p}^{-s},$$

where $f\sim g$ means $f-g$ is analytic at $s=1$. On the other hand, using that $\zeta_K(s)$ has only a simple pole at $s=1$,

$$\log\zeta_K(s) \sim \log\zeta_K(s) - \log((s-1)\zeta_K(s)) = \log\frac{1}{s-1}.$$

Hence Dirichlet density is also equal to

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

Proposition 5.6.8. *It follows that the Dirichlet density has the properties:*

1. $0 \le \delta(p) \le 1$;
2. *if P is finite, then $\delta(P) = 0$;*
3. *if $P = P_1 \sqcup P_2$, then $\delta(P) = \delta(P_1) + \delta(P_2)$ (if two of the three densities exist, so does the third);*
4. *if $P_1 \subset P_2$ both have densities, then $\delta(P_1) \le \delta(P_2)$;*
5. *if P has density and $\delta(P') = 1$, then $\delta(P) = \delta(P \cap P')$;*
6. *if P and P' are complementary sets and P has density, then $\delta(P) + \delta(P') = 1$.*

Theorem 5.6.9. *Let L/K be finite Galois. Let P be the set of finite primes of K that split completely in L. Then $\delta(P) = 1/[L : K]$.*

Proof. We can directly compute $\delta(P)$:

$$\sum_{\mathfrak{p} \in P} N\mathfrak{p}^{-s} \sim \frac{1}{[L:K]} \sum_{\substack{\mathfrak{q} \text{ in } L \\ f(q)=1}} N\mathfrak{q}^{-s} \sim \frac{1}{[L:K]} \sum_{\mathfrak{q} \text{ in } L} N\mathfrak{q}^{-s} = \frac{1}{[L:K]} \log \zeta_L(s) \sim \frac{1}{[L:K]} \log \frac{1}{s-1}$$

because all the other primes $\mathfrak{q}$ in L with $f(q) > 1$ contribute an analytic term. Dividing, we get $\delta(P) = 1/[L : K]$. □

5.7 The second inequality

We now want to show $[C_K : \mathrm{Nm}_{L/K} C_L] \le [L : K]$. By the previous section, we can interpret the right hand side as a density. Now we want to re-interpret $C_k/\mathrm{Nm}_{L/K} C_L$ in terms of the density of another set of primes.

Definition 5.7.1. Let $\mathfrak{m}$ be a modulus. Define the subgroup of **$\mathfrak{m}$-idèles**

$$\mathbb{I}_K(\mathfrak{m}) = \{(a_n) \in \mathbb{I}_K : a_\mathfrak{p} \in 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})} \, \forall \mathfrak{p} \mid \mathfrak{m} \text{ finite}, \ a_\mathfrak{p} \in K_{\mathfrak{p},>0} \, \forall \mathfrak{p} \mid \mathfrak{m} \text{ infinite}\}.$$

Define $K^\times(\mathfrak{m}) \coloneqq \mathbb{I}_K(\mathfrak{m}) \cap K^\times$.

Proposition 5.7.2. *$\mathbb{I}_K(\mathfrak{m})/K^\times(\mathfrak{m}) = \mathbb{I}_K/K^\times$, and the ray class group is $\mathrm{Cl}_\mathfrak{m} = I^\mathfrak{m}/K^\times(\mathfrak{m})$, where $I^\mathfrak{m}$ is the group of fractional ideals of K coprime to $\mathfrak{m}$.*

Proof. Write $\mathbb{I}_K(\mathfrak{m}) \hookrightarrow \mathbb{I}_K \to \mathbb{I}_K/K^\times$. Note that the kernel is contained in $K^\times(\mathfrak{m})$. Hence $\mathbb{I}_K(\mathfrak{m})/K^\times(\mathfrak{m}) \to \mathbb{I}_K/K^\times$ is injective. Surjectivity follows by weak approximation: we can modify any element in $\mathbb{I}_K$ by an element of $K^\times$ to get an element in $\mathbb{I}_K(\mathfrak{m})$. So $\mathbb{I}_K(\mathfrak{m})/K^\times(\mathfrak{m}) = \mathbb{I}_K/K^\times$. Now use the natural map

$$\mathbb{I}_K(\mathfrak{m}) \to \mathbb{I}^\mathfrak{m}, \quad (a_\mathfrak{p}) \mapsto \prod_{\mathfrak{p} \nmid m} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(a_\mathfrak{p})}.$$

