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

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

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 $|x + y| \leq |x| + |y|$.

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

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

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 $|nx| \leq |x|$ 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

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

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

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

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

Definition 2.1.7. An absolute value $|-|$ is *discrete* if $|K^\times| \subset \mathbb{R}$ 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. $A := \{a \in K \mid |a| \leq 1\}$. 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

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

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 v is a complex place it corresponds to a pair of complex embeddings $\sigma, \overline{\sigma}$, so we define

$$|x|_v := |\sigma(x)|^2$$

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

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*

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

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 $N \geq 1$ 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 $K_v := (K, |-|_v)$. When v is a finite place, denote by $\mathcal{O}_{K_v} = \mathcal{O}_{K,v} = \mathcal{O}_v$ the valuation ring $\{x \in K_v \colon |x| \leq 1\} \subseteq K_v$. 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 $x = \sum_{i \geq k} a_i p^i$, 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*
$$|\beta|_L = |N_{L/K}(\beta)|_K^{1/n}.$$

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

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 $\overline{f}(x) = f(x) \mod \mathfrak{p} \in A/\mathfrak{p}[x] = k[x]$ must satisfy $\overline{f}(x) = h(x)^m$ 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
   $$A[\beta]/\mathfrak{p}A[\beta] = A[x]/(\mathfrak{p}, f(x)) = k[x]/(\overline{f}(x)) = k[x]/(h(x))^m$$
   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 $a_i := \lim_{k\to\infty} a_{i.k} \in K$ 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
   $$|N_{L/K}(\beta)|_K = |N_{L/K}|_{\widetilde{L}} = \prod_{\sigma\colon L\to\widetilde{L}} |\sigma(\beta)|_{\widetilde{L}} = \prod_{\sigma\colon L\to\widetilde{L}} |\beta|_L = |\beta|_L^n,$$
   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 $e \geq 1$ such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e$. Next, define the *residual degree* $f(L/K)$ to be $f \geq 1$ 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 $\deg \overline{f} = \deg f = [K(\alpha) : K] \leq [L : K]$. But then we know that $\deg \overline{f} \geq [k(\alpha_0) : k] = [\ell : k] = [L : K]$. 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*

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

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 $n \geq 1$ 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 $\mathrm{Frob}_{L/K}(\alpha) \equiv \alpha^q \pmod{p_L}$ 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 $e(L/K) \geq n$ 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 $|L^\times|/|K^\times|$. 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 $\mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ 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

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

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

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

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

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

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, $\mathrm{Gal}(K^{\mathrm{ab}}/K) = G/\overline{[G,G]} =: G^{\mathrm{ab}}$, where $G = \mathrm{Gal}(\overline{K}/K)$.

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

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

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

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

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 $K^\times \xrightarrow{\phi_K} \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

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*

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

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*

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

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:

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

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

Proposition 2.7.13. *We have an isomorphism $\widehat{K}^\times \cong \mathcal{O}_K^\times \times \widehat{Z}$ 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 $(q + \mathfrak{p}_k^m) \times \pi^{n\mathbb{Z}}$ for some $m, n \geq 1$. 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 $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$ as topological groups for any choice of uniformizer π. Therefore, we have a decomposition $K^{\mathrm{ab}} = K_\pi \cdot K^{\mathrm{ur}}$, where $K_\pi = (K^{\mathrm{ab}})^{\phi_K(\pi)}$ and $K^{\mathrm{ur}} = (K^{\mathrm{ab}})^{\phi_K(\mathcal{O}_K^\times)}$ 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

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

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 $r \geq 0$ 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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & & \\ & & & & & & \searrow & & \\ & & H^1(G, A) & \longrightarrow & H^1(G, B) & \longrightarrow & H^1(C, G) & \longrightarrow & \cdots \end{array}$$

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

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

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

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

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

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

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

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

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

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

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

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

Then we have an explicit cochain description

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

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

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

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

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

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

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

Such functions are usually called *crossed homomorphisms*.

On the other hand, we have

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

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.

Definition 3.1.16. 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 3.1.17. For any $M \in \mathsf{Mod}_G$, we have $\mathrm{Ind}_G^G M = M$.

Definition 3.1.18. 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 3.1.19.

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

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

   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 3.1.20 (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 $r \geq 0$.*

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 3.1.21. 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 3.1.22. *If M is induced, then for all $r \geq 1$, $H^r(G, M) = 0$.*

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 3.1.23. Suppose $r = 0$. Then the functors are

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

Proposition 3.1.24. *The map* $\mathrm{Cor}\circ\mathrm{Res}\colon H^r(G,M) \to H^r(H,M) \to H^r(G,M)$ *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 3.1.25. *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 3.1.26. *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 3.1.27 (Inflation-restriction exact sequence)**.** *There is an exact sequence*

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

Proof. We will check this by hand.

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

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

is a coboundary. Thus there exists $m \in M$ such that $\mathrm{Inf}(\varphi)(g) = gm - m$ 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 3.1.28 (Inflation-restriction, general case)**.** *Let $r \geq 1$. Assume $H^i(H, M) = 0$ for all $1 \leq i < r$. 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 $i \geq 1$. 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 $i \geq 1$. 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 $i \geq 1$.

Now, by assumption, we have $H^i(H, M) = 0$ for all $1 \leq i \leq r-1$. Therefore, $H^i(H, M') = 0$ for all $1 \leq i \leq r-2$ 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 3.1.29. 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 $r \geq 1$.

Remark 3.1.30. 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.

3.2 Group Homology

Definition 3.2.1. Define the *G-coinvariants* of M by

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

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

Definition 3.2.2. 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 3.2.3. Define the *group homology* by

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

to be the left derived functor of $M \mapsto M_G$.