# Algebraic Number Theory

# Introduction

These are notes I wrote up from my study of algebraic number theory and class field theory.

## Algebraic number theory

This material is from 18.786 (Algebraic Number Theory, Fall 2011), Neukirch [11], Lang [8], Milne [10], and Serre [14]. The chapter on quadratic forms follows Cox [5]. Some of the sections are incomplete or not edited (in particular, Chapter 9).

## Class field theory

These are notes from my reading course on class field theory with Sug Woo Shin (Spring 2012). I first give an introduction to class field theory that encompasses the different formulations found in the literature (for instance, global class field theory using ideals and ideles). Next I develop the theory of group cohomology and some Galois cohomology, to be used in the proofs. The material on group cohomology mainly follows Rotman [12], and follows Atiyah-Wall in [3] and Serre [14] in some places. For the proofs of local class field theory, I follow Serre [14] pretty closely, including the abstractions on class formations. For the proofs of global class field theory, I follow Tate's article in [3] and Milne's book [9]. Finally, because class field theory is a very abstract subject and one should not lose sight of what it is used for, I include a chapter on its applications: the proof of quadratic, cubic, and biquadratic reciprocity, Hasse-Minkowski, splitting of primes, and so forth. This chapter follows exercises in Cassels-Frohlich [3], Cox's "Primes of the form $x^2 + ny^2$ [5], and Dalawat's survey article [6]. I give a rough idea of how class field theory fits in with the Langlands program. In the last chapter, I veer off in a slightly different direction, establishing the Main Theorem of Complex Multiplication for elliptic curves, highlighting the uses of class field theory along the way. The last chapter is based off Chapter 2 of Silverman [17]; the course 18.783 (Elliptic curves, Spring 2012) also helped a great deal.

Due to time constraints, I have had to omit some proofs, most notably Tate's Theorem in group cohomology and the existence theorem in global class field theory. I include references for the omissions. The prerequisites for these notes are encompassed by the preceding section on algebraic number theory, except for some basic theory of $L$-functions, and the basic theory of elliptic curves, required for the last chapter.

In the future, time allowing, I may fill in missing proofs and add a section on Lubin-Tate Theory.

## Contact

These notes (and others) will be made available on my website at `http://web.mit.edu/~holden1/www/math/notes.htm`. Please email corrections and suggestions to me at holden1@mit.edu.

# Contents

# Part I

# Algebraic Number Theory

# Chapter 1
# Rings of integers

ring-of-integers When we have a field extension $L$ of $\mathbb{Q}$, we would like to define a ring of integers for $L$, with properties similar to the ring $\mathbb{Z} \subseteq \mathbb{Q}$. We will define this ring of integers in a slightly more general context.

## §1 Integrality

**Definition 1.1:** Let $A$ be an integral domain and $L$ a field containing $A$. An element of $x \in L$ is **integral** over $A$ if it is the zero of a monic polynomial with coefficients in $A$:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,\ n \geq 1,\ a_0, \ldots, a_{n-1} \in A.$$

The **integral closure** of $A$ in $L$ is the set of elements of $L$ integral over $A$.

**Example 1.2:** The integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is simply $\mathbb{Z}$ itself (we see this more generally in Proposition 1.8). Thus, integral closure generalizes the notion of what it means to be an "integer" in other number fields. As we will see in Example 4.7, for $d$ squarefree, the integral closure of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$ when $d \equiv 3 \pmod 4$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \equiv 1 \pmod 4$. Algebra is much nicer in integral extensions—which is why, for instance, we would study $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ rather than just $\mathbb{Z}[\sqrt{-3}]$.

**Theorem 1.3:** Let $L$ be a field containing the ring $A$. Then the elements of $L$ integral over $A$ form a ring.

*Proof.* We give two proofs. We need to show that if $a, b$ are algebraic over $A$ then so are $a + b$ and $ab$.
Proof 1: Let $p, q$ be the minimal polynomials of $a, b$, let $a_1, \ldots, a_k$ be the conjugates of $a$ and $b_1, \ldots, b_l$ be the conjugates of $b$. The coefficients of

$$\prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (x - (a_i + b_j)), \qquad \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (x - (a_i b_j))$$

are symmetric in the $a_i$ and symmetric in the $b_j$ so by the Fundamental Theorem of Symmetric Polynomials can be written in terms of the elementary symmetric polynomials in the

$a_i$ and in the $b_j$, with coefficients in $A$. By Vieta's Theorem these are expressible in terms of the coefficients of $p, q$, which are in $A$. Hence these polynomials have coefficients in $A$. They have $a+b, ab$ as roots, as desired.

Proof 2: We use the following lemma.

**Lemma 1.4** (Criterion for integrality)**:** criterion-for-integrality An element $\alpha \in L$ is integral over $A$ if and only if there exists a nonzero finitely generated $A$-submodule of $L$ such that $\alpha M \subseteq M$. If so, then we can take $M = A[\alpha]$.

**Example 1.5:** For example, $\frac{1}{\sqrt{2}}$ fails this criterion over $\mathbb{Z}$—multiplying by it has the effect of making $M$ "finer." $\sqrt{2}$, however, is integral.

In the case $A = \mathbb{Z}$ and $B = \mathbb{Q}$, $a \in \mathbb{Q}$ is integral over $\mathbb{Z}$ iff $a \in \mathbb{Z}$. Indeed, $a \in \mathbb{Z}$ satisfies $x - a$, and if $a \notin \mathbb{Z}$, then powers of $a$ contain arbitrarily large denominators so $\mathbb{Z}[\alpha]$ is not finitely generated.

*Proof.* $\Rightarrow$: If $\alpha$ satisfies a monic polynomial of degree $n$, then $A[\alpha]$ is generated by $1, \alpha, \ldots, \alpha^{n-1}$.

$\Leftarrow$: Suppose $M$ is generated by $v_1, \ldots, v_n$. Then we can find a matrix $T$ with coefficients in $A$ such that

$$\alpha \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = T \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}.$$

Since $v_1, \ldots, v_n \neq 0$, $\alpha I - T$ is singular, and $\det(\alpha I - T) = 0$. This gives a monic polynomial equation satisfied by $\alpha$. $\square$

Now for $\alpha, \beta \in L$ and let $M = A[\alpha]$ and $N = A[\beta]$. Note

1. if $M, N$ are finitely generated by $\{\alpha_i\}$ and $\{\beta_j\}$, then $MN$ is finitely generated by $\{\alpha_i \beta_j\}$.
2. $\alpha\beta MN \subseteq MN$ and $(\alpha + \beta)MN \subseteq MN$.

Hence $\alpha\beta$ and $\alpha + \beta$ are integral over $A$ by Lemma 1.4 as needed. $\square$

For the rest of this chapter, $A$ is an integral domain, $K$ is its fraction field, $L$ is an extension of $K$, and $B$ is the integral closure of $A$ in $L$.

$$\text{aklb} \quad \begin{tikzcd} L \arrow[r, dash] \arrow[d, dash] & B \arrow[d, dash] \\ K \arrow[r, dash] & A \end{tikzcd} \tag{1.1}$$

**Definition 1.6:** $A$ is **integrally closed** or **normal** if its integral closure in $K = \mathrm{Frac}(A)$ is itself.

**Proposition 1.7:** If $L$ is algebraic over $K$ then every element of $L$ can be written as $\frac{b}{a}$ where $b \in B$ and $a \in A$. Thus $L = \text{Frac}(B)$. In particular, for any extension $L/\mathbb{Q}$, $\text{Frac}(\mathscr{O}_L) = L$.

*Proof.* Given $\alpha \in L$, suppose that it satisfies the equation

$$P(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $a_0, \ldots, a_n \in K$ and $a_n \neq 0$. Since $\text{Frac}(A) = K$, by multiplying by an element of $A$ as necessary we may assume $a_0, \ldots, a_n \in A$. Then

$$a_n^{n-1} P\left(\frac{x}{d}\right) := x^n + a_{n-1}x^{n-1} + a_n a_{n-2} x^{n-2} + \cdots + a_n^{n-1} a_0.$$

Hence $a_n \alpha$ is integral over $A$, i.e. $a_n \alpha \in B$. This shows $\alpha$ is in the desired form.

For the last part, take $K = \mathbb{Q}$ and $A = \mathbb{Z}$. $\square$

For short we call (1.1) the "AKLB" setup if we further assume $A$ is integrally closed in $K$. In the usual case, $A$ is the integral closure of $\mathbb{Z}$ in $K$. in this case, we write $A = \mathscr{O}_K$.[1]

When $F = \overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, $a \in \overline{\mathbb{Q}}$ is called an algebraic number and $a \in \mathscr{O}_{\mathbb{Q}}$ is an algebraic integer.

**Theorem 1.8** (Rational Roots Theorem)**:** rational-roots-thm A UFD is integrally closed.

*Proof.* Suppose $R$ is a UFD with field of fractions $K$. Let $x \in K$ be integral over $R$; suppose $x$ satisfies

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

where $a_0, \ldots, a_{n-1} \in R$. Write $x = \frac{p}{q}$ where $p, q \in R$ are relatively prime. Then multiplying the above by $q^n$ gives

$$\begin{aligned} p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n &= 0 \\ q(a_{n-1}p^{n-1} + \cdots + a_0 q^{n-1}) &= -p^n \end{aligned}$$

Thus $q \mid p$, possible only if $q = 1$. This shows $x \in R$. $\square$

Note that in the definition of integrality, an element is integral if it is the zero of *any* monic polynomial in $A[x]$. However, it suffices to check that its *minimal* polynomial is in $A[x]$.

**Proposition 1.9:** integral-min-poly Let $L$ be an algebraic extension of $K$ and $A$ be integrally closed. Then $\alpha \in L$ is integral over $A$ iff its minimal polynomial $f$ over $K$ has coefficients in $A$.

[1] Later on, when we take $K$ to be an extension of the $p$-adic field $\mathbb{Q}_p$, we will use $\mathscr{O}_K$ to denote the integral closure of $\mathbb{Z}_p$ in $K$.

*Proof.* The reverse direction is clear. For the forward direction, note all zeros of $f$ are integral over $K$ since they satisfy the same polynomial equation that $\alpha$ satisfies. The coefficients of $f$ are polynomial expressions in the roots so are integral over $A$, and hence in $A$ (since they are already in $K$). □

**Proposition 1.10** (Finite generation)**:** finite-generation

1. Let $A \subseteq B \subseteq C$ be rings. If $B$ is finitely generated as an $A$-module and $C$ is finitely generated as a $B$-module, then $C$ is finitely generated as an $A$-module.

2. If $B$ is integral over $A$ and finitely generated as an $A$-algebra, then it is finitely generated as an $A$-module.

*Proof.*

1. Take products of generators.

2. Let algebra generators be $\beta_1, \dots, \beta_m$. Then

$$A \subseteq A[\beta_1] \subseteq \cdots \subseteq A[\beta_1, \dots, \beta_m]$$

is a chain of integral extensions, so item 2 follows from 1. □

Combining this proposition with Lemma 1.4 we get the following:

**Proposition 1.11** (Transitivity of integrality)**:** integrality Let $A \subseteq B \subseteq C$ be integral domains and $K$, $L$, $M$ be their fraction fields.

1. If $B$ is integral over $A$ and $C$ is integral over $B$, then $C$ is integral over $A$.

2. Let $A'$ is the integral closure of $A$ over $B$ and $A''$ be the integral closure of $A'$ over $C$. Let $A'''$ be the integral closure of $A$ in $C$. Then $A'' = A'''$.

3. The integral closure of $A$ is integrally closed.

*Proof.*

1. For $\gamma \in C$, let $b_i$ be the coefficients of the minimal polynomial of $C$ over $B$. Then $\gamma$ is integral over $A[b_0, \dots, b_m]$, so by Proposition 1.10, item 2, $A[b_0, \dots, b_m, \gamma]$ is finitely generated over $A$. Since $\gamma A[b_0, \dots, b_m, \gamma] \subseteq A[b_1, \dots, b_m, \gamma]$, by Lemma 1.4, $\gamma$ is integral over $A$.

2. By item 1 applied to $A \subseteq A' \subseteq A''$, $A''$ is integral over $A$ so $A'' \subseteq A'''$. Conversely, any element $a \in A'''$ is integral over $A$ so *a fortiori* integral over $A''$; thus $A''' \subseteq A''$.

3. Follows from item 2 applied to $A = B = C$. □

# §2 Norms and Traces

Let $B$ be a free $A$-module of rank $n$. Then any element $\beta \in B$ defines an $A$-linear map $m_\beta$ (or $[\beta]$), multiplication by $\beta$. It is helpful to think of $\beta$ as a linear map because then we can apply results from linear algebra.

**Definition 2.1:** trace-det-char The trace, determinant, and characteristic polynomial of $m_\beta$ are called the **trace**, **norm**, and **characteristic polynomial** of $\beta$.

These are computed by choosing any basis of $e_1, \ldots, e_n$ for $B$ over $A$, and then computing the action of $\beta$ on this basis.

**Proposition 2.2** (Elementary properties)**:** nm-elem-pr The following hold ($a \in A; \beta, \beta' \in B$):

1. $\mathrm{Tr}(\beta + \beta') = \mathrm{Tr}(\beta) + \mathrm{Tr}(\beta')$
2. $\mathrm{Tr}(a\beta) = a\mathrm{Tr}(\beta)$
3. $\mathrm{Tr}(a) = na$
4. $\mathrm{Nm}(\beta\beta') = \mathrm{Nm}(\beta) \cdot \mathrm{Nm}(\beta')$
5. $\mathrm{Nm}(a) = a^n$

**Proposition 2.3** (Behavior with respect to field extensions)**:** ntr-fext Suppose $L/K$ is a degree $n$ field extension, $M$ is a finite extension of $L$, and $\beta \in L$.

1. (Relationship with roots of minimal polynomial) If $f(X)$ is the minimal polynomial of $\beta$ over $K$ and $\beta_1, \ldots, \beta_m$ are the roots of $f(X) = 0$ in a Galois closure of $K$, then letting $r = [L : K(\beta)] = \frac{n}{m}$,
   (a) $\mathrm{char}_{L/K}(\beta) = f(X)^r$
   (b) $\mathrm{Tr}_{L/K}(\beta) = r(\beta_1 + \cdots + \beta_m)$
   (c) $\mathrm{Nm}_{L/K}(\beta) = (\beta_1 \cdots \beta_m)^r$
2. (Relationship with embeddings) Suppose $L$ is separable over $K$, $M$ is a Galois extension of $K$, and $\sigma_1, \ldots, \sigma_n$ are the set of distinct embeddings $L \to M$ fixing $K$. Then
   (a) $\mathrm{Tr}_{L/K}(\beta) = \sigma_1(\beta) + \cdots + \sigma_n(\beta)$
   (b) $\mathrm{Nm}_{L/K}(\beta) = \sigma_1(\beta) \cdots \sigma_n(\beta)$

   In particular, this is true when $L = M$ is a Galois extension of $K$, and we can think of the $\sigma_k$ as simply the elements of $G(L/K)$.

3. (Transitivity of trace and norm) Suppose $\beta \in M$ and $M/K$ is separable.[2] Then
   (a) $\mathrm{Tr}_{M/K}(\beta) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\beta))$
   (b) $\mathrm{Nm}_{M/K}(\beta) = \mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\beta))$

4. (Integrality) Assume AKLB. If $\beta \in B$, then the coefficients of $\mathrm{char}_{L/K}(\beta)$, and hence $\mathrm{Tr}_{L/K}(\beta)$ and $\mathrm{Nm}_{L/K}(\beta)$, are integral over $A$. In particular, if $A$ is integrally closed in $L$ then they are in $A$.

