Algebraic Number Theory
Spring 2021

Notes by Patrick Lei

Lectures by Chao Li

Columbia University

Disclaimer

These notes were taken during lecture using the `vimtex` package of the editor `neovim`. Any errors are mine and not the instructor's. In addition, my notes are picture-free (but will include commutative diagrams) and are a mix of my mathematical style and that of the instructor. If you find any errors, please contact me at `plei@math.columbia.edu`.

Contents

1

Motivation

Here is a very classical question (that the ancients were interested in):

Question 1.0.1. *Which prime numbers* p *can be written as* $p = x^2 + y^2$ *for integers* x, y*?*

We can try to answer this by experiment. Clearly, $2 = 1 + 1, 5 = 1 + 4, 13 = 4 + 9, 17 = 1 + 16$ and the other primes below 20 cannot be written as a sum of two squares. Then, because any square is congruent to 0 or 1 modulo 4, we see that if p is an odd prime, then

Theorem 1.0.2 (Fermat, Christmas Day, 1640)**.** *An odd prime* p *can be written as a sum of two squares if and only if* $p \equiv 1 \pmod 4$.[1] *Similarly, we have:*

- $2 \neq p = x^2 + 2y^2$ *if and only if* $p \equiv 1, 3 \pmod 8$.
- $3 \neq p = x^2 + 3y^2$ *if and only if* $p \equiv 1 \pmod 3$.

In the modern day, we should reinterpret $p = x^2 + y^2$ as a factorization problem in the number field $k = \mathbb{Q}(i)$. Now we write our problem as $p = (x + iy)(x - iy)$. Similarly, the second problem can be written as $p = (x + \sqrt{-2}y)(x - \sqrt{-2}y)$ in $\mathbb{Q}(\sqrt{-2})$ and the third problem can be expressed in the field $\mathbb{Q}(\sqrt{-3})$. More generally, we can consider $k = \mathbb{Q}(\sqrt{d})$ for an arbitrary d, called the *discriminant* of k. For a general quadratic extension, the ring of integers is not a UFD, but it is Dedekind, so we have unique factorization of prime ideals. Therefore we can write

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \left(\frac{d}{p}\right) = 1 \\ \mathfrak{p} & \left(\frac{d}{p}\right) = -1 \\ \mathfrak{p}^2 & \left(\frac{d}{p}\right) = 0 (\text{ or } p \mid d). \end{cases}$$

What we want to know is when the ideal (p) splits, and this behavior is governed by the Legendre symbol. This symbol satisfies the miraculous identity (due to Gauss)

Theorem 1.0.3 (Quadratic Reciprocity)**.** *Let* p, q *be odd primes. Then we have the identity*

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

[1] Of course, Fermat never actually proved anything, and this statement was proved by Euler in the 1740s.

Recall that if p is odd and $p \nmid d$, then $\left(\frac{d}{p}\right) = 1$ if and only if $x^2 \equiv d \pmod{p}$ has solutions. Quadratic reciprocity tells us that the equation $x^2 \equiv q \pmod{p}$ is highly related to the equation $x^2 \equiv p \pmod{q}$. This ability to change the modulus is very helpful in solving these classical problems.

Example 1.0.4. A prime p splits in $\mathbb{Q}(\sqrt{-3})$ if and only if $\left(\frac{-3}{p}\right) = 1$ if and only if $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$.

Now we can generalize our question about splitting in quadratic fields to more general fields:

Question 1.0.5. *Is there a criterion of the form p splits in k if and only if $p \equiv * \pmod{N}$ for some N? If so, we can generalize quadratic reciprocity. This is one of the main questions of class field theory.*

Example 1.0.6. We have some examples of splitting behavior:

- p splits in $k = \mathbb{Q}(\sqrt{-5})$ if and only if $p \equiv 1, 3, 7, 9 \pmod{2}0$.
- p splits in $k = \mathbb{Q}(\sqrt{-5}, i)$ if and only if $p \equiv 1, 9 \pmod{2}0$.
- p splits in $k = \mathbb{Q}(\zeta_5)$ if and only if $p \equiv 1 \pmod{5}$.

However, there is no congruence condition for splitting in $k = \mathbb{Q}(\sqrt[3]{2})$ for any modulus N. The question is what is different about the last example. First, the fields $\mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-5}, i), \mathbb{Q}(\zeta_5)$ are all Galois extensions of $\mathbb{Q}$ with Galois groups $\mathbb{Z}/2, \mathbb{Z}/2 \times \mathbb{Z}/2, \mathbb{Z}/4$. On the other hand, $k = \mathbb{Q}(\sqrt[3]{2})$ is not Galois and its Galois closure $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ has Galois group S_3.

Definition 1.0.7. A field extension L/K is called *abelian* if L/K is Galois and $\mathrm{Gal}(L/K)$ is abelian.

This gives us the following slogan: given a number field k, class field theory

1. classifies all abelian extensions L/K in an accessible way;
2. describes factorization of primes of K in L in terms of groups intrinsic to K (for example the class group of K).

1.1 A Special Case of CFT

Here, we will classify all *unramified* abelian extensions L/K. Recall that the *class group* $\mathrm{Cl}(K)$ of a number field K is

$$\mathrm{Cl}(K) \coloneqq \{\text{fractional ideals of } K\}/\{\text{principal ideals of } K\}.$$

This is always a finite abelian group.

Definition 1.1.1. Let $H \subset \mathrm{Cl}(K)$ be a subgroup. Then a finite unramified abelian extension L/K is a *class field* for a subgroup $H \subset \mathrm{Cl}(K)$ if $\mathfrak{p}$ splits in L/K if and only if $[\mathfrak{p}] \in H \subset \mathrm{Cl}(K)$.

Theorem 1.1.2 (Unramified CFT)**.** *Given $H \subset \mathrm{Cl}(K)$, the class field for H exists and is unique. Moreover, each finite unramified abelian extension arises as a class field. This gives us a bijection*

$$\{\textit{finite unramified abelian extensions}\} \longleftrightarrow \{\textit{subgroups of } \mathrm{Cl}(K)\}.$$

Moreover, $\mathrm{Gal}(L/K) \cong \mathrm{Cl}(K)/H$.

Definition 1.1.3. Note that the class field for $H = 0$ is the maximal unramified abelian extension H_K of K, called the *Hilbert class field*. This gives a canonical isomorphism $\mathrm{Gal}(H_K/K) \cong \mathrm{Cl}(K)$. Also, we see that $\mathfrak{p}$ splits in H_K if and only if $\mathfrak{p}$ is a principal ideal.

Example 1.1.4. For the fields $K = \mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, we have $\mathrm{Cl}(K) = 0$ and thus $H_K = K$.

Example 1.1.5. The simplest example of a number field with nontrivial class group is $K = \mathbb{Q}(\sqrt{-5})$. Here, $\mathrm{Cl}(K) = \mathbb{Z}/2$ and $H_K = \mathbb{Q}(\sqrt{-5}, i)$.

Remark 1.1.6. More generally, class field theory will add ramification on both sides of the correspondence to obtain a correspondence

$$\{\text{finite abelian extensions}\} \longleftrightarrow \left\{\text{subgroups of } \mathcal{C}_K = \mathbb{A}_K^\times / K^\times\right\}.$$

1.2 Back to Fermat

Consider the equation $p = x^2 + 5y^2$. Recall that we have $2, 5 \neq p = x^2 + 5y^2$ if and only if $p \equiv 1, 9 \pmod 2 0$. Note that this is **different** from the splitting behavior in $K = \mathbb{Q}(\sqrt{-5})$. This happens because $\mathrm{Cl}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Z}/2$ is not trivial, and so we need both the condition that $(p) = \mathfrak{p}_1\mathfrak{p}_2$ **and** that the $\mathfrak{p}_i$ are principal. By unramified CFT, we know that $\mathfrak{p}_i$ are principal if and only if they split in $H_K = \mathbb{Q}(\sqrt{-5}, i)$, and therefore $p = x^2 + 5y^2$ if and only if p splits in $\mathbb{Q}(\sqrt{-5}, i)$. In this case, $H_K/\mathbb{Q}$ is abelian, so we have a nice answer.

Example 1.2.1. The primes of the form $p = x^2 + 14y^2$ **cannot** be described in terms of a congruence condition. The field $K = \mathbb{Q}(\sqrt{-14})$ has $\mathrm{Cl}(K) = \mathbb{Z}/4$ and $\mathrm{Gal}(H_K/\mathbb{Q}) \cong D_4$ is **non-abelian**.

Remark 1.2.2. We can study non-abelian extensions to get some nice answers that involve modular forms, and this is called the *Langlands program*, which is beyond the scope of this course.

Our outline for the semester is to prove local CFT, then prove global CFT, then do applications if time permits. This will be done using group cohomology.

2

Local Fields

Recall that it is very difficult to detect whether a polynomial equation over a global field like $\mathbb{Q}$ has solutions. However, we can embed $\mathbb{Q}$ into the local field $\mathbb{R}$ and then checking whether the polynomial has real solutions is very easy because we can do analysis. To try to recover all information about $\mathbb{Q}$, we can embed $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ for a prime p. We then have the following slogan, known as the local-to-global principle:

We will study problems in $\mathbb{Q}$ by studying problems in all the local fields $\mathbb{R}$ and $\mathbb{Q}_p$.

2.1 Absolute Values

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

1. $|-|$ sends $K^\times$ to $\mathbb{R}_{>0}$ and 0 to 0.
2. We have $|xy| = |x| \cdot |y|$ for all $x, y \in K$.
3. For all $x, y \in K$, we have $|x + y| \leqslant |x| + |y|$.

Example 2.1.2. The usual absolute value on $\mathbb{R}$ defines an absolute value in this semse. This induces an absolute value on $\mathbb{Q} \subseteq \mathbb{R}$ usually denoted by $|-|_\infty$. This is known as the archimedean absolute value on $\mathbb{Q}$.

Similarly, any embedding $K \overset{\sigma}{\hookrightarrow} \mathbb{R}$ or $K \overset{\sigma}{\hookrightarrow} \mathbb{C}$ induces an absolute value on K defined by $|x|_\sigma \coloneqq |\sigma(x)|$.

There is a different kind of absolute value that is not archimedian. Here, we will strengthen the triangle inequality.

Definition 2.1.3. If $|-|$ satisfies the ultrametric inequality

$$|x + y| \leqslant \max\{|x|, |y|\}$$

then we say $|-|$ is *nonarchimedean*.

Remark 2.1.4. Recall that $\mathbb{R}$ satisfies the archimedean property: If $0 \neq x \in \mathbb{R}$ there exists $n \in \mathbb{Z}$ such that $|nx| > 1$. This property fails for nonarchimedean absolute values because $|nx| \leqslant |x|$ for all $n \in \mathbb{Z}$. In fact, $|-|$ is nonarchimedean if and only if the set $\{|n \cdot 1|\}_{n \in \mathbb{Z}}$ is bounded.

Example 2.1.5. Let $a \in \mathbb{Q}^\times$ and p be a prime. Then define $\mathrm{ord}_p(a) \in \mathbb{Z}$ such that

$$a = \pm \prod_p p^{\mathrm{ord}_p(a)}.$$

Now for any $c < 1$, we define

$$|a|_p \coloneqq c^{\mathrm{ord}_p(a)}.$$

Then we simply need to check that $|-|_p$ is a nonarchimedean absolute value on $\mathbb{Q}$. Here, it is easy to check the ultrametric inequality, and this absolute value is called the p-*adic absolute value*. By convention, we will choose $c = p^{-1}$ and this is the *normalized* p-*adic absolute value* on $\mathbb{Q}$.

Example 2.1.6. For any number field K and prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Then we have a normalized $\mathfrak{p}$-adic absolute value

$$|a|_\mathfrak{p} \coloneqq \left(\frac{1}{N\mathfrak{p}}\right)^{\mathrm{ord}_\mathfrak{p}(a)}$$

where $N\mathfrak{p} = \#\mathcal{O}_K/\mathfrak{p}$.

Definition 2.1.7. An absolute value $|-|$ is *discrete* if $\left|K^\times\right| \subset \mathbb{R}$ is discrete under the usual topology on $\mathbb{R}$.

Example 2.1.8. For a number field K and prime $\mathfrak{p}$, the p-adic absolute value $|-|_\mathfrak{p}$ is discrete. On the other hand, $|-|_\infty$ is not discrete.

Definition 2.1.9. Suppose $|-|$ be nonarchimedean. Then define

1. $A \coloneqq \{a \in K \mid |a| \leqslant 1\}$. This is a subring of K.
2. Now define $A^\times = \{a \in K \mid |a| = 1\}$. This is a subgroup of A of invertible elements.
3. Set $\mathfrak{m} = \{a \in K \mid |a| < 1\}$. This is the unique maximal ideal of A.

Then $|-|$ is discrete if and only if $\mathfrak{m}$ is principal. In this case, a generator π of $\mathfrak{m}$ is called a *uniformizer*. Then every $a \in K$ can be uniquely written as $a = \pi^r \cdot u$ for some $r \in \mathbb{Z}, u \in A^\times$.

Example 2.1.10. (Non-example) Consider the field $\mathbb{Q}(\left\{p^{1/n}\right\}, n \in \mathbb{Z})$ with p-adic absolute value. This is not a discrete absolute value.

Definition 2.1.11. An absolute value defines a *metric* on K by $d(a,b) = |a-b|$ for all $a, b \in K$. This induces a topology on K where a basis of open neighborhoods of $a \in K$ is given by open balls

$$B(a,r) \coloneqq \{x \in K \mid |x-a| < r\}.$$

Example 2.1.12. In the p-adic topology, we see that $a, b \in \mathbb{Q}$ are closer under $|-|_p$ if and only if $|a-b|_p$ is smaller, which is equivalent to $\mathrm{ord}_p(a-b)$ being larger, which is equivalent to $a-b$ being divisible by a large power of p. In other words, $a \equiv b \pmod{p}^N$ for N large.

Definition 2.1.13. We say two absolute values on K are *equivalent*, or $|-| \sin |-|'$ if they induce the same topology on K.

Theorem 2.1.14 (Ostrowski, 1916)**.** *Let $|-|$ be an absolute value on $\mathbb{Q}$.*

1. *If $|-|$ is archimedean, then $|-| \sim |-|_\infty$.*
2. *If $|-|$ is nonarchimedean, then $|-| \sim |-|_p$ for a unique p.*

Remark 2.1.15. Similarly, absolute values on a number field K are given by

1. $|-|_{\mathfrak{p}}$ for a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ ($\mathfrak{p}$-adic place);
2. $|-|_\sigma$ for some $\sigma\colon K \hookrightarrow \mathbb{R}$ (real place);
3. $|-|_\sigma$ for some complex embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$ (complex place). Here, note that complex embeddings come in conjugate pairs.

Definition 2.1.16. An equivalence class of absolute values on K is called a *place (or prime)* of K.

Remark 2.1.17. When ν is a complex place it corresponds to a pair of complex embeddings $\sigma, \overline{\sigma}$, so we define

$$|x|_\nu \coloneqq |\sigma(x)|^2$$

and this is the *normalized absolute value for* ν.

One reason for this normalization is

Theorem 2.1.18 (Product Formula)**.** *Let K be a number field. Then for all $a \in K^\times$, we have*

$$\prod_{\nu \text{ place of } K} |a|_\nu = 1.$$

Remark 2.1.19. When $K = \mathbb{Q}$, let $a = \frac{m}{n}$ for $m, n \in \mathbb{Z}$. Then all but finitely many terms in the product are finite. Now it suffices to check this formula for $a = p$ and $a = -1$.

When $a = p$, we see that $|a|_p = p^{-1}$ and for primes $\ell \neq p$, we have $|a|_\ell = 1$. Finally, we see that $|a|_\infty = p$, so the formula holds. When $a = -1$, all absolute values are 1, so the product of all absolute values is trivial.

For a general number field, we can simply take the norm map $N_{K/\mathbb{Q}}$ to $\mathbb{Q}$ and check that it behaves well with respect to the places.

Theorem 2.1.20 (Weak Approximation)**.** *Let $|-|_1, \dots, |-|_n$ be inequivalent absolute values on a field K. Let $a_1, \dots, a_n \in K$. Then for all $\varepsilon > 0$, there exists $a \in K$ such that $|a - a_i|_i < \varepsilon$ for all $i = 1, \dots, n$.*

Remark 2.1.21. This allows us to approximate any finite collection $a_i \in K$ for inequivalent $|-|_i$.

Remark 2.1.22. As a sanity check, consider $K = \mathbb{Q}$ and suppose $|-|_i = |-|_{p_i}$. Then given $a_1, \dots, a_n$, we simply find $a \in \mathbb{Q}$ such that $a_i \equiv a \pmod{p}_i^N$, which is possible by the Chinese remainder theorem.

Remark 2.1.23. More generally, if $|-|_1 \not\sim |-|_2$ then one can choose $a \in K$ such that $|a|_1 > 1$ and $|a|_2 < 1$. Then if we consider $\frac{a^r}{1+a^r}$ as $r \to \infty$, the absolute value under $|-|_1$ approaches 1 and under $|-|_2$ it approaches 0.

2.2 Completions

Consider the field $\mathbb{Q}$ equipped with the the absolute value $|-|_\infty$. Then we can complete $\mathbb{Q}$ as a metric space to obtain the field $\mathbb{R}$. More generally, if $(K, |-|)$ is a field equipped with an absolute value (a *valued field*), then we will produce a general completion $\widehat{K}$. Our aim is to produce a field that contains the original field and whose arithmetic is easier to understand.

Definition 2.2.1. Let $(K, |-|)$ be a valued field. Then a sequence $\{a_n\}$ of elements in K is called *Cauchy* if for all $\varepsilon > 0$, there exists $N \geqslant 1$ such that $|a_n - a_m| < \varepsilon$ for all $n, m > N$. We say that K is *complete* if any Cauchy sequence in K has a limit in K.

Example 2.2.2. Consider the sequence of integers $\{a_n = 2^n\} = 2, 4, 8, 16, 32, \ldots$. Clearly, this is not Cauchy under the usual absolute value on $\mathbb{Q}$, but then if $m > n$, we see that

$$|a_n - a_m|_2 = \left(\frac{1}{2}\right)^n,$$

so $\{a_n\}$ is Cauchy in $(\mathbb{Q}, |-|_2)$. We then see that $|a_n - 0|_2 = \left(\frac{1}{2}\right)^n \to 0$ and thus the limit of the sequence is 0.

Example 2.2.3. Consider $\{a_n\} = \{4, 34, 334, 3334, \ldots\}$. Then if $m > n$, we have

$$|a_n - a_m|_5 = \left(\frac{1}{5}\right)^n$$

and therefore $\{a_n\}$ is Cauchy in $(\mathbb{Q}, |-|_2)$. We then see that

$$|3a_n - 2|_5 = \frac{1}{5^n} \xrightarrow{n\to\infty} 0$$

and therefore $a_n \to \frac{2}{3}$.

Remark 2.2.4. In general, the limit of a Cauchy sequence may not exist.

Theorem 2.2.5. *Let $(K, |-|)$ be a valued field. Then there exists a complete valued field $(\widehat{K}, |-|)$ and an embedding $K \hookrightarrow \widehat{K}$ of valued fields such that any other embedding $K \hookrightarrow L$ of K into a complete valued field factors uniquely through $\widehat{K}$. In particular, $\widehat{K}$ is unique up to isomorphism and is called the completion of $(K, |-|)$.*

Proof. Let $\widehat{K}$ be the set of all Cauchy sequences in K under the equivalence relation where $\{a_n\} \sim \{b_n\}$ where $\lim_{n\to\infty} |a_n - b_n| = 0$. Then $\widehat{K}$ is equipped with termwise addition and multiplication and absolute value $|\{a_n\}| = \lim_{n\to\infty} |a_n|$. Thus $\widehat{K}$ is a complete valued field.

To verify the universal property, we see that $x \mapsto (x, x, \ldots, x)$ embeds $K \hookrightarrow \widehat{K}$ and this satisfies the desired universal property. □

Definition 2.2.6. Let K be a number field and v a place of K. Denote by $K_v \coloneqq (K, |-|_v)$. When v is a finite place, denote by $\mathcal{O}_{K_v} = \mathcal{O}_{K,v} = \mathcal{O}_v$ the valuation ring $\{x \in K_v : |x| \leqslant 1\} \subseteq K_v$. When v is an infinite place, we see that $K_v \cong \mathbb{R}, \mathbb{C}$.

Example 2.2.7. Let $K = \mathbb{Z}$. Then we see that $\mathbb{Q}_\infty = \mathbb{R}$ and $\mathbb{Q}_p$ has a subring $\mathbb{Z}_p$, which is a discrete valuation ring. Here, elements of $\mathbb{Z}_p$ have a nonnegative lowest power of p.

Example 2.2.8. If $K = \mathbb{Q}(i)$, then $K_\infty = \mathbb{C}$ and $K_\mathfrak{p}$ for $\mathfrak{p} \subset \mathcal{O}_K = \mathbb{Z}[i]$ prime ideals are the completions of K.

Remark 2.2.9. Let K be a nonarchimedean discrete valued field. Then $\widehat{K}$ is a complete discrete valued field and the valuation ring $\widehat{A} \subset \widehat{K}$ is the closure of $A \subseteq K$ in $\widehat{K}$. Also, the maximal ideal $\widehat{\mathfrak{m}} \subseteq \widehat{A}$ is the closure of $\mathfrak{m} \subseteq A$ in $\widehat{K}$. Finally, a uniformizer π of K is also a uniformizer of $\widehat{K}$.

We also see that the natural map $A/\mathfrak{m}^n \to \widehat{A}/\widehat{\mathfrak{m}}^n$ is an isomorphism. This tells us that we can approximate elements in $\widehat{A}$ up to $\pi^n A$ using elements in A.

Proposition 2.2.10. *Let K be a discrete valued field. Let S be a complete set of representatives of $A/\mathfrak{m}$ and π be a uniformizer of K. Then any element of $\widehat{K}$ can be uniquely written as $a_k\pi^k + a_{k+1}\pi^{k+1} + \cdots$ where $a_i \in S$ and $k \in \mathbb{Z}$.*

Corollary 2.2.11. *Let $x \in \mathbb{Q}_p$. Then x has a p-adic expansion $x = \sum_{i \geqslant k} a_i p^i$, where $a_i \in S = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ and $k \in \mathbb{Z}$.*

Remark 2.2.12. The main term of the p-adic expansion is the lowest term p^k. This is completely unlike the situation with the decimal digits of $x \in \mathbb{R}$, where the highest power of 10 is the main term.

Remark 2.2.13. $\mathbb{Q}_p$ resembles $\mathbb{F}_p((T))$ but is more complicated arithmetically. When we add two power series, we simply add the coefficients, but addition in $\mathbb{Q}_p$ requires carrying. In addition, we see that $\mathbb{F}_p[[T]]/T^n \hookrightarrow \mathbb{F}_p[[T]]$ but $\mathbb{Z}_p/p^n$ does **not** embed in $\mathbb{Z}_p$.

Corollary 2.2.14. *We have an isomorphism*

$$\widehat{A} = \varprojlim \widehat{A}/\widehat{\mathfrak{m}}^n \cong \varprojlim A/\mathfrak{m}^n.$$

For example, we have

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Proof of Proposition 2.2.10. Let $x \in \widehat{K}^\times$. Then $x = \pi^k \cdot y$ for some $k \in \mathbb{Z}$ and $y \in \widehat{A}^\times$. Then we find the first digit a_0 by considering $y \equiv a_0$ in $A/\mathfrak{m} = S$. Then we replace $\pi^{-1}(y - a_0) = a_1 + a_2\pi^2 + \cdots$ and repeat the process. Repeating this, we simply use the completeness of $\widehat{K}$ to obtain the desired expansion. □

The advantage of completeness is that it is much easier to solve equations. Here, we take solutions modulo a high power of p and then take the limit.

Theorem 2.2.15 (Hensel's Lemma)**.** *Let K be a complete discrete valued field and $k = A/\mathfrak{m}$ be the residue field. Now let $f(x) \in A[x]$ be a monic polynomial and let $\overline{f}(x) \coloneqq f(x) \mod \mathfrak{m} \in k[x]$. Assume that $\overline{f}(x) = g_0(x)h_0(x)$ in $k[x]$ where g_0, h_0 are monic and coprime. Then there exist unique $g, h \in A[x]$ such that $f(x) = g(x)h(x)$ and $\overline{g} \equiv g_0, \overline{h} = h_0$.*

Corollary 2.2.16. *Suppose $\overline{f}$ has a simple root $\alpha_0 \in k$. Then $f(x)$ has a unique zero $\alpha \in A$ such that $\overline{\alpha} = \alpha_0$.*

Corollary 2.2.17. *If $k = \mathbb{F}_q$ for $q = p^t$, then $f(x) = x^q - x$ has q distinct roots in $k = \mathbb{F}_q$ and hence q distinct roots in K. In particular, $K^\times$ contains all $(q-1)$-th roots of unity, so we have a map $\mathbb{F}_q^\times \hookrightarrow K^\times$, called the Teichmuller lift.*

Proof of Hensel's lemma. Let $g_0, g_0 \in A[x]$ be arbitrary monic lifts. Then $f - g_0h_0 \in \pi A[x]$. Now inductiely we assume that there exist $g_n, h_n \in A[x]$ monic such that $f - g_nh_n \in \pi^{n+1}A[n]$. We simply write $g_{n+1} = g_n + \pi^{n+1}u$ for some $u \in A[x]$ such that $\deg u < \deg g_n$ and $h_{n+1} = h_n + \pi^{n+1}v$ where $\deg v < \deg h_n$. Then $f - g_{n+1}h_{n+1} \in \pi^{n+2}A$ if and only if

$$uh_n - vg_n \equiv \frac{f - g_nh_n}{\pi^{n+1}} \pmod{\pi}$$

but we can find such u, v by Bezout's lemma. Thus the desired g_{n+1}, h_{n+1} exist, and we obtain g, h by taking the limit. □

2.3 Extension of Absolute Values and Unramified Extensions

Let K be a complete discrete valued field and L be a finite separable extension of K. Suppose $[L : K] = n$. The main result is

Theorem 2.3.1. *Let K, L be as above. Then*

1. *$|-|_K$ extends uniquely to a discrete absolute value $|-|_L$ on L;*
2. *L is complete with respect to $|-|_L$;*
3. *For all $\beta \in L$, we have*
$$|\beta|_L = \left|N_{L/K}(\beta)\right|_K^{1/n}.$$

Remark 2.3.2. To perform a sanity check, if $\beta \in K$, we have $|\beta|_L = \left|N_{L/K}(\beta)\right|_K^{1/n} = |\beta^n|_K^{1/n} = |\beta|_K$.