By the definition of $\mathbb{I}_K(\mathfrak{m})$, the kernel of this map is $K^\times(\mathfrak{m})$. Hence we have an induced isomorphism $\mathrm{Cl}_\mathfrak{m} = \mathbb{I}_K/(K^\times \cdot \mathbb{I}_K^\mathfrak{m}) \cong I^\mathfrak{m}/K^\times(\mathfrak{m})$. □

So for any L/K Galois, there exists a modulus $\mathfrak{m}$ such that the global Artin map should induce an isomorphism

$$I_K^\mathfrak{m}/(K^\times(\mathfrak{m}) \cdot \mathrm{Nm}_{L/K} I_L^\mathfrak{m}) \cong \mathrm{Gal}(L/K)$$

if L/K is abelian.

Theorem 5.7.3. *Let $A \in I^\mathfrak{m}/H$ be an ideal class, where $K^\times(\mathfrak{m}) \subset H \subset I^\mathfrak{m}$. Then the Dirichlet density is $\delta(\mathfrak{p} \in A) = 1/[I^\mathfrak{m} : H]$.*

Proof. Let χ be a character of the finite group $I^{\mathfrak{m}}/H$. Then

$$\log L(s,\chi) \sim \sum_{\mathfrak{p}|\mathfrak{m}} \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s} = \sum_{B \in I^{\mathfrak{m}}/H} \chi(B) \sum_{\mathfrak{p} \in B} \frac{1}{N\mathfrak{p}^s}.$$

Recall that if G is a finite abelian group with group of characters $\widehat{G}$, we have

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & g = 0 \\ 0 & g \neq 0. \end{cases}$$

So multiply both sides by $\chi(A)^{-1}$ and sum up over all χ, to get

$$\sum_{\chi} \log L(s,\chi)\chi(A)^{-1} \sim \sum_{\chi} \sum_{B \in I^{\mathfrak{m}}/H} \chi(A)^{-1}\chi(B) \sum_{\mathfrak{p} \in B} \frac{1}{N\mathfrak{p}^s} = \sum_{\mathfrak{p} \in A} \frac{1}{N\mathfrak{p}^s}[I^{\mathfrak{m}} : H].$$

But recall that $L(s,\chi)$ is holomorphic unless $\chi = 1$, so

$$\sum_{\chi} \log L(s,\chi)\chi(A)^{-1} \sim \log \zeta_K(s) = \log \frac{1}{s-1}.$$

Hence we get that

$$\delta(\mathfrak{p} \in A) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in A} N\mathfrak{p}^{-s}}{\log(1/(s-1))} = \frac{1}{[I^{\mathfrak{m}} : H]}.$$ □

Theorem 5.7.4 (Second inequality)**.** $[C_K : \operatorname{Nm}_{L/K} C_L] \leq [L : K]$.

Proof. Take $H = K^\times(\mathfrak{m}) \cdot \operatorname{Nm}_{L/K} I_L^{\mathfrak{m}}$, and $A = [0] \in I^{\mathfrak{m}}/H$. The theorem implies $\delta(\mathfrak{p} \in K^\times(\mathfrak{m}) \cdot \operatorname{Nm} I_L^{\mathfrak{m}}) = 1/[I^{\mathfrak{m}} : K^\times(\mathfrak{m}) \operatorname{Nm} I_L^{\mathfrak{m}}]$. Clearly

$$\{\mathfrak{p} : \mathfrak{p} \text{ splits completely in } L\} \subset \{\mathfrak{p} : \mathfrak{p} \in K^\times(\mathfrak{m}) \cdot \operatorname{Nm} I_L^{\mathfrak{m}}\}$$

because if a prime splits completely, each of its local extensions is trivial, so the norm map is the identity. (Also, we use that $\mathfrak{m}$ is a finite set, so it does not make a difference in terms of density.) However, we know $\delta(\{\mathfrak{p} : \mathfrak{p} \text{ splits completely in } L\}) = 1/[L : K]$. Hence $1/[L : K] \leq 1/[I^{\mathfrak{m}} : K^\times(\mathfrak{m}) \cdot \operatorname{Nm} I_L^{\mathfrak{m}}]$, which is the desired inequality. □