*Proof.*

1. If $r = 1$, i.e. $K[\beta] = L$, then by the Cayley-Hamilton Theorem, $f(m_\beta) = 0$. Since $f(X)$ is irreducible, $f(X) \mid \mathrm{char}_{L/K}(\beta)$. However, these are monic polynomials of the same degree so they are equal.

   In the general case, take a basis $x_i$ of $K[\beta]$ over $K$ and a basis $y_j$ of $L$ over $K[\beta]$. Then $x_i y_j$ form a basis of $L$ over $K$, and the matrix of $m_\beta$ with respect to this basis is $n$ copies of $A$. This proves (a), which implies the rest of the statements.

2. Let $\beta_1, \ldots, \beta_m$ be the conjugates of $\beta$. There are $m$ distinct imbeddings $K(\beta) \to M$; they each take $\beta$ to a different $\beta_k$. Each of these imbeddings extend to $r := [L : K(\beta)] = \frac{n}{m}$ imbeddings $L \to M$. Now use item 1.

3. Note that for any finite extensions $K \subseteq L \subseteq N$ with $N$ Galois, an imbedding $L \hookrightarrow N$ fixing $K$ can be extended to a $K$-automorphism on $N$, and so be considered an element of the set $G(N/K)/G(N/L)$.[3]

   Let $N$ be a Galois extension containing $M$. By item 2,

$$\begin{aligned}
\mathrm{Tr}_{M/K}(\beta) &= \sum_{\sigma \in G(N/K)/G(N/M)} \sigma(\beta) \\
\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\beta)) &= \mathrm{Tr}_{L/K}\left( \sum_{\sigma \in G(N/L)/G(N/M)} \sigma(\beta) \right) \\
&= \sum_{\tau \in G(N/K)/G(N/L)} \sum_{\sigma \in G(N/L)/G(N/M)} \tau(\sigma(\beta))
\end{aligned}$$

   where in the second sum we take arbitrary representatives $\tau \in G(N/K)$ and $\sigma \in G(N/L)$. These are equal because for any choice of these representatives,

$$\{\sigma \in G(N/K)/G(N/M)\} = \{\tau\sigma \mid \tau \in G(N/K)/G(N/L), \sigma \in G(N/L)/G(N/M)\}$$

   when considered in $G(N/K)/G(N/M)$ (i.e. as imbeddings $M \hookrightarrow N$ fixing $K$). The same is true of the norm.

[2] The last condition is not necessary. TODO: Find a proof of the general case.

[3] Using the primitive element theorem, write $L = K(\beta)$. The imbeddings $L \to N$ are those taking $\beta$ to a conjugate; there are $[L : K]$ imbeddings. But we know $G(N/K)/G(N/L) = [L : K]$, so all of the imbeddings must be extendable. We also use this fact (in addition to a counting argument) in the proof of 2.

4. The minimal polynomial of $\alpha$ has coefficients in $A$, by Proposition 1.9. Hence the result follows from item 1.

$\square$

# §3 Discriminant

**Definition 3.1:** disc-df If $B$ is a ring and free $A$-module of rank $m$, and $\beta_1, \dots, \beta_m \in B$, then their **discriminant** is

$$D(\beta_1, \dots, \beta_m) = \det[\mathrm{Tr}_{B/A}(\beta_i \beta_j)]_{1 \le i,j \le m}.$$

**Proposition 3.2:** disc-basis If the change of basis matrix from $\gamma_i$ to $\beta_i$ is $T$, then

$$D(\gamma_1, \dots, \gamma_m) = \det(T)^2 \cdot D(\beta_1, \dots, \beta_m).$$

*Proof.* Let $M_1$ and $M_2$ be the matrices of the bilinear form

$$(\alpha, \alpha') = \mathrm{Tr}_{B/A}(\alpha\alpha')$$

with respect to the bases $(\beta_1, \dots, \beta_m)$ and $(\gamma_1, \dots, \gamma_m)$, respectively. Then, using the change of basis formula for bilinear forms,

$$\begin{aligned} D(\beta_1, \dots, \beta_m) &= \det(M_1) \\ D(\gamma_1, \dots, \gamma_m) &= \det(M_2) \\ M_2 &= T^t M_1 T \\ \det(M_2) &= \det(T)^2 \cdot \det(M_1) \end{aligned}$$

from which the result follows. $\square$

Consider the discriminant of an arbitrary basis of $B$ over $A$. By the above fact, this is well-defined up to multiplication by the square of a unit. The residue in $A/(A^\times)^2$ is called the discriminant $\mathrm{disc}(B/A)$. The discriminant also refers to the ideal of $A$ this element generates.

Note $\mathrm{disc}(B/A)$ can be thought of as the determinant of the matrix of the bilinear form $(\beta, \beta') = \mathrm{Tr}_{B/A}(\beta\beta')$.

**Proposition 3.3** (Criterion for integral basis)**:** crit-int-basis Let $A \subseteq B$ be integral domains and $B$ be a free $A$-module of rank $m$ with $\mathrm{disc}(B/A) \neq 0$. Then $\gamma_1, \dots, \gamma_m \in B$ form a basis for $B$ as an $A$-module iff

$$(D(\gamma_1, \dots, \gamma_m)) = (\mathrm{disc}(B/A))$$

as ideals.

*Proof.* Let $\beta_i$ be a basis. If the change of basis matrix from $\gamma_i$ to $\beta_i$ is $T$, then by Proposition 3.2,

$$D(\gamma_1, \ldots, \gamma_m) = \det(T)^2 \cdot D(\beta_1, \ldots, \beta_m) = \det(T)^2 \operatorname{disc}(B/A)$$

Now $\gamma_i$ is basis iff $T$ is invertible, iff $\det(T)$ is a unit, iff $(D(\gamma_1, \ldots, \gamma_m)) = (\operatorname{disc}(B/A))$. □

**Proposition 3.4** (Discriminants and Field Extensions)**:** disc-and-fe

1. (Relationship with embeddings) Let $L$ be separable finite over $K$ of degree $m$, and $\sigma_1, \ldots, \sigma_m$ be the embeddings of $L$ into a Galois extension $M$ fixing $K$. Then for any basis $\beta_1, \ldots, \beta_m$ of $L$ over $K$,

$$D(\beta_1, \ldots, \beta_m) = \det(\sigma_i \beta_j)^2 \neq 0.$$

2. (Nondegeneracy of trace pairing) If $B$ is free of rank $m$ over $A$ (with fraction fields $K, L$ as above), then the pairing

$$(\beta, \beta') \mapsto \operatorname{Tr}(\beta\beta')$$

   is a perfect $K$-bilinear pairing, and $\operatorname{disc}(B/A) = \operatorname{disc}(K/L) \neq 0$.

Here *perfect* means that the map $a \mapsto (b \mapsto (a, b))$ is an isomorphism $L \to L^*$, and similarly for $b \mapsto (a \mapsto (a, b))$. This is equivalent to saying that the bilinear form is nondegenerate.

*Proof.* (Unfinished) Use Proposition 2.3(1b), and that $\sigma_k, \det$ are both multiplicative. Inequality follows from independence of characters:

Let $G$ be a group, $F$ a field. Then the homomorphisms $G \to F^\times$ are linearly independent. □

Thus for $K$ of degree $m$ over $\mathbb{Q}$, we can talk of $\operatorname{disc}(\mathscr{O}_K/\mathbb{Z})$.

A closely related quantity to the discriminant is the *different*.

**Definition 3.5:** Assume AKLB, and suppose $L/K$ is a finite separable extension. The **codifferent** of $B$ with respect to $A$ is

$$B^* = \{y \in L \mid \operatorname{Tr}(xy) \in A \text{ for all } x \in B\}.$$

The **different** of $B$ with respect to $A$ is

$$\mathfrak{D}_{B/A} = (B^*)^{-1}.$$

In other words, it is the largest $B$-submodule satisfying $\operatorname{Tr}(E) \subseteq A$.

Note that $\mathfrak{D}_{B/A} = (B^*)^{-1}$.

**Remark:** two-def-disc We will define the discriminant in general, when $B$ is not necessarily a free $A$-module, in Chapter 9. The relationship between the two definitions is the following: Let $\mathfrak{p}$ be an ideal in $A$. Then $A_\mathfrak{p}$ is a principal ideal domain (in fact, a DVR). Let $S = A - \mathfrak{p}$; then $S^{-1}B$ is free over $S^{-1}A$ by the structure theorem for modules. We have $(\operatorname{disc}(S^{-1}B/S^{-1}A)) = (\mathfrak{p}A_\mathfrak{p})^{m(\mathfrak{p})}$ for some $m(\mathfrak{p})$. Then

$$\operatorname{disc}(B/A) = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}.$$

# §4 Integral bases

**Proposition 4.1** (Finite generation of integral extensions)**:** fgoie Let $A$ be integrally closed and $L$ separable of degree $m$ over $K$. There are free finite $A$-submodules $M$ and $M'$ of $L$ such that $M \subseteq B \subseteq M'$. $B$ is a finitely generated $A$-module if $A$ is Noetherian, and free of rank $m$ if $A$ is a PID.[4]

*Proof.* Let $\{\beta_1, \ldots, \beta_m\} \subseteq B$ be a basis for $L$ over $K$. Take a basis $\beta_i'$ so that $\operatorname{Tr}(\beta_i\beta_j') = \delta_{ij}$. Then

$$A\beta_1 + \cdots + A\beta_m \subseteq B \subseteq A\beta_1' + \cdots + A\beta_m'.$$

The second inclusion follows because if $\beta \in B$, then writing $\beta = \sum_j b_j\beta_j'$, we have that $b_i = \operatorname{Tr}(\beta\beta_i) \in A$. (In other words, the $\beta_i'$ form a basis for the codifferent $B^*$, which contains $B$.)Move some of the stuff on codiff?

If $A$ is Noetherian, then $M'$ is finitely generated, so its submodule $B$ is finitely generated over $A$. If $A$ is a PID, then by the Structure Theorem for Modules (over PIDs), $M$ is a direct sum of cyclic modules and a free module. Since it is contained in a free module of rank $m$ and contains a free module of rank $m$, it must be free of rank $m$. $\square$

The following is immediate:

**Theorem 4.2:** If $K$ is finite over $\mathbb{Q}$ (i.e. a number field), then $\mathscr{O}_K$ is a finitely generated $\mathbb{Z}$-module. It is the largest subring that is finitely generated over $\mathbb{Z}$.

**Definition 4.3:** A basis for $\mathscr{O}_K$ as a $\mathbb{Z}$-module is called an **integral basis**.

**Proposition 4.4:** disc-calc Suppose $K$ has characteristic 0 (so $L$ separable over $K$), $L = K[\beta]$, and $f$ is the minimal polynomial of $\beta$ over $K$. Let $f(X) = \prod(X - \beta_i)$ in the Galois closure of $L$. Then

$$D(1, \beta, \ldots, \beta^{m-1}) = \prod_{1\le i<j\le m} (\beta_i - \beta_j)^2 = (-1)^{m(m-1)/2} \cdot \operatorname{Nm}_{L/K}(f'(\beta)).$$

This is called the discriminant of $f$.[5]

[4] Alternative proof: proceed as in 5.8.

[5] This gives an alternative proof of the perfect pairing.

*Proof.* Note the $\beta_i$ are conjugates of $\beta$; assume $\beta = \beta_1$.

By Proposition 3.4, we have

$$D(1,\beta,\ldots,\beta^{m-1}) = \begin{vmatrix} 1 & \beta_1 & \cdots & \beta_1^{m-1} \\ 1 & \beta_2 & \cdots & \beta_2^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_m & \cdots & \beta_m^{m-1} \end{vmatrix}^2 = \prod_{1\le i<j\le m} (\beta_i - \beta_j)^2,$$

where the last statement follows by evaluating the Vandermonde determinant.

For the second equality, note by Proposition 2.3(1c) that

$$\begin{aligned} \mathrm{Nm}_{L/K}(f'(\beta)) = \mathrm{Nm}_{L/K}((\beta_1-\beta_2)\cdots(\beta_1-\beta_m)) &= \prod_{1\le i\le m}\ \prod_{1\le j\le m,\, j\ne i} (\beta_i-\beta_j) \\ &= (-1)^{\frac{m(m-1)}{2}} \prod_{1\le i<j\le m} (\beta_i-\beta_j)^2. \end{aligned}$$

□

**Proposition 4.5:** If $K = \mathbb{Q}[\alpha]$, $\alpha \in \mathscr{O}_K$, and $D(1,\alpha,\ldots,\alpha^{m-1}) = \mathrm{disc}(\mathscr{O}/\mathbb{Z})$ then $\{1,\alpha,\ldots,\alpha^{m-1}\}$ is an integral basis.

*Proof.* Using change-of-basis and the correspondence between index and determinant,

$$D(1,\alpha,\ldots,\alpha^{m-1}) = \mathrm{disc}(\mathscr{O}_K/\mathbb{Z}) \cdot [\mathscr{O}_K : \mathbb{Z}[\alpha]]^2.$$

Now $\mathrm{disc}(\mathscr{O}_K/\mathbb{Z}) \in \mathbb{Z}$ so $[\mathscr{O}_K : \mathbb{Z}[\alpha]] = 1$. □

**Theorem 4.6** (Stickelberger's Theorem)**:** stickelberger

1. Let $s$ is the number of complex (nonreal) embeddings $K \to \mathbb{C}$. Then
$$\mathrm{sign}[\mathrm{disc}(K/\mathbb{Q})] = (-1)^{s/2}.$$
2. $\mathrm{disc}(\mathscr{O}_K/\mathbb{Z}) \equiv 0 \text{ or } 1 \pmod 4$.

*Proof.*

1. Write $K = \mathbb{Q}[\alpha]$ by the Primitive Element Theorem and $\alpha_1,\ldots,\alpha_r$ be the real conjugates and $\beta_1,\overline{\beta_1},\ldots,\beta_s,\overline{\beta_s}$ be the complex conjugates. By Proposition 4.4,
$$\mathrm{sign}(D(1,\alpha,\ldots,\alpha^{m-1})) = \mathrm{sign}\left(\prod_{1\le j\le s} (\beta_j - \overline{\beta_j})^2\right) = \prod_{1\le j\le s} i^2 = (-1)^{s/2}.$$
2. Let $\alpha_1,\ldots,\alpha_m$ be an integral basis. Let $P$ and $-N$ be the sum of the terms in the expansion of $\det(\sigma_i\alpha_j)$ corresponding to even and odd permutations, respectively:
$$\begin{aligned} P &= \sum_{\text{even } \pi\in S_m} \prod_{i=1}^m \sigma_i \alpha_{\pi(i)} \\ N &= \sum_{\text{odd } \pi\in S_m} \prod_{i=1}^m \sigma_i \alpha_{\pi(i)}. \end{aligned}$$

Then

$$\begin{aligned}\operatorname{disc}(\mathscr{O}_K/\mathbb{Z}) &= \det(\sigma_i\alpha_j)^2 \\ &= (P-N)^2 \\ &= (P+N)^2 - 4PN.\end{aligned}$$

Take $\sigma \in G(K^{\text{gal}}/\mathbb{Q})$. Note composition by $\sigma$ permutes the $\sigma_i$, say by $\nu$. Then

$$P = \sum_{\text{even } \pi\in S_m} \prod_{i=1}^{m} \sigma_i\alpha_{\nu^{-1}\pi(i)}$$
$$N = \sum_{\text{odd } \pi\in S_m} \prod_{i=1}^{m} \sigma_i\alpha_{\nu^{-1}\pi(i)}$$

and hence $\sigma$ permutes $\{P, N\}$. Hence $\sigma$ fixes $P+N, PN$ and they are rational. Since they are integral over $\mathbb{Z}$ they are integers. Thus the above is congruent to 0 or 1 modulo 4.