Proof.

1. We first need to prove that a unique extension exists. We know that $|-|_K$ comes from a discrete valuation (hence is nonarchimedean), so let $A \subseteq K$ be the valuation ring. Then A is a Dedekind domain. Then let B be the integral closure of A in L. Then B is also a Dedekind domain. But then any absolute value on L extending $|-|_K$ comes from a maximal iddeal of B lying above the unique maximal ideal $\mathfrak{p} \subseteq A$. Therefore, we need to show that B is a local ring.

   To see this, assume not. Suppose there exist two prime ideals $\mathfrak{P}_1, \mathfrak{P}_2 \subseteq B$ lying above $\mathfrak{p}$. Let $\beta \in \mathfrak{P}$ but $\beta \notin \mathfrak{P}_2$. This implies that $A[\beta] \cap \mathfrak{P}_1 \neq A[\beta] \cap \mathfrak{P}_2$. Let $f(x) \in A[x]$ be the minimal polynomial of β. Then $\bar{f}(x) = f(x) \mod \mathfrak{p} \in A/\mathfrak{p}[x] = k[x]$ must satisfy $\bar{f}(x) = h(x)^m$ for an irreducible $h(x) \in k[x]$ (otherwise it has two distinct irreducible factors and Hensel tells us that the factorization can be lifted to $A[x]$). This implies that
$$A[\beta]/\mathfrak{p}A[\beta] = A[x]/(\mathfrak{p}, f(x)) = k[x]/(\bar{f}(x)) = k[x]/(h(x))^m$$
   has a unique prime ideal, generated by $h(x)$, which contradicts our original assumption that $A[\beta] \cap \mathfrak{P}_1, A[\beta] \cap \mathfrak{P}_2$ were distinct prime ideals.

2. Now we show that L is complete. Let $\{a_k\}$ be a Cauchy sequence in L. Choose a K-basis $\{e_1, \ldots, e_n\}$ of L and write
$$a_k = a_{1,k}e_1 + \cdots + a_{n,k}e_n \qquad a_{i,k} \in K.$$
   But then each sequence $\{a_{i,k}\}_k$ forms a Cauchy sequence in K. By completeness of K, we can take $a_i \coloneqq \lim_{k\to\infty} a_{i.k} \in K$ and so we have
$$\lim_{k\to\infty} a_k = a_1e_1 + \cdots + a_ne_n \in L,$$
   and thus L is complete.

3. Let $\widetilde{L}$ be the Galois closure of L/K. Then we know that $|-|_K$ also extends uniquely to $\widetilde{L}$. For any $\sigma \in \mathrm{Gal}(\widetilde{L}/K)$, the map $L \in \beta \mapsto |\sigma(\beta)|_{\widetilde{L}}$ is also an absolute value on L extending $|-|_K$. Therefore, by the uniqueness of the extension, we see that $|\beta|_L = |\sigma(\beta)|_{\widetilde{L}}$. This implies that
$$\left|N_{L/K}(\beta)\right|_K = \left|N_{L/K}\right|_{\widetilde{L}} = \prod_{\sigma\colon L\to\widetilde{L}} |\sigma(\beta)|_{\widetilde{L}} = \prod_{\sigma\colon L\to\widetilde{L}} |\beta|_L = |\beta|_L^n,$$
   as desired. □

Corollary 2.3.3. *If L/K is merely an algebraic and separable extension, then $|-|_K$ also extends uniquely to an absolute value on L, but $|-|_L$ may fail to be discrete or complete.*

Proof. Note that L is the union of all of its finite subextensions. □

Definition 2.3.4. Let K be a complete discrete valued field and L be a finite separable extension. Let $\mathcal{O}_K \subseteq K$ and $\mathcal{O}_L \subseteq L$ be the valuation rings and $\mathfrak{p} \subseteq \mathcal{O}_K, \mathfrak{P} \subseteq \mathfrak{O}_L$ be the maximal ideals. Next, let $k = \mathcal{O}_K/\mathfrak{p}, \ell = \mathfrak{O}_L/\mathfrak{P}$ be the residue fields.

Define the *ramification index* $e(L/K)$ to be the $e \geqslant 1$ such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e$. Next, define the *residual degree* $f(L/K)$ to be $f \geqslant 1$ such that $f = [\ell : k]$. Then $n = ef$.

Definition 2.3.5. The extension L/K is called

1. *Unramified* if $e(L/K) = 1$ (which implies $f(L/K) = n$ and $\mathfrak{p} = \mathfrak{P}$);
2. *Totally ramified* if $e(L/K) = n$ (which implies $\ell = k$ and $\mathfrak{p} = \mathfrak{P}^n$).

2.4 Unramified Extensions

We will study unramified extensions. Here, we will try to understand L/K via ℓ/k.

Proposition 2.4.1. *If L/K is unramified, write $\ell = k(\alpha_0), \alpha_0 \in \ell$. Then for any $\alpha \in \mathcal{O}_L$ such that $\overline{\alpha} = \alpha_0$ we have $L = K(\alpha)$.*

Proof. Let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Then $\deg \overline{f} = \deg f = [K(\alpha) : K] \leqslant [L : K]$. But then we know that $\deg \overline{f} \geqslant [k(\alpha_0) : k] = [\ell : k] = [L : K]$. But this implies that $\deg f = [L : K]$, so $K(\alpha) = L$. □

Proposition 2.4.2. *If $L = K(\alpha)$ with minimal polynomial of α given by $f(x)$ such that $\overline{f}(x)$ has no repeated roots over $\overline{k}$, then L/K is unramified.*

Proof. If $f(x)$ is irreducible, then by Hensel's lemma, we have $\overline{f}(x) = h(x)^m$ where $h(x) \in k[x]$ is irreducible. But then because $\overline{f}(x)$ has no repeated roots, we see that $m = 1$. But then we see that $[\ell : k] = [L : K]$ and thus L/K is unramified. □

Proposition 2.4.3.

1. *Let $K \subset L \subset M$ be a tower of field extensions. Then M/K is unramified if and only if M/L and L/K are unramified.*
2. *Assume k is perfect. If L/K is unramified and L'/K is finite, then LL'/L' is unramified.*
3. *Assume k is perfect. Then if L/K and L'/K are unramified, then LL'/K is unramified.*

Proof.

1. Note that M/K is unramified if and only if $e(M/K) = 1$, which is equivalent to $e(M/L) = e(L/K) = 1$ by multiplicativity of the ramification index.
2. Suppose L/K is unramified. Then let $L = K(\alpha)$ and let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Then the reduction $\overline{f}(x) \in k[x]$ is irreducible and $\ell = k(\overline{\alpha})$. Because k is perfect, $\overline{f}(x)$ has no repeated roots.

   Because $LL'/L' = L'(\alpha)/L'$, let $g(x) \in \mathcal{O}_{L'}[x]$ be the minimal polynomial of α. Then $\overline{g}(x) \mid \overline{f}(x)$ and thus $\overline{g}(x)$ has no repeated roots, so LL'/L' is unramified.

3. Consider the tower $K \subseteq L' \subseteq LL'$. Because $L/K, L'/K$ are unramified, we know LL'/L is unramified. This implies that LL'/K is unramified. □

Theorem 2.4.4. *Assume that* k *is perfect. Then there is an inclusion-preserving bijection*

$$\{L/K \textit{ finite unramified}\} \overset{\sim}{\leftrightarrow} \{\ell/k \textit{ finite}\} \qquad L \mapsto \ell.$$

Moreover, L/K *is Galois if and only if* ℓ/k *is Galois and* $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\ell/k)$ *in this case.*

Proof. We prove surjectivity. Let ℓ/k be a finite extension. Write $\ell = k(\alpha_0)$ and let $\overline{f}(x) = k[x]$ be the minimal polynomial of α_0. Then any monic lift $f(x) \in \mathcal{O}_K[x]$ of $\overline{f}(x)$ has a root α such that $\overline{\alpha} = \alpha_0$ by Hensel's Lemma. Then $L = K(\alpha)$ has residue field $\ell = k(\alpha_0)$. Because $\overline{f}$ is irreducible and k is perfect, we know L/K is unramified.

Now we will prove injectivity. Let $L/K, L'/K$ be unramified with the same residue field ℓ. Then LL'/K is also unramified with residue field ℓ. But this implies that

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

so we must have $L = LL' = L'$.

Now we will show the statements about Galois extensions. If L/K is Galois, then $\mathrm{Gal}(L/K)$ preserves $\mathcal{O}_L$ and $\mathfrak{p}_L \subseteq \mathcal{O}_L$ and acts trivially on $\mathcal{O}_K$ and $\mathfrak{p}_K \subseteq \mathcal{O}_K$. This implies that any $\sigma \in \mathrm{Gal}(L/K)$ induces $\overline{\sigma} \in \mathrm{Aut}(\ell/k)$. If $L = K(\alpha)$ and $\alpha_0 = \overline{\alpha}$, then L/K is Galois if and only if it contains α, but this is equivalent to ℓ containing all conjugates of α_0, which is equivalent to ℓ/k being Galois. Then the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k)$ is an isomorphism because the permutation on conjugates of α induces the same permutation on the conjuages of α_0. □

Corollary 2.4.5. *If* L/K *is an algebraic extension (possibly infinite), then there exists a largest unramified subextension* K_0/K *of* L/K*. Moreover,* L/K_0 *is totally ramified.*

Proof. Let K_0 be the compositum of all finite unramified subextensions of L/K. Then the residue field of K_0 is equal to the residue field of L (otherwise, we can create an even larger unramified extension). This implies L/K_0 is totally ramified. □

Corollary 2.4.6. *Assume* $k = \mathbb{F}_q$*. Then for all* $n \geqslant 1$ *there is a unique unramified extension* L/K *of degree* n *and* $\mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$*.*

Proof. There is a unique degree n extension of $\mathbb{F}_q$. □

Definition 2.4.7. Define the *Frobenius element* $\sigma \in \mathrm{Gal}(L/K)$ when $k = \mathbb{F}_q$ to be the generator of $\mathrm{Gal}(L/K)$ corresponding to the Frobenius map under $\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. We will call this element $\mathrm{Frob}_{L/K}$, and $\mathrm{Frob}_{L/K}(\alpha) \equiv \alpha^q \pmod{\mathfrak{p}_L}$ for all $\alpha \in \mathcal{O}_L$.

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

$$K^{\mathrm{ur}} = \bigcup_{(n,q)=0} K(\zeta_n).$$

In particular, we have

$$\mathbb{Q}_p^{\mathrm{ur}} = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n).$$

Proof. We know $\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta_{q^n-1})$, so $\overline{\mathbb{F}}_q$ is given by adjoining all coprime-to-p roots of unity. □

2.5 Totally Ramified Extensions

Definition 2.5.1. A polynomial $f(x) \in K[x]$ is *Eisenstein* if

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

such that $|a_n| = 1, |a_i| < 1, |a_0| = |\pi|$.

Example 2.5.2. The polynomial $x^n - \pi$ is Eisenstein. Note that $K[x]/f(x) = K(\sqrt[n]{\pi})$ is totally ramified.

Proposition 2.5.3. *A finite extension L/K is totally ramified if and only if $L = K(\alpha)$ where α is a root of an Eisenstein polynomial.*

Proof. Let α be the root of an Eisenstein polynomial. Then $|\alpha^n| = \prod_{\sigma\colon L \hookrightarrow \widetilde{L}} |\sigma(\alpha)| = |a_0| = |\pi|$. Therefore $e(L/K) \geqslant n$ and thus L/K is totally ramified.

Now suppose L/K is totally ramified. Let α be a uniformizer of L. Therefore $(\alpha^n) = (\pi)$ and thus $|\alpha|_L = |\pi|_L^{1/n}$. Then $1, \alpha, \ldots, \alpha^{n-1}$ have absolute values representing different cosets in $\left|L^\times\right|/\left|K^\times\right|$. Thus the minimal polynomial of α has degree n. Moreover, if we write the minimal polynomial as

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

then $|\alpha|^n = |a_0| = |\pi|$ and $|a_i| < 1$ so that the required cancellation happens. But this implies that α is a root of an Eisenstein polynomial. □

Proposition 2.5.4. *Assume $k = \mathbb{F}_q$. Then there are only finitely many totally ramified extensions of K.*

Proof. Recall **Krasner's lemma**: Let $f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^n b_i x^i \in K[x]$ and assume $|a_i - b_i|$ is sufficiently small for all i. If $f(x)$ is irreducible, then so is $g(x)$, and

$$\{K(\alpha) \mid f(\alpha) = 0\} = \{K(\beta)\colon g(\beta) = 0\}.$$

Therefore a totally ramified extension depends only on a small neighborhood of $(a_0, \ldots, a_{n-1})$ in the set

$$\{|a_0| = |\pi|\} \times \{|a_1| < 1\} \times \cdots \times \{|a_{n-1}| < 1\},$$

which is compact, so it can be covered by finitely many such small neighborhoods. □

Recall that if K is a complete discrete valued field with residue field $k = \mathbb{F}_q$, there exists a unique unramified extension L/K of degree n. Together with the proposition, there exist finitely many totally unramified extensions L/K of degree n. This is of course false for number fields; for example, $\mathbb{Q}$ has infinitely many quadratic extensions.

Remark 2.5.5. Krasner (1966) gave an explicit formula for the number of extensions of p-adic fields of degree n and an algorithm to construct the set of generating polynomials of degree n. More desirable is a way to organize all these extensions, and local class field theory achieves this for abelian extensions of all local fields.

Definition 2.5.6. A *local field* is a valued field K that is locally compact under the topology induced by the absolute value.

Remark 2.5.7. Recall that

1. A topological space is compact if and only if open cover has a finite subcover.

2. A topological space is locally compact if every point has compact neighborhood.

3. A metric space is compact if and only if it is complete and totally bounded.

4. A metric space is compact if and only if all closed balls are compact.

5. This tells us that local fields are always complete. To find a limit for a Cauchy sequence, everything is contained in a closed ball, which is complete and thus has a limit.

Example 2.5.8.

1. The easiest examples of local fields are $\mathbb{R}, \mathbb{C}$.

2. If K is archimedean and complete, then $K \simeq \mathbb{R}$ or $\mathbb{C}$.

Lemma 2.5.9. *Let K be a complete discrete valued field. Then K is locally compact if and only if the residue field k is finite.*

Proof. Let K be locally compact. Then $\mathcal{O}_K = \{x \in K \mid |x| \leqslant 1\}$ is a closed ball. This means that $\mathcal{O}_K$ is compact. If we consider an open cover

$$\mathcal{O}_K = \bigcup_{x \in k} (x + \mathfrak{p}_K),$$

this has a finite subcover. But all of the $x + \mathfrak{p}_K$ are disjoint, so k is finite.

Now suppose k is finite. We show that every $x \in K$ has a compact neighborhood. In particular, we will show that $x + \mathcal{O}_K$ is compact and therefore that $\mathcal{O}_K$ is compact. To do this, we need to show that $\mathcal{O}_K$ is totally bounded. Choose $r > 0$ and consider the open balls $B_{a,r}$ give a cover of $\mathcal{O}_K$ as long as $a \in \mathcal{O}_K/\mathfrak{p}_K^n$ and n is sufficiently large. By finiteness of k, we know that $\mathcal{O}_K/\mathfrak{p}_K^n$ is finite, as desired. □

Theorem 2.5.10. *Every local field is one of the following:*

1. *$\mathbb{R}$ or $\mathbb{C}$;*

2. *A finite extension of $\mathbb{Q}_p$;*

3. *$\mathbb{F}_q((t))$ for a prime power q.*

Proof. Suppose $\operatorname{char} K = 0$. Then $\mathbb{Q} \subseteq K$. If K is archimedean, then $K = \mathbb{R}$ or $\mathbb{C}$. Otherwise, $\mathbb{Q}_p \subseteq K$ and by local compactness, $K/\mathbb{Q}_p$ must be finite.

If $\operatorname{char} K = 0$, then $\mathbb{F}_p \subseteq K$. Let $k = \mathbb{F}_q$ be the residue field. Then

$$K = \left\{ \sum_{n \geqslant k} a_n \pi^n \mid k \in \mathbb{Z}, a_n \in S = \mathcal{O}_K/\mathfrak{p}_K \right\}.$$

By Hensel's lemma, we have $\mathbb{F}_q^\times \hookrightarrow K^\times$ and we thus have $\mathbb{F}_q \subseteq K$. Therefore $K \cong \mathbb{F}_q((\pi))$, as desired. □

2.6 Statement of Local Class Field Theory

Recall that a field extension L/K is *abelian* if it is Galois and $\mathrm{Gal}(L/K)$ is abelian.

Exercise 2.6.1. If $L_1/K, L_2/K$ are abelian, then L_1L_2/K is also abelian.

Define K^{ab} to be the maximal abelian extension of K. Equivalently, this is the compositum of all finite extensions of K. Then K^{ab}/K has infinite degree, and classifying abelian extensions of K is equivalent to understanding $\mathrm{Gal}(K^{ab}/K)$.

Definition 2.6.2. Let Ω/K be a possible infinite extension. We call Ω/K *Galois* if it is algebraic, separable, and normal. Equivalently, Ω is the union of all its finite Galois subextensions. In particular, we have

$$\mathrm{Gal}(\Omega/K) = \varprojlim_{L/K \text{ finite Galois}} \mathrm{Gal}(L/K)$$

is an inverse limit of finite groups, known as a *profinite* group. Then $\mathrm{Gal}(\Omega/K)$ has a *profinite topology* with a basis of open neighborhoods of 1 given by $\mathrm{Gal}(\Omega/L) \subseteq \mathrm{Gal}(\Omega/K)$ for finite subextensions L/K.

Example 2.6.3. Consider $\Omega/K = \overline{\mathbb{F}}_q/\mathbb{F}_q$. Then

$$\mathrm{Gal}(\overline{\mathbb{F}}_q, \mathbb{F}_q) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

The open neighborhoods of 1 are given by $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^n}) \cong n\widehat{\mathbb{Z}} \subseteq \widehat{\mathbb{Z}}$.

Remark 2.6.4. If L/K is finite, then $\mathrm{Gal}(\Omega/L)$ is an open subgroup. In addition, $\mathrm{Gal}(\Omega/L)$ is also closed, so it is clopen.

If L/K is any extension, then

$$\mathrm{Gal}(\Omega/L) = \bigcap_{\substack{L_i \subseteq L \\ L_i/K \text{ finite}}} \mathrm{Gal}(\Omega/L_i)$$

is a closed subgroup.

Theorem 2.6.5 (Galois correspondence)**.** *Let Ω/K be Galois. Then there is a Galois correspondence*

$$\{L/K \textit{ subextension of } \Omega/K\} \longleftrightarrow \{\textit{closed subgroups of } \mathrm{Gal}(\Omega/K)\}.$$

Moreover, L/K is Galois if and only if the corresponding closed subgroup $H \subseteq \mathrm{Gal}(\Omega/K)$ is normal.

Remark 2.6.6. If $H \subseteq \mathrm{Gal}(\Omega/K)$ is not necessarily closed (for example, $\mathbb{Z} \subset \widehat{\mathbb{Z}}$ is not closed and its closure is $\widehat{\mathbb{Z}}$), then Ω^H corresponds to $\overline{H}$ under the Galois correspondence. In particular, $\mathrm{Gal}(K^{ab}/K) = G/\overline{[G,G]} =: G^{ab}$, where $G = \mathrm{Gal}(\overline{K}/K)$.

This gives us the slogan, that when K is a local field, $\mathrm{Gal}(K^{ab}/K)$ can be understood in terms of $K^\times$.

Theorem 2.6.7 (Local Artin reciprocity)**.** *There exists a unique $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ (local Artin reciprocity map) such that*

1. *For any finite abelian* L/K*, there is a commutative diagram*

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow \\ K^\times/N(L^\times) & \xrightarrow[\phi_{L/K}]{\sim} & \mathrm{Gal}(L/K). \end{array}$$

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

2.7 Norm Subgroups

Let K be a nonarchimedean local field.

Definition 2.7.1. A subgroup of $K^\times$ is a *norm subgroup* if it is of the form $N(L^\times)$ for some finite abelian extension L/K.

Proposition 2.7.2. *Assume local CFT I.*

1. $N(L_1^\times) \cap N(L_2^\times) = N((L_1L_2)^\times)$.
2. $N(L_1^\times) \subseteq N(L_2^\times)$ *if and only if* $L_1 \supseteq L_2$.
3. *A subgroup of* $K^\times$ *containing a norm subgroup is also a norm subgroup.*
4. $N(L_1^\times)N(L_2^\times) = N((L_1 \cap L_2)^\times)$.

Proof. Recall that there exists a unique local Artin reciprocity map $K^\times \xrightarrow{\phi_K} \mathrm{Gal}(K^{ab}/K)$.

1. Note that if $K \subseteq L_2 \subseteq L_1$, then $N(L_1^\times) \subseteq N(L_2^\times)$, so clearly for L_1, L_2, we see that $N((L_1L_2)^\times) \subseteq N(L_1^\times) \cap N(L_2^\times)$. Conversely, if $a \in N(L_1^\times) \cap N(L_2^\times)$, then by local Artin reciprocity, we see that $a \in \ker \phi_{L_1/K} \cap \ker \phi_{L_2/K}$. But this means that $\phi_K(a)\big|_{L_1} = \phi_K(a)\big|_{L_2} = 1$, and thus $\phi_K(a)\big|_{L_1L_2} = 1$. But this implies that $a \in \ker \phi_{L_1L_2/K} = N((L_1L_2)^\times)$.

2. One direction is obvious. Assume that $N(L_1^\times) \subseteq N(L_2^\times)$. Therefore
$$N(L_1^\times) = N(L_1^\times) \cap N(L_2^\times) = N((L_1L_2)^\times).$$
However, we know that
$$[L_1L_2 : K] = [K^\times : N((L_1L_2)^\times)] = [K^\times : N(L_1^\times)] = [L_1 : K],$$
which implies that $L_1 = L_1L_2$, so $L_1 \supseteq L_2$.

3. Assume $H \supseteq N(L^\times)$. Let $M = L^{\phi_{L/K}(H) \subseteq \mathrm{Gal}(L/K)}$. Then by local Artin reciprocity, we have a commutative diagram
$$\begin{array}{ccc} H/N(L^\times) & \xrightarrow{\simeq} & \mathrm{Gal}(L/M) \\ \downarrow & & \downarrow \\ K^\times/N(L^\times) & \xrightarrow[\sim]{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ K^\times/H = K^{\times}/N(M^\times) & \xrightarrow[\sim]{\phi_{M/K}} & \mathrm{Gal}(M/K). \end{array}$$

This tells us that $H = N(M^\times)$ is also a norm subgroup.

4. Note that $L_1 \cap L_2$ is the largest subextension contained in both L_1, L_2. On the other hand, $N((L_1 \cap L_2)^\times)$ is the smallest subgroup containing both $N(L_1^\times), N(L_2^\times)$, and the desired result follows. □

Corollary 2.7.3. *The map* $L \mapsto N(L^\times)$ *defines a bijection*

$$\{L/K \textit{ finite abelian}\} \longleftrightarrow \left\{\textit{norm subgroups of } K^\times\right\}.$$

The idea of local Artin reciprocity was to understand extrinsic data about extensions using intrinsic data about the group $K^\times$. However, the notion of a norm subgroup still still extrinsic, so we want a more intrinsic characterization of norm subgroups.

Lemma 2.7.4. *Let* L/K *be a finite extension. If* $N(L^\times)$ *has finite index in* $K^\times$*, it must be open.*

Proof. Note that $N\colon L^\times \to K^\times$ is continuous and $\mathcal{O}_L^\times$ is compact. Then $N(\mathcal{O}_L^\times) \subseteq K^\times$ ic compact and hence closed. But then $\mathcal{O}_K^\times/N(\mathcal{O}_L^\times) \to K^\times/N(L^\times)$, and thus $N(\mathcal{O}_L^\times) \subseteq \mathcal{O}_K^\times$ is open (and closed). But this implies that $N(\mathcal{O}_L^\times) \subseteq K^\times$ is open (because $\mathcal{O}_K^\times \subseteq K^\times$ is open), and thus $N(L^\times)$ must be open. □

Corollary 2.7.5. *If* L/K *is finite abelian, then* $N(L^\times) \subseteq K^\times$ *is a finite index open subgroup.*

Theorem 2.7.6 (Local CFT II: local existence)**.** *Every finite index open subgroup of* $K^\times$ *is a norm subgroup.*

Corollary 2.7.7. *We have a bijection*

$$\{L/K \textit{ finite abelian}\} \longleftrightarrow \left\{\textit{finite index open subgroups of } K^\times\right\}.$$

Remarks 2.7.8.