Corollary 5.7.5 (Global version of Hilbert 90)**.** *If L/K is finite Galois, then $H^1(G, C_L) = 0$.*

Proof. Assume G is abelian and cyclic. The first inequality gives

$$[L : K] = h(C_L) = [C_K : \operatorname{Nm}_{L/K} C_L]/|H^1(G, C_L)|.$$

By the second inequality,

$$[C_K : \operatorname{Nm}_{L/K} C_L]/|H^1(G, C_L)| \leq [L : K]/1 = [L : K].$$

Hence equality holds, and $[C_K : \operatorname{Nm}_{L/K} C_L] = [L : K]$ and $|H^1(G, C_L)| = 1$. Now assume G is a p-group. Take $H \subset G$ of index p and use the inflation-restriction sequence

$$0 \to H^1(G/H, C_{L^H}) \to H^1(G, C_L) \to H^1(H, C_L).$$

By the cyclic case, $H^1(G/H, C_{L^H}) = 0$. By induction on $|G|$, we know $H^1(H, C_L) = 0$. Hence $H^1(G, C_L) = 0$. Finally, for G an arbitrary group, use that $H^1(G, C_L) \hookrightarrow \prod_{\mathfrak{p}} H^1(G_{\mathfrak{p}}, C_L)$ is an injection, and each of the terms in the product are 0. □

Corollary 5.7.6. *Let L/K be finite Galois. Then the natural map*

$$H^2(L/K) \to \bigoplus_v H^2(L^v/K_v)$$

is an injection. (Recall $H^2(L/K) \coloneqq H^2(\mathrm{Gal}(L/K), L^\times)$.)

Proof. Consider the exact sequence of G-modules $0 \to L^\times \to \mathbb{I}_L \to C_L \to 0$. The long exact sequence gives

$$\cdots \to H^1(G, C_L) \to H^2(L/K) \to H^2(G, \mathbb{I}_L) \to \cdots .$$

By global Hilbert 90, $H^1(G, C_L) = 0$. We already computed $H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(L^v/K_v)$. Hence we get the desired injection. □

Corollary 5.7.7. *For all $\beta \in H^2(K) \coloneqq H^2(K^{\mathrm{sep}}/K, (K^{\mathrm{sep}})^\times)$, there exists a cyclic cyclotomic extension L/K such that the image of β under $H^2(K) \xrightarrow{\mathrm{res}} H^2(L)$ is zero.*

Remark. This corollary will be used to reduce the proof of global CFT to cyclic cyclotomic extensions, which are much more explicit.

Proof. Let β_v denote the image of β in $H^2(L^v/K_v)$. By the previous corollary, β is completely determined by $\{\beta_v\}$. By local CFT, $H^2(L^v/K_v) \cong (1/[L^v : K_v])\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$, given by the invariant map inv_v. Moreover, given $\beta_v \in H^2(K)$, we can look at $\mathrm{inv}_w(\beta_v|_L)$ for $w \mid v$ a place of L. We know

$$\mathrm{inv}_w(\beta_v|_L) = [L^v : K_v] \, \mathrm{inv}_v(\beta_v)$$

by the functoriality of restriction/corestriction. Let $n_v \coloneqq [L^v : K_v]$. By the previous theorem, if $\beta \in H^2(K)$, then $\mathrm{inv}_v(\beta_v) = 0$ for all but finitely many v. So there exists some integer $m \geq 1$ such that $m \cdot \mathrm{inv}_v(\beta_v) = 0$ for all v. So it remains to prove the following lemma. □

Lemma 5.7.8. *Let S be a finite set of finite primes of K. Let $m \geq 1$ be an integer. Then there exists a cyclic cyclotomic extension L/K such that $m \mid n_v$ for all $v \in S$.*