□

**Example 4.7** (Quadratic extensions)**:** quadratic-extensions Any quadratic extension of $\mathbb{Q}$ is in the form $\mathbb{Q}(\sqrt{m})$ for some squarefree integer $m$. We find the ring of integers of $\mathbb{Q}(\sqrt{m})$. Consider two cases.

1. $m \equiv 2, 3 \pmod 4$: The minimal polynomial of $\sqrt{m}$ is $X^2 - m$, so

   $$\operatorname{disc}(1, \sqrt{m}) = (\sqrt{m} - (-\sqrt{m}))^2 = 4m.$$

   Note $\frac{\operatorname{disc}(1,\sqrt{m})}{\operatorname{disc}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})}$ must be a square by Proposition 3.2 so $\operatorname{disc}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$ equals $m$ or $4m$. However, by Stickelberger's Theorem, $\operatorname{disc}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \equiv 0, 1 \pmod 4$. Hence $\operatorname{disc}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \neq m$ and $\operatorname{disc}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) = 4m$. By Proposition 3.3, $1, \sqrt{m}$ is an integral basis.

2. $m \equiv 1 \pmod 4$: Note $\frac{1+\sqrt{m}}{2}$ is integral with minimal polynomial $X^2 - X - \frac{m-1}{4}$, so

   $$\operatorname{disc}\left(1, \frac{1+\sqrt{m}}{2}\right) = \left(\frac{1+\sqrt{m}}{2} - \frac{1-\sqrt{m}}{2}\right)^2 = m.$$

   Since $m$ is squarefree, $\operatorname{disc}(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) = m$ and Proposition 3.3 says $1, \frac{1+\sqrt{m}}{2}$ is an integral basis.

The following tells us about integral bases for products of fields. Can we generalize from $\mathbb{Q}$ to extensions of $\mathbb{Q}$?

**Proposition 4.8:** disc-compositum Suppose that $K, L$ are field extensions of $\mathbb{Q}$ such that

$$[KL:\mathbb{Q}] = [K:\mathbb{Q}][L:\mathbb{Q}].$$

Let $d = \gcd(\mathrm{disc}(K/\mathbb{Q}), \mathrm{disc}(L/\mathbb{Q}))$. Then

1. $\mathscr{O}_K \subseteq d^{-1}\mathscr{O}_K\mathscr{O}_L$.
2. If $\mathscr{O}_{KL} = \mathscr{O}_K\mathscr{O}_L$, then $\mathrm{disc}(KL/\mathbb{Q}) = \mathrm{disc}(K/\mathbb{Q})^{[L:\mathbb{Q}]}\,\mathrm{disc}(L/\mathbb{Q})^{[K:\mathbb{Q}]}$.

   In particular, COROLLARY.

*Proof.* Let $\{\alpha_1, \ldots, \alpha_m\}$ be an integral basis for $K$ and $\{\beta_1, \ldots, \beta_n\}$ be an integral basis for $L$. By the degree assumption, we know that $\{\alpha_i\beta_j\}$ is a basis for $KL$ over $\mathbb{Q}$. Any element of $KL$ integral over $\mathbb{Q}$ can be written as

$$ga-integral\gamma = \sum_{\substack{1\le i\le m\\ 1\le j\le m}} \frac{a_{ij}}{r}\alpha_i\beta_j \tag{1.2}$$

where $\gcd(r, \gcd(a_{ij})) = 1$.

We need to show that $r \mid d$. Let $x_i = \sum_{j=1}^{n} \frac{a_{ij}}{r}\beta_j$. We will turn (1.2) into a system of equations by considering all embeddings $K \hookrightarrow \mathbb{C}$, solve for the $x_i$ using Cramer's rule, and in this way show that each $x_i$ is an algebraic integer in $L$ divided by a bounded denominator.

Note given embeddings $\sigma_K : K \hookrightarrow \mathbb{C}$ and $\sigma_L : L \hookrightarrow \mathbb{C}$, there is exactly one embedding $\sigma_{KL} : KL \hookrightarrow \mathbb{C}$ such that restricts to $\sigma_K$ and $\sigma_L$. It is clearly unique if it exists. To show existence, write $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}(x)/(f(x))$ by PET, and note that the characteristic polynomial of $f$ does not change upon passing to $L$ because of the degree assumption. Hence $KL = L(\alpha) = L(x)/(f(x))$, and in extending $\sigma_L$ to $\sigma_{KL}$, we are allowed to send $\alpha = x$ to $\sigma_L(\alpha)$.

Fix an embedding $\sigma : L \hookrightarrow \mathbb{C}$, and let $\sigma_1, \ldots, \sigma_m$ be all embeddings $K \hookrightarrow \mathbb{C}$. Then applying $\sigma_k$ to 1.2 we obtain the system of equations

$$\sum_{i=1}^{m} \sigma_k(\alpha_i)x_i = \sigma_k(\gamma), \quad 1 \le k \le m.$$

By Cramer's rule, letting $D = \det[(\sigma_k(\alpha_i))_{k,i}]$ we get $Dx_i = D_i$ where $D_i$ has the $i$th column of $D$ replaced by $(\sigma_k(\alpha_i))_{k=1}^{m}$. Note that $D$ and $D_i$ are both algebraic integers. Using $\mathrm{disc}(\mathscr{O}_K/\mathbb{Z}) = D^2$ (Proposition 3.4), we get

$$\mathrm{disc}(\mathscr{O}_K/\mathbb{Z})x_i = DD_i.$$

Hence $\mathrm{disc}(\mathscr{O}_K/\mathbb{Z})x_i$ is an algebraic integer (in $\mathscr{O}_L$). Since the $\beta_j$ are an integral basis for $\mathscr{O}_L$, this forces $r \mid \mathrm{disc}(\mathscr{O}_K/\mathbb{Z})$. Similarly, $r \mid \mathrm{disc}(\mathscr{O}_L/\mathbb{Z})$, as needed.

Now we prove the second part. Choose $(\alpha_1, \ldots, \alpha_m)$ a basis for $K/\mathbb{Q}$ and $(\beta_1, \ldots, \beta_n)$ a basis for $L/\mathbb{Q}$. Then $(\alpha_j\beta_k)_{1\le j\le m, 1\le k\le n}$ is a basis for $KL/\mathbb{Q}$. For $\gamma \in KL$, let $(\gamma)_{j,k}$ denote the coordinate of $\alpha_j\beta_k$ in $\gamma$. Then the $mn \times mn$ matrix

$$\begin{aligned}
[\mathrm{Tr}(\alpha_{i_1}\beta_{i_2}\alpha_{i_1'}\beta_{i_2'})] &= \left[\sum_{1\le j\le m, 1\le k\le n} (\alpha_{i_1}\beta_{i_2}\alpha_{i_1'}\beta_{i_2'}\alpha_j\beta_k)_{j,k}\right] \\
&= \left[\sum_{1\le j\le m, 1\le k\le n} (\alpha_{i_1}\alpha_{i_1'}\alpha_j)_j(\beta_{i_2}\beta_{i_2'}\beta_k)_k\right] \\
&= \left[\sum_{1\le j\le m}\sum_{1\le k\le n} (\alpha_{i_1}\alpha_{i_1'}\alpha_j)_j(\beta_{i_2}\beta_{i_2'}\beta_k)_k\right] \\
&= [\mathrm{Tr}(\alpha_{i_1}\alpha_{i_1'})] \otimes [\mathrm{Tr}(\beta_{i_2}\beta_{i_2'})].
\end{aligned}$$

Taking determinants and using

$$\det(A \otimes B) = \det(A)^n \det(B)^m, \quad A \in M_{m\times m}, B \in M_{n\times n}$$

we get

$$\mathrm{disc}(KL/\mathbb{Q}) = \mathrm{disc}(K/\mathbb{Q})^{[L:\mathbb{Q}]}\,\mathrm{disc}(L/\mathbb{Q})^{[M:\mathbb{Q}]}.$$

$\square$

[ADD an algorithm for computing integral bases]

# §5 Problems

1. Suppose that $f \in \mathbb{Z}[x]$ is irreducible and has a root of absolute value at least $\frac{3}{2}$. Prove that if $\alpha$ is a root of $f$ then $f(\alpha^3 + 1) \neq 0$.

2. Let $a_1, \ldots, a_n$ be algebraic integers with degrees $d_1, \ldots, d_n$. Let $a_1', \ldots, a_n'$ be the conjugates of $a_1, \ldots, a_n$ with greatest absolute value. Let $c_1, \ldots, c_n$ be integers. Prove that if the LHS of the following expression is not zero, then

$$|c_1a_1 + \ldots + c_na_n| \ge \left(\frac{1}{|c_1a_1'| + \cdots + |c_na_n'|}\right)^{d_1d_2\cdots d_n - 1}.$$

   For example,

$$|c_1 + c_2\sqrt{2} + c_3\sqrt{3}| \ge \left(\frac{1}{|c_1| + |2c_2| + |2c_3|}\right)^3.$$

3. Let $p$ be a prime and consider $k$ $p$th roots of unity whose sum is not 0. Prove that the absolute value of their sum is at least $\frac{1}{k^{p-2}}$.

# Chapter 2
# Ideal factorization

factorization

## §1 Discrete Valuation Rings

**Definition 1.1:** Let $K$ be a field. A **discrete valuation** on $K$ is a surjective function $v : K^{\times} \to \mathbb{Z}$ such that for every $x, y \in K^{\times}$,

1. $\pi$ is a group homeomorphism: $v(xy) = v(x)v(y)$.
2. $v(x + y) \geq \min(v(x), v(y))$.

We set $v(0) = \infty$.

A **discrete valuation ring** (over $\mathbb{Z}$) is a local integral domain $R$ (not a field), whose fraction field has a discrete valuation $v$.

An element $t$ with $v(t) = 1$ is a **uniformizing parameter**.

**Proposition 1.2:** Suppose $R$ is a DVR with fraction field $K$. Let $v$ be the valuation on $K$.

1. The units are exactly the elements with 0 valuation:
$$R^{\times} = v^{-1}(0).$$
2. Its maximal idea is the set of elements with positive valuation.
$$\mathfrak{m} = \{x : v(x) > 0\}.$$
3. $R$ is a PID with ideals $\mathfrak{m}^n = \{x : v(x) \geq n\} = (t^n)$ for $n \in \mathbb{N}$.
4. $R$ is a UFD; any element can be written uniquely in the form $ut^n$ where $u$ is a unit.

**Lemma 1.3:** Let $A$ be a local domain with maximal ideal $\mathfrak{m}$ principal and nonzero. If $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$ then $A$ is a DVR.

**Theorem 1.4:** Let $(A, \mathfrak{m})$ be a Noetherian local domain. The following conditions are equivalent.

1. $A$ is a DVR.
2. $A$ is a normal domain of dimension 1. (Dimension 1 means that the longest chain of prime ideals is 2: $\mathfrak{p}_0 \subseteq \mathfrak{p}_1$.) (Since $A$ is local this means it has only two prime ideals.)
3. $A$ is a normal domain of depth 1. (There is a nonzero $x \in A$ with $\mathfrak{m} \in \operatorname{Ass}(A/\langle x \rangle)$.)
4. $A$ is a regular local ring of dimension 1. (Regular means its maximal ideal is generated by a number of elements equal to its dimension. So here it means $\mathfrak{m}$ is principal.)
5. $\mathfrak{m}$ is principal and nonzero.

*Proof.* Note (5) $\implies$ (1) uses Krull Intersection Theorem: For $R$ a Noetherian ring, $\mathfrak{a}$ an ideal, and $M$ a finitely generated module (esp. when $M = R$), then there exists $x \in \mathfrak{a}$ such that

$$(1 + x) \bigcap_{n=0}^{\infty} \mathfrak{a}^n M = 0.$$

$\square$

# §2 Dedekind Domains

**Definition 2.1:** A **Dedekind domain** is a normal Noetherian integral domain $A$ such that every nonzero prime ideal is maximal.

**Proposition 2.2:** A local integral domain is Dedekind iff it is a DVR.

**Proposition 2.3:** For every nonzero prime ideal $\mathfrak{p}$ in a Dedekind domain $A$, the localization $A_{\mathfrak{p}}$ is a DVR. (*Locally, Dedekind domains are DVR's.*)

(The converse, i.e. if $A_{\mathfrak{p}}$ is a DVR for every $\mathfrak{p}$, then $A$ is Dedekind, holds using Serre's criterion.)

**Theorem 2.4** (Unique factorization of prime ideals)**:** uf-dedekind Let $A$ be a Dedekind domain. Every proper nonzero ideal of $A$ can be written uniquely as a product of prime ideals.

*Proof.* Let $\mathfrak{a}$ be a proper nonzero ideal of $A$.

1. If $A$ is Noetherian, then every ideal $\mathfrak{a} \subseteq A$ contains a product $\mathfrak{b} = \prod \mathfrak{p}_k^{r_k}$ of nonzero prime ideals: Otherwise, choose a maximal counterexample $\mathfrak{a}$ (possible since $A$ is Noetherian). Since $\mathfrak{a}$ is not prime, there exist $x, y \notin \mathfrak{a}$ such that $xy \in \mathfrak{a}$. By the maximality assumption both $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ contain a product of prime ideals, and so does $\mathfrak{a} \supseteq (\mathfrak{a} + (x))(\mathfrak{a} + (y))$.

2. By the Chinese Remainder Theorem

$$A/\mathfrak{b} \cong \prod_k A/\mathfrak{p}_k^{r_k}$$

via the natural map.

3. If $\mathfrak{p}$ is a maximal ideal in a ring $A$, and $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$, then the natural map $A/\mathfrak{p}^m \to (A/\mathfrak{p}^m)_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{q}^m$ is an isomorphism. (Indeed, it is injective because $\mathfrak{p}$ is prime and surjective because any $s \in A - \mathfrak{p}$ is invertible modulo $\mathfrak{p}^m$, on account of $(s) + \mathfrak{p}^m = A$.) Thus

$$\prod_k A/\mathfrak{p}_k^{r_k} \cong \prod_k A_{\mathfrak{p}_k}/\mathfrak{q}_k^{r_k}.$$

(This is where we use the fact that nonzero prime ideals are maximal.)