1. This bijection also holds for archimedean local fields. For $K = \mathbb{R}$, the two extensions $\mathbb{R}, \mathbb{C}$ correspond to $\mathbb{R}^\times, \mathbb{R}_{>0}$, while $\mathbb{C}$ is algebraically closed and $\mathbb{C}^\times$ is the only finite-index open subgroup of itself.

2. If K is a finite extension of $\mathbb{Q}_p$, then any finite index subgroup of $K^\times$ is automatically open. However, this is not true for $K = \mathbb{F}_q((t))$. In fact, if $H \subseteq K^\times$ has finite index n, then $(K^\times)^n \subseteq H$. Therefore, it suffices to show that $(K^\times)^n$ is open. It is easy to see that $(K^\times)^n \supseteq 1 + \mathfrak{p}_K^m$ for some $m \gg 0$. Therefore the equation $x^n - a = 0$ has solutions in K for $a \in 1 + \mathfrak{p}_K^m$ by Hensel for $p \nmid n$ and a stronger version for $p \mid n$ (that does not always hold).

Now we want a reformulation of local CFT using the norm topology.

Definition 2.7.9. The *norm topology* on $K^\times$ is given by declaring a basis of open neighborhoods of 1 to be the norm subgroups of $K^\times$, which are the same as finite index open subgroups in the usual topology.

Example 2.7.10. Note that $\mathcal{O}_K^\times$ is open under the usual topology, but is not open under the norm topology.

Remark 2.7.11. The norm topology has fewer open sets and is therefore coarses than the usual topology.

Definition 2.7.12. Define $\widehat{K}^\times$ to be the completion of $K^\times$ under the norm topology:

$$\widehat{K}^\times \coloneqq \varprojlim_{L/K \text{ finite abelian}} K^\times/N(L^\times).$$

Then the Artin reciprocity map induces an isomorphism $\widehat{K}^\times \simeq \mathrm{Gal}(K^{ab}/K)$.

Proposition 2.7.13. *We have an isomorphism $\widehat{K}^\times \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$ as topological groups.*

Proof. Choose a uniformizer π of K. Then $K^\times \cong \mathcal{O}_K^\times \times \pi^{\mathbb{Z}}$. Then a basis of finite index open subgroups is given by $(\mathfrak{q} + \mathfrak{p}_K^m) \times \pi^{n\mathbb{Z}}$ for some $m, n \geqslant 1$. This implies that

$$\widehat{K}^\times \cong \varprojlim_m \mathcal{O}_K^\times/(1+\mathfrak{p}_K^m) \times \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}. \qquad \square$$

Corollary 2.7.14. *There is an isomorphism $\mathrm{Gal}(K^{ab}/K) \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$ as topological groups for any choice of uniformizer π. Therefore, we have a decomposition $K^{ab} = K_\pi \cdot K^{ur}$, where $K_\pi = (K^{ab})^{\Phi_K(\pi)}$ and $K^{ur} = (K^{ab})^{\Phi_K(\mathcal{O}_K^\times)}$ is the maximal unramified extension. This means that K_π is the totally ramified part of K^{ab}.*

Remark 2.7.15. More canonically, consider the short exact sequence

$$0 \to \mathcal{O}_K^\times \to K^\times \to \mathbb{Z} \to 0.$$

If we consider the profinite completion of this, we obtain an exact sequence

$$0 \to \mathcal{O}_K^\times \to \widehat{K}^\times \to \widehat{\mathbb{Z}} \to 0.$$

Because $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$ is dense, so is $K^\times \hookrightarrow \widehat{K}^\times$.

Now, it remains to prove local class field theory. First, we will construct the local Artin reciprocity map ϕ_K using Galois cohomology. After we prove that ϕ_K has the desired property, we will prove the local existence theorem by constructing enough norm subgroups using cyclic extensions.

3

Group Cohomology

Definition 3.0.1. Let G be a group. Then a G-*module* is a (left) module over the ring $\mathbb{Z}[G]$, or in other words, an abelian group with a linear (left) G-action.

Example 3.0.2. Let L/K be a finite Galois extension of fields and $G = \mathrm{Gal}(L/K)$. Then $M = L$ and $M = L^\times$ are both G-modules.

Example 3.0.3. Any abelian group M can be regarded as a G-module under the trivial action.

Definition 3.0.4. A *homomorphism of* G-*modules* $\alpha\colon M \to N$ is a G-equivariant group homomorphism, or equivalently a morphism of $\mathbb{Z}[G]$-modules. The set of such morphisms is denoted $\mathrm{Hom}_G(M, N)$.

We will denote the category of G-modules with G-linear maps by Mod_G. Because $\mathsf{Mod}_G = \mathsf{Mod}_{\mathbb{Z}[G]}$, it is an abelian category with enough injectives and projectives. This allows us to develop the full theory of homological algebra in a concrete way.

Definition 3.0.5. $M \in \mathsf{Mod}_G$ is *injective* if the functor $\mathrm{Hom}_G(-, M)$ is exact. Dually, $M \in \mathsf{Mod}_G$ is *projective* if $\mathrm{Hom}_G(M, -)$ is exact.

Definition 3.0.6. An abelian category has *enough injectives* if any object can be embedded in an injective object. Similarly, an abelian category has *enough projectives* if any object has a surjection from a projective object.

Example 3.0.7. The free $\mathbb{Z}[G]$-module $M = \mathbb{Z}[G]$ is projective. In fact, $\mathrm{Hom}_G(\mathbb{Z}[G], M) = M$.

3.1 Definition of Cohomology

Definition 3.1.1. Let $M \in \mathsf{Mod}_G$. Define its G-*invariants* by

$$M^G \coloneqq \{x \in M \mid gx = x \text{ for all } g \in G\} \subseteq M$$

to be the largest submodule with trivial G-action.

Example 3.1.2. Let $G = \mathrm{Gal}(L/K)$. Then if $M = L$, Galois theory tells us that $M^G = K$. Similarly, if $M = L^\times$, then $M^G = K^\times$.

Remark 3.1.3. In other words, we have $M^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, where $\mathbb{Z}$ has the trivial action. This implies that the functor $M \mapsto M^G$ is always left-exact. Therefore, for a short exact sequence

$$0 \to A \to B \to C,$$

we have an exact sequence

$$0 \to A^G \to B^G \to C^G.$$

However, this may fail to be right-exact.

We may resolve this failure of right-exactness by constructing the derived functor of $(-)^G$. This will give us a long exact sequence.

Definition 3.1.4. The *group cohomology* $H^r(G, M)$ for any $r \geqslant 0$ is defined by be the functor $\mathrm{Ext}^r(G, M)$. This is the right derived functor of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. It is characterized by

1. $H^0(G, M) = M^G$.
2. A short exact sequence $0 \to A \to B \to C \to 0$ induces a long exact sequence in group cohomology

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(C, G) \longrightarrow \cdots$$

3. If $I \in \mathsf{Mod}_G$ is injective, then $H^r(G, I) = 0$ for all $r \geqslant 1$.

Remark 3.1.5. More concretely, we can compute $H^r(G, M)$ using an injective resolution of M. If we consider an injective resolution

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

then we apply $(-)^G$ to obtain a complex

$$(I^0)^G \to (I^1)^G \to (I^2)^G \to \cdots$$

and then we have $H^r(G, M) = H^r((I^\bullet)^G)$.

Remark 3.1.6. We can also compute $H^r(G, M)$ using a projective resolution of $\mathbb{Z}$. If we consider a projective resolution

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

then we apply $\mathrm{Hom}_G(-, M)$ to this and obtain a complex

$$\mathrm{Hom}_G(P_0, M) \to \mathrm{Hom}_G(P_1, M) \to \mathrm{Hom}_G(P_2, M) \to \cdots$$

and then $H^\bullet(G, M)$ is just the cohomology of this complex.

Now we will give a description of the cohomology in low degree. In particular, what we will do is use an explicit free resolution of $\mathbb{Z}$.

Definition 3.1.7. Define $P_r = \mathbb{Z}[\underbrace{G \times \cdots G}_{r+1}]$ where G acts on P_r by

$$g \cdot (g_0, \ldots, g_r) = (gg_0, \ldots, gg_r).$$

Note that P_r is a free $\mathbb{Z}[G]$-module with basis $\{(1, g_1, \ldots, g_r)\}$. Now we define the morphism $P_r \to P_{r-1}$ by

$$(g_0, \ldots, g_r) \mapsto \sum_{i=0}^{r} (-1)^i (g_0, \ldots, \widehat{g_i}, \ldots, g_r).$$

Lemma 3.1.8. *The previous definition gives a free resolution of $\mathbb{Z}$ in Mod_G.*

Definition 3.1.9. This is clearly a complex. To prove exactness, let

$$k_r \colon P_r \to P_{r+1} \qquad (g_0, \ldots, g_r) \mapsto (1, g_0, \ldots, g_r).$$

Then we can check that $d_r \circ k_r + k_{r-1} \circ d_{r-1} = \mathrm{id}$. Then taking the image of both sides of $\ker d_{r-1}$, we obtain $d_r \circ k_r(\ker d_{r-1}) = \ker d_{r-1}$ and thus $\ker d_{r-1} \subseteq \operatorname{Im} d_r$.

Corollary 3.1.10. *We can compute* $H^r(G, M) = H^r(\mathrm{Hom}_G(P_\bullet, M))$.

Definition 3.1.11. We have an identification

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

These are called the *homogeneous r-cochains of G with values in M* and are denoted by $\widetilde{C}^r(G, M)$. Then the differentials are given by

$$\widetilde{C}^r(G, M) \xrightarrow{\widetilde{d}^r} \widetilde{C}^{r+1}(G, M) \qquad (\widetilde{d}^r \varphi)(g_0, \ldots, g_{r+1}) = \sum_{i=0}^{r+1} (-1)^i \varphi(g_0, \ldots, \widehat{g_i}, \ldots, r+1).$$

Then we have an explicit cochain description

$$H^r(G, M) = \frac{\ker \widetilde{d}^r}{\operatorname{Im} \widetilde{d}^{r-1}} = \frac{\{\text{homogeneous } r\text{-cocycles}\}}{\{\text{homogeneous } r\text{-coboundaries}\}}.$$

Note that homogeneous r-cocycles $\varphi \colon G^{r+1} \to M$ are determined by their values on elements of the form $(1, g_1, \ldots, g_r)$ for $g_i \in G$, or equivalently on elements of the form $(1, g_1, g_1g_2, \ldots, g_1 \cdots g_r)$. Therefore we may eliminate one degree of freedom.

Definition 3.1.12. Define the group of *inhomogeneous r-cochains* to be the group

$$C^r(G, M) \coloneqq \{\varphi \colon G^r \to M \text{ arbitrary function}\}.$$

Now we have an isomorphism $\widetilde{C}^r(G, M) \simeq C^r(G, M)$ given by

$$\widetilde{\varphi} \mapsto \varphi(g_1, \ldots, g_r) \coloneqq \widetilde{\varphi}(1, g_1, g_1g_2, \ldots, g_1 \cdots g_r).$$

The differentials $C^r(G, M) \xrightarrow{d^{r+1}} C^{r+1}(G, M)$ are given by

$$\begin{aligned}(d^r \varphi)(g_1, \ldots, g_{r+1}) = {} & g_1 \varphi(g_2, g_3, \ldots, g_r) \\ & + \sum_{i=1}^{r} (-1)^i \varphi(g_1, g_2, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_r) \\ & + (-1)^r \varphi(g_1, g_2, \ldots, g_r).\end{aligned}$$

Now we can define the r-*cocycles* $Z^r(G, M)$ and r-*coboundaries* $B^r(G, M)$ and the corresponding cohomology groups $H^r(G, M)$.

Example 3.1.13. Suppose $r = 1$. Then we have

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

Such functions are usually called *crossed homomorphisms*.

On the other hand, we have

$$\begin{aligned} B^1(G, M) &= \left\{ d^0\varphi \mid \varphi \colon \{1\} \to M \right\} \\ &= \left\{ (d^0\varphi)(g) = gm - m \mid m \in M \right\} \\ &= \{\varphi \colon G \to M \mid \varphi(g) = gm - m \text{ for some } m \in M\}. \end{aligned}$$

These functions are called *principal crossed homomorphisms*. Therefore, we have

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

Example 3.1.14. If M acts trivially on G, then $Z^1(G, M) = \mathrm{Hom}_{\mathsf{Grp}}(G, M)$ and $B^1(G, M)$ is trivial. Thus $H^1(G, M) = \mathrm{Hom}_{\mathsf{Grp}}(G, M)$.

Remark 3.1.15. There is an explicit cochain description for $H^r(G, M)$, but computing using this definition is extremely tedious. Instead, we will try to break G and M into smaller pieces and then piece them back together.

3.2 Change of Groups

Definition 3.2.1. Let $H \subseteq G$ be a subgroup and let $M \in \mathsf{Mod}_H$. Define the *induced module*

$$\mathrm{Ind}_H^G M \coloneqq \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M) = \{\varphi \colon G \to M \mid \varphi(hg) = h\varphi(g)\}$$

with the action of G given by

$$(g\varphi)(x) \coloneqq \varphi(xg).$$

Example 3.2.2. For any $M \in \mathsf{Mod}_G$, we have $\mathrm{Ind}_G^G M = M$.

Definition 3.2.3. Let $M \in \mathsf{Mod}_G$. Then define the *restriction* $\mathrm{Res}_H^G M$ to be the same M but viewed as an H-module.

Proposition 3.2.4.

1. *(Frobenius reciprocity) For any $M \in \mathsf{Mod}_G, N \in \mathsf{Mod}_H$, we have*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G N) \cong \mathrm{Hom}_H(\mathrm{Res}_H^G M, N).$$

2. *The functor Ind_H^G is an exact functor.*

3. *The functor Ind_H^G preserves injections.*

Proof.

1. We will construct explicit mutual inverses. We will define

$$\begin{aligned} \mathrm{Hom}_G(M, \mathrm{Ind}_H^G N) &\xleftrightarrow{\sim} \mathrm{Hom}_H(\mathrm{Res}_H^G M, N) \\ \alpha &\mapsto \beta(m) \coloneqq \alpha(m)(1_G) \\ \alpha(m)(g) \coloneqq \beta(gm) &\hookleftarrow \beta \end{aligned}$$

   It is easy to check that these are inverse to each other.

2. Now we need to show that induction is right exact. Suppose $M \twoheadrightarrow N$ is a surjective map of H-modules. Now let $\varphi \in \mathrm{Ind}_H^G N$. Note that φ is uniquely determined by its values on a complete set of representatives $s \in H\backslash G$. Then we lift $\varphi(s) \in N$ to $\widetilde{\varphi(s)} \in M$ using the surjection $M \twoheadrightarrow N$. Now define $\widetilde{\varphi}(hs) = h\widetilde{\varphi}(s)$ for all $h \in H$, and now we obtain an element $\widetilde{\varphi} \in \mathrm{Ind}_H^G M$ mapping to φ.

3. Let $I \in \mathsf{Mod}_H$ be injective. Then $\mathrm{Ind}_H^G I$ is injective if and only if $\mathrm{Hom}_G(-, \mathrm{Ind}_H^G I)$ is exact. By Frobenius reciprocity, this is equivalent to exactness of $\mathrm{Hom}_H(\mathrm{Res}_H^G -, I)$, which is obvious. □

Proposition 3.2.5 (Shapiro's lemma)**.** *Let* $N \in \mathsf{Mod}_H$. *Then* $H^r(G, \mathrm{Ind}_H^G N) \simeq H^r(H, N)$ *for all* $r \geqslant 0$.

Proof. Choose an injective resolution $N \to I^\bullet$ in Mod_H. But then exactness of induction and preservation of injectives imply that $\mathrm{Ind}_H^G \to \mathrm{Ind}_H^G I^\bullet$ is an injective resolution in Mod_G. But now we see that

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

Definition 3.2.6. A module $M \in \mathsf{Mod}_G$ is called *induced* if $M = \mathrm{Ind}_1^G M_0$ for some abelian group M_0.

Corollary 3.2.7. *If* M *is induced, then for all* $r \geqslant 1$, $H^r(G, M) = 0$.

Proof. By Shapiro, this reduces to computing cohomology $H^r(1, M_0)$, but then we know that $\mathrm{Hom}(\mathbb{Z}, -) = (-)$ is exact, so all higher derived functors vanish. □

Now we will consider functorial properties of group cohomology with respect to change of groups. Given $H \subseteq G$ and $M \in \mathsf{Mod}_G$, we will define

1. The *restriction* functor $\mathrm{Res}\colon H^r(G, M) \to H^r(H, M)$.
2. The *corestriction* functor $\mathrm{Cor}\colon H^r(H, M) \to H^r(G, M)$ whenever $[G : H] < \infty$.
3. The *inflation* functor $\mathrm{Inf}\colon H^r(G/H, M^H) \to H^r(G, M)$ when H is a normal subgroup of G.

Suppose we are given $\alpha\colon G' \to G$ and $\mathsf{Mod}_G \ni M \xrightarrow{\beta} M' \in \mathsf{Mod}_{G'}$ that are compatible in the sense that

$$\beta(\alpha(g')m) = g'\beta(m)$$

for all $g' \in G', m \in M$. Then we obtain a morphism of cochain complexes

$$C^r(G, M) \to C^r(G', M') \qquad (\varphi\colon G^r \to M) \to \beta \circ \varphi \circ \alpha^r\colon (G')^r \to G^r \to M \to M'.$$

This is compatible with the differentials, so we obtain a morphism $H^r(G, M) \to H^r(G', M')$. Now using this generality, we can define the three functors.

1. (Restriction) We will set $\alpha\colon H \hookrightarrow G$ and $\beta\colon M \xrightarrow{\mathrm{id}} M$.

2. (Corestriction) We will set $\alpha\colon G \xrightarrow{\mathrm{id}} G$ and

$$\beta\colon \operatorname{Ind}_H^G M \to M \qquad \varphi \mapsto \sum_{g \in G/H} g\varphi(g^{-1}).$$

   This gives us the corestriction map by Shapiro.

3. (Inflation) We take $\alpha\colon G \twoheadrightarrow G/H$ and $\beta\colon M^H \hookrightarrow M$.

Remark 3.2.8. Suppose $r = 0$. Then the functors are

$$\begin{aligned} \text{Res}\colon M^G &\hookrightarrow M^H \\ \text{Cor}\colon M^H &\xrightarrow{N_{G/H}} M^G \\ m &\mapsto \sum_{g \in G/H} gm. \end{aligned}$$

Proposition 3.2.9. *The map* $\text{Cor} \circ \text{Res}\colon H^r(G, M) \to H^r(H, M) \to H^r(G, M)$ *is given by multiplication by* $[G : H]$.

Proof. Consider $M \to \operatorname{Ind}_H^G M \to M$. Then this map is given by

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

Corollary 3.2.10. *If* G *is finite, then* $H^r(G, M)$ *is killed by* $|G|$.

Proof. Take $H = 1$ and apply the previous proposition together with the fact that all higher cohomology vanishes for $H = 1$. $\square$

Corollary 3.2.11. *If* G *is finite and* M *is a finitely generated abelian group, then* $H^r(G, M)$ *is finite.*

Proof. If M is finitely generated, then so is $H^r(G, M)$ because the cochain complex is finitely generated. But then $H^r(G, M)$ is torsion, so it must be finite. $\square$

Theorem 3.2.12 (Inflation-restriction exact sequence)**.** *There is an exact sequence*

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(H, M).$$

Proof. We will check this by hand.

First map is injective: Let $\varphi \in Z^1(G/H, M^H)$. Now assume that

$$\text{Inf}(\varphi)\colon G \twoheadrightarrow G/H \xrightarrow{\varphi} M^H \hookrightarrow M \in Z^1(G, M)$$

is a coboundary. Thus there exists $m \in M$ such that $\text{Inf}(\varphi)(g) = gm - m$ for all $g \in G$. But then $\varphi(\overline{g}) = gm - m$, but then for all $h \in H$, we see that $\varphi(\overline{h}) = hm - m = 0$ because h fixes M^H. Therefore φ is a coboundary.

Composition is zero: Clearly we have $\mathrm{Res} \circ \mathrm{Inf} = 0$ because the composition

$$H \hookrightarrow G \twoheadrightarrow G/H \xrightarrow{\varphi} M^H \hookrightarrow M$$

is trivial because it passes through G/H.

Exactness on right: Assume that $\mathrm{Res}(\varphi) \in B^1(H, M)$. Then there exists $m \in M$ such that $\varphi(h) = hm - m$ for all $h \in H$. Now define

$$\varphi' \in Z^1(G, M) \qquad \varphi'(g) \coloneqq \varphi(g) - (gm - m).$$

Now φ', φ are cohomologous. We will now write φ' as an inflation. Because $\varphi'(h) = \varphi(h) - (hm - m) = 0$, we know that φ' factors through G/H. Moreover, we see that

$$\begin{aligned}\varphi'(hg) &= h\varphi'(g) + \varphi'(h) = h\varphi'(g) \\ &= \varphi'(gh') = g\varphi'(h') + \varphi'(g) = \varphi'(g).\end{aligned}$$

This implies that φ' is valued in M^H, so it must have been an inflation. □

Theorem 3.2.13 (Inflation-restriction, general case)**.** *Let* $r \geqslant 1$. *Assume* $H^i(H, M) = 0$ *for all* $1 \leqslant i < r$. *Then we have an exact sequence*

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

Proof. We will proceed by induction on r using a dimension-shifting argument. Consider the induced G-module $M_* = \mathrm{Ind}_1^G M$. Then look at the exact sequence

$$0 \to M \to M_* \to M' \to 0,$$

where we have the map $m \mapsto (g \mapsto gm)$. But then the higher cohomology of M_* vanishes, so we have isomorphisms $H^i(G, M') \simeq H^{i+1}(G, M)$ for all $i \geqslant 1$. But then $M_* = \mathrm{Ind}_H^G \mathrm{Ind}_1^H M$, so we have isomorphisms $H^i(H, M') \simeq H^{i+1}(H, M)$ for all $i \geqslant 1$. Similarly, because $H^1(H, M) = 0$, we have an exact sequence

$$0 \to M^H \to H_*^H \to (M')^H \to 0,$$

and therefore M_*^H is also an induced G/H-module. Therefore $H^i(G/H, (M')^H) \simeq H^{i+1}(G/H, M^H)$ for all $i \geqslant 1$.

Now, by assumption, we have $H^i(H, M) = 0$ for all $1 \leqslant i \leqslant r-1$. Therefore, $H^i(H, M') = 0$ for all $1 \leqslant i \leqslant r-2$ and now we can apply the inductive hypothesis to obtain an exact sequence

$$0 \to H^{r-1}(G/H, (M')^H) \xrightarrow{\mathrm{Inf}} H^{r-1}(G, M') \xrightarrow{\mathrm{Res}} H^{r-1}(H, M').$$

This implies that

$$0 \to H^r(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^r(G, M') \xrightarrow{\mathrm{Res}} H^r(H, M)$$

is also exact. □

Remark 3.2.14. We have a more general version of the dimension shift. Given an exact sequence

$$0 \to M \to A^1 \to \cdots \to A^k \to N \to 0,$$

where each A^i is induced, then $H^r(G, M) \simeq H^{r+1}(G, N)$ for all $r \geqslant 1$.

Remark 3.2.15. The inflation-restriction exact sequence is a special case of the *Hochschild-Serre spectral sequence.* We have

$$E_2^{p,q} = H^p(G/H, H^q(H, M)) \Rightarrow H^{p+q}(G, M).$$

In our case, only the rows $q = 0, q = r$ are nontrivial.

3.3 Group Homology

Definition 3.3.1. Define the G-*coinvariants* of M by

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

This is the largest quotient module of M where G acts trivially.

Definition 3.3.2. The *augmentation ideal* is defined to be

$$I_G \coloneqq \ker(\mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}) = \mathbb{Z}[g-1 \mid g \neq 1].$$

Then we see that $M_G = M/I_G M = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]/I_G = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. In particular, the coinvariants functor is right-exact. Applying the derived functor package, we obtain

Definition 3.3.3. Define the *group homology* by

$$H_r(G, M) \coloneqq \mathrm{Tor}_r^{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

to be the left derived functor $\mathrm{Tor}_r^{\mathbb{Z}[G]}(\mathbb{Z}, M)$ of $M \mapsto M_G$.

Remarks 3.3.4. Group homology is characterized by

1. $H_0(G, M) = M_G$;
2. A short exact sequence $0 \to A \to B \to C \to 0$ in Mod_G gives a long exact sequence

$$\cdots \longrightarrow H_r(G, A) \longrightarrow H_r(G, B) \longrightarrow H_r(G, C)$$
$$H^{r-1}(G, A) \longrightarrow H^{r-1}(G, B) \longrightarrow H^{r-1}(C, G) \longrightarrow \cdots$$

3. If $P \in \mathsf{Mod}_G$ is projective, then $H_r(G, P) = 0$ for all $r \geqslant 1$.

Remark 3.3.5. Let $P_\bullet \to M$ be a projective resolution. Then $H_r(G, M) = H^r((P_\bullet)_G)$.

Proposition 3.3.6. *For any* G, *we have* $H_1(G, \mathbb{Z}) \simeq G^{ab} = G/[G, G]$.