Proof. We can reduce to the case $K = \mathbb{Q}$, by replacing m by $m[K : \mathbb{Q}]$. (If we have such a construction over $\mathbb{Q}$, we can take the compositum to get the desired construction over K.) We can also reduce to the case $m = \ell^s$ where s is a prime power. (We can repeat the construction for each prime in m, and the product of cyclic groups of coprime order is still cyclic.) Hence it suffices to construct a cyclic cyclotomic extension $L/\mathbb{Q}$ such that $\ell^s \mid [L_p : \mathbb{Q}_p]$ for all $p \in S$. Recall that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q}) = (\mathbb{Z}/\ell^r)^\times = \begin{cases} \mathbb{Z}/(\ell-1) \oplus \mathbb{Z}/\ell^{r-2} & \ell \text{ odd} \\ \mathbb{Z}/2 \oplus \mathbb{Z}/2^{r-3} & \ell = 2. \end{cases}$$

Hence take the cyclic cyclotomic extension

$$L = \begin{cases} \mathbb{Q}(\zeta_{\ell^r})^{\mathbb{Z}/(\ell-1)} & \ell \text{ odd} \\ \mathbb{Q}(\zeta_{\ell^r})^{\mathbb{Z}/2} & \ell = 2, \end{cases}$$

which is of degree ℓ^{r-2} or ℓ^{r-3}. Now compute $[L_p : \mathbb{Q}_p]$.

1. If $p = \ell$, then $L_p/\mathbb{Q}_p$ is totally ramified. Then $[L_p : \mathbb{Q}_p] = \varphi(\ell^r)$ and we can choose $r \gg 0$ such that $\ell^s \mid [L_p : \mathbb{Q}_p]$.
2. If $p \neq \ell$, then $L_p/\mathbb{Q}_p$ is unramified. Then $[L_p : \mathbb{Q}_p] = t$, the smallest integer such that $\ell^r \mid (p^t - 1)$ and we can choose $r \gg 0$ such that $\ell^s \mid t$. □

5.8 Chebotarev density theorem

Theorem 5.8.1 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension (not necessarily abelian) of number fields. Let $\sigma \in G \coloneqq \mathrm{Gal}(L/K)$. Let C_σ be the conjugacy class of σ in G. Then*

$$\delta(\{\mathfrak{p} \subset K : \mathrm{Frob}_\mathfrak{p} \in C_\sigma\}) = \frac{|C_\sigma|}{|G|}.$$

Example 5.8.2. For example, if σ is trivial, then the lhs is $\delta(\{\mathfrak{p} : \mathfrak{p} \text{ splits completely } inL\})$, and the rhs is $1/|G| = 1/[L : K]$. So the calculation of the density of the split primes we saw earlier is a special case of the Chebotarev density theorem.

Example 5.8.3. If $L/K = \mathbb{Q}(\zeta_N)/\mathbb{Q}$, then $G = (\mathbb{Z}/N)^\times$. Choose $\sigma = a \in (\mathbb{Z}/N)^\times$. Then the lhs is $\delta(\{p : p \equiv a \bmod N\})$, and the rhs is $1/\varphi(N)$. In particular, this implies Dirichlet's theorem: there are infinitely many primes in any arithmetic progression.

Example 5.8.4. Let $f(x) = x^3 - 2$ and $K = \mathbb{Q}$. Let $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ be the Galois closure of $f(x)$. Then $G = \mathrm{Gal}(L/K) = S_3$. This group has 3 conjugacy classes:

1. $\sigma = (1)$, with $|C_\sigma| = 1$, and $\mathrm{Frob}_p \in C_\sigma$ iff $x^3 - 2$ splits into 3 linear factors mod p;
2. $\sigma = (1\ 2)$, with $|C_\sigma| = 3$ because there are 3 transpositions (1 2), (1 3), (2 3), and $\mathrm{Frob}_p \in C_\sigma$ iff $x^3 - 2$ splits into a linear and a quadratic factor mod p;
3. $\sigma = (1\ 2\ 3)$, with $|C_\sigma| = 2$ because there are 2 cyclic permutations (1 2 3) and (1 3 2), and $\mathrm{Frob}_p \in C_\sigma$ iff $x^3 - 2$ is irreducible mod p.