4. Combining the above, we get a one-to-one correspondence between ideals in $A$ containing $\mathfrak{b}$, and ideals in $\prod_k A_{\mathfrak{p}_k}/\mathfrak{q}_k^{r_k}$. All ideals in the last ring are in the form $\prod_k \mathfrak{q}_k^{s_k}/\mathfrak{q}_k^{r_k}$, so $\mathfrak{a}$ is of the form $\prod_k \mathfrak{q}_k^{s_k}$. Moreover, different prime ideals containing $\mathfrak{b}$ correspond to different $\prod_k \mathfrak{q}_k^{s_k}/\mathfrak{q}_k^{r_k}$, which are different for different $s_k$, giving uniqueness. □

**Corollary 2.5:** uf-dedekind-cor Let $A$ be a Dedekind domain.

1. If $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}_k^{r_k}$ and $\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}_k^{s_k}$ are ideals in $A$ and $\mathfrak{p}$ is a nonzero prime ideal then

$$\begin{aligned} \mathfrak{a} \supseteq \mathfrak{b} &\iff r_k \ge s_k \text{ for all } k \\ &\iff \mathfrak{a}A_\mathfrak{p} \supseteq \mathfrak{b}A_\mathfrak{p} \text{ for all } \mathfrak{p}. \end{aligned}$$

2. If $\mathfrak{a} \supset \mathfrak{b} \neq 0$ are ideals in $A$ then $\mathfrak{a} = \mathfrak{b} + (a)$ for some $a \in A$. In particular, if $b \in \mathfrak{a}$ then there exists $a \in A$ such that $\mathfrak{a} = (a, b)$; i.e. each ideal is generated by at most two elements.

3. (Inverses) Let $\mathfrak{a} \neq 0$ be an ideal of $A$. There exists a nonzero ideal $\mathfrak{a}^*$ such that $\mathfrak{a}\mathfrak{a}^*$ is principal.
   (a) We can choose $\mathfrak{a}^*$ so $\mathfrak{a}\mathfrak{a}^* = (a)$ for given $a \in \mathfrak{a}$.
   (b) Alternatively we can choose $\mathfrak{a}^*$ to be relatively prime to a given ideal $\mathfrak{c} \neq 0$.

*Proof.* 1. The forward direction was shown in the course of the theorem. The reverse directions are easy.

2. Choose any $a \in \mathfrak{a}\backslash\{0\}$. By unique factorization, we can write

$$\begin{aligned} (a) &= \mathfrak{p}_1^{u_1} \cdots \mathfrak{p}_r^{u_r} \\ \mathfrak{a} &= \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r} \end{aligned}$$

for primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and $u_j \geq v_j \geq 0$. Now choose $b_j \in \mathfrak{p}_j^{v_j} \backslash \mathfrak{p}_j^{v_j+1}$. By the Chinese remainder theorem we can choose $b$ such that $b \equiv b_j \pmod{\mathfrak{p}_j^{v_j+1}}$ for all $j$. Since $\mathrm{ord}_{\mathfrak{p}_j}(b_j) = v_j$, by item 1, the highest power of $\mathfrak{p}_j$ dividing $(b)$ is $v_j$. The highest power of $\mathfrak{p}_j$ dividing $(a)$ is $u_j \geq v_j$, so the highest power of $\mathfrak{p}_j$ dividing $(a, b)$ is $v_j$. Now for a prime $\mathfrak{q} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$, we have $a \notin \mathfrak{q}$ (else $\mathfrak{q}$ would divide $\mathfrak{a}$), so $\mathfrak{q}$ does not divide $(a, b)$. We conclude

$$(a, b) = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_r^{v_r},$$

as needed.

3. (a) follows from item 1; for (b), use item 2 and 3(a) to write $\mathfrak{a} = \mathfrak{a}\mathfrak{c} + (a) = \mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}(\mathfrak{c} + \mathfrak{a}^*)$.

□

**Theorem 2.6:** extension-dedekind Assume AKLB, and $K/L$ is finite separable. If $A$ is a Dedekind domain, then so is $B$. In particular, taking $A = \mathbb{Z}$ and $K = \mathbb{Q}$, every ring of integers in a finite separable extension of $\mathbb{Q}$ is Dedekind. [Separability is not needed. TODO: proof of general case, Janusz I.6.1]

*Proof.*

1. $B$ is noetherian: By Proposition 1.4.1, $B$ is a finitely generated $A$-module, hence a Noetherian $A$-module, hence Noetherian as a ring.

2. $B$ is integrally closed by Proposition 1.1.11(2).

3. Every nonzero prime ideal $\mathfrak{q}$ of $B$ is maximal: Take a nonzero $\beta \in \mathfrak{q}$ and let its minimal polynomial be $x^n + a_{n-1}x^{n-1} + \cdots + a_n$. Then $a_n = -\beta^n - \cdots - a_1\beta \in \beta B \cap A \subseteq \mathfrak{q} \cap A$. This shows $\mathfrak{q} \cap A \neq 0$; since $A$ is Dedekind and $\mathfrak{q} \cap A$ is prime, $\mathfrak{q} \cap A$ is maximal and $A/\mathfrak{q}$ is a field. Since $B$ is integral over $A$, $B/\mathfrak{q}$ is integral over $A/\mathfrak{q}$.

   **Lemma 2.7:** int-dom-field An integral domain $B$ containing a field $k$ and algebraic over $k$ is a field.

   *Proof.* Let $\beta \in B$ be nonzero. Then $k[\beta]$ is a finite dimensional vector space and the multiplication-by-$\beta$ map $m_\beta : k[\beta] \to k[\beta]$ is injective, hence surjective. Thus there exists $\beta'$ so $\beta\beta' = 1$, i.e. $\beta$ has an inverse. □

   The lemma shows $B/\mathfrak{q}$ is a field. Hence $\mathfrak{q}$ is maximal.

   Alternatively, this follows directly from "lying-over" and "going up" for integral extensions. □

**Theorem 2.8:** ok-dedekind Suppose $K$ is a finite extension of $\mathbb{Q}$. Then unique factorization of ideals holds in $\mathcal{O}_K$.

*Proof.* Combine Theorem 2.4 and Theorem 2.6. □

# §3 Primary decomposition*

[ADD: Commutative algebra generalization, and a new proof of unique ideal factorization]

# §4 Ideal class group

Let $A$ be a Dedekind domain with fraction field $K$.

**Definition 4.1:** A **fractional ideal** of $A$ is a nonzero $A$-submodule of $K$ such that $d\mathfrak{a} \in A$ for some $d \in A$.

A principal fractional ideal is one of the form

$$(b) := bA := \{ba | a \in A\}.$$

The product of two fractional ideals is

$$\mathfrak{a}\mathfrak{b} = \left\{\sum a_i b_i | a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}.$$

Note that given a nonzero $A$-submodule of $K$, it is finitely generated iff it is a fractional ideal. (Take common denominators of the generators.)

We can extend unique factorization to fractional ideals, in the same way that we can extend unique factorization from $\mathbb{Z}$ to $\mathbb{Q}$.

**Theorem 4.2:** The set $\mathrm{Id}(A)$ of fractional ideals is a free abelian group on the set of prime ideals. Thus each fraction ideal can be uniquely written in the form

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}}.$$

*Proof.* Freeness follows from unique factorization (Theorem 2.4) and existence of inverses follows from Corollary 2.5(3a). □

Now we are ready for the following definition.

**Definition 4.3:** Let $P(A)$ be the group of principal ideals of $A$. The **ideal class group** $C(A)$ is $\mathrm{Id}(A)/P(A)$. Its order is the **class number**.

The ideal class group and class number of $K$ are defined as the ideal class group and class number of $\mathcal{O}_K$.

Note that we have an exact sequence

$$0 \to P(A) \to I(A) \to C(A) \to 0.$$

The class number is 1 iff all $A$ is a PID. Thus in some sense it measures how far $A$ is from being a PID.

Alternatively there is an exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \to I_K \to C_K \to 1$$

where the map $K^\times \to K$ is given by $a \mapsto (a)$.

**Theorem 4.4** (Approximation Theorem)**:** Let $x_1, \ldots, x_m \in A$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct prime ideals. For any $x \in \mathbb{N}$, there is $x \in A$ such that

$$\operatorname{ord}_{\mathfrak{p}_i}(x - x_i) > n$$

for all $i$.

*Proof.* Immediate from the Chinese Remainder Theorem. □

# §5 Factorization in extensions

Assume AKLB, with $A$ Dedekind and $L/K$ finite separable. A prime ideal $\mathfrak{p} \subset A$ will factor in $B$:

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

We say $e_i$ is the **ramification index** of $\mathfrak{P}_i$. For $\mathfrak{P} \mid \mathfrak{p}$, we write $e(\mathfrak{P}/\mathfrak{p})$ for the ramification index and $f(\mathfrak{P}/\mathfrak{p})$ for the **residue class degree** $[B/\mathfrak{P} : A/\mathfrak{p}]$.

1. If $e_k > 1$ for some $k$, $\mathfrak{p}$ is **ramified** in $B$.
   (a) If $g = 1$ and $e_1 > 1$, $\mathfrak{p}$ is **totally ramified**.
   (b) When $|A/\mathfrak{p}| = p^n$, $p$ prime, and $p \nmid [B/\mathfrak{P} : A/\mathfrak{p}]$, then $\mathfrak{p}$ is **tamely ramified**.
2. If $e_i = f_i = 1$ for all $i$, $\mathfrak{p}$ **splits completely**.
3. If $\mathfrak{p}B$ stays prime, $\mathfrak{p}$ is **inert**.

**Lemma 5.1:** div-int A prime ideal $\mathfrak{P}$ divides $\mathfrak{p}$ iff $\mathfrak{P} \cap K = \mathfrak{p}$.

**Theorem 5.2** (Degree equation)**:** deg-eq Let $m = [L : K]$ and suppose $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Then

$$\sum_{i=1}^{g} e_i f_i = m.$$

If $L/K$ is Galois, then all the $e_i$ are equal and all the $f_i$ are equal. Letting $e$ and $f$ denote these common values,

$$efg = m.$$

*Proof.* We show both sides of the equation equal $\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B)$.

For the LHS, by the Chinese Remainder Theorem $B/\mathfrak{p}B \cong \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$ so

$$deg - eq - 1 \dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i=1}^{g} \dim_{A/\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}). \tag{2.1}$$

Consider the filtration

$$B \supset \mathfrak{P}_i \supset \cdots \supset \mathfrak{P}_i^{e_i}.$$

There are no ideals between any two consecutive ideals by Corollary 2.5 (the first iff), so there are no proper $B/\mathfrak{P}_i$-ideals (i.e. subspaces) of $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$. Hence $\dim_{B/\mathfrak{P}_i}(\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}) = 1$ and $\dim_{A/\mathfrak{p}}(\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}) = f_i$. Thus

$$deg - eq - 2 \dim_{A/\mathfrak{p}}(B/\mathfrak{P}_i^{e_i}) = e_i f_i. \tag{2.2}$$

Combining (2.1) and (2.2) give

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i=1}^{g} e_i f_i.$$

For the RHS, let $A' = (A - \mathfrak{p})^{-1}A = A_\mathfrak{p}$ and $B' = (A - \mathfrak{p})^{-1}B$. First note that

$$A/\mathfrak{p} = \mathrm{Frac}(A/\mathfrak{p}) \cong (A/\mathfrak{p})_\mathfrak{p} = A'/\mathfrak{p}A'$$

and

$$B/\mathfrak{p} \overset{(*)}{\cong} (A - \mathfrak{p})^{-1}(B/\mathfrak{p}B) = B'/\mathfrak{p}B',$$

where in (*) we use the fact that all elements of $A - \mathfrak{p}$ are invertible modulo $\mathfrak{p}B$, on account of $A/\mathfrak{p}$ being a field. Note $A'$ is a a DVR and hence a PID. Since $B$ is finitely generated over $A$, and localization is exact, $B'$ is finitely generated over $A'$. Furthermore, $B'$ is $A'$-torsion free. The previous three statements along with the Structure Theorem for Modules gives that $B' \cong A'^n$ (as $A'$-modules) for some $n$. Perform the following operations:

$$\begin{tikzcd}
 & B' \cong A'^n \arrow[dl, "\otimes K"'] \arrow[dr, "\bullet/\mathfrak{p}\bullet"] & \\
K \cong L^n & & B'/\mathfrak{p}B' \cong (A'/\mathfrak{p}A')^n \arrow[d, equal] \\
 & & B/\mathfrak{p}B \cong (A/\mathfrak{p})^n
\end{tikzcd}$$

Hence

$$[L:K] = n = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B$$

as needed.

Now suppose $L/K$ is Galois. Then $G(L/K)$ permutes the primes $\mathfrak{P}$ dividing $\mathfrak{p}$. Since $e(\mathfrak{P}/\mathfrak{p}) = e(\sigma\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p}) = f(\sigma\mathfrak{P}/\mathfrak{p})$, it suffices to show $G(L/K)$ acts transitively.

Suppose by way of contradiction that $\mathfrak{P}$ and $\mathfrak{Q}$ are not in the same orbit. By the Chinese Remainder Theorem there exists $\beta \in \mathfrak{Q} - \{\sigma\mathfrak{P} \mid \sigma \in G(L/K)\}$. Now

$$\mathrm{Nm}_{L/K}(\beta) = \prod_{\sigma \in G(L/K)} \sigma(\beta) \in \mathfrak{Q} \cap A = \mathfrak{p} \subseteq \mathfrak{P},$$

the first because $\beta \in \mathfrak{Q}$ and the second because $\beta \in B$ is integral over $A$ (which is integrally closed in $K$). But $\sigma(\beta) \notin \mathfrak{P}$ so

$$\prod_{\sigma \in G(L/K)} \sigma(\beta) \notin \mathfrak{P},$$

a contradiction. $\square$

Note that the ramification indices and residue degrees multiply under field extension.

**Proposition 5.3:** ef-multiply Suppose that $M/L$ and $L/K$ are finite separable extensions (with Dedekind ring of integers), and that $\mathfrak{Q} \mid \mathfrak{P} \mid \mathfrak{p}$ are primes in $M, L, K$ respectively. Then

$$e(\mathfrak{Q}/\mathfrak{p}) = e(\mathfrak{Q}/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p})$$
$$f(\mathfrak{Q}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p})$$

*Proof.* The first comes from substituting the factorization of $\mathfrak{P}\mathcal{O}_M$ in the factorization of $\mathfrak{p}\mathcal{O}_L$. The second comes from multiplicativity of degrees of field extensions. $\square$

# §6 Computing factorizations

**Theorem 6.1** (Criterion for ramification)**:** crit-ram Assume AKLB, with $L/K$ finite, $A$ Dedekind, and $B$ free over $A$. (The last condition is satisfied when $A$ is a PID.) Then $\mathfrak{p}$ ramifies in $L$ iff $\mathfrak{p} \mid \mathrm{disc}(B/A)$. In particular, only finitely many prime ideals ramify.

*Proof.*

1. If $A$ is a ring, $B$ is a ring containing $A$ and admitting a finite basis $\{e_1, \ldots, e_m\}$ as an $A$-module, and $\mathfrak{a}$ is an ideal of $A$, then $\{\overline{e_1}, \ldots, \overline{e_m}\}$ is a basis for $B/\mathfrak{a}B$ as a $A/\mathfrak{a}$ module, and $D(\overline{e_1}, \ldots, \overline{e_m}) = D(e_1, \ldots, e_m) \bmod \mathfrak{a}$. Hence

$$\mathrm{disc}(B/A) \bmod \mathfrak{p} = \mathrm{disc}((B/\mathfrak{p}B)/(A/\mathfrak{p})).$$

2. **Lemma 6.2:** Let $k$ be a perfect field and $B$ be a $k$-algebra of finite dimension. Then $B$ is reduced (has no nilpotent elements) iff $\mathrm{disc}(B/k) \neq 0$.

*Proof.* First suppose $\beta \neq 0$ is a nilpotent element of $B$. Choose a basis $e_1 = \beta, e_2, \ldots, e_m$ of $B$. Then $\beta e_i$ is nilpotent, so has trace 0. The first row of $(\mathrm{Tr}(e_i e_j))$ is zero, so $\mathrm{disc}(B/k) = \det(\mathrm{Tr}(e_i e_j)) = 0$.