Proof. Consider the short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \to \mathbb{Z} \to 0.$$

This gives a long exact sequence

$$H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0.$$

This becomes

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z} \xrightarrow{\sim} \mathbb{Z} \to 0.$$

But this tells us that $H_1(G, \mathbb{Z}) \simeq I_G/I_G^2$. Now define the map

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

By the identity

$$g_1 g_2 - 1 = (g_1 - 1) + (g_2 - 1) + (g_1 - 1)(g_2 - 1),$$

we see that this is a group homomorphism. Because I_G/I_G^2 is abelian, the group homomorphism factors through $G^{ab} \to I_G/I_G^2$. One can easily check that have an inverse $I_G/I_G^2 \to G^{ab}$ given by $g - 1 \mapsto g$. □

Remark 3.3.7. This gives a homological interpretation of $\mathrm{Gal}(L/K)^{ab}$ as $H_1(\mathrm{Gal}(L/K), \mathbb{Z})$.

Remark 3.3.8. This is analogous to the topological fact that if X is path-connected, then $H_1(X, \mathbb{Z}) = \pi_1(X)^{ab}$. In fact, for any group G, we can define a space $BG = K(G, 1)$ such that $\pi_1(BG) = G$ and $\pi_i(BG) = 0$ for $i \neq 1$. We have $H_r(BG, \mathbb{Z}) = H_r(G, \mathbb{Z})$, where the LHS is singular homology and the RHS is group homology. If we choose $r = 1$, we recover $H_1(G, \mathbb{Z}) = G^{ab}$.

Example 3.3.9.

1. If $G = \mathbb{Z}$, then we have $B\mathbb{Z} = \mathbb{R}/\mathbb{Z} = S^1$.
2. If $G = \underbrace{\mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}}_{n}$, then $BG = \underbrace{S^1 \vee \cdots \vee S^1}_{n}$.

3.4 Tate Cohomology

The idea is that for a finite group G, we will patch both group cohomology and group homology into a single theory.

Definition 3.4.1. Let G be a finite group and $M \in \mathrm{Mod}_G$. Define the *norm map*

$$\mathrm{Nm}_G : M \to M \qquad m \mapsto \sum_{g \in G} gm.$$

By definition, the image of the norm map lies in the invariants and $\mathrm{Nm}_G(gm - m) = 0$, so the kernel always contains $I_G M$. This gives us a commutative diagram

$$\begin{array}{ccc} M & \xrightarrow{\mathrm{Nm}_G} & M \\ \downarrow & & \uparrow \\ M_G & \xrightarrow{\mathrm{Nm}_G} & M^G \end{array}$$

and an exact sequence

$$0 \to \frac{\ker \mathrm{Nm}_G}{I_G} \to M_G \xrightarrow{\mathrm{Nm}_G} M^G \to \frac{M^G}{\mathrm{Im}\,\mathrm{Nm}_G} \to 0.$$

In particular, this gives us

$$0 \to \widehat{H}^{-1}(G, M) \to H_0(G, M) \to H^0(G, M) \to \widehat{H}^0(G, M) \to 0,$$

where $\widehat{H}$ just means a modified version of cohomology.

Definition 3.4.2. For $r \in \mathbb{Z}$, define the *Tate cohomology groups*

$$\widehat{H}^r(G, M) \coloneqq \begin{cases} H^r(G, M) & r \geqslant 1 \\ \frac{M^G}{\mathrm{Im}\,\mathrm{Nm}_G} & r = 0 \\ \frac{\ker \mathrm{Nm}_G}{I_G M} & r = -1 \\ H_{-(r+1)}(G, M) & r \leqslant -2. \end{cases}$$

Example 3.4.3. Given a short exact sequence

$$0 \to A \to B \to C \to 0$$

in Mod_G, we obtain a long exact sequence

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

and by the snake lemma, these can be patched to form a very long exact sequence

$$\cdots \to \widehat{H}^{-1}(G,C) \to \widehat{H}^{-1}(G,A) \to \widehat{H}^{-1}(G,B) \to \widehat{H}^{-1}(G,C) \to \widehat{H}^{0}(G,A) \to \cdots$$

Remark 3.4.4.

1. If $M \in \mathrm{Mod}_G$ is induced, then $\widehat{H}^r(G,M) = 0$ for all $r \in \mathbb{Z}$.
2. The dimension shift argument works for $\widehat{H}^r$ in both directions. If $M \hookrightarrow \mathrm{Ind}_1^G M$, then $\widehat{H}^r(M^1) = \widehat{H}^{r+1}(M)$, where M^1 is the cokernel. Similarly, if $\mathrm{Ind}_1^G M \twoheadrightarrow M$, then $\widehat{H}^r(M) = \widehat{H}^{r+1}(M^1)$, where M^1 is the kernel.
3. Shapiro's lemma still holds for $\widehat{H}^r$.
4. The property that $\mathrm{Cor}_H^G \circ \mathrm{Res}_H^G$ is multiplication by $[G:H]$ holds for $\widehat{H}^r$.

Remark 3.4.5. Take $P_\bullet \to \mathbb{Z}$ to be a free resolution in Mod_G. Taking the dual $M \mapsto M^* = \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ where $(g\varphi)(m) = \varphi(g^{-1}m)$. This gives a resolution $\mathbb{Z} \to P^\bullet$. If we take $P_{-n} \coloneqq P_{n-1}^*$, we obtain

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

Then we can compute $\widehat{H}^r(G,M) = H^r(\mathrm{Hom}_G((P_\bullet),M))$.

Now we will compute Tate cohomology explicitly for finite cyclic groups $G = \langle\sigma\rangle$. We can very explicitly write down the norm map, invariants, and coinvariants:

$$\begin{aligned}
\mathrm{Nm}_G(m) &= \sum_{g\in G} gm = (1+\sigma+\sigma^2+\cdots+\sigma^{n-1})m \\
M^G &= M^{\sigma=1} = \ker(\sigma-1) \\
I_G M &= \mathrm{Im}(\sigma-1) \\
M_G &= \mathrm{coker}(\sigma-1).
\end{aligned}$$

This implies that

$$\begin{aligned}
\widehat{H}^0(G,M) &= \frac{M^G}{\mathrm{Im}(\mathrm{Nm}_G)} = \frac{\ker(\sigma-1)}{\mathrm{Im}(1+\sigma+\cdots+\sigma^{n-1})} \\
\widehat{H}^{-1}(G,M) &= \frac{\ker(\mathrm{Nm}_G)}{I_G M} = \frac{\ker(1+\sigma+\cdots+\sigma^{n-1})}{\mathrm{Im}(\sigma-1)}.
\end{aligned}$$

Remark 3.4.6. All remaining $\widehat{H}^r(G,M)$ are determined by $\widehat{H}^0, \widehat{H}^{-1}$.

Theorem 3.4.7 (Period 2). *Let* $G = \langle \sigma \rangle$. *Then we have isomorphisms* $\widehat{H}^r(G, M) \simeq \widehat{H}^{r+2}(G, M)$.

Proof. Note that we have a free resolution of $\mathbb{Z}$ in Mod_G given by

$$\cdots \to \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{1+\sigma+\cdots+\sigma^{n-1}} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}.$$

This computes the Tate cohomology and has period 2, so the Tate cohomology also must have period 2. □

Definition 3.4.8. Define the *Herbrand quotient*

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

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

Proposition 3.4.9. *If* $0 \to A \to B \to C \to 0$ *is an exact sequence, then* $h(B) = h(A) \cdot h(C)$.

Proof. Consider the long exact sequence

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

This implies that

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

From this, we obtain

$$\frac{h(B)}{h(A)h(C)} = \frac{|Q|}{|K|},$$

so it suffices to show that $|Q| = |K|$. But here, we see that

$$Q = \operatorname{coker}(\widehat{H}^1(B) \to \widehat{H}^1(C)) = \operatorname{coker}(\widehat{H}^{-1}(B) \to \widehat{H}^{-1}(C)) = K$$

because Tate cohomology has period 2. □

Proposition 3.4.10. *If* M *is finite, then* $h(M) = 1$.

Proof. Note that we have the exact sequence

$$0 \to M^G \to M \xrightarrow{\sigma-1} M \to M_G \to 0.$$

This tells us that $\left|M^G\right| = |M_G|$. Next, we note that

$$0 \to \widehat{H}^{-1}(G, M) \to M_G \xrightarrow{\mathrm{Nm}_G} M^G \to \widehat{H}^0(G, M) \to 0$$

is exact, so $\left|\widehat{H}^{-1}(G, M)\right| = \left|\widehat{H}^0(G, M)\right|$. □

Corollary 3.4.11. *If* $\alpha \colon M \to N$ *has finite kernel and cokernel, then* $h(M) = h(N)$.

Proof. Consider the exact sequence

$$0 \to \ker \alpha \to M \to N \to \operatorname{coker} \alpha \to 0.$$

This tells us that

$$h(\ker \alpha) \cdot h(M)^{-1} \cdot h(N) \cdot h(\operatorname{coker} \alpha)^{-1} = 1.$$

Because α has finite kernel and cokernel, $h(\ker \alpha) = h(\operatorname{coker} \alpha) = 1$, so $h(M) = h(N)$. □

Now we want to compute Tate cohomology for more general G.

Theorem 3.4.12. *Let G be a finite group. If for any subgroup $H \subseteq G$ we have $H^1(H, M) = H^2(H, M) = 0$, then $\widehat{H}^r(G, M) = 0$ for all $r \in \mathbb{Z}$.*

Proof. If G is cyclic, then it follows from the period 2 isomorphism. In the general case, if G is solvable, we can induct on $|G|$. If $H \triangleleft G$ is normal such that G/H is cyclic. By the induction hypothesis, we know $\widehat{H}^r(H, M) = 0$ for all $r \in \mathbb{Z}$. Applying inflation-restriction, we have an exact sequence

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

By assumption, $H^r(G, M) = 0$ for $r = 1, 2$. By exactness, we know $H^r(G/H, M^H) = 0$ for $r = 1, 2$, so $\widehat{H}^r(G/H, M^H) = 0$ for all $r \in \mathbb{Z}$ because G/H is cyclic. By exactness and the inductive hypothesis, we know $\widehat{H}^r(G, M) = 0$ for all $r \geqslant 1$. But now the hypotheses are invariant under dimension shift, so we obtain the desired result.

Finally, if G is an arbitrary finite group, reduce to the solvable case. If we consider the Sylow subgroups $G_p \subseteq G$, we know G_p is solvable. Therefore $\widehat{H}^r(G_p, M) = 0$ for all $r \in \mathbb{Z}$. By an exercise from the homework, we see $\widehat{H}^r(G, M) = 0$ for all $r \in \mathbb{Z}$. □

Unfortunately, H^2 generally does not vanish, but we can still gain insight about the behavior of Tate cohomology in this case.

Theorem 3.4.13 (Tate)**.** *Let G be a finite group. If for any subgroup $H \subseteq G$ we have*

1. $H^1(H, M) = 0$;
2. $H^2(H, M) = \mathbb{Z}/|H|\mathbb{Z}$,

then $\widehat{H}^r(G, \mathbb{Z}) \simeq \widehat{H}^{r+2}(G, M)$ for all $r \in \mathbb{Z}$.

Example 3.4.14. We will apply Tate's theorem to construct the local Artin map. Let $G = \operatorname{Gal}(L/K)$ and $M = L^\times$ and set $r = -2$. Then both conditions of the theorem are satisfied, and so

$$\operatorname{Gal}(L/K)^{ab} = H_1(G, \mathbb{Z}) = \widehat{H}^{-1}(G, \mathbb{Z}) \simeq \widehat{H}^0(G, M) = M^G / \operatorname{Im}(Nm_G) = K^\times / N_{L/K}(L^\times).$$

Now we have defined the inverse of the local Artin map!

Remark 3.4.15. Chao says that Tate was very brave to go from the object $\widehat{H}^0(G, M)$ that we want to understand to an object that did not exist at the time!

Before we prove Tate's theorem, we will give an explicit description of $H^2(G, M)$. Recall that

$$Z^2(G, M) = \left\{ \varphi \colon G^2 \to M \mid g_1 \varphi(g_2, g_3) - \varphi(g_1 g_2, g_3) + \varphi(g_1, g_2 g_3) - \varphi(g_1, g_2) = 0 \right\}.$$

We also know that

$$B^2(G, M) = \left\{ \varphi \colon G^2 \to M \mid \varphi(g_1, g_2) = g_1 \psi(g_2) - \psi(g_1 g_2) + \psi(g_1), \psi \colon G \to M \right\}.$$

Proposition 3.4.16. *The cohomology group* $H^2(G,M) = \frac{Z^2(G,M)}{B^2(G,M)}$ *parameterizes extensions*

$$0 \to M \to E \to G \to 0$$

such that the conjugation action of $E/M \cong G$ *on* M *agrees with the* G*-module structure. Moreover,* $0 \in H^2(G,M)$ *corresponds to the split extension.*

Proof. Given such an extension, choose a splitting of $E = G \times M$ as **sets**. This gives us a section $s\colon E \to G$ Then for all $g_1, g_2 \in G$, we have $s(g_1)\cdot s(g_2) = \varphi(g_1,g_2)s(g_1g_2)$ for some $\varphi\colon G^2 \to M$.

We check that φ is actually a cocycle. To see this, note that

$$(s(g_1)s(g_2))s(g_3) = s(g_1)(s(g_2)s(g_3))$$

by associativity, which gives us

$$(\varphi(g_1,g_2) + \varphi(g_1g_2,g_3))s(g_1g_2g_3) = (g_1\varphi(g_2,g_3) + \varphi(g_1,g_2g_3))s(g_1g_2g_3),$$

and therefore φ is a cocycle. We can check that any φ gives such an extension together with a section s and that different choices of the section s give coboundary relations. □

Definition 3.4.17. For any $\varphi \in Z^2(G,M)$, define its *splitting module* to be

$$M(\varphi) \coloneqq M \oplus \left(\bigoplus_{g\neq 1} \mathbb{Z}X_g\right)$$

with the action of G given by

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

for any choice of $g_1, g_2 \in G$. By convention, we write $X_1 \coloneqq \varphi(1,1) \in M$.

Remark 3.4.18. By construction, we have an exact sequence

$$0 \to M \to M(\varphi) \to I_G \to 0,$$

where $X_g \mapsto g - 1$.

Lemma 3.4.19. *The image of* φ *under* $H^2(G,M) \to H^2(G,M(\varphi))$ *is* 0.

Proof. Note that $\varphi(g_1,g_2) = g_1X_{g_2} - X_{g_1g_2} + X_{g_1}$ is the coboundary of $g \mapsto X_g$. □

Remark 3.4.20. The extension E' associated to φ

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & M(\varphi) & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

of $M(\varphi)$ is a split extension.

Proof of Tate's theorem. There are two steps to the proof.

1. We know that $H^2(G, M) = \mathbb{Z}/|G|\mathbb{Z} = \langle \varphi \rangle$ with splitting module $M(\varphi)$. We also know that $H^1(H, M) = 0$. We will show that $H^1(H, M(\varphi)) = 0$ and $H^2(H, M(\varphi)) = 0$. Consider the short exact sequence
$$0 \to M \to M(\varphi) \to I_G \to 0.$$
This gives a long exact sequence
$$H^1(H, M) \to H^1(H, M(\varphi)) \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M(\varphi)) \to H^2(H, I_G).$$
However, we know that $H^1(H_1, M) = 0, H^1(H, I_G) = \mathbb{Z}/|H|\mathbb{Z}$, and $H^2(H, I_G) = 0$. We also know that $H^2(H, M) \to H^2(H, M(\varphi))$ is the zero map (the restriction of φ to $H^2(H, M)$ is a generator), so the map $H^1(H, I_G) \to H^2(H, M)$ must be an isomorphism and therefore $H^1(H, M(\varphi)) = H^2(H, M(\varphi)) = 0$.

2. Now we know that all Tate cohomology $\widehat{H}^r(G, M(\varphi)) = 0$ for all $r \in \mathbb{Z}$. Now we use the four term exact sequence
$$0 \to M \to M(\varphi) \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$
Because $\widehat{H}^r(G, M(\varphi)) = 0$ and $\widehat{H}^r(G, \mathbb{Z}[G]) = 0$ for all $r \in \mathbb{Z}$, By dimension shift, we have $\widehat{H}^r(G, \mathbb{Z}) \cong \widehat{H}^{r+2}(G, M)$. □

Remark 3.4.21. There is an alternative description of $\widehat{H}^r(G, \mathbb{Z}) \simeq \widehat{H}^{r+2}(G, M)$ as a cup product with some generator $\varphi \in H^2(G, M)$. Here, if $M, N \in \mathsf{Mod}_G$, we can consider the tensor product $M \otimes N$ as a G-module with the action $g(m \otimes n) = gm \otimes gn$.

Now a *cup product* is a family of $\mathbb{Z}$-bilinear maps
$$H^r(G, M) \otimes H^s(G, N) \to H^{r+s}(G, M \otimes N)$$
given by the following properties:

1. The cup product is functorial in both M, N.
2. For $r = s = 0$, it is given by the natural map $M^G \otimes N^G \to (M \otimes N)^G$.
3. If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence such that
$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$
is also exact, then for all $m'' \in H^r(G, M'')$ and $n \in H^s(G, N)$, we have $\delta m'' \cup n = \delta(m'' \cup n) \in H^{r+s+1}(G, M' \otimes N)$.
4. If $0 \to N' \to N \to N'' \to 0$ is a short exact sequence such that
$$0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$
is also exact, then for all $m \in H^r(G, M), n'' \in H^s(G, N'')$, we have $m \cup \delta n'' = (-1)^r \delta(m \cup n'')$.

The cup product exists and is unique. Given cocycles φ, ψ, we write
$$(\varphi \cup \psi)(g_1, \dots, g_{r+s}) = \varphi(g_1, \dots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \dots, g_{r+s})$$
and this is unique by dimension shift. If G is finite, then the cup product extends to Tate cohomology.

4

Local Class Field Theory

Now our goal is to understand $H^i(\mathrm{Gal}(L/K), L^\times)$ for $i = 1, 2$. This will allow us to construct the local Artin reciprocity map.

4.1 Vanishing of first cohomology

This result was proved by Hilbert in 1894 Zahlbericht for cyclic extensions and then by Noether for general extensions.

Theorem 4.1.1 (Hilbert Theorem 90)**.** *Let* L/K *be a finite Galois extension of fields. Then*

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

Remark 4.1.2. Note that this applies to extensions of arbitrary fields, not just local fields.

Proof. Choose $\varphi \in Z^1(\mathrm{Gal}(L/K), L^\times)$. We want $\varphi(g) = \frac{gm}{m}$ for some $m \in L^\times$. For any $a \in L^\times$, construct

$$m \coloneqq \sum_{g \in \mathrm{Gal}(L/K)} \varphi(g) \cdot ga.$$

Because $g \colon L^\times \to L^\times$ are distinct characters of $L^\times$ for $g \in G \coloneqq \mathrm{Gal}(L/K)$, we know that they are L-linearly independent, so the map

$$\sum_{g \in G} \varphi(g) \cdot g$$

is not the zero map and thus there exists $a \in L^\times$ such that $m \neq 0$. But now we compute

$$\begin{aligned} gm &= g \sum_{h \in G} \varphi(h) \cdot ha \\ &= \sum_{h \in G} g\varphi(h) \cdot gha \\ &= \sum_{h \in G} \frac{\varphi(gh)}{\varphi(g)} \cdot gha \\ &= \frac{1}{\varphi(g)} \sum_{h \in G} \varphi(gh) \cdot gha \\ &= \frac{1}{\varphi(g)} \sum_{h \in G} \varphi(h) \cdot ha \\ &= \frac{m}{\varphi(g)}, \end{aligned}$$

and thus $\varphi(g) = \frac{n}{gm} = \frac{gm^{-1}}{m^{-1}}$, so $\varphi \in B^1(G, L^\times)$. □

Example 4.1.3. In the case where L/K is a cyclic extension and $G = \langle \sigma \rangle$, then $\widehat{H}^{-1}(G, L^\times) = H^1(G, L^\times) = 0$, and thus $\ker \mathrm{Nm}_G = \mathrm{Im}(\sigma - 1)$, which means that if $a \in L^\times$ satisfies $\mathrm{Nm}_{L/K}(a) = 1$, then $a = \frac{\sigma b}{b}$ for some $b \in L^\times$.

Example 4.1.4. Let $L/K = \mathbb{Q}(i)/\mathbb{Q}$ be the simplest quadratic extension. Let $a = x + iy \in L^\times$ with $x, y = \mathbb{Q}$. Then we know $\mathrm{Nm}_{L/K}(a) = x^2 + y^2$. If $b = m + in \in L^\times$ for $m, n \in \mathbb{Q}$, we see that

$$\frac{\sigma b}{b} = \frac{m - in}{m + in} = \frac{m^2 - n^2}{m^2 + n^2} + \frac{2mn}{m^2 + n^2} \cdot i.$$

By Hilbert 90, if $x^2 + y^2 = 1$, then there exist $m, n \in \mathbb{Z}$ such that

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

In particular, this tells us how to classify all Pythagorean triples.

Remark 4.1.5. We may also consider infinite Galois extensions L/K, for example $L = K^{\mathrm{sep}}, K^{\mathrm{ab}}$. Then we know

$$\mathrm{Gal}(L/K) = \varprojlim_{\substack{L' \subseteq L \\ L'/K \text{ finite Galois}}} \mathrm{Gal}(L'/K).$$

This allows us to define *continuous Galois cohomology*

$$H^r_{\mathrm{cts}}(\mathrm{Gal}(L/K), L^\times) \coloneqq \varinjlim_{L'} H^r(\mathrm{Gal}(L'/K), (L')^\times).$$

The H^r_{cts} can be computed using continuous cochains.

Remark 4.1.6. More generally, if $G = \varprojlim_H G/H$ is a profinite group and M is a **discrete** G-module (which means $G \times M \to M$ is continuous with respect to the profinite topology on G and the discrete topology on M), we may consider the continuous group cohomology

$$H^r_{\mathrm{cts}}(G, M) \coloneqq \varinjlim_H H^r(G/H, M^H),$$

where the maps in the directed system are inflation.

Notation 4.1.7. Let $G = \mathrm{Gal}(L/K)$. We will simply write

$$H^r(L/K, M) \coloneqq H^r_{\mathrm{cts}}(\mathrm{Gal}(L/K), M) \qquad H^r(K, M) \coloneqq H^r_{\mathrm{cts}}(\mathrm{Gal}(K^{\mathrm{sep}}/L), M)$$

for the continuous Galois cohomology.

Example 4.1.8. Hilbert Theorem 90 implies that $H^1(K, (K^{\mathrm{sep}})^\times) = 0$. Equivalently, we have $H^1_{\text{ét}}(\mathrm{Spec}\, K, \mathbb{G}_m) \cong \mathrm{Pic}\, \mathrm{Spec}\, K = 0$. In other words, all line bundles on a point are trivial.

4.2 Second Cohomology

Let L/K be a finite unramified extension of local fields. Recall that

$$G = \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\ell/k) = \left\langle \mathrm{Frob}_{L/K} \right\rangle,$$

where ℓ/k is the extension of residue fields. Our goal is to compute $H^2(L/K, L^\times) \cong \mathbb{Z}/n\mathbb{Z}$, where $n = [L : K]$. The idea is to break $L^\times$ into pieces, so choose a uniformizer π_L. Then we have $L^\times \cong \mathcal{O}_L^\times \times \pi_L^{\mathbb{Z}}$. Because L/K is unramified, we may choose $\pi_L = \pi_K \in K^\times$. Therefore, as a Galois module, we have $L^\times \cong \mathcal{O}_L^\times \oplus \mathbb{Z}$.

Definition 4.2.1. Let $U_K = \mathcal{O}_K^\times$. Then write $U_K^{(i)} \coloneqq 1 + \mathfrak{m}_K^i$ for all $i \geqslant 1$.

This gives us a natural filtration

$$U_K \supseteq U_K^{(i)} \supseteq U_K^{(2)} \supseteq U_K^{(3)} \supseteq \cdots$$

with short exact sequences

$$1 \to U_K^{(1)} \to U_K \to k^\times \to 1$$

and similarly

$$1 \to U_K^{(i+1)} \to U_K^{(i)} \to k \to 1$$

for $i \geqslant 1$.

Lemma 4.2.2. *We have* $\widehat{H}^r(G, \ell^\times) = \widehat{H}^r(G, \ell) = 0$ *for all* $r \in \mathbb{Z}$.

Proof. By Hilbert Theorem 90, we know $H^1(G, \ell^\times) = 0$. Because G is cyclic and $\ell^\times$ is finite, we can understand the Herbrand quotient. Therefore $h(\ell^\times) = 1$, so $H^2(G, \ell^\times) = 0$. Because G is cyclic, we may apply period 2 to obtain the desired result.