Note that for each of these cases, there is no congruence condition on p, because S_3 is not abelian. (In the abelian case we will get congruence conditions.)

Proof. If G is abelian, then global CFT implies there exists a modulus $\mathfrak{m}$ and a subgroup $H \subset I^\mathfrak{m}$ such that $I^\mathfrak{m}/H \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K)$ is an isomorphism. Let $A \in I^\mathfrak{m}/H$ be an ideal class such that $\phi_{L/K}(A) = \sigma$. Then

$$\delta(\{\mathfrak{p} : \mathrm{Frob}_\mathfrak{p} = \sigma\}) = \delta(\{\mathfrak{p} : \mathfrak{p} \in A\}) = 1/[I^\mathfrak{m} : H] = 1/|G|.$$

If G is non-abelian, take the group $\langle\sigma\rangle \subset G$ generated by σ. Take $M = L^{\langle\sigma\rangle}$, so that L/M is a cyclic, and therefore abelian, extension. Consider

$$S_1 \coloneqq \{\mathfrak{q} \text{ prime of } M : \mathrm{Frob}_\mathfrak{q} = \sigma \in \mathrm{Gal}(L/M)\}.$$

Then the abelian case gives $\delta(S_1) = 1/|\langle\sigma\rangle|$. Consider

$$S_2 \coloneqq \{\mathfrak{q} \text{ prime of } M : \mathrm{Frob}_\mathfrak{q} = \sigma \in \mathrm{Gal}(L/M),\ M_\mathfrak{q} = K_\mathfrak{p},\ \mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K\} \subset S_1.$$

(In other words, $f(\mathfrak{q}/\mathfrak{p}) = 1$.) Then $\delta(S_2) = \delta(S_1)$, since the infinitely many primes we threw away have density 0. Consider

$$S_3 \coloneqq \{\mathfrak{p} \text{ prime of } K : \mathrm{Frob}_\mathfrak{p} \in C_\sigma \subset \mathrm{Gal}(L/K)\}.$$

Then there is a surjection $S_2 \to S_3$ given by $\mathfrak{q} \mapsto \mathfrak{p} \coloneqq \mathfrak{q} \cap \mathcal{O}_K$. The fiber of this map is isomorphic to

$$\{\tau \in G : \tau\sigma = \sigma\tau\}/\langle\sigma\rangle = Z_G(\sigma)/\langle\sigma\rangle.$$

Hence we have the following chain of equalities:

$$\delta(S_3) = \delta(S_2)\frac{|\langle\sigma\rangle|}{|Z_G(\sigma)|} = \frac{1}{|\langle\sigma\rangle|}\frac{|\langle\sigma\rangle|}{|Z_G(\sigma)|} = \frac{1}{|Z_G(\sigma)|} = \frac{|C_\sigma|}{|G|}$$

where the last equality is the orbit-stabilizer theorem. □

5.9 Proof of global CFT

Lemma 5.9.1. *$\phi_{L/K}\colon \mathbb{I}_K \to \mathrm{Gal}(L/K)$ is surjective.*

Proof. Consider the subgroup H generated by $\{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p} \text{ is unramified in } L\}$. We want $H = G \coloneqq \mathrm{Gal}(L/K)$. Let $M = L^H$. By Galois theory it suffices to show $M = K$. Then $\mathrm{Frob}_{\mathfrak{p}}$ is trivial in $\mathrm{Gal}(M/K)$ for all but finitely many primes $\mathfrak{p}$. So there are only finitely many primes that do not split completely in M. By the first inequality (or Chebotarev density), it follows that $M = K$. □

Theorem 5.9.2 (Theorem A)**.** *$\phi_{L/K}(K^\times) = 1$.*

Theorem 5.9.3 (Theorem B)**.** *For any class $\alpha \in H^2(L/K)$, we have $\sum_v \mathrm{inv}_v(\alpha) = 0$.*

Proof of global CFT. By theorem A and local class field theory, $K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L \subset \ker(\phi_{L/K})$. By the lemma, there the resulting map $\mathbb{I}_K/(K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L) \twoheadrightarrow \mathrm{Gal}(L/K)$ is surjective. By the second inequality, $[C_K : \mathrm{Nm}_{L/K}\,C_L] \le [L : K]$. Hence this surjection is actually an isomorphism. □

Remark. Hence to finish the proof of global CFT, it suffices to prove theorem A. Here is an outline of the proof:

0. Prove theorem A for cyclotomic extensions $L/K = \mathbb{Q}(\zeta_n)/\mathbb{Q}$.
1. Prove theorem A for L/K cyclic cyclotomic.
2. Prove theorem B for L/K cyclic cyclotomic.
3. Prove theorem B for L/K finite Galois.
4. Prove theorem A for L/K finite Galois.