Now suppose $B$ is reduced. By the Scheinnullstellensatz, $\cap_{\mathfrak{p} \text{ prime}} \mathfrak{p} = \mathrm{nil}(R) = \{0\}$. Since $B/\mathfrak{p}$ is integral and algebraic over $k$, Lemma 2.7 shows it is a field. Hence $\mathfrak{p}$ is maximal, and different $\mathfrak{p}$ are relatively prime. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be prime ideals of $B$. By the Chinese Remainder Theorem, $B/\bigcap_{i=1}^r \mathfrak{p}_i = \prod_{i=1}^r B/\mathfrak{p}_i$ so

$$\dim_k B \geq \dim_k \left( B/\bigcap_{i=1}^{r} \mathfrak{p}_i \right) = \sum_{i=1}^{r} \dim_k(B/\mathfrak{p}_i) \geq r.$$

Since $\dim_k B$ is assumed finite, $B$ has only finitely many prime ideals, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$.

Each $B/\mathfrak{p}_i$ is a *finite separable* (as $k$ is perfect) extension of $k$, so by Proposition 1.3.4(2) (nondegeneracy of trace pairing), $\mathrm{disc}((B/\mathfrak{p}_i)/k) \neq 0$. Since $B = B/\cap_{i=1}^g \mathfrak{p}_i = \prod_{i=1}^g \mathfrak{p}_i$, by taking the union of the bases for $B/\mathfrak{p}_i$, we get $\mathrm{disc}(B/k) \neq 0$. □

3. Let $\mathfrak{p}B = \prod_i \mathfrak{P}_i^{e_i}$. From the lemma, since $A/\mathfrak{p}$ is perfect (as it is a finite field),

$$\mathrm{disc}((B/\mathfrak{p}B)/(A/\mathfrak{p})) = 0$$

iff $B/\mathfrak{p}B$ is not reduced. By the Chinese Remainder Theorem $B/\mathfrak{p}B = \prod_i B/\mathfrak{P}_i^{e_i}$, and this is nonreduced iff some $e_i > 1$, i.e. $\mathfrak{p}$ ramifies. □

**Theorem 6.3** (Computing the factorization of $\mathfrak{p}B$)**:** compute-fact-pB Assume AKLB, $A$ is Dedekind and $L/K$ is separable. Suppose $B = A[\alpha]$ and $f(X)$ is the minimal polynomial of $\alpha$ over $K$. Let $\mathfrak{p}$ be a prime ideal in $A$, and suppose $f(X)$ factorizes into irreducible polynomials modulo $\mathfrak{p}$ as

$$f(X) \equiv \prod_{i=1}^{r} g_i(X)^{e_i} \pmod{\mathfrak{p}}.$$

Then

$$\mathfrak{p}B = \prod_{i=1}^{r} (\mathfrak{p}, g_i(\alpha))^{e_i}$$

is the prime factorization of $\mathfrak{p}B$. Moreover, letting $\bar{g}_i = g_i \bmod \mathfrak{p}$,

$$B/(\mathfrak{p}, g_i(\alpha)) \cong (A/\mathfrak{p})[X]/(\bar{g}_i)$$
$$f_i = \deg g_i.$$

Generalize to when $\mathfrak{p}$ relatively prime to conductor.

*Proof.* The map $X \mapsto \alpha$ gives an isomorphism

$$A[X]/(f(X)) \cong B.$$

Modding out by $\mathfrak{p}$ gives

$$k[X]/(\bar{f}(X)) \cong B/\mathfrak{p}.$$

This gives a correspondence between ideals in $k[X]/(\bar{f}(X))$ and ideals in $B$ containing $\mathfrak{p}$:

$$\begin{array}{llr} & \text{Maximal ideals of } k[X]/(\bar{f}(X)) & (\bar{g}_i) \\ \longleftrightarrow & \text{Maximal ideals of } B/\mathfrak{p} & (\bar{g}_i(\alpha)) \\ \longleftrightarrow & \text{Maximal ideals of } B \text{ containing } \mathfrak{p} & (\mathfrak{p}, g_i(\alpha)) \end{array}$$

But the maximal ideals of $B$ containing $\mathfrak{p}$ are exactly the prime ideals (since $B$ is Dedekind) dividing $\mathfrak{p}$ (Lemma 5.1).

Now $\prod(\bar{g}_i)^{e_i} = 0$ but no power with smaller exponents is 0. Hence $\mathfrak{p}B \supseteq \prod(\mathfrak{p}, \bar{g}_i)^{e_i}$ but does not contain any power with smaller exponents, and equality holds. □

Note that the condition that $\mathfrak{p}$ be relatively prime to the conductor is somewhat pesky. The problem is that the we may have prime ideals dividing $\mathfrak{p}$ that are in the form $(\mathfrak{p}, g(\alpha))$ where $g$ does has coefficients with elements of $\mathfrak{p}$ in the denominator. So looking at the polynomial modulo $\mathfrak{p}$ fails to capture this behavior. We can't look at them modulo a power of $\mathfrak{p}$ either—because then we would not be in a field. The solution is to pass to the completion with respect to $\mathfrak{p}$—we will do this in Chapter ??.

**Example 6.4** (Quadratic extensions)**:** quad-ext-primes

1.

| Prime $p$ | $x^2+1$ mod $p$ | $(p)$ |
|---|---|---|
| 2 | $(x+1)^2$ | Ramifies: $(i+1)^2$ |
| $p \equiv 1 \pmod 4$ | factors since $\left(\frac{-1}{p}\right) = 1$ | Splits |
| $p \equiv 3 \pmod 4$ | irreducible since $\left(\frac{-1}{p}\right) = -1$ | Remains prime |

2.

| Prime $p$ | $x^2+2$ mod $p$ | $(p)$ |
|---|---|---|
| 2 | $x^2$ | Ramifies: $(\sqrt{-2})^2$ |
| $p \equiv 1, 3 \pmod 8$ | factors since $\left(\frac{-2}{p}\right) = 1$ | Splits |
| $p \equiv 5, 7 \pmod 8$ | irreducible since $\left(\frac{-2}{p}\right) = -1$ | Remains prime |

3.

| Prime $p$ | $x^2+x+1$ mod $p$ | $(p)$ |
|---|---|---|
| 3 | $(x-1)^2$ | Ramifies: $\left(\frac{-3+\sqrt{-3}}{2}\right)^2$ |
| $p \equiv 1 \pmod 3$ | factors since $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$ | Splits |
| $p \equiv 2 \pmod 3$ | irreducible since $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1$ | Remains prime |

Note we used quadratic reciprocity to translate the "square" condition into a modular condition on $p$. This is true in general for any quadratic ring: whether a prime $p$ splits is entirely determined by a modular condition on $p$, because of quadratic reciprocity.

Mention some geometrical intuition.

# §7 Decomposition and inertia groups

sec:decomposition-and-inertia Let $L/K$ be a finite Galois extension, with residue fields $l$ and $k$.

For a prime $\mathfrak{p}$ of $K$, we know that there are three kinds of behavior it could express when we pass to $L$:

1. It can split into distinct primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$.
2. The primes have some residue degree $f = [\mathcal{O}_L/\mathfrak{P}_j : \mathcal{O}_K/\mathfrak{p}]$ over $\mathfrak{p}$.
3. There can be ramification, the primes $\mathfrak{P}_j$ appearing with exponent $e$.

Moreover, $[L : K] = efg$. We would like to separate these three kinds of behavior by defining two intermediate extensions $L^{D(\mathfrak{P})}$ and $L^{I(\mathfrak{P})}$.

**Definition 7.1:** Let $\mathfrak{P} \mid \mathfrak{p}$ be primes in $L$ and $K$.

The **decomposition group** of $\mathfrak{P}$ is

$$D_{L/K}(\mathfrak{P}) = \{\sigma \in G(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

The **inertia group** of $\mathfrak{P}$ is

$$I_{L/K}(\mathfrak{P}) = \{\sigma \in G(L/K) : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

Equivalently, letting $l, k$ be the residue fields of $L$ and $K$, $I_{L/K}(\mathfrak{P})$ is the kernel of the map $\varepsilon : D(\mathfrak{P}) \to G(l/k)$.

We drop the subscript when there is no confusion. The main theorem is the following.

**Theorem 7.2:** decomposition-and-inertia Let $L/K$ be a finite Galois extension with residue fields $l, k$, with $l/k$ separable.[1] Let $\mathfrak{P} \mid \mathfrak{p}$ be primes of $L$ and $K$. Let $e, f, g$ be the ramification index, residue class degree, and number of prime divisors of $\mathfrak{p}$ in $L$.

Let $\mathfrak{P}_D = \mathfrak{P} \cap L^{D(\mathfrak{P})}$ and $\mathfrak{P}_I = \mathfrak{P} \cap L^{I(\mathfrak{P})}$ (the fixed fields of the decomposition and inertia groups). Then the following hold.

1. $[L : L^{I(\mathfrak{P})}] = e$ and $\mathfrak{P}_I$ totally ramifies in $L/L^{I(\mathfrak{P})}$.

$$\mathfrak{P}_I \mathcal{O}_L = \mathfrak{P}^e.$$

2. $[L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}] = f$ and $\mathfrak{P}_D$ remains inert in the extension $L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}$.

$$\begin{aligned} \mathfrak{P}_D \mathcal{O}_{L^{I(\mathfrak{P})}} &= \mathfrak{P}_I \\ f(\mathfrak{P}_I/\mathfrak{P}_D) &= f. \end{aligned}$$

Moreover, $L^{I(\mathfrak{P})}/K$ is Galois.

[1] If $l/k$ is not assumed separable, then $[L : L^{I(\mathfrak{P})}] = e[l : k]_i$, $[L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}] = [l : k]_s$, and $[L^{D(\mathfrak{P})} : L] = g$.

3. $[L^{D(\mathfrak{P})} : K] = g$, and $\mathfrak{p}$ splits completely in $L^{D(\mathfrak{P})}$ if $L^{D(\mathfrak{P})}/K$ is Galois[2]:

$$\mathfrak{p}\mathcal{O}_{L^{D(\mathfrak{P})}} = \mathfrak{P}_{1,D} \cdots \mathfrak{P}_{g,D}.$$

We have the following picture. By Galois theory, the groups on the right are the Galois groups acting on each extension; we set $G = G(L/K)$.

$$\begin{tikzcd}
\mathfrak{P} \arrow[d, dash, "\text{total ramification}"] & L \arrow[d, dash, "e"'] \arrow[d, dotted, dash, bend left, "I(\mathfrak{P})"] \arrow[ddd, dotted, dash, bend right=60, "G"'] \\
\mathfrak{P}_I \arrow[d, dash, "\text{inert}"] & L^{I(\mathfrak{P})} \arrow[d, dash, "f"'] \arrow[d, dotted, dash, bend left, "D(\mathfrak{P})/I(\mathfrak{P})"] \\
\mathfrak{P}_D \arrow[d, dash, "\text{totally split if Galois}"] & L^{D(\mathfrak{P})} \arrow[d, dash, "g"'] \arrow[d, dotted, dash, bend left, "G/D(\mathfrak{P}) \text{ if Galois}"] \\
\mathfrak{p} & K
\end{tikzcd}$$

**Remark:** To study ramification, we can define subgroups of $I(\mathfrak{P})$ called ramification groups and get fixed fields in between $L$ and $L^{I(\mathfrak{P})}$. See Chapter 9.

The rest of this section is devoted to the proof of Theorem 7.2. We keep the notations and assumptions in the theorem.

## 7.1 Decomposition group

**Proposition 7.3:** The decomposition group $D(\mathfrak{P})$ has order $ef$, and for $\sigma \in G(L/K)$,

$$D(\sigma(\mathfrak{P})) = \sigma D(\mathfrak{P})\sigma^{-1}.$$

Moreover, the following are equivalent:

1. $D(\mathfrak{P})$ is normal in $G$.
2. The groups $D(\mathfrak{Q})$ are equal for all $\mathfrak{Q} \mid \mathfrak{p}$.
3. $L^{D(\mathfrak{P})}/L$ is Galois.

*Proof.* Since $D(\mathfrak{P})$ is the stabilizer of $\mathfrak{P}$ under the action of $G := G(L/K)$, $|G/D(\mathfrak{P})|$ is simply the size of the orbit of $G$. This equals $g$ since $G$ acts transitively on the primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ above $\mathfrak{p}$. Hence

$$|D(\mathfrak{P})| = \frac{|G|}{|G/D(\mathfrak{P})|} = \frac{n}{g} = ef.$$

[2]This is actually an iff. Exercise!

The second part follows from the fact that if $G$ acts on $S$ and $G$ is the stabilizer of $s \in S$, then $tGt^{-1}$ is the stabilizer of $ts$.

For the equivalences, use the second part and the fundamental theorem of Galois theory **??.??**. □

We first show that $\mathfrak{P}_D$ is non-split in $L$ and prove item 3 of Theorem 7.2.

By the Fixed Field Theorem, $D(\mathfrak{P}) = G(L/L^{D(\mathfrak{P})})$, and

$$decomp - ef[L : L^{D(\mathfrak{P})}] = |D(\mathfrak{P})| = ef. \tag{2.3}$$

Since $L/L^{D(\mathfrak{P})}$ is Galois, $D(\mathfrak{P})$ acts transitively on the primes of $L$ above $\mathfrak{P}_D$. However, $D(\mathfrak{P})$ stabilizes $\mathfrak{P}$; thus $\mathfrak{P}$ is the only prime above $\mathfrak{P}_D$.

By the degree equation,

$$ef = [L : L^{D(\mathfrak{P})}] = e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}_D/\mathfrak{p}).$$

By Proposition 5.3,

$$\begin{aligned} e &= e(\mathfrak{P}/\mathfrak{P}_D)e(\mathfrak{P}_D/\mathfrak{p}) \\ f &= f(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}_D/\mathfrak{p}). \end{aligned}$$

All equations are satisfied only when $e = e(\mathfrak{P}/\mathfrak{P}_D)$, $f = f(\mathfrak{P}/\mathfrak{P}_D)$, and $e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1$.

If $L^{D(\mathfrak{P})}$ is Galois, then $e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1$ are the same as the $e$ and $f$ values for all primes in $L^{D(\mathfrak{P})}$ over $L$. Thus $\mathfrak{p}$ is totally split over $L$.

## 7.2 Inertia group

First we study the homomorphism

$$\varepsilon : D(\mathfrak{P}) \to G(l/k).$$

**Proposition 7.4:** Suppose $\mathfrak{P} \mid \mathfrak{p}$ are primes in $L$ and $K$, and let $k$ and $l$ be the residue fields of $L$ and $K$ with respect to $\mathfrak{P}$ and $\mathfrak{p}$.

1. $l/k$ is normal (and hence Galois if separable).

2. Let $\varepsilon$ be the map $D(\mathfrak{P}) \to G(l/k)$. Then $\varepsilon$ is surjective.

*Proof.* Let $G = G(L/K)$.

1. We need to show that for $\overline{\alpha} \in l$, its minimal polynomial over $k$ splits completely. Let $\alpha$ be a lift to $\mathcal{O}_L$ and let

   $$f(X) = \prod_{\sigma \in G} (X - \sigma(\alpha)) \in \mathcal{O}_K[X].$$

   Taking this modulo $\mathfrak{P}$ gives a polynomial in $k[X]$ containing $\overline{\alpha}$ as a root and splitting completely.