Now we consider ℓ. We know that ℓ is actually an induced module by the homework, so all Tate cohomology vanishes by period 2. □

Corollary 4.2.3. *The norm map* $\mathrm{Nm}_{\ell/k} \colon \ell^\times \to k^\times$ *and the trace map* $\mathrm{Tr}_{\ell/k} \colon \ell \to k$ *are surjective.*

Proof. We know that $\widehat{H}^0(G, \ell^\times) = \frac{k^\times}{\mathrm{Nm}_{\ell/k}(\ell^\times)} = 0$, so the norm map is surjective. Similarly, we know $\widehat{H}^0(G, \ell) = \frac{k}{\mathrm{Tr}_{\ell/k}(\ell)} = 0$, so the trace is surjective. □

Lemma 4.2.4. *The norm map* $\mathrm{Nm}_{L/K} \colon U_L \to U_K$ *is surjective.*

Proof. Consider the commutative diagram

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

Given any $a \in U_K$, we want $b \in U_L$ such that $\mathrm{Nm}(b) = a$. Because $\mathrm{Nm}\colon \ell^\times \to k^\times$, we may find $b_0 \in U_L$ such that $\mathrm{Nm}(b_0) \equiv a \pmod{\pi_K}$. Now let $a_1 \coloneqq \frac{a}{\mathrm{Nm}(b_0)} \in U_K^{(1)}$. Because $\mathrm{Tr}\colon \ell \to k$ is surjective, we may find $b_1 \in U_L^{(1)}$ such that $a_2 \coloneqq \frac{a_1}{\mathrm{Nm}(b_1)} \in U_K^{(2)}$. Repeating this to infinity, we can find $b_i \in U_L^{(i)}$ such that $a_{i+1} \coloneqq \frac{a_i}{\mathrm{Nm}(b_i)} \in U_K^{(i+1)}$. Setting

$$b \coloneqq \prod_{i=1}^{\infty} b_i,$$

we know

$$\frac{a}{\mathrm{Nm}(b)} \in \bigcap_{i=0}^{\infty} U_K^{(i)} = \{1\},$$

so $a = \mathrm{Nm}(b)$. □

Corollary 4.2.5. *For all $r \in \mathbb{Z}$, we have $\widehat{H}^r(G, U_L) = 0$.*

Proof. By the Lemma, we know that $\mathrm{Nm}\colon U_L \to U_K$ is surjective, so $\widehat{H}^0(G, U_L) = 0$. But then we know $H^1(G, U_L) \subseteq H^1(G, L^\times) = 0$ is a direct factor, so $H^1(G, U_L) = 0$. The desired result is simply an application of period 2. □

Theorem 4.2.6. *If L/K is an unramified extension, then $H^2(G, L^\times) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.*

Proof. We know $H^2(G, L^\times) \cong H^2(G, U_L) \oplus H^2(G, \mathbb{Z}) = H^2(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ by the homework. The final isomorphism is obvious. □

Definition 4.2.7. Define the *invariant map*

$$\mathrm{inv}_{L/K}\colon H^2(L/K, L^\times) \simeq H^2(L/K, \mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}.$$

Taking the limit over all unramified extensions, we obtain a map

$$H^2(K^{\mathrm{ur}}/K, (K^{\mathrm{ur}})^\times) \xrightarrow{\sim} \bigcup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z} = \mathbb{Q}/\mathbb{Z}.$$

To simplify our notation, we will write $H^2(L/K) \coloneqq H^2(L/K, L^\times)$, so we have

$$\mathrm{inv}_K\colon H^2(K^{\mathrm{ur}}/K) \simeq \mathbb{Q}/\mathbb{Z}.$$

Our goal now will be to extend this to $H^2(K^{\mathrm{sep}}/K) \simeq \mathbb{Q}/\mathbb{Z}$.

Remark 4.2.8. We always have an injective inflation map $H^2(K^{\mathrm{ur}}/K) \xrightarrow{\mathrm{Inf}} H^2(K^{\mathrm{sep}}/K)$. The map exists, and injectivity is by Hilbert 90 and inflation-restriction. We want to prove that this is indeed an isomorphism.

Lemma 4.2.9. *Let* L/K *be a finite extension of degree* n*. Then the diagram*

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

commutes.

Remark 4.2.10. Because $L^{ur} = L \cdot K^{ur}$, we may view $\text{Gal}(L^{ur}/L)$ as a subgroup of $\text{Gal}(K^{ur}/K)$, and the inclusion is comparible with $(K^{ur})^\times \to (L^{ur})^\times$, so restriction makes sense.

Proof. Recall that inv_K is computed by $H^2(K^{ur}/K) \simeq H^2(K^{ur}/K, \mathbb{Z}) \simeq H^1(K^{ur}/K, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$. Now we need to see the effect of restriction on the groups on the right of the chain of isomorphisms. Note that if $e = e(L/K)$ and $f = f(L/K)$, then $\pi_L^e = \pi_K$, so the diagram

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

commutes. Therefore, the maps on $H^2(K^{ur}/K, \mathbb{Z}) \to H^2(L^{ur}/L, \mathbb{Z})$ are given by multiplication by e. Finally, for $\varphi \in H^1(K^{ur}/K, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(\text{Gal}(K^{ur}/K), \mathbb{Q}/\mathbb{Z})$, we see that $\varphi \mapsto \varphi(\text{Frob}_K)$. Because $\text{Frob}_L = \text{Frob}_K^f$, we see that $\text{Res}(\varphi)(\text{Frob}_L) = f\varphi(\text{Frob}_K)$. Therefore, the final map is simply $f \cdot e \cdot \text{Res} = n \cdot \text{Res}$. □

Corollary 4.2.11. *Let* L/K *be a finite Galois extension of degree* n*. Then* $H^2(L/K)$ *contains a subgroup of* $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$*.*

Proof. By Hilbert 90 and inflation-restriction, we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\text{Inf}} & H^2(K^{sep}/K) & \xrightarrow{\text{Res}} & H^2(L^{sep}/L) \\ & & & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(K^{ur}/K) & \xrightarrow{\text{Res}} & H^2(L^{ur}/L) \\ & & & & \cong\uparrow & & \cong\uparrow \\ & & & & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\times n} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Therefore, $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ injects into $H^2(L/K)$. □

Proposition 4.2.12. *We have* $\left|H^2(L/K)\right| = n$*. In particular,* $H^2(L/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$*.*

Proof. We know this is true with L/K is cyclic. We know $h(L^\times) = n$ and $H^1(L/K) = 0$, so $\left|H^2(L/K)\right| = n$. In general, we will reduce to the cyclic case because L/K is always solvable (because K is a local field). We will induct on $[L : K]$. Choose a tower of fields $K \subset K' \subset L$ such that K'/K is cyclic. Applying inflation-restriction, we have an exact sequence

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

We know that $\left|H^2(K'/K)\right| = [K' : K]$ because it is cyclic. We also know that $\left|H^2(L/K')\right| = [L : K']$ by the inductive hypothesis, so $\left|H^2(L/K)\right| \leqslant [K' : K] \cdot [L : K'] = [L : K] = n$. But we know that $H^2(L/K)$ contains a subgroup of order n, so $\left|H^2(L/K)\right| = n$. □

Corollary 4.2.13. *We have a commutative diagram*

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \xrightarrow{\text{Inf}} & H^2(K^{\text{sep}}/K) & \xrightarrow{\text{Res}} & H^2(L^{\text{sep}}/L) \\ & & \| & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & H^2(K^{\text{ur}}/K) & \xrightarrow{\text{Res}} & H^2(L^{\text{ur}}/L). \end{array}$$

In particular, we may view $H^2(L/K) \xrightarrow{\text{Inf}} H^2(K^{\text{ur}}/K)$.

Theorem 4.2.14. *There is an isomorphism* $H^2(K^{\text{ur}}/K) \xrightarrow{\text{Inf}} H^2(K^{\text{sep}}/K)$.

Proof. Recall that $H^2(L/K) \hookrightarrow H^2(K^{\text{ur}}/K) \hookrightarrow H^2(K^{\text{sep}}/K)$. Taking the limit over finite Galois extensions L/K, we have an injection $H^2(K^{\text{sep}}/K) \hookrightarrow H^2(K^{\text{ur}}/K) \hookrightarrow H^2(K^{\text{sep}}/K)$, but the composition is the identity, so all inclusions are equalities. □

Definition 4.2.15. We can extend the *invariant map* to $\text{inv}_K \colon H^2(K^{\text{sep}}/K) \simeq \mathbb{Q}/\mathbb{Z}$.

Remark 4.2.16. For any field K, define the *Brauer group* $\text{Br}(K) \coloneqq H^2(K^{\text{sep}}/K, (K^{\text{sep}})^\times)$. This is in fact $H^2_{\text{ét}}(\operatorname{Spec} K, \mathbb{G}_m)$. The goal of local class field theory is to compute $\text{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$ for a local field K.

Remark 4.2.17. Classically, the group $\text{Br}(K)$ classifies *central simple algebras* over K. In fact, it classifies central simple algebras up to the relation $A \sim B$ if and only if $A \otimes_K M_n(K) \simeq B \otimes M_m(K)$ for some n, m. The group structure is defined by $[A] \otimes [B] = [A \otimes_K B]$ with identity $0 = [M_n(k)]$.

Theorem 4.2.18 (Wedderburn)**.** *Each class of* $\text{Br}(K)$ *is represented by a central division algebra over* K.

Example 4.2.19. If K is a local field, then we may define the invariant $\text{inv}_K(B)$ for any central division algebra B over K. If $B = K$, then $\text{inv}_K(K) = 0$. Now if B is the quaternion algebra over K, we have $\text{inv}_K(B) = \frac{1}{2}$. In fact there is an explicit construction of a central division algebra associated to $\frac{1}{n}$ for every n. If L/K is a quadratic extension, then

$$\text{inv}_L(B \otimes_K L) = [L : K]\text{inv}_K(B) = 2 \cdot \frac{1}{2} = 0 \in \mathbb{Q}/\mathbb{Z},$$

so $B \otimes_K L = M_2(L)$.

Example 4.2.20. Call the element $u_{L/K} \in H^2(L/K)$ with $\text{inv}_K(u_{L/K}) = \frac{1}{n}$ the *fundamental class* of L/K.

Remark 4.2.21. The local Artin reciprocity isomorphism $\widehat{H}^{-2}(G, \mathbb{Z}) \to \widehat{H}^0(G, L^\times)$ can be realized as the cup product by the fundamental class $u_{L/K}$.

4.3 Proof of Local Class Field Theory

Our goal is to prove the following result:

Theorem 4.3.1 (Local class field theory)**.**

1. *(Local Artin reciprocity) There exists a unique homomorphism*

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

such that

   a) *For any finite Galois extension* L/K*, we have a commutative diagram*

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

   b) *For any finite unramified extension,* $\phi_{L/K}(\pi) = \mathrm{Frob}_{L/K}$*, where* π *is an uniformizer of* K*.*

2. *(Local existence theorem) There is a bijection between norm subgroups of* $K^\times$ *and finite index open subgroups of* $K^\times$*. In addition, if* $\mathrm{char}\, K = 0$*, then the finite index open subgroups of* $K^\times$ *are precisely the finite index subgroups of* $K^\times$*.*

4.3.1 Proof of local Artin reciprocity To construct ϕ_K, we will use Tate's theorem. Recall that by Hilbert 90, we have $H^1(L/K, L^\times) = 0$. We also computed $H^2(L/K, L^\times) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, where $n = [L : K]$. By Tate's theorem, we have an isomorphism $\widehat{H}^r(L/K, \mathbb{Z}) \simeq \widehat{H}^{r+2}(L/K, L^\times)$ for all $r \in \mathbb{Z}$. We will specialize to the case where $r = -2$, and this gives us an isomorphism

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

Then we define $\phi^{\mathrm{ab}}_{L/K} \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}$ to be its inverse. Taking the limit over all finite Galois extensions L/K, we obtain a map

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

By construction, the property a) is satisfied.

To finish the proof, we need to check property b). Let L/K be a finite unramified extension. Our goal is to explicitly describe the shift by 2 isomorphism produced by Tate's theorem. Recall that Tate's theorem comes from $M = L^\times$ and $G = \mathrm{Gal}(L/K)$. Then we construct the splitting module for some $\varphi \in H^2(G, M) = H^2(L/K, L^\times) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by defining

$$M(\varphi) = M \oplus \bigoplus_{g \neq 1} X_g \qquad g_1 X_{g_2} = X_{g_1 g_2} - X_{g_1} + \varphi(g_1, g_2).$$

Then we have short exact sequences

$$0 \to M \to M(\varphi) \xrightarrow{X_g \mapsto g-1} I_g \to 0$$

and

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{g \mapsto 1} \mathbb{Z} \to 0.$$

Now we need to trace through the isomorphisms

$$\begin{array}{ccccc} \widehat{H}^{-2}(G,\mathbb{Z}) & \xrightarrow{\sim} & \widehat{H}^{-1}(G,I_G) & \xrightarrow{\sim} & \widehat{H}^{0}(G,M) \\ \| & & \| & & \| \\ G = \left\langle \mathrm{Frob}_{L/K} \right\rangle & \xrightarrow{\sim} & I_G/I_G^2 & \xrightarrow{\sim} & K^\times/\mathrm{Nm}(L^\times). \end{array}$$

The first isomorphism is given by $\mathrm{Frob}_{L/K} =: \sigma \mapsto \sigma - 1$. Therefore it remains to write down the connecting homomorphism $\widehat{H}^{-1}(G,I_G) \to \widehat{H}^0(G,M)$. This is described using the exact sequences

$$\begin{array}{ccccccc} & & M_G & \longrightarrow & M(\varphi)_G & \longrightarrow & (I_G)_G = I_G/I_G^2 \longrightarrow 0 \\ & & \downarrow \mathrm{Nm} & & \downarrow \mathrm{Nm} & & \downarrow \mathrm{Nm} \\ 0 & \longrightarrow & M^G & \longrightarrow & M(\varphi)^G & \longrightarrow & (I_G)^G \end{array}$$

by lifting $(\sigma - 1) \in I_G/I_G^2$ to $M(\varphi)_G$ and then taking Nm. This will automatically land in M^G. An obvious list of $\sigma - 1$ to $M(\varphi)_G$ is X_σ, so we need to compute $\mathrm{Nm}(X_\sigma)$. Therefore we have

$$\begin{aligned} \mathrm{Nm}(X_\sigma) &= (1 + \sigma + \cdots + \sigma^{n-1})X_\sigma \\ &= X_\sigma + \sigma X_\sigma + \cdots + \sigma^{n-1}X_\sigma \\ &= X_\sigma + (X_{\sigma^2} - X_\sigma + \varphi(\sigma,\sigma)) + \cdots + (X_{\sigma^n} - X_{\sigma^{n-1}} + \varphi(\sigma^{n-1},\sigma)) \\ &= X_{\sigma^n} + \varphi(\sigma,\sigma) + \varphi(\sigma^2,\sigma) + \cdots + \varphi(\sigma^{n-1},\sigma) \\ &= \varphi(1,1) + \varphi(\sigma,\sigma) + \varphi(\sigma^2,\sigma) + \cdots + \varphi(\sigma^{n-1},\sigma). \end{aligned}$$

Now it remains to describe this explicitly for $\varphi \in H^2(G,M) = H^2(L/K,L^\times) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.Recall that this comes from $H^2(L/K,L^\times) \xrightarrow{\sim} H^1(L/K,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ coming from the exact sequence

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

Now if $f \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ such that $f(\sigma) = \frac{1}{n}$, then we can lift f to $\widetilde{f} \in Z^1(G,\mathbb{Q})$ and take $d\widetilde{f}$. This gives us $\widetilde{f}(\sigma^i) = \frac{i}{n} \in \mathbb{Q}$. If $\varphi = d\widetilde{f}$, then we have

$$\begin{aligned} \varphi(\sigma^i,\sigma^j) &= \sigma^i\widetilde{f}(\sigma^j) - \widetilde{f}(\sigma^{i+j}) + \widetilde{f}(\sigma^i) \\ &= \frac{j}{n} - \frac{(i+j) \mod n}{n} + \frac{i}{n} \\ &= \begin{cases} 0 & 0 \leqslant i+j \leqslant n-1 \\ 1 & i+j \geqslant n. \end{cases} \end{aligned}$$

This gives us

$$\begin{aligned}\operatorname{ord}_K(\operatorname{Nm}(X_\sigma)) &= \varphi(1,1)+\varphi(\sigma,\sigma)+\varphi(\sigma^2,\sigma)+\cdots+\varphi(\sigma^{n-1},\sigma)\\ &= 0+0+0+\cdots+1\\ &= 1\end{aligned}$$

and thus $\operatorname{Nm}(X_\sigma)=\pi\in K^\times/\operatorname{Nm}(L^\times)$. □

4.3.2 Proof of Local Existence We will assume that $\operatorname{char} K = 0$. We will establish a bijection

$$\{\text{norm subgroups of } K^\times\} \xleftrightarrow{1:1} \{\text{finite index subgroups of } K^\times\}.$$

Recall that any subgroup of $K^\times$ containing a norm subgroup is also a norm subgroup. Also note that any finite index subgroup of index n contains $(K^\times)^n$. Therefore it suffices to show that $(K^\times)^n$ is a norm subgroup. Our goal is to study the n-th power may using the *Kummer sequence*

$$1\to\mu_n\to(K^{\text{sep}})^\times\xrightarrow{x\mapsto x^n}(K^{\text{sep}})^\times\to 1.$$

This is an exact sequence in Mod_G for $G=\operatorname{Gal}(K^{\text{sep}}/K)$, so it induces a long exact sequence in cohomology

$$0\to\mu_n(K)\to K^\times\xrightarrow{x\mapsto x^n}K^\times\to H^1(G,\mu_n)\to H^1(G,(K^{\text{sep}})^\times)=0.$$

This gives us the *Kummer isomorphism* $K^\times/(K^\times)^n\cong H^1(G,\mu_n)$.

1. In the simplest case, when $\mu_n\subseteq K^\times$, then the isomorphism becomes

   $$K^\times/(K^\times)^n\cong\operatorname{Hom}(G,\mu_n)\cong\operatorname{Hom}(\operatorname{Gal}(L/K),\mu_n),$$

   where L/K is the maximal abelian extension of exponent n. Now the pairing

   $$K^\times/(K^\times)^n\times\operatorname{Gal}(L/K)\to\mu_n\qquad(b,\sigma)\mapsto\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$$

   is in fact a perfect pairing. Therefore $\left|K^\times/(K^\times)^n\right|=|\operatorname{Gal}(L/K)|$, so by local Artin reciprocity, we have the map

   $$\phi_{L/K}\colon K^\times/\operatorname{Nm}(L^\times)\xrightarrow{\sim}\operatorname{Gal}(L/K).$$

   Also, we know $\operatorname{Nm}(L^\times)\supseteq(K^\times)^n$, and therefore $(K^\times)^n=\operatorname{Nm}(L^\times)$.

2. In general, if μ_n is not contained in $K^\times$, then take $K_1=K(\mu_n)$. Now we can find L_1/K_1 such that $\operatorname{Nm}(L_1^\times)=(K_1^\times)^n$. Now take L/K Galois such that $L_1\subseteq L$. Then

   $$\begin{aligned}\operatorname{Nm}_{L/K}(L^\times)&=\operatorname{Nm}_{K_1/K}(\operatorname{Nm}_{L/K_1}(L^\times))\\ &\subseteq\operatorname{Nm}_{K_1/K}(\operatorname{Nm}_{L_1/K_1}(L_1^\times))\\ &=\operatorname{Nm}_{K_1/K}((K_1^\times)^n)\\ &\subseteq(K^\times)^n.\end{aligned}$$

   Therefore $(K^\times)^n$ contains a norm subgroup, and is thus also a norm subgroup. □

5

Global class field theory

Recall that a number field K is a finite extension of $\mathbb{Q}$. The goal of global class field theory is to understand $\mathrm{Gal}(\overline{K}/K)^{ab}$, or equivalently to understand finite abelian extensions of K in terms of **intrinsic** data associated to K. Analogously to the local case, we would like to construct a *global Artin reciprocity map*

$$\phi_K \colon C_k \to \mathrm{Gal}(\overline{K}/K)^{ab}$$

which induces isomorphisms

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

Remark 5.0.1. When K is a local field, we took $C_K = K^\times$. When K is global, we can again try to take $C_K = K^\times$, but in fact this fails.

Example 5.0.2. Choose $L/K = \mathbb{Q}(i)/\mathbb{Q}$. Then $\mathrm{Gal}(L/K) = \mathbb{Z}/2$, but

$$\mathbb{Q}^\times / \mathrm{Nm}(\mathbb{Q}(i)^\times) = \mathbb{Q}^\times / \left\{ x \in \mathbb{Q}^\times \mid x = a^2 + b^2, a, b \in \mathbb{Q} \right\} \neq \mathbb{Z}/2\mathbb{Z}.$$

For example, any $p \equiv 3 \pmod 4$ cannot be written as $a^2 + b^2$, and in fact the quotient is infinite.

Instead of $K^\times$, we will take C_K to be a generalization of the ideal class group Cl_K, which is the quotient of all fractional ideals by the principal ones. Thus the class group measures the failure of unique factorization in K.

5.1 Idèles

Our generalization of ideals will be the idèle class group of K, which is again given by

$$C_K \coloneqq \frac{\mathbb{I}_K}{K^\times}$$

for some group $\mathbb{I}_K$. We need to define $\mathbb{I}_K$ and $\mathrm{Nm}_{L/K} \colon C_L \to C_K$.

Notations 5.1.1. We will denote a (finite or infinite) place of K by v and $|-|_v$ the absolute value associated to v such that

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

for all $a \in K^\times$. Then we will denote the completion of K with respect to $|-|_\nu$ by K_ν. When ν is a finite place, we write $\mathcal{O}_V \subseteq K_V$ for the ring of integers, $\mathfrak{p}_\nu \subseteq \mathcal{O}_K$ the corresponding maximal ideal, and $\widehat{\mathfrak{p}}_\nu \subseteq \mathcal{O}_\nu$ for the completion of the maximal ideal.

Remark 5.1.2. We may attempt to take $\mathbb{I}_K = \prod_\nu K_\nu^\times$. The problem is that this group is too large in the sense that it is not locally compact.

Instead of this, we will allow only finitely many coordinates to be not a unit in $\mathcal{O}_\nu$. This will make our group locally compact.

Definition 5.1.3. The group of *idèles* (from the French élément idéal for ideal element) is

$$\mathbb{I}_K \coloneqq \left\{ (a_\nu)_\nu \in \prod_\nu K_\nu^\times \mid a_\nu \in \mathcal{O}_V^\times \text{ for all but finitely many } \nu \right\}.$$

This is the *restricted product* of $\prod_\nu K_\nu^\times$ with respect to $\prod_\nu \mathcal{O}_V^\times$.

Remark 5.1.4. The idèles are equipped with the restricted product topology with a basis of open neighborhoods given by

$$\prod_\nu U_\nu \subseteq \mathbb{I}_K,$$

where U_ν is open in $K_\nu^\times$ for all ν and $U_\nu = \mathcal{O}_V^\times$ for all but finitely many ν.

Let S be a finite set of places containing $S_\infty = \{\nu \text{ infinite}\}$. Then define

$$\mathbb{I}_{K,S} \coloneqq \prod_{\nu \in S} K_\nu^\times \times \prod_{\nu \notin S} \mathcal{O}_\nu^\times \subseteq \mathbb{I}_K.$$

Note the first factor is locally compact and the second product is compact, so $\mathbb{I}_{K,S}$ is locally compact. Then we can write

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

and each $\mathbb{I}_{K,S}$ is open in $\mathbb{I}_K$, so in particular $\mathbb{I}_K$ is locally compact.

Remark 5.1.5. The group $\mathbb{I}_K$ has a basis of open neighborhoods of 1 given by

$$U(S, \varepsilon) \coloneqq \{(a_\nu) \in \mathbb{I}_K \mid |a_\nu - 1| < \varepsilon \text{ for all } \nu \in S, |a_\nu| = 1 \text{ for all } \nu \notin S\}.$$

Remark 5.1.6. For all places ν, there is a natural injection

$$K_\nu^\times \hookrightarrow \mathbb{I}_K \qquad a \mapsto (1, \dots, 1, a, 1, \dots),$$

where a goes in the coordinaate corresponding to ν. The induced topology on $K_\nu^\times$ agrees with the usual topology.

Remark 5.1.7. If I_K is the group of fractional ideals of K, then there is a natural surjection

$$\mathbb{I}_K \twoheadrightarrow I_K \qquad (a_\nu) \mapsto \prod_{\nu \nmid \infty} \mathfrak{p}_\nu^{\operatorname{ord}_\nu(a_\nu)}$$

with kernel given by

$$\prod_{\nu \mid \infty} K_\nu^\times \times \prod_{\nu \nmid \infty} \mathcal{O}_\nu^\times = \mathbb{I}_{K,S_\infty}.$$

In particular, $\mathbb{I}_K$ can be thought of as an enlargement of I_K with extra information from the infinite places and units at finite places.

Remark 5.1.8. The group $\mathbb{I}_K$ is completely local.

Proposition 5.1.9. *The natural map*

$$K^\times \hookrightarrow \mathbb{I}_K \qquad a \mapsto (a, a, \dots, a, \dots)$$

has discrete image.

Proof. It suffices to show that $1 \in K^\times$ is open in its imaage. Equivalently, for some $S \supseteq S_\infty$ and some $\varepsilon > 0$, we have $K^\times \cap U(s, \varepsilon) = \{1\}$. Let $a \in K^\times \cap U(S, \varepsilon)$. Then $|a-1|_v < \varepsilon$ for all $v \in S$ and $|a|_v = 1$ for all $v \notin S$. Note that $|a-1|_v \leqslant 1$ for all $v \notin S$. Therefore

$$\prod_v |a-1|_v < \varepsilon^{|s|}.$$

On the other hand, by the product formula, we know $\prod_v |a-1|_v = 1$ unless $a - 1 = 0$. In particular, for S sufficiently large and ε sufficiently small, we must have $a = 1$. □

Remark 5.1.10. Note that $K^\times \hookrightarrow K_v^\times$ has dense image for any single v. However, the product formula implies that for $a \in K^\times$, its absolute values $|a|_v$ at different places v "repel" each other and makes $K^\times \hookrightarrow \mathbb{I}_K$ have discrete image.