Proof of step 0. To show: for all $a \in \mathbb{Q}^\times$, we have $\phi(a) = 1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. It suffices to show $\phi(a) = 1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q})$ where $\ell^r \mid m$ is a prime power. So wlog assume $m = \ell^r$.

1. If $v = p \neq \ell$ is a prime and $a = u \cdot p^s$ where u is coprime to p, then since p is unramified, $\phi_v(a) = (\zeta_{\ell^r} \mapsto \zeta_{\ell^r}^{p^s}) \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q})$. (Equivalently, it is the element $p^s \in (\mathbb{Z}/\ell^r)^\times$.)
2. If $v = p = \ell$, then p is ramified. Again write $a = u \cdot p^s$ where again u is coprime to p. By a homework exercise, $\phi_v(a) = (\zeta_{\ell^r} \mapsto \zeta_{\ell^r}^{u^{-1}}) \in \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q})$. (Equivalently, it is the element $u^{-1} \in (\mathbb{Z}/\ell^r)^\times$.)
3. Finally, if $v = \infty$ and $a = \mathrm{sgn}(a)|a|$, then $\phi_v(a) = \mathrm{sgn}(a) \in \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\pm 1\}$.

To show $\phi(a) = 1$, it suffices to show $\phi(q) = 1$, $\phi(\ell) = 1$, and $\phi(-1) = 1$. Compute

$$\begin{aligned}
\phi(q) &= \prod_v \phi_v(q) = \phi_q(q)\phi_\ell(q) = qq^{-1} = 1 \\
\phi(\ell) &= \prod_v \phi_v(\ell) = \phi_\ell(\ell) = 1^{-1} = 1 \\
\phi(-1) &= \prod_v \phi_v(-1) = \phi_\ell(-1)\phi_\infty(-1) = (-1)^{-1}(-1) = 1.
\end{aligned}$$

□

Lemma 5.9.4. *If theorem A holds for L/K, then it also holds for L'/K' where K'/K is a finite extension, and $L' = L \cdot K'$ is the compositum. It also holds for sub-extensions $M \subset L$.*

Proof. We use functoriality in local CFT, which says that the diagram

$$\begin{array}{ccc} \mathbb{I}_{K'} & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ {\scriptstyle \mathrm{Nm}}\downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

commutes. Then for all $a \in (K')^\times$, we have

$$\phi_{L'/K'}(a) = \phi_{L/K}(\mathrm{Nm}_{K'/K}(a)) \in \phi_{L/K}(K^\times) = 1.$$

Similarly, we can factor $\phi_{M/K}$ as $\phi_{M/K} \colon \mathbb{I}_K \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(M/K)$. Hence for all $a \in K^\times$, if $\phi_{L/K}(a) = 1$ then $\phi_{M/K}(a) = 1$. □

Proof of (0) $\implies$ (1). Apply the lemma to $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_m)$, and K' to be any number field. Hence L'/K' and any sub-extension M/K' satisfies theorem A. □

Proof of (2) $\implies$ (3). Recall that for all $\alpha \in H^2(K)$, there exists L/K cyclic cyclotomic such that $\alpha \in \ker(H^2(K) \to H^2(L)) = H^2(L/K)$ (by inflation-restriction). Step 2 therefore says $\sum_v \mathrm{inv}_v(\alpha) = 0$. Hence $\sum_v \mathrm{inv}_v(\alpha) = 0$ for all L/K finite Galois. □