   Thus $l/k$ is normal, and hence Galois if it is separable.

2. First note we may assume $l/k$ is separable. Indeed, we have $G(l/k) \cong G(l^{\text{sep}}/k)$[3].

   It suffices to show that $\varepsilon(D(\mathfrak{P}))$ acts transitively on the conjugates of $\overline{\alpha}$ over $k$ (as then the image has at least $[l:k] = |G(l/k)|$ elements). By the Chinese Remainder Theorem, choose $\alpha \in \mathcal{O}_L$ such that

$$\alpha \equiv \begin{cases} \overline{\alpha} \pmod{\mathfrak{P}} \\ 0 \pmod{\mathfrak{P}'}, \quad \mathfrak{P}' \neq \mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}. \end{cases}$$

   Define $f$ as in item 1. Then, noting that for $\sigma \in G \backslash D(\mathfrak{P})$, we have $\alpha \equiv 0 \pmod{\sigma^{-1}(\mathfrak{P})}$ and hence $\sigma(\alpha) \equiv 0 \pmod{\mathfrak{P}}$,

$$\begin{aligned} \overline{f}(X) &= \prod_{\sigma \in D(\mathfrak{P})} (X - \overline{\sigma(\alpha)}) \prod_{\sigma \notin D(\mathfrak{P})} x \\ &= \underbrace{\prod_{\sigma \in D(\mathfrak{P})} (X - \varepsilon(\sigma)(\overline{\alpha}))}_{(*)} \prod_{\sigma \notin D(\mathfrak{P})} x \in k[x] \end{aligned}$$

   Now $(*)$ is in $k[x]$, so is divisible by the minimal polynomial of $\alpha$ over $k$. Given a conjugate $\overline{\alpha'}$ of $\overline{\alpha}$, it divides $(*)$, so equals $(\varepsilon(\sigma))(\overline{\alpha})$ for some $\sigma$. $\square$

**Corollary 7.5:** ses-inertia-decomp There is a short exact sequence

$$1 \to I(\mathfrak{P}) \to D(\mathfrak{P}) \to G(l/k) \to 1,$$

i.e. $D(\mathfrak{P})/I(\mathfrak{P}) \cong G(l/k)$.

Note $I(\mathfrak{P})$ is normal in $D(\mathfrak{P})$ as it is a kernel, so $L^{I(\mathfrak{P})}/K$ is Galois.
Now we finish the proof of Theorem 7.2. The above corollary gives

$$|D(\mathfrak{P})/I(\mathfrak{P})| = |G(l/k)| = [l:k] = f.$$

Since $G(L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}) = |D(\mathfrak{P})/I(\mathfrak{P})| = f$, we get $[L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}] = f$. From (2.3) we get $[L : L^{I(\mathfrak{P})}] = e$.

We will apply Corollary 7.5 to $L/L^{I(\mathfrak{P})}$. Note

$$D_{L/L^{I(\mathfrak{P})}}(\mathfrak{P}) = I_{L/L^{I(\mathfrak{P})}}(\mathfrak{P}) = G(L/L^{I(\mathfrak{P})}) = I(\mathfrak{P})$$

since the fact that $I(\mathfrak{P})$ operates trivially on $l/k$ implies that it operates trivially on $l/\kappa(\mathfrak{P}_I)$. Hence the corollary gives

$$G(l/\kappa(\mathfrak{P}_I)) = 1,$$

[3]From the Fixed Field Theorem $l/l^{G(l/l^{\text{sep}})}$ is Galois. But $l/l^{\text{sep}}$ is purely inseparable and normal. Thus we must have $l = l^{G(l/l^{\text{sep}})}$, i.e. every automorphism of $l/k$ is trivial on $l/l^{\text{sep}}$.

i.e. $l = \kappa(\mathfrak{P}_I)$ and $f(\mathfrak{P}/\mathfrak{P}_I) = 1$. We know that $\mathfrak{P}_D$ is non-split in $L$, so

$$e = [L : L^{I(\mathfrak{P})}] = e(\mathfrak{P}/\mathfrak{P}_I)\underbrace{f(\mathfrak{P}/\mathfrak{P}_I)}_{=1}$$
$$f = [L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}] = e(\mathfrak{P}_I/\mathfrak{P}_D)f(\mathfrak{P}_I/\mathfrak{P}_D).$$

Now

$$e = e(\mathfrak{P}/\mathfrak{P}_D) = e(\mathfrak{P}/\mathfrak{P}_I)e(\mathfrak{P}_I/\mathfrak{P}_D)$$
$$f = f(\mathfrak{P}/\mathfrak{P}_D) = f(\mathfrak{P}/\mathfrak{P}_I)f(\mathfrak{P}_I/\mathfrak{P}_D),$$

so we must have

$$e(\mathfrak{P}/\mathfrak{P}_I) = e, \qquad f(\mathfrak{P}/\mathfrak{P}_I) = 1$$
$$e(\mathfrak{P}_I/\mathfrak{p}) = 1, \qquad f(\mathfrak{P}_I/\mathfrak{p}) = f.$$

This finishes the proof.

## 7.3 Further properties and applications

**Theorem 7.6:** Let $M/K$ be a Galois extension and $L/K$ a subextension. Then

1. $$D_{M/L}(\mathfrak{P}) = D_{M/K}(\mathfrak{P}) \cap G(M/L)$$
$$I_{M/L}(\mathfrak{P}) = I_{M/K}(\mathfrak{P}) \cap G(M/L).$$

2. If $L/K$ is Galois, the following commutes and has exact rows and columns.

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & I_{M/L} \arrow[r] \arrow[d] & I_{M/K} \arrow[r] \arrow[d] & I_{L/K} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & D_{M/L} \arrow[r] \arrow[d] & D_{M/K} \arrow[r] \arrow[d] & D_{L/K} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & G(M/L) \arrow[r] \arrow[d] & G(M/K) \arrow[r] \arrow[d] & G(L/K) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

**Theorem 7.7:** unram-in-compositum Let $L/K$ and $L'/K$ be finite extensions. Then $\mathfrak{p}$ unramified in $L, L'$ if and only if $\mathfrak{p}$ is unramified in $LL'$.

Make notation consistent

*Proof.* First we prove the result for $L, L'$ Galois. Note that for any Galois extension $M/K$, with $\mathfrak{P} \mid \mathfrak{p}$ primes in $M$ and $K$,

$$inertia-1-iff-unramified I_{\mathfrak{P}} = 1 \iff \mathfrak{p} \text{ unramified in } M. \tag{2.4}$$

Now there is a injective homomorphism

$$\Phi : G(LL'/K) \hookrightarrow G(L/K) \times G(L'/K)$$
$$\Phi(\sigma) = (\sigma|_L, \sigma|_{L'}).$$

Take $\mathfrak{Q} \mid \mathfrak{p}$ with $\mathfrak{Q}$ a prime in $LL'$, and let $\mathfrak{P} = \mathfrak{Q} \cap \mathcal{O}_L$ and $\mathfrak{P}' = \mathfrak{Q} \cap \mathcal{O}_{L'}$. Suppose $\sigma \in I_{\mathfrak{Q}}$. Then $\sigma(\mathfrak{Q}) = \mathfrak{Q}$ and hence, taking the intersections with $\mathcal{O}_L, \mathcal{O}_{L'}$ (which are fixed by $\sigma$ since $L, L'$ are Galois)

$$\sigma|_L(\mathfrak{P}) = \mathfrak{P}$$
$$\sigma|_{L'}(\mathfrak{P}') = \mathfrak{P}'.$$

This shows $\sigma|_L \in I_{\mathfrak{P}}, \sigma|_{L'} \in I_{\mathfrak{P}'}$; by assumption and (2.4), we get $(\sigma|_L, \sigma|_{L'}) = (1, 1)$. By injectivity of $\Phi$, $\sigma = 1$. This shows $I_{\mathfrak{Q}} = 1$, by (2.4) again, we get $\mathfrak{Q}$ is unramified over $\mathfrak{p}$, as needed.

Now consider the general case. Given $\mathfrak{P} \mid \mathfrak{p}$ in $L$ and $K$, let $\mathfrak{Q}$ be a prime above $\mathfrak{P}$ in the Galois closure $L^{\text{gal}}$. Now $(L^{\text{gal}})^{I_{\mathfrak{Q}}(L^{\text{gal}}/L)}$ is a Galois extension containing $L$; since $L^{\text{gal}}$ is the Galois closure of $L$, we get

$$L^{\text{gal}} = (L^{\text{gal}})^{I_{\mathfrak{Q}}(L^{\text{gal}}/L)},$$

But $[L^{\text{gal}} : (L^{\text{gal}})^{I_{\mathfrak{Q}}(L^{\text{gal}}/L)}]$ is the ramification degree of $\mathfrak{Q}/\mathfrak{P}$; we see that it is 1, i.e. $\mathfrak{Q}$ is not ramified over $\mathfrak{P}$ and hence not ramified over $\mathfrak{p}$. Thus $L^{\text{gal}}/K$ is unramified. Similarly, $L'^{\text{gal}}/K$ is unramified. By the above, $L^{\text{gal}}L'^{\text{gal}}/K$ is unramified, so $LL'/K$ is unramified. ☐

# §8 Problems

sec:factorization-problems

1. A **half-factorial domain** (HFD) $A$ is an integral domain where any given factorization of $a$ has the same length. Prove Carlitz's Theorem:

   **Theorem 8.1** (Carlitz)**:** The ring of integers $\mathcal{O}_K$ is a HFD iff the class group has order at most 2.

   See AMM, 12/2011, for related results.

2. Show that if $\mathfrak{p}$ splits completely in $L^{D(\mathfrak{P})}$, then $L^{D(\mathfrak{P})}/L$ is Galois.

   Conclude that if $\mathfrak{p}$ splits completely in $L$, then $\mathfrak{p}$ splits completely in the Galois closure $L^{\text{gal}}$.

# Chapter 3
# The class group

class-group

## §1 Norms of ideals

Assume AKLB, $A$ is Dedekind, and $L/K$ is separable. We generalize the definition of norm to ideals, not just elements, so that it is a map $\mathrm{Id}(B) \to \mathrm{Id}(A)$ that is consistent with our old condition, i.e.

$$\mathrm{Nm}_{L/K}((a)) = \left(\mathrm{Nm}_{L/K}(b)\right).$$

Consider a principal ideal $\mathfrak{p} = (p) \subseteq A$, and suppose it factors in $B$ as $\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}^{e_i}$. We want the norm to satisfy

$$\textit{norm}-\textit{ideal}-\textit{motivate}\; \mathrm{Nm}_{L/K}(p) = \mathrm{Nm}_{L/K}(\mathfrak{p}B) = \prod_{i=1}^{g} \mathrm{Nm}_{L/K}(\mathfrak{P})^{e_i}, \tag{3.1}$$

since we want it to be multiplicative. But $\mathrm{Nm}(p) = p^n$ where $n = [L : K]$. By the degree equation, if $\mathrm{Nm}(\mathfrak{P}) = \mathfrak{P}^{f_i}$ where $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$, then (3.1) will be satisfied. Hence we make the following definition.

**Definition 1.1:** For $\mathfrak{P}$ is a prime of $B$, let $\mathfrak{p} = \mathfrak{P} \cap A$ and $f(\mathfrak{P}/\mathfrak{p}) = [B/\mathfrak{P} : A/\mathfrak{p}]$. Define the norm of $\mathfrak{P}$ to be

$$\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}.$$

This extends uniquely to a homomorphism $\mathrm{Id}(A) \to \mathrm{Id}(B)$, since the ideal group is free.

**Proposition 1.2** (Behavior with respect to field extensions)**:**

1. For an ideal $\mathfrak{a} \subseteq A$,
$$\mathrm{Nm}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^m,$$
where $m = [L : K]$.

2. If $L/K$ is Galois and $\mathfrak{p} \neq 0$ is a prime ideal of $A$, and $\mathfrak{P} \mid \mathfrak{p}$, then
$$\mathrm{Nm}_{L/K}(\mathfrak{p}) = \prod_{\sigma \in G(L/K)} \sigma\mathfrak{P}.$$

3. For any nonzero $\beta \in B$, $\mathrm{Nm}_{L/K}(\beta B) = \mathrm{Nm}_{L/K}(\beta)A$. (I.e. this is consistent with our previous definition.)

Compare the first two items to Chapter 1, Proposition 2.2(5) and Proposition 2.3(2b), respectively.

*Proof.*

1. By the degree equation (Theorem 5.2), for $\mathfrak{p}$ prime
$$\mathrm{Nm}_{L/K}(\mathfrak{p}B) = \mathrm{Nm}_{L/K}\left(\prod_i \mathfrak{P}_i^{e_i}\right) = \mathfrak{p}^{\sum_i e_i f_i} = \mathfrak{p}^m.$$
The general statement follows by multiplicativity of $\mathrm{Nm}_{L/K}$.

2. $G(L/K)$ acts transitively on $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$, so each $\mathfrak{P}_i$ occurs $\frac{m}{g} = ef$ times in $\{\sigma\mathfrak{P} \mid \sigma \in G(L/K)\}$.

3. First suppose $L/K$ is Galois. We use the description in terms of Galois conjugates to relate the norms of elements with the norms of ideals. By part 2 and Proposition 1.2.3(2b), we have
$$\mathrm{Nm}_{L/K}(\beta B) \cdot B \overset{(2)}{=} \prod_{\sigma \in G(L/K)} \sigma(\beta B) = \left(\prod_{\sigma \in G(L/K)} \sigma(\beta)\right) B \overset{1.2.3}{=} \mathrm{Nm}_{L/K}(\beta) \cdot B.$$
Hence, $\mathrm{Nm}_{L/K}(\beta) \cdot A$ and $\mathrm{Nm}_{L/K}(\beta \cdot B)$ determine the same ideal in $B$. Since $\mathrm{Id}(A) \to \mathrm{Id}(B)$ is injective, they are equal in $A$.

   Now consider the general case. Let $M$ be the Galois closure of $L$ over $K$, let $C = \mathcal{O}_M$, and let $d = [M : L]$. Then the above, together with part 1 and Proposition 1.2.2(5), give
$$\mathrm{Nm}_{L/K}(\beta \cdot B)^d \overset{(1)}{=} \mathrm{Nm}_{M/K}(\beta \cdot B) = \mathrm{Nm}_{M/K}(\beta) \cdot A \overset{1.2.2(5)}{=} \mathrm{Nm}_{L/K}(\beta)^d \cdot A.$$
Since $\mathrm{Id}(B)$ is torsion-free, $\mathrm{Nm}_{L/K}(\beta \cdot B) = \mathrm{Nm}_{L/K}(\beta) \cdot A$. □

**Definition 1.3:** The **numerical norm** of $\mathfrak{a}$ in $\mathcal{O}_K$ is its index in the lattice of integers:
$$\mathfrak{N}\mathfrak{a} = [\mathcal{O}_K : \mathfrak{a}].$$

Note the following comparisons between the ideal and numerical norms.

1. The ideal norm is defined for a field extension $K/F$ while the numerical norm is defined for any number field $K/\mathbb{Q}$.

2. The ideal norm returns an ideal while the numerical norm returns an integer.

3. However, if we take the base field $F$ to be $\mathbb{Q}$, and identify integers with the ideals they generate, the two norms are equivalent. This is the content of the following proposition.