Example 5.1.11. Consider the ring $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}$. Because $\sqrt{2}$ is irrational, this has dense image. However, the embedding

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

has discrete image. In fact, the image is a lattice in $\mathbb{R}^2$.

Similarly, $\mathbb{Z}\left[\frac{1}{p}\right] \hookrightarrow \mathbb{R}, \mathbb{Q}_p$ both have dense image, but

$$\mathbb{Z}\left[\frac{1}{p}\right] \hookrightarrow \mathbb{R} \times \mathbb{Q}_p$$

has discrete image.

Now it should not be surprising that $K^\times \hookrightarrow \mathbb{I}_K$ has discrete image. This is simply an infinite dimensional generalization of this phenomenon.

Definition 5.1.12. Define the *idèle class group* $C_K \coloneqq \mathbb{I}_K / K^\times$ and equip it with the quotient topology. Because $K^\times$ is discrete, this group is locally compact.

Remark 5.1.13. The $\mathbb{I}_K \twoheadrightarrow I_K$ descends to $C_K \twoheadrightarrow \mathrm{Cl}_K$. In particular, C_K can be viewed as an enlargement of Cl_K.

Definition 5.1.14. Let L/K be a finite extension. Recall that

$$L \otimes_K K_v \cong \prod_{w|v} L_w,$$

given $K_v[x]/f(x) = \prod(K_v[x]/f_i(x))$, where f_i are the irreducible factors of f after the extension. Therefore, for all $\alpha \in L^\times$, we have

$$\mathrm{Nm}_{L/K}(\alpha) = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(\alpha).$$

Now we can define

$$\mathrm{Nm}_{L/K} \colon \mathbb{I}_L \to \mathbb{I}_L \qquad (a_w)_w \mapsto (b_v)_v \qquad b_v \coloneqq \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a_w).$$

Definition 5.1.15. By definition, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \mathbb{I}_K \\ \uparrow & & \uparrow \\ L^\times & \xrightarrow{\mathrm{Nm}_{L/K}} & L^\times. \end{array}$$

Therefore, we have an induced map $\mathrm{Nm}_{L/K} \colon C_L \to C_K$.

5.2 Statement of global class field theory

Our goal is now to construct the global Artin reciprocity map. We hope to do this using the local Artin reciprocity maps. First, we recall some properties from algebraic number theory.[1] If L/K is a finite Galois extension of number fields, v a place of K, and $w \mid v$ a place of L above v, we can define the *decomposition group*

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

Remark 5.2.1. Suppose that $w' \mid v$ is another place of L above v. Then $D(w), D(w')$ are conjugate in $\mathrm{Gal}(L/K)$. In particular, if $\mathrm{Gal}(L/K)$ is abelian, then $D(w) = D(w')$ only depends on v. By local class field theory, we obtain

$$\phi_v \colon K_v^\times \to \mathrm{Gal}(L_w/K_v) = D(w) \hookrightarrow \mathrm{Gal}(L/K)$$

which only depends on v.

Proposition 5.2.2. *There exists a unique continuous homomorphism*

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

such that for any finite abelian extension L/K *and any place* v *of* K*, the diagram*

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ \uparrow & & \uparrow \\ K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \end{array}$$

commutes.

Proof. Let $a = (a_v) \in \mathbb{I}_K$. If $a_v \in \mathcal{O}_v^\times$ and L_w/K_v is unramified (true for all but finitely many places), then $\phi_v(a_v) = 1 \in \mathrm{Gal}(L_w/K_v)$. Now ϕ_K is uniquely determined by a finite product

$$\phi_K((a_v)) = \prod_v \phi_v(a_v) \in \mathrm{Gal}(L/K),$$

where v runs over the places where $a_v \notin \mathcal{O}_v^\times$ or L_v/K_v is ramified. Therefore, varying L/K and taking a limit, this determines ϕ_K uniquely.

[1] The note taker does not actually know any number theory. Please send help.

Now it remains to check that ϕ_K is continuous. In particular, we need the kernel to be open. Let S be the set of ramified places of L/K. Then by local class field theory, the diagram

$$\begin{array}{ccc} \mathbb{I}_{K,S} & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ {\scriptstyle \mathrm{Nm}_{L/K}}\uparrow & & \uparrow \\ \mathbb{I}_{L,S} & \xrightarrow{\phi_{L/L}} & \mathrm{Gal}(L/L) \end{array}$$

commutes. Therefore $\ker(\phi_{L/K}) \supseteq \mathrm{Nm}_{L/K}(\mathbb{I}_{L,S})$, which is open. Therefore the kernel itself is also open. □

Theorem 5.2.3 (Global class field theory)**.**

1. *(Global Artin reciprocity) The homomorphism* $\phi_K \colon \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ *satisfies*
   a) $\phi_K(K^\times) = 1$. *Therefore we obtain a global Artin map* $\phi_K \colon C_k \to \mathrm{Gal}(K^{ab}/K)$.
   b) *For any finite abelian extension* L/K, ϕ_K *induces an isomorphism*
   $$\phi_{L/K} \colon C_k / \mathrm{Nm}(C_L) \simeq \mathrm{Gal}(L/K).$$
2. *(Global existence theorem) For any finite index open subgroup* $N \subseteq C_K$*, there exists a finite abelian extension* L/K *such that* $N = \mathrm{Nm}(C_L)$.

Corollary 5.2.4. *We have a bijection between finite abelian extensions* L/K *and finite index open subgroups of* C_K.

Before we turn to the proof of global class field theory, we will describe some consequences of this bijection. We will begin with ray class fields.

Definition 5.2.5. A *modulus* of K is a function

$$\mathfrak{m} \colon \{\text{places of } K\} \to \mathbb{Z}_{\geqslant 0}$$

such that

1. $\mathfrak{m}(v) = 0$ for all but finitely many places v.
2. $\mathfrak{m}(v) = 0, 1$ if v is a real place.
3. $\mathfrak{m}(v) = 0$ if v is a complex place.

Definition 5.2.6. For a modulus $\mathfrak{m}$, define the *principal congruence subgroup*

$$\mathbb{I}_K^{\mathfrak{m}} \coloneqq \prod_{v \nmid \infty} U_{v,\mathfrak{m}(v)} \times \prod_{v \mid \infty} K_{v,\mathfrak{m}(v)}^\times,$$

where $U_{v,0} = \mathcal{O}_v^\times$ and $U_{v,i} = 1 + \mathfrak{p}_v^i$ for $i \geqslant 1$ for finite places. For infinite places, we have $K_{v,0}^\times = K_v^\times$, and $K_{v,1}^\times = \mathbb{R}_{>0}$.

Definition 5.2.7. For a modulus $\mathfrak{m}$, define

$$C_k^{\mathfrak{m}} \coloneqq \frac{\mathbb{I}_K^{\mathfrak{m}} \cdot K^\times}{K^\times}.$$

Then define the *ray class group* to be

$$\mathrm{Cl}_{\mathfrak{m}} \coloneqq C_K / C_K^{\mathfrak{m}}.$$

Here, the term "ray" comes from a positivity condition $\mathbb{R}_{>0} \subset \mathbb{R}^\times$ at real places, which geometrically means specifying a ray.

Definition 5.2.8. Write $\mathfrak{m} = \prod_v \mathfrak{p}_v^{\mathfrak{m}(v)} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$. Then we have a description

$$\mathrm{Cl}_{\mathfrak{m}} \coloneqq \frac{\{\text{fractional ideals coprime to } \mathfrak{m}_0\}}{\left\{x \in K^\times, x \in U_{v,\mathfrak{m}(v)}(v \mid \mathfrak{m}_0), x \in \mathbb{R}_{v,>0}(v \mid \mathfrak{m}_\infty)\right\}}.$$

In particular, if $\mathfrak{m}(v) \equiv 0$, then $\mathfrak{m} = \prod_v \mathfrak{p}_v^0 = 1$ and $\mathrm{Cl}_1 = \mathrm{Cl}_K$. On the other hand, if $\mathfrak{m} = \mathfrak{m}_\infty$, then

$$\mathrm{Cl}_{\mathfrak{m}_\infty} = \frac{\{\text{fractional ideals}\}}{\{x \in K^\times \mid x \text{ totally positive}\}} = \mathrm{Cl}_K^+.$$

This is called the *narrow class group*.

Definition 5.2.9. The abelian extension L/K associated to $\mathrm{Cl}_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$ under global class field theory is called the *ray class field of* $\mathfrak{m}$. The case of $\mathfrak{m} = 1$ is called the *Hilbert class field* and is denoted by H with $\mathrm{Cl}_K = \mathrm{Gal}(H/K)$. The case where $\mathfrak{m} = \mathfrak{m}_\infty$ gives us the *narrow Hilbert class field* and is denoted by H^+. This is characterized by $\mathrm{Cl}_K^+ = \mathrm{Gal}(H^+/K)$. In particular, $H \subseteq H^+$.

Remark 5.2.10. By local class field theory, the ramified places of the ray class field of $\mathfrak{m}$ is contained in $\mathfrak{m}$. In particular, H/K is the maximal abelian abelian extension unramified everywhere, and H^+/K is the maximal abelian extension unramified at all finite places.

Example 5.2.11. If $K = \mathbb{Q}$, then $\mathrm{Cl}_K = \mathrm{Cl}_L^+ \cong \{1\}$ and thus $H = H^+ = \mathbb{Q}$.

Example 5.2.12. If $K = \mathbb{Q}(\sqrt{3})$, then $\mathrm{Cl}_K = \{1\}$. However, we have

$$\mathrm{Cl}_K^+ = \frac{K^\times}{K_{>0}^\times \cdot \mathcal{O}_K^\times} = \mathbb{Z}/2.$$

Therefore $H = K = \mathbb{Q}(\sqrt{3})$ and $H^+ = K(i) = \mathbb{Q}(\sqrt{3}, i)$.

Example 5.2.13. Let $K = \mathbb{Q}$ and let $\mathfrak{m} = (m)$ for some $m \in \mathbb{Z}$. Then

$$\mathrm{Cl}_{(m)} = \frac{\left\{\left(\frac{r}{s}\right) \in \mathbb{Q}^\times \mid (r, m) = (s, m) = 1\right\}}{\left\{\frac{r}{s} \in \mathbb{Q}^\times \mid \frac{r}{s} \equiv 1 \pmod{m}\right\}} = (\mathbb{Z}/m)^\times/(\pm 1).$$

If $\mathfrak{m} = (m) \cdot \infty$, then $\mathrm{Cl}_{(m)\cdot\infty} = (\mathbb{Z}/m)^\times$.

Now the ray class fields $L/\mathbb{Q}$ for either $2 \nmid m$ or $4 \mid m$ are given by $\mathrm{Cl}_{(m)\cdot\infty} \cong \mathrm{Gal}(L/\mathbb{Q})$, where $L = \mathbb{Q}(\zeta_m)$, and the field given by $\mathrm{Cl}_{(m)}$ is $L = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. In particular, by varying $\mathfrak{m}$, we obtain the *Kronecker-Weber theorem*.

Theorem 5.2.14 (Kronecker-Weber)**.** *We have* $\mathbb{Q}^{\mathrm{ab}} = \bigcup_{m \geqslant 1} \mathbb{Q}(\zeta_m)$ *and thus*

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \varprojlim_m (\mathbb{Z}/m)^\times = \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times.$$

Remark 5.2.15. Hilbert's 12th problem asks for an explicit description of the ray class fields for a general number field. For $K = \mathbb{Q}$, we have the Kronecker-Weber theorem. For imaginary quadratic fields, we have modular functions and elliptic curves with complex multiplication. In general, this problem is still open.

We will use the following strategy to prove global Artin reciprocity:

1. We will prove the first inequality[2] that $[C_K : \mathrm{Nm}(C_L)] \geqslant [L : K]$. This will be a consequence of the cohomology of $\mathbb{I}_K, C_K$. In particular, we will show that $h(C_K) = [L : K]$. This will imply that $\left|\widehat{H}^0(G, C_L)\right| \geqslant [L : K]$, but this is precisely the index we need.

2. Next, we will prove the surjectivity of $\mathbb{I}_K \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K)$. This is an application of the first inequality and the weak Chebotarev density theorem.

3. We will prove the second inequality[3] $[C_K : \mathrm{Nm}(C_L)] \leqslant [L : K]$. This is a consequence of Chebotarev density and we will use the analytic tool of L-functions.[4]

4. We will prove that $\phi_K(K^\times) = 1$. This will follow from the determination of the Brauer groups of K.

5.3 Cohomology of Idèles and first inequality

Let L/K be a finite Galois extension of number fields. Recall that if v is a place of K, then $L \otimes_K K_v = \prod_{w|v} L_w$. The action of $\mathrm{Gal}(L/K)$ on $L \otimes K_v$ induces an action on the product by permuting the places above v. If $\alpha = (\alpha_w)_{w|v}$ and $\sigma \in \mathrm{Gal}(L/K)$, then $(\sigma\alpha)_{\sigma w} = \sigma(\alpha_w) \in L_{\sigma w}$.

Proposition 5.3.1. *Fix $w_0 \mid v$. Then there exists an isomorphism of $G \coloneqq \mathrm{Gal}(L/K)$-modules*

$$\prod_{w|v} L_w \cong \mathrm{Ind}_{G_{w_0}}^{G} L_{w_0},$$

where $G_{w_0} = D(w_0)$ is the decomposition group.

Proof. Recall that $\mathrm{Ind}_{G_{w_0}}^{G} L_{w_0} \coloneqq \left\{f \colon G \to L_{w_0} \mid f(\tau\sigma) = \tau f(\sigma) \text{ for all } \tau \in G_{w_0}, \sigma \in G\right\}$. For any $\alpha = (\alpha_w)_w$, we define

$$f_\alpha \colon G \to L_{w_0} \qquad \sigma \mapsto \sigma(\alpha_{\sigma^{-1}w_0}).$$

Then it is easy to compute

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

Conversely, for $f \in \mathrm{Ind}_{G_{w_0}}^{G} L_{w_0}$, we define $(\alpha_f)_{\sigma w_0} \coloneqq \sigma f(\sigma^{-1})$. This is well-defined by G_{w_0}-equivariance, and we can check that these two assignments are inverse to each other. □

Corollary 5.3.2. *By Shapiro's lemma, we have $H^r\left(G, \prod_{w|v} L_w\right) = H^r(G_{w_0}, L_{w_0})$ for all $r \geqslant 0$.*

Similarly, we have

Corollary 5.3.3. *For all $r \geqslant 0$, $H^r\left(G, \prod_{w|v} L_w^\times\right) = H^r(G_{w_0}, L_{w_0}^\times)$ and $H^r\left(G, \prod_{w|v} U_w\right) = H^r(G_{w_0}, U_{w_0})$.*

In particular, all of these are independent of the choice of $w_0 \mid v$. To stress the independence, we write $G^v \coloneqq G_{w_0}, L^v \coloneqq L_{w_0}$, and so on and so forth.

[2] Some other references will call this the second inequality because they prove this second.

[3] In the first proof of class field theory, this was the first inequality.

[4] This is the difference between algebraic geometry and number theory. In number theory, there are infinite places, so analysis cannot be avoided.

Proposition 5.3.4. *We have the following cohomology of the idèles:*

1. $H^0(G, \mathbb{I}_L) = \mathbb{I}_K$.
2. *For all* $r \in \mathbb{Z}$, $H^r(G, \mathbb{I}_L) = \bigoplus_v \widehat{H}^r(G^v, (L^v)^\times)$.

Proof.

1. We know that $a = (a_w) \in \mathbb{I}_L$ is G-invariant if and only if $(a_w)_{w|v}$ is G-invariant for all places v of K if and only if $a_w \in K_v^\times$ is independent of the choice of $w \mid v$ for all v, and this is equivalent to $a = (a^v)_v \in \mathbb{I}_K$.
2. Let S be a finite set of places of K containing S_∞. Write

$$\mathbb{I}_{L,S} = \left(\prod_{v \in S} \prod_{w|v} L_w^\times \right) \times \left(\prod_{v \notin S} \prod_{w|v} U_w \right).$$

Then $\mathbb{I}_L = \varinjlim \mathbb{I}_{L,S}$ and therefore

$$\begin{aligned} \widehat{H}^r(G, \mathbb{I}_L) &= \varinjlim \widehat{H}^r(G, \mathbb{I}_{L,S}) \\ &= \varinjlim \left(\prod_{v \in S} \widehat{H}^r(G^v, (L^v)^\times) \right) \times \left(\prod_{v \notin S} \widehat{H}^r(G^v, U^v) \right). \end{aligned}$$

If S contains all places of K that are ramified in L, then for all $v \notin S$, L^v/K^v is unramified. By local class field theory, $\widehat{H}^r(G^v, U^v) = 0$, so

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

Corollary 5.3.5. *We have* $H^1(G, \mathbb{I}_L) = 0$ *and* $H^2(G, \mathbb{I}_L) = \bigoplus_v \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$, *where* $n_v = [L^v : K_v]$.

These statements follow from collecting all of the local information.

Corollary 5.3.6. *Assume* L/K *is cyclic. Assume* S *contains all places of* K *that are ramified in* L *and the infinite places. Then* $h(\mathbb{I}_L, S) = \prod_{v \in S} n_v$.

Proof. By local class field theory, we have

$$h(\mathbb{I}_{L,S}) = \prod_{v \in S} h((L^v)^\times) \prod_{v \notin S} h(U^v) = \prod_{v \in S} n_v \prod_{v \notin X} 1 = \prod_{v \in S} n_v. \qquad \square$$

Definition 5.3.7. Let $T \coloneqq \{w \mid v : v \in S\}$ be a finite set of places of L. Define the group of T-*units* of L to be

$$U(T) \coloneqq L^\times \cap \mathbb{I}_{L,S} = \left\{ \alpha \in L^\times \mid \alpha \in U_w, w \notin T \right\}.$$

Our next goal is to compute $h(U(T))$ and use this to prove the first inequality. First, we must compute the cohomology of units. Let L/K be a finite Galois extension of number fields and S be a finite set of places containing S_∞. Let T be the set of places of L above S.

Proposition 5.3.8. *Assume* L/K *is cyclic. Then*

$$h(U(T)) = \frac{\prod_{v \in S} n_v}{n},$$

where $n_v = [L^v : K_v], n = [L : K]$.

Proof. We need to use the following comparison result for Herbrand quotients from the homework: let G be a cyclic group and V an $\mathbb{R}[G]$-module. If $M, N \subseteq V$ are two G-stable lattices, then $h(M) = h(N)$. We will apply this to the case where $V = \mathbb{R}^{|T|} = \mathrm{Hom}_{\mathsf{Set}}(T, \mathbb{R})$.

1. Consider $N = \mathrm{Hom}_{\mathsf{Set}}(T, \mathbb{Z})$. This is clearly a G-stable lattice. As a G-module, we have

$$\begin{aligned} N &= \bigoplus_{v \in S} \mathrm{Hom}_{\mathsf{Set}}(G/G^v, \mathbb{Z}) \\ &= \bigoplus_{v \in S} \mathrm{Ind}_{G^v}^G \mathbb{Z}. \end{aligned}$$

   In particular, we have

$$\begin{aligned} h(N) &= \prod_{v \in S} h(\mathrm{Ind}_{G^v}^G \mathbb{Z}) \\ &= \prod_{v \in S} h(\mathbb{Z}) \\ &= \prod_{v \in S} |G^v| \\ &= \prod_{v \in S} n_v. \end{aligned}$$

2. Now consider $\lambda \colon U(T) \to V = \mathbb{R}^{|T|}$ given by $\alpha \mapsto (\log |\alpha|_w)_{w \in T}$. If $M^0 = \mathrm{Im}(\lambda)$, Dirichlet's unit theorem for $U(T)$ says that M^0 is a lattice of rank $|T| - 1$ in the hyperplane $\left\{\sum_{w \in T} x_w = 0\right\}$. Then $M = M^0 \oplus \mathbb{Z} \cdot (1, \ldots, 1)$ is a G-stable lattice.

   Now we know that $h(M) = h(N)$, so $h(U(T)) = h(M^0)$ because the kernel of λ is the set of roots of unity in L, which is finite. Now we obtain

$$h(U(T)) = h(M^0) = \frac{h(M)}{h(\mathbb{Z})} = \frac{\prod_{v \in S} n_v}{n},$$

   as desired. □

Now we are able to compute the cohomology of the idèle class group C_K.

Lemma 5.3.9. *For* L/K, *we have* $H^0(G, C_L) = C_K$.

Proof. The short exact sequence in Mod_G

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

gives a long exact sequence

$$0 \to H^0(G, L^\times) \to H^0(G, \mathbb{I}_L) \to H^0(G, C_L) \to H^1(G, L^\times) = 0,$$

where the last equality is by Hilbert 90. This implies that $H^0(G, C_L) = \mathbb{I}_K / K^\times = C_K$. □

We need to compute the Herbrand quotient of the idèle class group, so first we will rewrite $\mathbb{I}_K$ in terms of S-units.

Lemma 5.3.10. *Choose S containing a generating set of prime ideals in Cl_K. Then $\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$.*

Proof. Recall that we have a surjection

$$\mathbb{I}_K \twoheadrightarrow I_K \qquad (a_\nu)_\nu \mapsto \prod_{\nu \nmid \infty} \mathfrak{p}_\nu^{\mathrm{ord}_\nu(a_\nu)}.$$

with kernel $\mathbb{I}_{K,S_\infty}$. In particular, we can write

$$\mathrm{Cl}_K = \mathbb{I}_K / K^\times = \mathbb{I}_K / K^\times \mathbb{I}_{K,S_\infty}.$$

By the choice of S, we have

$$\mathbb{I}_K / K^\times \mathbb{I}_{K,S} = \mathrm{Cl}_K \,/\, \langle \mathfrak{p} \in S \rangle = \mathrm{Cl}_K \,/\, \mathrm{Cl}_K = 0. \qquad \square$$

Theorem 5.3.11. *Assume L/K is cyclic. Then $h(C_L) = [L : K]$. In particular, $[C_K : \mathrm{Nm}(C_L)] \geqslant [L : K]$.*

Proof. Choose S such that T a generating set of prime ideals for Cl_L. Then we can rewrite

$$C_L = \mathbb{I}_L / L^\times = L^\times \mathbb{I}_{L.T} / L^\times = \mathbb{I}_{L,T} / I_{L,T} \cap L^\times = \mathbb{I}_{L,T} / U(T).$$

Now we have

$$h(C_L) = \frac{h(\mathbb{I}_{L,T})}{h(U(T))} = \frac{\prod_{\nu \in S} n_\nu}{\frac{1}{n} \prod_{\nu \in S} n_\nu} = n = [L : K]. \qquad \square$$

As an application of the first inequality, we will prove

Lemma 5.3.12. *Asssume L/K is solvable. If there exists $D \subseteq \mathbb{I}_K$ such that $D \subseteq \mathrm{Nm}(\mathbb{I}_L)$ and $K^\times \cdot D \subseteq \mathbb{I}_K$ is dense, then $L = K$.*

Proof. Assume $L \neq K$. Then we may find a tower $K \subseteq K' \subseteq L$ such that K'/K is cyclic. Then we know $D \subseteq \mathrm{Nm}(\mathbb{I}'_K)$. By local class field theory, $\mathrm{Nm}(\mathbb{I}_{K'}) \subseteq \mathbb{I}_K$ is an open subgroup, so $K^\times \cdot \mathrm{Nm}(\mathbb{I}_{K'})$ is also an open subgroup. Therefore $K^\times \cdot \mathrm{Nm}(\mathbb{I}_{K'})$ is also closed. By density, we see that $K^\times \mathrm{Nm}(I_{K'}) = \mathbb{I}_K$. In particular, $[C_K : \mathrm{Nm}(C_{K'})] = 1$, so $[K' : K] = 1$, which is a contradiction. Thus $L = K$. $\square$

Proposition 5.3.13. *Assume L/K is solvable. If all but finitely many places ν of K split completely in L, then $L = K$. Equivalently, if $L \neq K$, then there are infinitely many places ν of K that do not split completely in L.*

Proof. Choose S to contain the set of all ν that do not split completely in L. Also choose

$$D = \left\{ (a_\nu)_\nu \mid a_\nu \in K_\nu^\times (\nu \in S), a_\nu = 1 (\nu \notin S) \right\} \subseteq \mathbb{I}_K.$$

Then if $\nu \notin S$, it splits completely in L, so L^ν / K_ν is a trivial extension. Therefore $D \subseteq \mathrm{Nm}(\mathbb{I}_L)$. On the other hand, by weak approximation, any $(a_\nu)_{\nu \in S}$ can be approximated by a global element $a \in K^\times$, so $K^\times \cdot D$ is dense in $\mathbb{I}_K$. By the previous lemma, $L = K$. $\square$

Proposition 5.3.14. *Assume that L/K is solvable. Then $\left\{ \mathrm{Frob}_{w/\nu} \right\}_{\nu \text{ unramified}}$ generate $\mathrm{Gal}(L/K)$.*

Proof. Take $H = \left\langle \mathrm{Frob}_{w/v} \right\rangle \subseteq \mathrm{Gal}(L/K)$. Choose $E = L^H$. If v is unramified in L, then v splits completely in L^H. But this means that $E = K$ because only finitely many places are ramified, so $H = \mathrm{Gal}(L/K)$. □

Corollary 5.3.15. *Assume* L/K *is abelian. Then the Artin map* $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ *is surjective.*

Proof. By local class field theory, if v is unramified in L, then $\phi_K(1, 1, \ldots, \pi_v, 1, \ldots) = \mathrm{Frob}_{w/v}$. We know that the $\mathrm{Frob}_{w/v}$ generate $\mathrm{Gal}(L/K)$, so ϕ_K is surjective onto $\mathrm{Gal}(L/K)$. □

5.4 Analytic aspects and second inequality

Recall that if L/K is solvable and $L \neq K$, then there exist infinitely many places of K that do not split completely in L. For example, if $L/K = \mathbb{Q}(i)/\mathbb{Q}$, then p splits in L if and only if $p \equiv 1 \pmod 4$. Thus there are infinitely many primes $p \equiv 3 \pmod 4$. This result is sometimes called the *weak Chebotarev density theorem*, so what is the **strong** Chebotarev density theorem? In our example, we expect that half of all primes are congruent to 1 modulo 4 and that the other half are congruent to 3 modulo 4. Of course, there are infinitely many primes, so we need to understand what is meant by "half of all primes" here.