Proof of (1) $\implies$ (2) *and* (3) $\implies$ (4). If M, N are G-modules, there is a cup product

$$\begin{aligned} H^r(G, M) \times H^r(G, N) &\to H^{r+s}(G, M \otimes N) \\ (\varphi, \psi) &\mapsto ((g_1, \dots, g_{r+s}) \mapsto \varphi(g_1, \dots, g_r) \otimes (g_1 \cdots g_r)\psi(g_{r+1}, \dots, g_{r+s})). \end{aligned}$$

We will apply this to $H^0(G, M) \times H^2(G, \mathbb{Z}) \to H^2(G, M)$. Recall that $H^2(G, \mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$. Take $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ and let $\delta_\chi \in H^2(G, \mathbb{Z})$ be the corresponding element under these identifications. Let $M = L^\times$ or $\mathbb{I}_L$. Then we get a diagram

$$\begin{array}{ccccc} H^0(G, L^\times) = K^\times & \longrightarrow & H^0(G, \mathbb{I}_L) = \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ {\scriptstyle \cup\delta_\chi}\downarrow & & {\scriptstyle \cup\delta_\chi}\downarrow & & {\scriptstyle \chi}\downarrow \\ H^2(G, L^\times) = H^2(L/K) & \longrightarrow & H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(L^v/K_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} \end{array}$$

which relates theorem A and theorem B. Hence we can actually compute $\phi_{L/K}$ using $\sum_v \mathrm{inv}_v$ after cupping.

If theorem A holds for L/K cyclic cyclotomic, then the top row of this diagram (for L/K) is zero. By commutativity, we conclude that the bottom row is also zero. But this is precisely the statement of theorem B. Similarly, if theorem B holds for L/K finite Galois, then theorem A also holds for L/K finite Galois. □

5.10 Primes $p = x^2 + ny^2$

We can apply class field theory to the problem of determining which primes can be written in the form $x^2 + ny^2$. Recall that an odd prime p is of the form $x^2 + y^2$ iff $p \equiv 1 \bmod 4$. More generally, in $K = \mathbb{Q}(\sqrt{d_K})$, either p splits, is inert, or is ramified. For $K = \mathbb{Q}(i)$, set $d_K = -4$. Then p odd implies p does not ramify in K. Then

$$p \text{ splits} \iff \left(\frac{-4}{p}\right) = 1 \iff (-1)^{(p-1)/2} = 1 \iff p \equiv 1 \bmod 4.$$

Since $\mathcal{O}_K = \mathbb{Z}[i]$ has class number 1, the primes $\mathfrak{p}_1, \mathfrak{p}_2$ lying over p are principal, and generated by conjugates $x \pm iy$. The two ingredients making this work are quadratic reciprocity (which generalizes to Artin reciprocity), and that $\mathfrak{p}_i$ is principal (which generalizes to using the Hilbert class field).

Recall that the idèle class group of $\mathbb{Q}$ is $C_{\mathbb{Q}} = \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^\times$. The Kronecker–Weber theorem says $\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$, so $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \prod_p \mathbb{Z}_p^\times$. Then the Artin map

$$\phi_{\mathbb{Q}} \colon C_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$$

is given by projection onto the second factor. Take the modulus $\mathfrak{m} = (N)\infty$. Then $\mathrm{Cl}_{(N)\infty} = (\mathbb{Z}/N)^\times$, and Artin reciprocity gives an isomorphism

$$\mathrm{Cl}_{(N)\infty} \cong (\mathbb{Z}/N)^\times \xrightarrow{\phi_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}), \quad a \mapsto (\zeta_N \mapsto \zeta_N^a).$$

In particular, $p \equiv 1 \bmod N$ iff Frob_p is trivial, iff p splits completely in $\mathbb{Q}(\zeta_N)/\mathbb{Q}$. For example, if $N = 4$, then $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ and we get $p \equiv 1 \bmod 4$ iff p splits, which is precisely quadratic reciprocity.