**Proposition 1.4** (Relationship between ideal and numerical norm)**:**

1. For any ideal $\mathfrak{a} \subseteq \mathcal{O}_K$,
$$\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{a}) = (\mathfrak{N}(a)).$$
Therefore, $\mathfrak{N}(ab) = \mathfrak{N}(a)\mathfrak{N}(b)$.

2. Let $\mathfrak{b} \subseteq \mathfrak{a} \subseteq K$ be fractional ideals. Then
$$[\mathfrak{a} : \mathfrak{b}] = \mathfrak{N}(\mathfrak{a}^{-1}\mathfrak{b}).$$

In other words, *the norm of an ideal is its index in the ring of integers.*

*Proof.*

1. Write $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$ and let $(p_i) = \mathbb{Z} \cap \mathfrak{p}_i$, $f_i = f(\mathfrak{p}_i/(p_i))$. By the Chinese remainder theorem,
$$\mathcal{O}_K/\mathfrak{a} \cong \prod_i \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$
Since $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ is a vector space over $\mathbb{F}_{p_i}$ of dimension $e_i f_i$, we find
$$\mathfrak{N}\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}| = \prod_i p_i^{e_i f_i} = \mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{a}).$$
Multiplicativity follows from the same property for the ideal norm.

2. We can multiply by an integer $d$ so that $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals. Then
$$[\mathfrak{a} : \mathfrak{b}] = [d\mathfrak{a} : d\mathfrak{b}] = \frac{[\mathcal{O}_K : d\mathfrak{b}]}{[\mathcal{O}_K : d\mathfrak{a}]} = \frac{\mathfrak{N}(d\mathfrak{b})}{\mathfrak{N}(d\mathfrak{a})} \overset{(1)}{=} \mathfrak{N}(\mathfrak{a}^{-1}\mathfrak{b}).$$ □

# §2 Minkowski's Theorem

**Theorem 2.1** (Minkowski)**:** Let $V$ be a subset of $\mathbb{R}^n$ that is convex and symmetric around the origin ("centrally symmetric"). Let $L$ be a full lattice with fundamental paralleopiped $D$. If
$$\mu(T) > 2^n \mu(D)$$
then $T$ contains a point of $L$ other than the origin. If furthermore $D$ is compact, we can weaken the hypothesis to
$$\mu(T) \geq 2^n \mu(D).$$

*Proof.* First note that if $S$ is a measurable set such that $\mu(S) > \mu(D)$, then $S$ contains two points $a, b$ such that $a - b \in L$. Indeed, we can tile the space with fundamental parallelopipeds, and translate each of them to the origin. We consider the intersections of these parallelopipeds with $S$. Since the sum of these volumes is $\mu(S) > \mu(D)$, and they are all packed in $D$, there must be overlap, i.e. unequal $a, b \in S$ that were translated to the same point. This implies $a - b \in L$.

The set $S = \frac{1}{2}T$ has volume $\frac{1}{2^n}T > \mu(D)$. Hence by the above, there exist $\frac{1}{2}a \neq \frac{1}{2}b \in S$ ($a, b \in T$) such that $\frac{1}{2}a - \frac{1}{2}b \in L$. Since $T$ is symmetric, $-b \in T$; since $T$ is convex, $\frac{1}{2}(a - b) \in T$. This is the desired lattice point.

Now suppose instead $T$ is convex and $\mu(T) \geq 2^n \mu(D)$. Let $L_n$ be the set of lattice points in $\left(1 + \frac{1}{n}\right) T$ other than the origin. By the first part, $L_n$ is nonempty; since $T$ is bounded it must be finite. We have that $L_n \subseteq L_m$ when $n \geq m$. Hence

$$T \cap L = \bigcap_{n=1}^{\infty} \left(1 + \frac{1}{n}\right) T \cap L = \bigcap_{n=1}^{\infty} L_n \neq \phi. \qquad \square$$

**Theorem 2.2** (Sums of four squares)**:** (A digression, but nice to talk about)

# §3 Finiteness of the class number

finite-class There's a more natural way to "transfer" the inner product on $\mathbb{C}^n$ to $\mathbb{R}^r \times \mathbb{C}^s$...

We now show that the class number is finite (Theorem 3.6). The idea of the proof is as follows.

1. Embed $K$ as a $\mathbb{Q}$-vector space in $\mathbb{R}^r \times \mathbb{C}^s$. Under the $\mathbb{R}$-vector space isomorphism $K \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{R}^r \times \mathbb{C}^s$, the ideal $\mathfrak{a}$ is realized as a lattice $L$ in $V = \mathbb{R}^r \times \mathbb{C}^s$ (Proposition 3.1). The norm on $K$ translates into a "norm" on $V$.

2. Find an element in $\mathfrak{a}$ of small norm (Theorem 3.2): Find a compact, symmetric convex set in $V$ consisting of elements of norm at most $R$. Choosing $R$ large enough, we can make sure $V$ has large volume. By Minkowski's Theorem, $V$ contains an element of $L$.

3. Using step 2, show that every ideal class contains an representative of norm at most a constant (Theorem 3.5).

4. Show that there are a finite number of ideals with bounded norm (Lemma 3.7).

We first embed $\mathfrak{a}$ as a full lattice using the embeddings of $K$, and find the volume of the fundamental parallelopiped in terms of the discriminant (the discriminant is related to the embeddings by Proposition 3.4).

Let $\{\sigma_1, \dots, \sigma_r\}$ be the real embeddings and $\{\sigma_{r+1}, \bar{\sigma}_{r+1}, \dots, \sigma_{r+s}, \bar{\sigma}_{r+s}\}$ be the complex embeddings of $K$. This gives an embedding[1]

$$\sigma : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$$
$$\sigma(\alpha) = (\sigma_1\alpha, \dots, \sigma_{r+s}\alpha).$$

Identify $V = \mathbb{R}^r \times \mathbb{C}^s$ with $\mathbb{R}^n$ using the basis $\{1, i\}$ for $\mathbb{C}$.

**Proposition 3.1:** ideal-lattice Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. Then $\sigma(\mathfrak{a})$ is a full lattice in $V$ and the volume of its parallelopiped is $2^{-s} \cdot \mathbb{N}\mathfrak{a} \cdot |\Delta_K|^{\frac{1}{2}}$.

*Proof.* Let $\alpha_1, \dots, \alpha_n$ be a basis for $\mathfrak{a}$ as a $\mathbb{Z}$-module. To prove that $\sigma(\mathfrak{a})$ is a lattice, we need to show $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ are linearly independent, i.e. the following has nonzero determinant:

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \Re(\sigma_{r+1}(\alpha_1)) & \Im(\sigma_{r+1}(\alpha_1)) & \cdots \\ \sigma_1(\alpha_2) & \cdots & \sigma_r(\alpha_2) & \Re(\sigma_{r+1}(\alpha_2)) & \Im(\sigma_{r+1}(\alpha_2)) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

To do this we relate this to the matrix

$$B = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \sigma_{r+1}(\alpha_1) & \overline{\sigma_{r+1}(\alpha_1)} & \cdots \\ \sigma_1(\alpha_2) & \cdots & \sigma_r(\alpha_2) & \sigma_{r+1}(\alpha_2) & \overline{\sigma_{r+1}(\alpha_1)} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Note $\det(B) = \pm \operatorname{disc}(\alpha_1, \dots, \alpha_n)^{\frac{1}{2}} \neq 0$. Let $J = \begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix}$. Then

$$A = B \begin{pmatrix} I_r & 0 & 0 & \cdots \\ 0 & J & 0 & \cdots \\ 0 & 0 & J & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Using

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = [\mathcal{O}_K : \mathfrak{a}]^2 \cdot |\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})|$$

we get that the volume of a fundamental parallelopiped for $D$ is

$$\mu(D) = |\det(A)| = 2^{-s}|\det(B)| = 2^{-s}|\operatorname{disc}(\alpha_1, \dots, \alpha_n)|^{\frac{1}{2}} = 2^{-s} \cdot \mathbb{N}\mathfrak{a} \cdot |\Delta_K|^{\frac{1}{2}}.$$

(In particular, this is nonzero.) □

[1] This is the canonical embedding $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R}$: Indeed, by Chinese Remainder

$$K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{Q}[x]/(f(x)) \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{i=1}^{r} \mathbb{R}[x]/(x - \sigma_i\alpha) \times \prod_{j=1}^{s} (\mathbb{R}[x]/(x - \sigma_{r+j}\alpha)(x - \overline{\sigma_{r+j}}\alpha)) \cong \mathbb{R}^r \times \mathbb{C}^s.$$

**Theorem 3.2:** ideal-representative Let $\mathfrak{a}$ be a nonzero ideal in $\mathcal{O}_K$. Then $\mathfrak{a}$ contains a nonzero element $\alpha$ of $K$ with

$$|\operatorname{Nm}(\alpha)| \le \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \mathbb{N}\mathfrak{a} |\Delta_K|^{\frac{1}{2}}.$$

*Proof.* The norm on $K$ translates into the "norm"

$$\operatorname{Nm}(x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s}) = |x_1| \cdots |x_r| |z_{r+1}|^2 \cdots |z_{r+s}|^2.$$

However, $\mathbb{N}\mathbf{x} < r$ is by no means a compact convex set. Fortunately, however, we note by the AM-GM inequality that

$$norm-ineq-am-gm |\operatorname{Nm}(\mathbf{x})| = |x_1| \cdots |x_r| |z_{r+1}|^2 \cdots |z_{r+s}|^2 \le \left(\frac{\sum_{k=1}^r |x_k| + 2\sum_{k=1}^s |z_{r+k}|}{n}\right)^n. \tag{3.2}$$

Defining the norm $\|\cdot\|$ on $V = \mathbb{R}^r \times \mathbb{C}^s$ by

$$\|(x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s})\| = \sum_{k=1}^r |x_i| + 2\sum_{k=r+1}^s |z_i|,$$

and letting $B(t) = \{x \in V : \|x\| < t\}$, $B(\operatorname{Nm}, t) = \{x \in V : |\operatorname{Nm}(x)| < t\}$, we see from (3.2) that

$$norm-ineq-am-gm2 B(t) \subseteq B\left(\operatorname{Nm}, \frac{t^n}{n^n}\right). \tag{3.3}$$

To apply Minkowski we need some computations.

**Lemma 3.3:** class-volume The volume of $B(t) = \{x \in V : \|x\| < t\}$ is

$$\mu(B(t)) = 2^{r-s}\pi^s \frac{t^n}{n!}.$$

*Proof.* We write the complex variables as $z_k = x_k + y_k i$. Let

$$B'(t) = \{(x_1, \ldots, x_r, x_{r+1}, y_{r+1}, \ldots, x_{r+s}, y_{r+s}) \in B(t) : x_1, \ldots, x_r \ge 0\}.$$

Write $dV = dx_1 \cdots dx_n$. Using symmetry and a polar change of coordinates, we compute

$$volume1 \mu(B(t)) = 2^r \int_{B'(t)} dV\, dx_{r+1}\, dy_{r+1} \cdots dx_{r+s}\, dy_{r+s} \tag{3.4}$$

$$volume2 = 2^r \int_{x_1, \ldots, x_r \ge 0, \sum x_k + 2\sum \rho_k \le t} (\rho_{r+1} \cdots \rho_{r+s})\, dV\, d\rho_{r+1}\, d\theta_{r+1} \cdots d\rho_{r+s}\, d\theta_{r+s} \tag{3.5}$$

$$= 2^{r-2s} \int_{x_1, \ldots, x_r \ge 0, \sum x_k + \sum \rho_k \le t} (\rho_{r+1} \cdots \rho_{r+s})\, dV\, d\rho_{r+1}\, d\theta_{r+1} \cdots d\rho_{r+s}\, d\theta_{r+s}$$

$$= 2^{r-2s}(2\pi)^s \int_{x_1, \ldots, x_r \ge 0, \sum x_k + \sum \rho_k \le t} (\rho_{r+1} \cdots \rho_{r+s})\, dV\, d\rho_{r+1} \cdots d\rho_{r+s}$$

$$volume3 = 2^{r-s}\pi^s t^{(r+s)+s} \frac{1}{((r+s)+s)!} \tag{3.6}$$

$$= 2^{r-s}\pi^s \frac{t^n}{n!}.$$

Note (3.4) follows by symmetry, (3.5) follows from polar change of coordinates, and (3.6) follows from the lemma below. $\square$

**Lemma 3.4:**

$$\int_{x_i \geq 0, \sum x_i \leq t} x_1^{a_1} \cdots x_m^{a_m}\, dx_1 \cdots dx_m = t^{m+\sum_{i=1}^m a_i} \frac{\Gamma(a_1+1)\cdots\Gamma(a_m+1)}{\Gamma(a_1+\cdots+a_m+m+1)}.$$

*Proof.* Making the substitution $x_i = tx_i'$, $dx_i = t\, dx_i'$, we find that the integral equals

$$t^{m+\sum_{i=1}^m a_i} \int_{x_i \geq 0, \sum x_i \leq 1} x_1^{a_1} \cdots x_m^{a_m}\, dx_1 \cdots dx_m.$$

Hence it suffices to prove the lemma for $t = 1$.

For $m = 1$, note

$$\int_0^1 x^a\, dx = \frac{1}{a+1} = \frac{\Gamma(a+1)}{\Gamma(a+2)}.$$

For $m = 2$, let $B(\alpha, \beta) = \int_0^1 v^{\alpha-1}(1-v)^{\beta-1}\, dv$. We need to show $B(\alpha, \beta) = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$. By Fubini,

$$\Gamma(\alpha)\Gamma(\beta) = \int_0^\infty \int_0^\infty s^{\alpha-1}e^{-s}t^{\beta-1}e^{-t}\, ds\, dt = \int_0^\infty \int_0^\infty s^{\alpha-1}t^{\beta-1}e^{-(s+t)}\, ds\, dt.$$

Note $F : (0,\infty) \times (0,1) \to (0,\infty)^2$ with $F(u,v) = (uv, u(1-v))$ is a diffeomorphism. Indeed, it has an inverse $F^{-1}(s,t) = \left(t+s, \frac{s}{t+s}\right)$ hence is bijective and its Jacobian is $\det\left(\begin{smallmatrix} v & u \\ 1-u & -u \end{smallmatrix}\right) = u \neq 0$. Using the change of variables $(s,t) = F(u,v)$ gives

$$\begin{aligned}
\int_0^1 \int_0^\infty (uv)^{\alpha-1}(u(1-v))^{\beta-1}e^{-(uv+u(1-v))}u\, du\, dv &= \int_0^1 \int_0^\infty u^{\alpha+\beta-1}e^{-u}v^{\alpha-1}(1-v)^{\beta-1}\, du\, dv \\
&= \left(\int_0^\infty u^{\alpha+\beta-1}e^{-u}\, du\right)\left(\int_0^1 v^{\alpha-1}(1-v)^{\beta-1}\, dv\right) \\
&= \Gamma(\alpha+\beta)B(\alpha,\beta),
\end{aligned}$$

as needed.