Definition 5.4.1. Let P be a set of primes in $\mathbb{Z}$. Define the *natural density* of P to be

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

if this limit exists.

Definition 5.4.2. Let P be a set of finite places of a number field K. Define the *natural density* of P to be

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

if this limit exists.

Of course, this definition is a terrible way to do analysis because we are throwing away so much information, so we would like a definition better suited to analytic methods.

Definition 5.4.3. Define the *Dirichlet density*

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

if this limit exists.

The fundamental fact, proved in any first course in analytic number theory, is that if $\mu(P)$ exists, then $\delta(P)$ exists and $\mu(P) = \delta(P)$. Thus natural density is a stronger notion than Dirichlet density. The proof of this fact uses the prime number theorem and is omitted here because this is not a course in analytic number theory.

Remark 5.4.4. It is possible that the Dirichlet density exists, but the natural density does not. For $a \in \{1, \ldots, 9\}$, choose P_a to be the set of primes starting with the digit a. Then $\mu(P_a)$ does not exist, but $\delta(P_a) = \log_{10}\left(1 + \frac{1}{a}\right)$, a result due to Bombieri.[5]

[5]This pattern also appears in many other places, and is called *Benford's law*.

Dirichlet density is easier to study because we can use the tool of L-functions, which generalize the Riemann zeta function.

Definition 5.4.5. The *Riemann zeta function* is defined by

$$\zeta(s) \colon \sum_{n \geqslant 1} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}.$$

For a general number field K, the *Dedekind zeta function* is defined by

$$\zeta_K(s) \coloneqq \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \text{ideal}}} \frac{1}{N\mathfrak{a}^s} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{prime ideals}}} \frac{1}{1-N\mathfrak{p}^{-s}}.$$

These series converge when $\operatorname{Re}(s) \gg 0$. When $K = \mathbb{Q}$, $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.

Definition 5.4.6. Let $\chi \colon (\mathbb{Z}/m)^\times \to \mathbb{C}^\times$ be a character. The *Dirichlet L-function* of χ is given by

$$L(s,\chi) \coloneqq \sum_{n \geqslant 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}},$$

where $\chi(n) = 0$ if $(n,m) \neq 1$. When $\chi = \mathbb{1}$, then $L(s,\mathbb{1}) = \zeta(s)$.

Definition 5.4.7. Let K be a number field and $\mathfrak{m}$ be a modulus of K. Let $\chi \colon \mathrm{Cl}_{\mathfrak{m}} \to \mathbb{C}^\times$ be a character. The *Weber L-function* of χ is given by

$$L(s,\chi) \coloneqq \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \text{ideal}}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{prime ideals}}} \frac{1}{1-\chi(\mathfrak{p})N\mathfrak{p}^{-s}}.$$

Again, we write $\chi(\mathfrak{a}) = 0$ if $(\mathfrak{a},\mathfrak{m}) \neq 1$. These series converge absolutely when $\operatorname{Re}(s) \gg 0$. When $K = \mathbb{Q}$, $\mathfrak{m} = (m) \cdot \infty$ and we have $\mathrm{Cl}_{(m)\cdot\infty} = (\mathbb{Z}/m)^\times$, so the Weber L-function recovers the Dirichlet L-function. Of course, when $\chi = \mathbb{1}$, we recover the Dedekind zeta function.

Theorem 5.4.8 (Analytic properties of Weber L-functions)**.**

1. *If $\chi \neq \mathbb{1}$, then $L(s,\chi)$ has an analytic continuation to all $s \in \mathbb{C}$ and $L(1,\chi) \neq 0$.*
2. *If $\chi = \mathbb{1}$, then $L(s,\chi) = \zeta_K(s)$ has an analytic continuation to all $s \in \mathbb{C} \setminus \{1\}$ and a simple pole at $s = 1$. The residue $\operatorname{Res}_{s=1} \zeta_K(s)$ is given by the class number formula for K.*
3. *The function $L(s,\chi)$ satisfies the functional equation relating the values at s and $1-s$.*

Remark 5.4.9. In general, there are more complicated complicated notions of L-functions, although this is a vaguely defined notion. In general, L-functions are series of the form $\sum_{n \geqslant 1} \frac{a_n}{n^s}$ satisfying

1. The series has an Euler product $\prod_p \frac{1}{\text{polynomial}(p^{-s})}$.
2. The series has an analytic continuation to $\mathbb{C}$ except for poles for $\zeta(s)$ at $s = 1$.
3. The analytic continuation satisfies a functional equation relating the values at s and $1-s$.

Corollary 5.4.10. *For any number field K, $\log \zeta_K(s) \sim \log \frac{1}{s-1}$ (this means the difference is analytic at $s = 1$).*

Proof. By the theorem, $\zeta_K(s)(s-1)$ is analytic at $s=1$, so $\log \zeta_K(s) = \log \zeta_K(s)(s-1) - \log(s-1)$. Because $\log \zeta_K(s)(s-1)$ is analytic at $s=1$, so we obtain the desired result after rearranging. □

Proposition 5.4.11. *We have the identity*

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s}.$$

Proof. We compute

$$\begin{aligned}
\log \zeta_K(s) &= \log \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}} \\
&= -\sum_{\mathfrak{p}} \log\left(1 - N\mathfrak{p}^{-s}\right) \\
&= \sum_{\mathfrak{p}} \sum_{n \geqslant 1} \frac{N\mathfrak{p}^{-ns}}{n} \\
&= \sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}^s} + \sum_{\mathfrak{p}} \sum_{n \geqslant 2} \frac{N\mathfrak{p}^{-ns}}{n}.
\end{aligned}$$

The second term is analytic at $s=1$, so we obtain the desired result. □

Corollary 5.4.12. *We can rewrite*

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

Theorem 5.4.13. *Let* L/K *be a finite Galois extension and* P *be the set of primes of* K *splitting completely in* L*. Then*

$$\delta(P) = \frac{1}{[L:K]}.$$

Example 5.4.14. Let $K = \mathbb{Q}, L = \mathbb{Q}(i)$. Then we have $\delta(p \equiv 1 \pmod 4) = \delta(p \equiv 3 \pmod 4) = \frac{1}{2}$.

Proof. We can rewrite

$$\begin{aligned}
\sum_{\mathfrak{p} \in P} \frac{1}{N\mathfrak{p}^s} &= \frac{1}{[L:K]} \sum_{\substack{\mathfrak{q} \subseteq \mathcal{O}_L \\ f(\mathfrak{q})=1}} \frac{1}{N\mathfrak{q}^s} \\
&\sim \frac{1}{[L:K]} \sum_{\mathfrak{q} \subseteq \mathcal{O}_L} \frac{1}{N\mathfrak{q}^s} \\
&\sim \frac{1}{[L:K]} \log \frac{1}{s-1}
\end{aligned}$$

because the terms with $f(\mathfrak{q}) \geqslant 2$ contribute to an analytic function and the second item on the right hand side is $\zeta_L(s)$. Now we obtain

$$\begin{aligned}\delta(P) &= \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in P} N\mathfrak{p}^{-s}}{\log \frac{1}{s-1}} \\ &= \lim_{s\to 1^+} \frac{\frac{1}{[L:K]} \log \frac{1}{s-1}}{\log \frac{1}{s-1}} \\ &= \frac{1}{[L:K]}.\end{aligned}$$

□

Now we want to use these tools to prove the second inequality. The idea is to show that

$$\frac{1}{[C_K : \mathrm{Nm}(C_L)]} \geqslant \frac{1}{[L:K]}.$$

We will reinterpret the right-hand side as the density of primes of K that split completely in L. Now we will reinterpret the left-hand side as a certain density also. Recall that for $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ a modulus of K, we have the ray class group $\mathrm{Cl}_{\mathfrak{m}}$.

Theorem 5.4.15. *Let $K^{\mathfrak{m}} \subseteq H \subseteq I_K^{\mathfrak{m}}$. Then let $A \in I_K^{\mathfrak{m}}/H$ be an ideal class. Then*

$$\delta(\{\mathfrak{p} \in A\}) = \frac{1}{[I_K^{\mathfrak{m}} : H]}.$$

Proof. Let χ be a character of $\mathbb{I}_K^{\mathfrak{m}}/H$. This is a quotient of $\mathrm{Cl}_{\mathfrak{m}}$, so it induces a quotient of $\mathrm{Cl}_{\mathfrak{m}}$. Now let $L(s,\chi)$ be the Weber L-function. But now

$$\begin{aligned}\log L(s,\chi) &\sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s} \\ &= \sum_{B\in\mathbb{I}_K^{\mathfrak{m}}/H} \sum_{\mathfrak{p}\in B} \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s} \\ &= \sum_{B\in I_K^{\mathfrak{m}}/H} \chi(B) \sum_{\mathfrak{p}\in B} \frac{1}{N\mathfrak{p}^s}.\end{aligned}$$

But now we want to pick out a single ideal class, so we need to use some Fourier analysis. We use the fact that

$$\sum_{\chi} \chi(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$$

for any $g \in G$. Multiplying $\chi(A)^{-1}$ and summing over all χ, we see that

$$\begin{aligned}\sum_{\chi} \chi(A)^{-1} \log L(s,\chi) &\sim \sum_{\chi} \sum_{B} \chi(A^{-1}B) \sum_{\mathfrak{p}\in B} \frac{1}{N\mathfrak{p}}^s \\ \log \frac{1}{s-1} &= [I_K^{\mathfrak{m}} : H] \sum_{\mathfrak{p}\in A} \frac{1}{N\mathfrak{p}^2},\end{aligned}$$

and thus $\delta(\mathfrak{p} \in A) = \frac{1}{[I_K^{\mathfrak{m}}:H]}$, as desired. □

Remark 5.4.16. Every finite abelian extension L/K admits a modulus $\mathfrak{m}$ such that

$$C_k/\operatorname{Nm}(C_K) \simeq I_K^{\mathfrak{m}}/K^{\mathfrak{m}} \cdot \operatorname{Nm}(I_L^{\mathfrak{m}}).$$

is a quotient of the ray class group $\mathrm{Cl}_{\mathfrak{m}}$. In particular, we may reinterpret the global Artin map as a map $\phi_{L/K} \colon I_K^{\mathfrak{m}} \to \operatorname{Gal}(L/K)$ given by $\mathfrak{p} \mapsto \operatorname{Frob}_{\mathfrak{p}}$.

Theorem 5.4.17 (Second inequality)**.** *We have* $[I_K^{\mathfrak{m}} : K^{\mathfrak{m}} \cdot \operatorname{Nm}(I_L^{\mathfrak{m}})] \leqslant [L : K]$.

Proof. Apply the previous theorem to $H = K^{\mathfrak{m}} \cdot \operatorname{Nm}(I_L^{\mathfrak{m}})$ and $A = [0]$. Then we know

$$\delta(\mathfrak{p} \in A) = \frac{1}{[I_K^{\mathfrak{m}} : K^{\mathfrak{m}} \cdot \operatorname{Nm}(I_L^{\mathfrak{m}})]}.$$

On the other hand, we know

$$\delta(\mathfrak{p} \text{ splits completely in } L) = \frac{1}{[L : K]}.$$

But now we know $\mathfrak{p}$ splits completely in L only if $\mathfrak{p} \in \operatorname{Nm}(I_L^{\mathfrak{m}})$, which is the same thing as $\mathfrak{p} \in A$. Thus $\delta(\mathfrak{p} \in A) \geqslant \delta(\mathfrak{p} \text{ splits completely in } L)$, as desired. □

Before we continue with the proof of global class field theory, we will prove an important result in analytic number theory.

Theorem 5.4.18 (Chebotarev density theorem)**.** *Let* L/K *be a finite Galois extension of number fields. Let* $\sigma \in G \coloneqq \operatorname{Gal}(L/K)$ *and* C_σ *be the conjugacy class of* σ*. Then*

$$\delta(\mathfrak{p} \mid \operatorname{Frob}_{\mathfrak{p}} \in C_\sigma) = \frac{|C_\sigma|}{|G|}.$$

Proof. We will use global Artin reciprocity, so in the future we will not be using the Chebotarev density theorem. By global Artin reciprocity for abelian extensions, we have an isomorphism $I_k^{\mathfrak{m}}/H \to \operatorname{Gal}(L/K)$ for some modulus $\mathfrak{m}$. But then it is easy to see that

$$\frac{1}{|G|} = \frac{1}{[I_K^{\mathfrak{m}} : H]} = \delta(\mathfrak{p} \in A) = \delta(\mathfrak{p} \in C_\sigma)$$

because G is abelian. Now when L/K is nonabelian, we will reduce to the abelian case. Let $\sigma \in G$ and write $M = L^{\langle \sigma \rangle}$. Applying the abelian case to the abelian extension L/M, write

$$S_1 \coloneqq \{\mathfrak{q} \subset \mathcal{O}_M \mid \operatorname{Frob}_{\mathfrak{q}} = \sigma \in \operatorname{Gal}(L/M)\}.$$

We know $\delta(s_1)\frac{1}{|\sigma|}$. Now consider a subset of degree 1 primes of M and write

$$S_2 \coloneqq \{\mathfrak{q} \in S_1 \mid f(\mathfrak{q}/\mathfrak{p}) = 1\}.$$

We know that $\delta(S_1) = \delta(S_2)$. Finally, consider

$$S_3 \coloneqq \{\mathfrak{p} \mid \operatorname{Frob}_{\mathfrak{p}} \in C_\sigma\}.$$

Now we have a surjection $S_2 \twoheadrightarrow S_3$ and the fiber has size $\frac{|Z_G(\sigma)|}{|\sigma|}$. This is because if $\mathfrak{q} \mapsto \mathfrak{p}$ with $\operatorname{Frob}_{\mathfrak{p}} = \sigma$, then $\tau\mathfrak{q} \mapsto \mathfrak{p}$ if and only if $\operatorname{Frob}_{\tau\mathfrak{q}} = \tau \operatorname{Frob}_{\mathfrak{q}} \tau^{-1}$ if and only if $\tau\sigma = \sigma\tau$. Therefore $\tau\mathfrak{q} = \mathfrak{q}$ if and only if $\tau \in D(\mathfrak{q}) = \langle \sigma \rangle = \operatorname{Gal}(L/M)$. Then we know that

$$\frac{1}{|\sigma|} = \delta(S_2) = \delta(S_3) \cdot \frac{|Z_G(\sigma)|}{|\sigma|},$$

and therefore

$$\delta(S_3) = \frac{1}{|Z_G(\sigma)|} = \frac{|C_\sigma|}{|G|}. \qquad \square$$

Example 5.4.19. Suppose $\sigma = 1$. Then $C_\sigma = \{1\}$, so Chebotarev density tells us that

$$\delta(\mathfrak{p} \text{ splits completely in } L) = \frac{1}{[L : K]}.$$

Example 5.4.20. Choose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_N)$, where either N is odd or $4 \mid N$. Then we know $G = (\mathbb{Z}/N)^\times$. If we choose $\sigma = a \in (\mathbb{Z}/N)^\times$, then $C_\sigma = \{a\}$, so by Chebotarev, we see that

$$\delta(p \equiv a \pmod N) = \frac{1}{\phi(N)}.$$

Thus we have recovered a strengthening of Dirichlet's theorem on primes in arithmetic progression!

Remark 5.4.21. The original proof of Chebotarev density does not rely on global Artin reciprocity. Instead, it reduces to the cyclotomic case, where global Artin reciprocity is known explicitly. In fact, Artin's proof of global Artin reciprocity was inspired by Chebotarev's proof (will be reduced to the cyclotomic case).

Example 5.4.22 (Simplest nonabelian example)**.** Let $K = \mathbb{Q}$ and $L = \mathbb{Q}[x]/(x^3 - x^2 + 1)$. This is the cubic extension with minimal $|d_L|$, and here $d_L = -23$. Then $\mathrm{Gal}(\widetilde{L}/\mathbb{Q}) \cong S_3$. Now S_3 has three distinct conjugacy classes $(1), (12), (123)$. These correspond to $f(x)$ splitting completely in $\mathbb{F}_p$, $f(x)$ splitting into a quadratic and a linear factor in $\mathbb{F}_p$, and $f(x)$ being irreducible in $\mathbb{F}_p$, respectively. Now we can compute (possibly using a computer) the table

Table 5.1: Primes in each conjugacy class

σ	p
(1)	$59, \ldots$
(12)	$5, 7, 11, 17, 19, 37, 43, 53, \ldots$
(123)	$2, 3, 13, 29, 31, 41, 47, \ldots$

Chebotarev predicts that the three classes will occur in a ratio of $1 : 3 : 2$.

Remark 5.4.23. There is no simple congruence condition on p to determine Frob_p. However, there is a criterion on p in terms of *modular forms*. For example, for $z \in \mathcal{H}$, we may consider the function

$$\begin{aligned} f(z) &= q \prod_{n \geqslant 1} (1 - q^n)(1 - q^{23n}) && q = e^{2\pi i z} \\ &= \sum_{n \geqslant 1} a_n q^n && a_n \in \mathbb{Z}. \end{aligned}$$

Now some of the coefficients are

Table 5.2: Coefficients at primes

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
a_p	-1	-1	0	0	0	-1	0	0	1	-1	-1	0	-1	0	-1	0	2

So we see that the conjugacy classses corresppond to the coefficients being $2, 0, -1$. In fact, these are the character values for the two-dimensional irreducible representation ρ of S_3. By a miracle, we have $\operatorname{Tr}\rho(\operatorname{Frob}_p) = a_p$!

Remark 5.4.24. Recall that abelian extensions can be understood in terms of the idèle class group using Artin reciprocity. But if we write $\mathbb{I}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q}}^{\times}$, we can consider the idèle class group as a space related to GL_1. But now abelian extensions now correspond to 1-dimensional representations of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and the Langlands program gives a conjectural correspondence between n-dimensional representations of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and automorphic forms on $[GL_n] = GL_n(\mathbb{A}_{\mathbb{Q}})/GL_n(\mathbb{Q})$. For example, when $n = 2$, the 2-dimensional representations correspond to modular forms relating $\operatorname{Tr}\rho(\operatorname{Frob}_p)$ and coefficients a_p of the modular form $f(z)$.

5.5 Brauer groups and proof of global Artin reciprocity

We have already proved the first inequality that $[C_K : \operatorname{Nm}(C_L)] \geqslant [L : K]$, at least when L/K is cyclic. We have also proved the second inequality that $[C_K : \operatorname{Nm}(C_L)] \leqslant [L : K]$ in general.

Corollary 5.5.1 (Global version of Hilbert 90)**.** *Let L/K be finite Galois. Then $H^1(G, C_L) = 0$.*

Proof. We begin in the case when G is cyclic. Here, $[C_K : \operatorname{Nm}(C_L)] = [L : K]$. However, $h(C_L) = \frac{[C_K:\operatorname{Nm}(C_L)]}{|H^1(G,C_L)|} = [L : K]$, so $H^1(G, C_L) = 0$.

Now it remains to reduce the general case to the cyclic case. First, we will consider G solvable and induct on $|G|$. Consider $H \triangleleft G$ such that G/H is cyclic. Then inflation-restriction gives us an exact sequence

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

Now the two outside terms vanish by G/H being cyclic and the inductive hypothesis, so $H^1(G, C_L) = 0$.

Finally, if G is an arbitrary group, we simply consider the restriction to all Sylow subgroups

$$H^1(G, C_L) \xrightarrow{\text{Res}} \prod_p H^1(G_p, C_L) = 0.$$

However, this restriction is injective by a past homework, so we are done. □

Now our goal is to compute the Brauer group $H^2(K)$. We will do this in terms of the local Brauer groups.

Proposition 5.5.2. *The natural restriction map $H^2(L/K) \to \bigoplus_v H^2(L^v/K_v)$ is injective.*

Proof. The short exact sequence

$$0 \to L^{\times} \to \mathbb{I}_L \to C_L \to 0$$

gives a long exact sequence

$$0 \to H^1(G, C_L) \to H^2(G, L^{\times}) \to H^2(G, \mathbb{I}_L).$$

But now from the computation of the cohomology of idèles and the previous corollary, we have an injection

$$H^2(G, L^{\times}) = H^2(L/K) \hookrightarrow H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(L^v/K_v).$$ □

Corollary 5.5.3. *Given $\beta \in H^2(K)$, there exists a cyclic extension L/K with $L \subseteq K(\zeta_m)$ for some m such that β is split by L ($\beta \in H^2(L/K) = \ker(H^2(K) \to H^2(L))$).*

Proof. By the proposition, we know that $\beta \in H^2(K)$ is completely determined by its local restrictions $\{\beta_v\}_v$. We also know that all but finitely many β_v vanish. By local class field theory, we know that $\beta \in H^2(K_v) = \mathbb{Q}/\mathbb{Z}$ (the isomorphism is given by the invariant map). But now there exists $m \geqslant 1$ such that $m \cdot \mathrm{inv}_v(\beta_v) = 0$ for all v. However, by functoriality of inv_v for $w \mid v$, we obtain

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

by one of the homeworks. Once we prove the following lemma, we will be done. □

Lemma 5.5.4. *Let S be a finite set of finite places of K and $m \geqslant 1$. Then there exists a cyclic cyclotomic extension L/K such that $m \mid [L^v : K_v]$ for all $v \in S$.*

Proof. First we reduce to the case $K = \mathbb{Q}$. Here, we can just take the composite with K and replace m with $m \cdot [K : \mathbb{Q}]$. Also, we will reduce to the case where $m = \ell^s$, wheere ℓ is some prime. Here, we can just take the composite of the extensions for all prime power factors of m. We need $\ell^s \mid [L^p : \mathbb{Q}_p]$ for some cyclic cyclotomic extension $L/\mathbb{Q}$. Now

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

Now we can form a cyclic cyclotomic extension

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

Now we can compute for all $p \in S$ that

$$[\mathbb{Q}_p(\zeta_{\ell^r}) : \mathbb{Q}_p] = \begin{cases} \phi(\ell^r) & p = \ell \\ t & p \neq \ell \end{cases}$$

Where t is the smallest integer such that $\ell^r \mid \left|\mathbb{F}_{p^t}^\times\right| = p^t - 1$. In particular, as we increase r, $[\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p] \to \infty$, so $[L^p : \mathbb{Q}_p] \to \infty$ as we increase r, so we may choose $r \gg 0$ such that $\ell^s \mid [L^p : \mathbb{Q}_p]$. □

We have already proved that $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ is surjective, so it remains to show that it factors through $C_K/\mathrm{Nm}(C_L)$. We need to prove that

Theorem 5.5.5. *$K^\times$ is contained in the kernel of $\phi_{L/K}$. This means $\phi_{L/K}(K^\times) = 1$.*

This will imply that the global Artin map is an isomorphism. To prove this, we will use a global relation from Brauer groups.

Theorem 5.5.6. *For all $\beta \in H^2(L/K)$, we have*

$$\beta \in \ker\left(H^2(L/K) \to \bigoplus_v H^2(L^v/K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}\right).$$

Equivalently, $\sum_v \mathrm{inv}_v(\beta) = 0$.

Our strategy will contain the following steps:

0. We will prove Theorem 5.5.5 for $L/K = \mathbb{Q}(\zeta_m)/\mathbb{Q}$.
1. Next, we will prove Theorem 5.5.5 for L/K cyclic cyclotomic.
2. Next, we will prove Theorem 5.5.6 for L/K cyclic cyclotomic.
3. Next, we will prove Theorem 5.5.6 for L/K finite abelian.
4. Finally, we will prove Theorem 5.5.5 for L/K finite abelian.

5.5.1 Step 0 Choose $a \in \mathbb{Q}^\times$. We need to show that $\phi(a) = 1 \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. It suffices to treat the case where $m = \ell^r$ is a prime power, so we compute explicitly $\phi = \prod_p \phi_p$. There are several cases:

1. $p \neq \ell$ is finite. Then p is unramified, so $\phi_p(a) = (\zeta_{\ell^r} \mapsto \zeta_{\ell^r}^{p^s}) = p^s \in (\mathbb{Z}/\ell^r)^\times$, where $a = u \cdot p^s$.
2. $p = \ell$. Here p is ramified, so $\phi_p(a) = (\zeta_{\ell^r} \mapsto \zeta_{\ell^r}^{u^{-1}}) = u^{-1} \in (\mathbb{Z}/\ell^r)^\times$, where $a = u\ell^s$.
3. $p = \infty$. Here, $\phi_\infty(a) = \mathrm{sign}(a) \in \{\pm 1\} = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

To show that $\phi(a) = 1$, it suffices to consider $a = p, \ell, -1$.