Theorem 5.10.1. *$p = x^2 + 5y^2$ for $p \neq 5$ iff $p \equiv 1, 9 \bmod 20$.*

To prove this theorem, we want to look at splitting in $K = \mathbb{Q}(\sqrt{-5})$. Recall that the existence theorem says open subgroups of finite index in $C_{\mathbb{Q}}$ are in 1-to-1 correspondence with finite abelian extensions of $\mathbb{Q}$. Out of these extensions, we look at the sub-extensions of $\mathbb{Q}(\zeta_N)$. They correspond to subgroups H of $(\mathbb{Z}/N)^\times$. For example, when $N = 5$, clearly $(\mathbb{Z}/5)^\times$ has subgroups $\{1\}$, $\{1, 4\}$, and $\{1, 2, 3, 4\}$, corresponding to extensions $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}$.

But we want $\mathbb{Q}(\sqrt{-5})$. It has discriminant 20, so let's look at $N = 20$. Then $(\mathbb{Z}/20)^\times = (\mathbb{Z}/4)^\times \times (\mathbb{Z}/5)^\times$. The subgroup $\{1, 19\}$ corresponds to invariants under complex conjugation, i.e. $\mathbb{Q}(\zeta_{20} + \bar{\zeta}_{20})$. We also know $\mathbb{Q}(\zeta_5)$ corresponds to $\{1 \bmod 5\} = \{1, 11\}$. There should be a third degree-4 extension corresponding to $\{1, 9\}$, but we don't know what the extension is. We also have the obvious extensions $\mathbb{Q}(i)$, corresponding to $\{1 \bmod 4\}$, and $\mathbb{Q}(\sqrt{5})$, corresponding to $\{1, 4 \bmod 5\}$. By the existence theorem, $\{1, 9\}$ contains both $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(i)$, and therefore must be $\mathbb{Q}(\sqrt{5}, i)$. Since $\mathbb{Q}(\sqrt{-5})$ is a sub-extension of $\mathbb{Q}(\sqrt{5}, i)$, it must correspond to the last order-4 subgroup containing $\{1, 9\}$, i.e. $\{1, 3, 7, 9\}$. Hence $p \equiv 1, 3, 7, 9 \bmod 20$ iff p splits in $\mathbb{Q}(\sqrt{-5})$. Warning: $\mathbb{Q}(\sqrt{-5})$ has non-trivial class number. So we need to see when $p = \mathfrak{p}_1\mathfrak{p}_2$ has $\mathfrak{p}_i$ principal. For example, we have $(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$, and both are non-principal, so at least we should exclude 3. To do this in general, use the Hilbert class field H_K.

Theorem 5.10.2. *Let K be a number field and H_K/K be its Hilbert class field. Then $\mathfrak{p}$ is principal iff $\mathfrak{p}$ splits completely in H_K.*

Proof. We know $\mathrm{Cl}_K \cong \mathrm{Gal}(H_K/K)$. Then $\mathfrak{p}$ is principal iff $[\mathfrak{p}] = [0]$ in Cl_K, iff $\mathrm{Frob}_{\mathfrak{p}}$ is trivial, iff $\mathfrak{p}$ splits completely in H_K. □

So $p = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1$ and $\mathfrak{p}_2$ principal iff p splits completely in $H_{\mathbb{Q}(\sqrt{-5})}$. But we know $H_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Q}(\sqrt{5}, i)$. This extension corresponds to $\{1, 9\}$, i.e. $p \equiv 1, 9 \bmod 20$.

Remark. If $K/\mathbb{Q}$ is non-abelian, then we can never find a congruence condition for p splitting in K. For example, take $K = \mathbb{Q}[x]/(x^3 - x^2 + 1)$, which has the smallest discriminant $d_K = -23$ out of all cubic extensions. Then $\mathrm{Gal}(K/\mathbb{Q}) = S_3$. We computed the splitting behavior of primes for this extension earlier, for the Chebotarev density theorem, and noted that the primes do not satisfy any congruence conditions. However, we can look at the **modular form**

$$q \prod_{n\geq 1} (1 - q^n)(1 - q^{23n}) = \sum_{n\geq 1} a_n q^n.$$

We can compute a_p for p prime to get the table:

p	2	3	5	7	11	13	17	19	23	29	31
a_p	-1	-1	0	0	0	-1	0	0	1	-1	-1.

Note that the primes p when $a_p = -1$ are precisely the primes splitting completely. This is a hint at the Langlands program.