1. If $p \neq \ell$, then $\phi_p(p)\phi_\ell(p) = p \cdot p^{-1} = 1$.
2. If $p = \ell$, then $\phi(\ell) = \phi_\ell(\ell) = 1^{-1} = 1$.
3. Finally, $\phi(-1) = \phi_\ell(-1)\phi_\infty(-1) = (-1)^{-1}(-1) = 1$.

5.5.2 Step 1 We will prove the following result. Because we already proved Theorem 5.5.5 for cyclotomic extensions, this will give us the result for cyclic cyclotomic extensions.

Lemma 5.5.7. *If Theorem 5.5.5 holds for L/K, then it also holds for subextensions M/K of L/K and for composites L'/K', where $L' = L \cdot K'$.*

Proof. By functoriality of the local Artin maps, $\phi_{M/K} = \mathbb{I}_K \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(M/K)$. Therefore if $\phi_{L/K}(K^\times) = 1$, $\phi_{M/K}(K^\times) = 1$ also.

For the composites, we use functoriality of the local Artin maps to obtain a commutative diagram

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

But now the desired result follows from diagram chasing with $(K')^\times$. □

5.5.3 Step 3 Every $\beta \in H^2(K)$ is split by a cyclic cyclotomic extension by Corollary 5.5.3. This means there exists L/K cyclic cyclotomic such that $\beta \in H^2(L/K)$. This reduces the finite abelian case to the cyclic cyclotomic case.

5.5.4 Steps 2 and 4 We will relate the global Artin maps with Brauer groups. Recall that $H^2(G,\mathbb{Z}) = H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$. Denote this map by $\delta_\chi \mapsto \chi$. Now the cup product with δ_χ gives us a map $H^0(G,M) \to H^2(G,M)$. If L/K is an extension of local fields, then for $M = L^\times$, we have a commutative diagram

$$\begin{array}{ccc} H^0(G,L^\times) = K^\times & \xrightarrow{\phi_{L/K}} & G = \mathrm{Gal}(L/K) \\ \downarrow \cup\delta_\chi & & \downarrow \chi \\ H^2(G,L^\times) = H^2(L/K) & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

If L/K is an extension of global fields, we consider $M = \mathbb{I}_L$. Then we have a commutative diagram

$$\begin{array}{ccccc} K^\times & \hookrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G = \mathrm{Gal}(L/K) \\ \downarrow \cup\delta_\chi & & \downarrow \cup\delta_\chi & & \downarrow \chi \\ H^2(L/K) & \hookrightarrow & H^2(G,\mathbb{I}_L) = \bigoplus_v H^2(L^v/K_v) & \xrightarrow{\sum \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z}. \end{array} \tag{5.1}$$

5.5.5 Step 2 Assume that Theorem 5.5.5 holds for L/K cyclic cyclotomic. Then the top row is trivial, so because G is cyclic, the bottom row is also trivial (in the cyclic case, the shift in degree map is an isomorphism). But this means that $\beta \in H^2(L/K)$ satisfies $\sum \mathrm{inv}_v(\beta) = 0$, which is the same thing as Theorem 5.5.6 holding for L/K cyclic cyclotomic.

5.5.6 Step 4 Assume that Theorem 5.5.6 holds for L/K finite abelian. But this means the bottom row of (5.1) is trivial, so in particular, $\chi(\phi_{L/K}(K^\times)) = 0$. But χ is arbitrary in $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$, so $\phi_{L/K}(K^\times) = 1$. This gives Theorem 5.5.5 for all finite abelian extensions.

5.5.7 Brauer groups As a consequence of global Artin reciprocity, we can determine the Brauer group of an arbitrary number field.

Theorem 5.5.8. *Let K be a number field. Then*

$$H^2(K) = \ker\left(\bigoplus_v H^2(K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}\right).$$

Proof. By Theorem 5.5.6, we know that $H^2(K)$ is contained in the kernel. It remains to prove the reverse inclusion. Consider $(\beta_v) \in \ker$. We know there exists L/K cyclic cyclotomic such that $(\beta_v)_v \in \bigoplus_v H^2(L^v/K_v)$. Because L/K is cyclic, we have an isomorphism of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^\times/\mathrm{Nm}(L^\times) & \longrightarrow & \mathbb{I}_K/\mathrm{Nm}(\mathbb{I}_L) & \longrightarrow & C_K/\mathrm{Nm}(C_L) & \longrightarrow & 0 \\ & & \downarrow \cup\delta_\chi & & \downarrow \cup\delta_\chi & & \downarrow \sim & & \\ 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(G,\mathbb{I}_L) = \bigoplus_v H^2(L^v/K_v) & \xrightarrow{\sum_v \mathrm{inv}_v} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & 0. \end{array}$$

By definition, the top row is exact, so the bottom row is also exact. But this means that for $(\beta_v) \in \ker(\sum \mathrm{inv}_v)$, there exists $\beta \in H^2(L/K)$ such that $(\beta_v) = \beta$. □

Example 5.5.9. Consider $K = \mathbb{Q}$. Then we have a map

$$H^2(\mathbb{Q}) = \{\text{central simple algebras } B/\mathbb{Q}\} \to \bigoplus_v H^2(K_v) = \{(B_v) \mid B_v \text{ CSA over } \mathbb{Q}_v\}.$$

This is given by $B_v = B \otimes \mathbb{Q}_v$. Now by the theorem, we note that $(B_v)_v$ comes from $B/\mathbb{Q}$ if and only if $\sum \mathrm{inv}_v(B_v) = 0$. For example, we have

$$\mathrm{inv}_v(B_v) = \begin{cases} 0 & B_v = M_2(\mathbb{Q}_v) \\ \frac{1}{2} & B_v \text{ is quaternion algebra.} \end{cases}$$

This means that quaternion algebras B/Q are in bijection with the set of $(B_v)_v$ where an even number of B_v are not $M_2(\mathbb{Q}_v)$.

5.6 Proof of global existence

We will now complete the proof of global class field theory. We need to prove the following statement:

Theorem (Global existence)**.** *For any finite index open subgroup $U \subseteq C_K$, there exists a finite abelian extension L/K such that $U = \mathrm{Nm}(C_L)$.*

Definition 5.6.1. A subgroup of C_K is a *norm subgroup* if it is of the form $\mathrm{Nm}(C_L)$ for some finite abelian extension L/K.

Now global existence is the same thing as every finite index open subgroup being a norm subgroup.

Lemma 5.6.2. *Any subgroup containing a norm subgroup is also a norm subgroup.*

Proof. Assume $U = \mathrm{Nm}(C_L)$ and $V \supseteq U$. Then global Artin reciprocity implies that $C_K/U \simeq \mathrm{Gal}(L/K)$. Now we have a commutative diagram

$$\begin{array}{ccc} C_K/U & \xrightarrow{\sim} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ C_K/V & \xrightarrow{\sim} & \mathrm{Gal}(M/K) \end{array}$$

by the fundamental theorem of Galois theory. By construction, $V = \ker(C_K \to \mathrm{Gal}(M/K))$, so in particular, $V = \mathrm{Nm}(C_M)$ by global Artin reciprocity. □

Now it suffices to produce a enough norm subgroups such that every finite index open subgroup contains a norm subgroup. Here, we will use Kummer extensions. Let K be a field and $\mu_n \subseteq K$. Then if L_n is the maximal abelian extension of K with exponent n, then by considering the Kummer sequence

$$1 \to \mu_n \to (K^{\mathrm{sep}})^\times \to (K^{\mathrm{sep}})^\times \to 1$$

we obtain a perfect pairing $\mathrm{Gal}(L_n/K) \otimes K^\times/(K^\times)^n \to \mu_n$ given by $(\sigma, b) \mapsto \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$. This gives a bijection between finite subgroups of $K^\times/(K^\times)^n$ and finite abelian extensions of K of exponent n. Here, to a subgroup B, we associate field $L = K(\sqrt[n]{B})$ given by adjoining all n-th roots of elements in B and to an extension L/K we simply take the n-th powers of all elements in $L^\times$. Here, it is easy to see that $|B| = [L : K]$.

Example 5.6.3. Let K be a local field and assume $\mu_n \subseteq K$. Then L_n/K is finite and

$$[L_n : K] = \left|K^\times/(K^\times)^n\right| = \frac{n^2}{|n|_K}.$$

Here, we know $K^\times = \mathcal{O}_K^\times \times \mathbb{Z}$, so $K^\times/(K^\times)^n = \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n \times \mathbb{Z}/n$. Because $\mathcal{O}_K^\times$ contains a finite index subgroup isomorphic to $\mathcal{O}_K$, we have $\left|\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n\right| = \left|\mu_n(\mathcal{O}_K^\times)\right| \cdot |\mathcal{O}_K/n\mathcal{O}_K| = n\frac{1}{|n|_K}$, as desired.

Now assume K is a number field.

Lemma 5.6.4. *Assume $\mu_n \subseteq K$. Assume that $S \supseteq S_\infty \cup \{v \mid n\}$. Assume S is large enough so that $\mathbb{I}_K = K^\times \cdot \mathbb{I}_{K,S}$. Let $a \in K^\times$ such that $a \in (K_v^\times)^n$ for all $v \in S$ and $a \in U_v$ for all $v \notin S$. Then $a \in (K^\times)^n$.*

Proof. Let $L = K(\sqrt[n]{a})$. Then we see that $L^v = K_v$ for all $v \in S$ and L^v/K_v is unramified for all $v \notin S$. By local class field theory, in the first case we have $\mathrm{Nm}((L^v)^\times) = K_v^\times$, and in the second case $\mathrm{Nm}(U^v) = U_v$. Therefore $\mathrm{Nm}(\mathbb{I}_L) \supseteq \mathbb{I}_{K,S}$, so $K^\times \mathrm{Nm}(\mathbb{I}_L) \supseteq K^\times \mathbb{I}_{K,S} = \mathbb{I}_K$, and therefore $\mathrm{Nm}(C_L) \supseteq C_K$, so $L = K$. □

Proposition 5.6.5. *Assume $\mu_n \subseteq K$. Let $U \subseteq C_K$ be a finite index open subgroup and assume C_K/U has exponent n. Then U is a norm subgroup.*

Proof. Let $S \supseteq S_\infty \cup \{v \mid n\}$ and

$$E \coloneqq \prod_{v \in S} (K_v^\times)^n \prod_{v \notin S} U_v \subseteq \mathbb{I}_K.$$

Then let $V \coloneqq K^\times \cdot E/K^\times \subseteq C_K$. Because C_K/U has exponent n, we know $U \supseteq V$ for S sufficiently large. It remains to show that V is a norm subgroup. Enlarging S we may assume that $\mathbb{I}_K = K^\times \mathbb{I}_{K,S}$.

Let $U(S) = K^\times \cap \mathbb{I}_{K,S}$ be the S-units. By the previous lemma, $K^\times \cap E = U(S) \cap E = U(S)^n$. Set $L = K(\sqrt[n]{U(S)})$. This is a finite abelian extension of exponent n unramified away from S. By local class field theory, we know $\mathrm{Nm}((L^v)^\times) \supseteq (K_v^\times)^n$ for all $s \in S$ and $\mathrm{Nm}(U^v) = U_v$ for all $v \notin S$. But now $E \subseteq \mathrm{Nm}(\mathbb{I}_L)$ and thus $\mathrm{Nm}(C_L) \supseteq V$. Now we show that $\mathrm{Nm}(C_L) = V$.

We will show that $[C_K : \mathrm{Nm}(C_L)] = [C_K : V]$. But now we have

$$\begin{aligned}
[C_K : V] &= [\mathbb{I}_K : K^\times \cdot E] \\
&= [K^\times \cdot \mathbb{I}_{K,S} : K^\times \cdot E] \\
&= \frac{[I_{K,S} : E]}{[K^\times \cap \mathbb{I}_{K,S} : K^\times \cap E]}
\end{aligned}$$

Now we compute

$$\begin{aligned}
[\mathbb{I}_{K,S} : E] &= \prod_{v \in S} [K_v^\times : (K_v^\times)^n] \\
&= \prod_{v \in S} \frac{n^2}{|n|_v} \\
&= n^{2|S|}.
\end{aligned}$$

We also compute

$$\begin{aligned}[K^\times \cap \mathbb{I}_{K,S} : K^\times \cap E] &= [U(S) : U(S)^n] \\ &= \left|(\mathbb{Z}/n)^{|S|}\right| \\ &= n^{|S|}\end{aligned}$$

by Dirichlet's unit theorem. Thus $[C_K : V] = n^{|S|}$. On the other hand, we have

$$\begin{aligned}[C_K : \mathrm{Nm}(C_L)] &= [L : K] \\ &= \left|U(S) \cdot (K^\times)^n / (K^\times)^n\right| \\ &= \left|U(S)/U(S) \cap (K^\times)^n\right| \\ &= |U(S)/U(S)^n| \\ &= n^{|S|}\end{aligned}$$

using Kummer theory and the Dirichlet unit theorem. This implies that $V = \mathrm{Nm}(C_L)$. □

To finish the proof of global existence, we reduce to the case of Kummer extensions.

Lemma 5.6.6. *Let $U \subseteq C_K$ be a finite index open subgroup and $V = \mathrm{Nm}^{-1}_{K'/K}(U)$ for some finite extension K'/K. If V is a norm subgroup, then so is U.*

Proof. Write $V = \mathrm{Nm}_{L/K'}(C_L)$ for some finite abelian L/K'. Now let M be the maximal abelian subextension of L/K. Then

$$\mathrm{Nm}_{M/K}(C_M) = \mathrm{Nm}_{L/K}(C_L) = \mathrm{Nm}_{K'/K}(\mathrm{Nm}_{L/K'}(C_L)) = \mathrm{Nm}_{K'/K}(V) \subseteq U.$$

Therefore U is a norm subgroup. □

We are now able to complete the proof of global existence. We will induct on $[C_K : U]$ and assume $p \mid [C_K : U]$. If $\mu_p \subseteq K$, choose $U_1 \subseteq C_K$ containing U such that $[C_K : U_1] = p$. Then U_1 is a norm subgroup, so write $U_1 = \mathrm{Nm}(C_L)$. Now $\mathrm{Nm}_{L/K} \colon C_L \to C_K/U$ has image U_1/U with kernel $V \coloneqq \mathrm{Nm}^{-1}_{L/K}(U)$. Then $[C_L : V] = |U_1/U| = \frac{[C_K:U]}{p}$, and by the inductive hypothesis, V is a norm subgroup, so U is also a norm subgroup.

If $\mu_p \not\subseteq K$, then take $K' = K(\mu_p)$. Now $U' = \mathrm{Nm}^{-1}_{K'/K}(U)$. Then U' is a norm subgroup by the above, so by the lemma, U is also a norm subgroup.

5.7 Primes of the form $x^2 + ny^2$

In this section we discuss a classical application of class field theory. This was discussed at the beginning of these notes. Recall that if $K = \mathbb{Q}(\sqrt{d})$ with discriminant d_K, then the splitting behavior of

$$(p) = \begin{cases} \mathfrak{p}_1\mathfrak{p}_2 & \left(\frac{d_K}{p}\right) = 1 \\ \mathfrak{p} & \left(\frac{d_K}{p}\right) = -1 \\ \mathfrak{p}^2 & p \mid d_K \end{cases}$$

is determined by the Legendre symbol $\left(\frac{d_K}{p}\right)$.

Example 5.7.1. Consider $K = \mathbb{Q}(\sqrt{-1})$ with $d_K = 4$. Then p splits in K if and only if $\left(\frac{-4}{p}\right) = 1$, which is equivalent to $\left(\frac{-1}{p}\right) = 1$, is equivalent to $p \equiv 1 \pmod 4$ by basic arithmetic.

On the other hand, $\mathcal{O}_K = \mathbb{Z}[i]$ is a PID, so p splits in K if and only if $p = (x+iy)(x-iy)$, which is equivalent to $p = x^2 + y^2$ for integers $x, y \in \mathbb{Z}$. Combining the two equivalences, we see that $p = x^2 + y^2$ if and only if $p \equiv 1 \mod 4$.

Example 5.7.2. Consider $K = \mathbb{Q}(\sqrt{-5})$ with $d_K = -40$. Then p splits in K if and only if $\left(\frac{-5}{p}\right) = 1$, and by quadratic reciprocity this is equivalent to $p \equiv 1, 3, 7, 9 \pmod{20}$. However, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is no longer a PID, so we have a different criterion for $p = x^2 + 5y^2$.

Theorem 5.7.3. *If $p \neq 2, 5$, then $p = x^2 + 5y^2$ if and only if $p \equiv 1, 9 \pmod{20}$.*

Some examples are given below.

Table 5.3: Primes of the form $x^2 + 5y^2$

p	(x, y)
29	$(3, 2)$
41	$(6, 1)$
61	$(4, 3)$
89	$(3, 4)$

Similarly, we have

Theorem 5.7.4. *If $p \neq 2, 3$, then $p = x^2 + 6y^2$ if and only if $p \equiv 1, 7 \pmod{24}$.*

Some examples are given below.

Table 5.4: Primes of the form $x^2 + 6y^2$

p	(x, y)
7	$(1, 1)$
31	$(5, 1)$
73	$(7, 2)$

Our goal is to explain the proof of these results using class field theory.

Lemma 5.7.5. *Let $\mathfrak{p}$ be a finite prime for a number field K. Then $\mathfrak{p}$ is principal if and only if $\mathfrak{p}$ splits completely in H_K, where H_K is the Hilbert class field of K.*

Proof. By global Artin reciprocity, $\mathrm{Cl}_K \cong \mathrm{Gal}(H_K/K)$. But then $\mathfrak{p}$ is principal if and only if $[\mathfrak{p}] \in \mathrm{Cl}_K$ is trivial. However, this is equivalent to $\mathrm{Frob}_{\mathfrak{p}}$ being trivial, which is equivalent to p splitting completely in H_K. □

Proposition 5.7.6.

1. *If $p \neq 2, 5$, then $p = x^2 + 5y^2$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.*
2. *If $p \neq 2, 3$, then $p = x^2 + 6y^2$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-6}, \sqrt{-3})$.*

Proof.

1. If $p \neq 2, 5$, then $p = x^2 + 5y^2$ if and only if $(p) = \mathfrak{p}_1\mathfrak{p}_2$ splits as a product of principal ideals in $K = \mathbb{Q}(\sqrt{-5})$. By the lemma, this is equivalent to $\mathfrak{p}_1, \mathfrak{p}_2$ splitting completely in $H_K = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$, and combining, we see this is equivalent to p splitting completely in H_K.
2. This is the same argument, except $H_K = \mathbb{Q}(\sqrt{-6}, \sqrt{-3})$ when $K = \mathbb{Q}(\sqrt{-6})$. □

Therefore, to prove the main theorems, it remains to prove the following result.

Proposition 5.7.7.

1. p *splits completely in* $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ *if and only if* $p \equiv 1, 9 \pmod{20}$.
2. p *splits completely in* $\mathbb{Q}(\sqrt{-6}, \sqrt{-3})$ *if and only if* $p \equiv 1, 7 \pmod{20}$.

The key to this result is that in these cases, $H_K/\mathbb{Q}$ is an abelian extension, so we may apply global Artin reciprocity. Recall that for $\mathbb{Q}$, $\mathrm{Cl}_{(N)\cdot\infty} = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N)^\times$. Then under the Artin reciprocity map, $p \equiv 1 \pmod{N}$ if and only if p splits completely in $\mathbb{Q}(\zeta_N)$.

Example 5.7.8. When $N = 4$, we have $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, so we recover the result that $p \equiv 1 \pmod{4}$ if and only if p splits in $\mathbb{Q}(i)$.

More generally, the global existence theorem gives a bijection between finite index open subgroup of $C_\mathbb{Q}$ and finite abelian extensions of $\mathbb{Q}$. In particular, we obtain a bijection between finite subgroups of $(\mathbb{Z}/N)^\times$ and finite abelian subextensions $K/\mathbb{Q}$ of $\mathbb{Q}(\zeta_N)$. This is given by $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/N)^\times/H$. Thus we see that $p \in H$ if and only if p splits completely in K.

Example 5.7.9. Let $N = 5$. Then $(\mathbb{Z}/5)^\times \cong \mathbb{Z}/4$, and so the possibilities for H are $H = \{1\}, \{\pm 1\}, (\mathbb{Z}/5)^\times$. Clearly the trivial subgroup corresponds to $\mathbb{Q}(\zeta_5)$ and $(\mathbb{Z}/5)^\times$ corresponds to $\mathbb{Q}$, and $\{\pm 1\}$ corresponds to $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$. By global class field theory, this is the only abelian subextension $K/\mathbb{Q}$ of $\mathbb{Q}(\zeta_5)$.

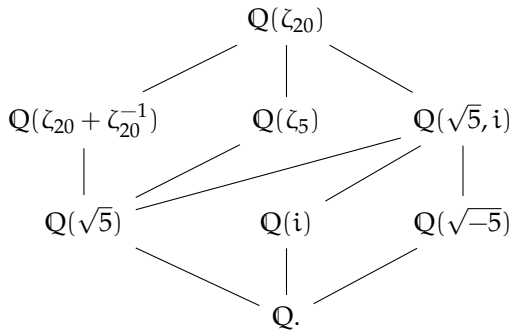
Note that because quadratic extensions are abelian, every quadratic extension is contained in a cyclotomic extension. For example, $\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$.

Example 5.7.10. Consider $N = 20$. Then $(\mathbb{Z}/20)^\times \cong \mathbb{Z}/4 \times \mathbb{Z}/2$. Now the subgroups and corresponding subextensions are given below.

Table 5.5: Subgroups and subfields

$H \subseteq (\mathbb{Z}/20)^\times$	K
$\{1\}$	$\mathbb{Q}(\zeta_{20})$
$\{\pm 1\}$	$\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$
$\{1, 11\}$	$\mathbb{Q}(\zeta_5)$
$\{1, 9, 11, 19\}$	$\mathbb{Q}(\sqrt{5})$
$\{1, 9, 13, 17\}$	$\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$
$\{1, 9\}$	$\mathbb{Q}(\sqrt{5}, \sqrt{i})$
$\{1, 3, 7, 9\}$	$\mathbb{Q}(\sqrt{-5})$
$(\mathbb{Z}/20)^\times$	$\mathbb{Q}$

This gives us the following diagram of field extensions:



In particular, we see that $p \equiv 1, 9 \pmod{20}$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$.

Example 5.7.11. When $N = 24$, then $(\mathbb{Z}/24)^\times = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. Then we see that $\mathbb{Q}(\sqrt{-6})$ corresponds to $\{1, 5, 7, 11\}$ and $\mathbb{Q}(\sqrt{-3})$ corresponds to $\{1, 7, 13, 23\}$, so $\mathbb{Q}(\sqrt{-6}, \sqrt{-2})$ corresponds to $\{1, 7\}$. Therefore $p \equiv 1, 7 \pmod{24}$ if and only if p splits completely in $\mathbb{Q}(\sqrt{-6}, \sqrt{-3})$.

Remark 5.7.12. When $K/\mathbb{Q}$ is abelian, class field theory gives us a congruence condition for primes splitting completely in K. On the other hand, when $K/\mathbb{Q}$ is nonabelian, then such a congruence condition does not exist.

Lemma 5.7.13. *Denote by* $\mathrm{Spl}(L/K)$ *to be the set of primes* $\mathfrak{p}$ *of* K *splitting completely in* L. *Then* $L_1 \subseteq L_2$ *if and only if* $\mathrm{Spl}(L_1/K) \supseteq \mathrm{Spl}(L_2/K)$. *In particular,* $L_1 = L_2$ *if and only if* $\mathrm{Spl}(L_1/K) = \mathrm{Spl}(L_2/K)$.

Proof. One direction is clear. In the other direction, suppose $\mathrm{Spl}(L_1/K) \supseteq \mathrm{Spl}(L_2/K)$. Then $\mathrm{Spl}(L_1L_2/K) \supseteq \mathrm{Spl}(L_2/K)$. But now Chebotarev density tells us that $[L_1L_2 : K] \leqslant [L_2 : K]$, and this is only possible if $L_1L_2 = L_2$, which means $L_1 \subseteq L_2$. □

Proposition 5.7.14. *If* $K/\mathbb{Q}$ *is nonabelian, then there does not exist a congruence condition for* p *splitting completely in* K.

Proof. If there exists such a congruence condition, then choose $p \in \mathrm{Spl}(K(\zeta_N)/\mathbb{Q})$. Thus $p \in \mathbb{Q}(\zeta_N/\mathbb{Q})$, and therefore $p \equiv 1 \pmod{N}$. By the criterion, $\{p \equiv 1 \pmod{N}\} \subseteq \mathrm{Spl}(K/\mathbb{Q})$. But this means that $\mathrm{Spl}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \subseteq \mathrm{Spl}(K/\mathbb{Q})$, so $\mathbb{Q}(\zeta_N) \supseteq K$. This implies $K/\mathbb{Q}$ is abelian. □

Example 5.7.15. If $K = \mathbb{Q}(\sqrt{-14})$, then $\mathrm{Cl}_K = \mathbb{Z}/4$, so $H_K = \mathbb{Q}(\sqrt{2\sqrt{2}-1})$ with $\mathrm{Gal}(H_K/\mathbb{Q}) \cong D_4$. Thus there is no congruence condition for $p = x^2 + 14y^2$.

Remark 5.7.16. Even though there is no congruence condition, non-abelian reciprocity gives us a condition using coefficients of modular forms.