Now we use induction; suppose the theorem proved for $m-1$. We have

$$\begin{aligned}
\int_{x_i \geq 0, \sum_{i=1}^m x_i \leq 1} x_1^{a_1} \cdots x_m^{a_m}\, dx_1 \cdots dx_m &= \int_0^1 x_m^{a_m} \int_{x_i \geq 0, \sum_{i=1}^{m-1} x_i \leq 1-x_m} x_1^{a_1} \cdots x_{m-1}^{a_{m-1}}\, dx_1 \cdots dx_{m-1}\, dx_m \\
&= \int_0^1 x_m^{a_m}(1-x_m)^{m-1+\sum_{i=1}^{m-1} a_i} \frac{\Gamma(a_1+1)\cdots\Gamma(a_{m-1}+1)}{\Gamma(a_1+\cdots+a_{m-1}+m)}\, dx_m \\
&= \frac{\Gamma(a_m+1)\Gamma(\sum_{i=1}^{m-1} a_i + m)}{\Gamma(a_1+\cdots+a_m+m+1)} \cdot \frac{\Gamma(a_1+1)\cdots\Gamma(a_{m-1}+1)}{\Gamma(a_1+\cdots+a_{m-1}+m)} \\
&= \frac{\Gamma(a_1+1)\cdots\Gamma(a_m+1)}{\Gamma(a_1+\cdots+a_m+m+1)},
\end{aligned}$$

using the induction hypothesis and the $m = 2$ case. $\square$

Taking

$$t = \sqrt[n]{n! \cdot \frac{2^{n-r}}{\pi^s} \cdot \mathbb{N}\mathfrak{a}|\Delta_K|^{\frac{1}{2}}}$$

we find by Lemma 3.3 that

$$\mu(B(t)) = 2^{r-s}\pi^s \frac{t^n}{n!} = 2^n \left(2^{-s}\mathbb{N}\mathfrak{a}|\Delta_K|^{\frac{1}{2}}\right) = 2^n \mu(D)$$

where $D$ is the fundamental parallelopiped. Note that $B(t)$ is a closed ball, and it is convex by the triangle inequality. Hence by Minkowski's Theorem, $B(t)$ contains an element of $\sigma(\mathfrak{a})$. For this element, we have by (3.3) that

$$\mathrm{Nm}_{K/\mathbb{Q}}(a) \le \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\mathbb{N}\mathfrak{a}|\Delta_K|^{\frac{1}{2}}. \qquad \square$$

**Theorem 3.5:** ideal-class-group-rep Suppose $K/\mathbb{Q}$ is an extension of degree $n$, and let $\Delta_K = \mathrm{disc}(K/\mathbb{Q})$. Let $2s$ be the number of nonreal complex embeddings of $K$. Then there exists a set of representatives for the ideal class group $C(K)$ consisting of integral ideals $\mathfrak{a}$ with

$$\mathbb{N}(\mathfrak{a}) \le \underbrace{\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s}_{C_K} |\Delta_K|^{\frac{1}{2}}.$$

*Proof.* Given a fractional ideal $\mathfrak{c}$, there exists $\mathfrak{b}$ such that

$$\mathfrak{b}\mathfrak{c} = (d)$$

is principal. By Theorem 3.2, there is an element $\beta \in \mathfrak{b}$ of norm at most $\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\mathbb{N}\mathfrak{b}|\Delta_K|^{\frac{1}{2}}$. Since $(\beta) \subseteq \mathfrak{b}$ we have

$$\mathfrak{a}\mathfrak{b} = (\beta)$$

for some $\mathfrak{a}$. Note $\mathfrak{a} \sim \mathfrak{b}^{-1} \sim \mathfrak{c}$, and taking norms of the above equation gives

$$\mathfrak{N}\mathfrak{a}\mathfrak{N}\mathfrak{b} = \mathfrak{N}(\beta) \le \left(\frac{4}{\pi}\right)^2 \frac{n!}{n^n}\mathbb{N}\mathfrak{b}|\Delta_K|^{\frac{1}{2}}.$$

Canceling $\mathfrak{N}\mathfrak{b}$ gives that $\mathfrak{a}$ is the desired representative. $\square$

**Theorem 3.6:** class-number-finite The class number of $K$ is finite.

*Proof.* By Theorem 3.5, every ideal class has a representative with norm at most $C_K|\Delta_K|^{\frac{1}{2}}$. Thus it suffices show the following (take $C = C_K|\Delta_K|^{\frac{1}{2}}$).

**Lemma 3.7:** finite-bounded-norm There are only a finite number of integral ideals $\mathfrak{a}$ with $\mathbb{N}\mathfrak{a} \le C$ (take $C = C_K|\Delta_K|^{\frac{1}{2}}$).

*Proof.* Suppose $\mathfrak{a}$ is an integral ideal. Write $\mathfrak{a} = \prod \mathfrak{p}_i^{r_i}$. Let $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$ and $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/(p_i)]$. Then

$$\mathbb{N}\mathfrak{a} = \prod_i p_i^{f_i r_i}.$$

Given $\mathbb{N}\mathfrak{a} \le C$, there are a finite possibilities for the $p_i$ and hence $\mathfrak{p}_i$, as well as for the $r_i$. □

□

The bound in Theorem 3.5 also gives the following corollaries.

**Theorem 3.8:** q-ramifies Every algebraic extension of $\mathbb{Q}$ ramifies over $\mathbb{Q}$.

*Proof.* It suffices to prove this statement for finite extensions. Let $K/\mathbb{Q}$ be a finite extension. By Theorem 3.2, every ideal contains a representative $\alpha$ with

$$1 \le |\operatorname{Nm}(\alpha)| \le \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}.$$

Hence we have

$$dk-bound|\Delta_K| \ge \frac{n^{2n}}{n!^2}\left(\frac{\pi}{4}\right)^{2s} > 1. \tag{3.7}$$

The last inequality comes from the fact that defining $a_n = \frac{n^{2n}}{n!^2}\left(\frac{\pi}{4}\right)^{2s}$, we have that $a_2 > 1$ and $\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{\frac{1}{2}}\left(1+\frac{1}{n}\right)^n > 1$ for $n \ge 2$.

Since $\Delta_K > 1$ and every prime dividing the discriminant ramifies (Theorem 6.1), $K/\mathbb{Q}$ is ramified. □

**Corollary 3.9:** There does not exist an irreducible monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree greater than 1 with discriminant $\pm 1$.

*Proof.* Let $f$ be an irreducible monic polynomial of degree greater than 1. Let $\alpha$ be a root of $f$. By Theorem 3.8, $\mathbb{Q}[\alpha]$ is ramified over $\mathbb{Q}$. By (3.7), $|\Delta_K| > 1$. Then

$$\operatorname{disc}(f) = \operatorname{disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = |\Delta_K| \cdot [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 > 1.$$ □

# §4 Example: Quadratic extensions

To compute the class group in quadratic extensions, note the following two facts.

1. The complete description of prime ideals is given by Example **??** (actually put this in!).

2. By Theorem 3.2, each ideal class has a representative of norm at most $\frac{4}{\pi}|\Delta_K|^{\frac{1}{2}}$.

In fact, Minkowski's bound can be improved in the quadratic case.

**Theorem 4.1:** (*) Let $K = \mathbb{Q}(\sqrt{d})$ where $d$ is a negative squarefree integer. Let

$$\mu = \begin{cases} \sqrt{\frac{|d|}{3}}, & d \equiv 1 \pmod 4 \\ 2\sqrt{\frac{|d|}{3}}, & d \equiv 2, 3 \pmod 4. \end{cases}$$

Every ideal class in $\mathcal{O}_K$ has a representative $\mathfrak{a}$ with

$$\mathfrak{N}\mathfrak{a} \le \mu.$$

*Proof.* First we show that every ideal $\mathfrak{a}$ has an element $a \neq 0$ with $\mathrm{Nm}_{K/\mathbb{Q}}(a) \le \mu\mathfrak{N}(\mathfrak{a})$. For a lattice $L$ let $\Delta(L)$ be the area of a fundamental parallelogram.

Note that $\mathrm{Nm}_{K/\mathbb{Q}}(z) = |z|^2$. An ideal $\mathfrak{a}$ of $K$ forms a lattice in $\mathbb{C}$. Let $a$ be the element of minimal nonzero norm in $\mathfrak{a}$ and $b$ be the element of minimal nonzero norm that is not a integer multiple of $a$. By the minimality assumption, since $b-a$ cannot be a integer multiple of $a$, we have

$$|b-a| \ge |b| \ge |a|.$$

Let $A, B$ denote the points $a, b$ and $O$ the origin. Using the fact that in a triangle the side lengths are in the same order least-to-greatest as the opposite angles, we get that in the triangle $AOB$, the angle at $O$ is largest, in particular at least $60°$. Let $O'$ be so that $OAO'B$ is a parallelogram. The minimality assumption similarly forces $OO' \ge AO, AO'$, so we get $\angle OAO' \ge 60°$. Thus

$$angle 60° \le \angle AOB \le 120°. \tag{3.8}$$

Furthermore, the parallelogram with sides $OA$ and $OB$ is a fundamental parallelogram: Suppose $C$ is the point $c \in \mathfrak{a}$, and is in the triangle $OAB$ but not any of the vertices. Let $OC$ intersect $AB$ at $C'$. We have $\angle OC'B > \angle OAB \ge \angle ABO = \angle C'BO$, where the middle inequality is from $OB \ge OA$. Hence looking at $\triangle OC'B$, $OB > OC' \ge OC$, contradicting minimality of $b$. Similarly, if $C$ is in $ABO'$, then we have $|a+b-c| < |b|$, also a contradiction.

By (3.8), the area of the fundamental parallelogram is

$$\Delta(\mathcal{O}_K)\mathfrak{N}\mathfrak{a} = \Delta(\mathfrak{a}) = |ab| \sin \angle AOB \ge |a|^2 \frac{\sqrt{3}}{2} = \frac{\sqrt{3}}{2} \mathrm{Nm}_{K/\mathbb{Q}}(a).$$

Solving gives

$$\mathrm{Nm}_{K/\mathbb{Q}}(a) \le \frac{2}{\sqrt{3}} \Delta(\mathcal{O}_K)\mathfrak{N}\mathfrak{a}.$$

Finally note that for $d \equiv 1 \pmod 4$, a basis for $\mathcal{O}_K$ is $\left(1, \frac{1+\sqrt{d}}{2}\right)$ while for $d \equiv 2, 3 \pmod 4$ the basis is $\left(1, \sqrt{d}\right)$. The fundamental parallelograms have areas $\frac{\sqrt{d}}{2}$ and $\sqrt{d}$, respectively, giving

$$\mathrm{Nm}_{K/\mathbb{Q}}(a) \le \mu\mathfrak{N}\mathfrak{a}.$$

Given a fractional ideal $\mathfrak{c}$, there exists $\mathfrak{b}$ such that

$$\mathfrak{b}\mathfrak{c} = (d)$$

is principal. By the above, there is an element $b \in \mathfrak{b}$ of norm at most $\mu \mathfrak{N}\mathfrak{b}$. Since $(b) \subseteq \mathfrak{b}$ we have

$$\mathfrak{a}\mathfrak{b} = (b)$$

for some $\mathfrak{a}$. Note $\mathfrak{a} \sim \mathfrak{b}^{-1} \sim \mathfrak{c}$, and taking norms of the above equation gives

$$\mathfrak{N}\mathfrak{a}\mathfrak{N}\mathfrak{b} = \mathfrak{N}(b) \leq \mu \mathfrak{N}\mathfrak{b}.$$

Canceling $\mathfrak{N}\mathfrak{b}$ gives that $\mathfrak{a}$ is the desired representative. □

We give an example of computing the class group. The general procedure to compute the class group of $A = \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{d})$ and $d$ is negative and squarefree is as follows.

1. List the primes $p \leq \lfloor \mu \rfloor$.
2. For each $p$, determine whether $p$ splits in $A$ by checking whether

   $$f(x) := \begin{cases} x^2 - x + \frac{d-1}{4}, & d \equiv 1 \pmod 4 \\ x^2 - d, & d \equiv 2, 3 \pmod 4 \end{cases}$$

   is irreducible.
3. If $p = \mathfrak{a}\overline{\mathfrak{a}}$ splits in $A$, include it in the list of generators.
4. Compute the norm of some small elements (with prime divisors in the list found above), like $k + \delta$ for $k \in \mathbb{N}_0$, $\delta = \sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ depending on $d \pmod 4$. Factor $\mathrm{Nm}_{K/\mathbb{Q}}(a)$ to factor

   $$(a)(\overline{a}) = (\mathrm{Nm}_{K/\mathbb{Q}}(a));$$

   match factors using unique factorization. Note $(a) \sim (\overline{a}) \sim 1$. Repeat until there are enough relations to determine the group.
5. For the prime 2, if $d \equiv 2, 3 \pmod 4$, 2 ramifies, $(2) = \mathfrak{p}^2$, and $\mathfrak{p}$ has order 2 for $d \neq -1, -2$. (Note $\mathfrak{p} = (2, \delta)$ and $(2, 1 + \delta)$ in these two cases, respectively.)

We first consider the cases when the class group is trivial.

**Theorem 4.2:** The rings

$$\mathbb{Z}[\sqrt{-1}],\ \mathbb{Z}[\sqrt{-2}],\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right],\ d = -3, -7, -19, -43, -67, -163$$

are unique factorization domains.

In fact, they are the only ones (part of Gauss's class number problem).

*Proof.* Note $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ are Euclidean domains and hence unique factorization domain.

The class group of $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ is generated by the classes of prime ideals whose norms are prime integers $p \le \mu$, which are the factors of $(p)$ when it splits. When $d \equiv 1 \pmod 4$ as in all the remaining cases, an integer prime $p$ remains prime in $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ iff $x^2 - x - \frac{1}{4}(1-d)$ is irreducible modulo $p$, iff $x^2 - x - \frac{1}{4}(1-d)$ has no zero modulo $p$. We show that for $d = -7, -11, -19, -43, -67, -163$, $x^2 - x - \frac{1}{4}(1-d)$ is irreducible modulo all primes less than $\mu$. Then no prime ideals have norms that are prime integers $p \le \mu$, and the only ideal class is that of the principal ideals. It follows that $\mathbb{Z}[\sqrt{d}]$ is a principal ideal domain and hence a unique factorization domain.

| $d$ | $\lfloor\mu\rfloor, \mu = \sqrt{\frac{\lvert d\rvert}{3}}$ | $x^2 - x + \frac{1}{4}(1-d)$ | Primes $p \le \lfloor\mu\rfloor$, $x^2 - x + \frac{1}{4}(1-d) \pmod p$ |
|---|---|---|---|
| -7 | $\left\lfloor\sqrt{\frac{7}{3}}\right\rfloor = 1$ | | None |
| -11 | $\left\lfloor\sqrt{\frac{11}{3}}\right\rfloor = 1$ | | None |
| -19 | $\left\lfloor\sqrt{\frac{19}{3}}\right\rfloor = 2$ | $x^2 - x + 5$ | 2: $x^2 + x + 1 = 1$ for $x = 0, 1$ |
| -43 | $\left\lfloor\sqrt{\frac{43}{3}}\right\rfloor = 3$ | $x^2 - x + 11$ | 2: $x^2 + x + 1 = 1$ for $x = 0, 1$<br>3: $x^2 - x - 1 = \begin{cases} -1 & \text{for } x = 0, 1 \\ 1 & \text{for } x = 2 \end{cases}$ |
| -67 | $\left\lfloor\sqrt{\frac{67}{3}}\right\rfloor = 4$ | $x^2 - x + 17$ | 2: $x^2 + x + 1 = 1$ for $x = 0, 1$<br>3: $x^2 - x - 1 = \begin{cases} -1 & \text{for } x = 0, 1 \\ 1 & \text{for } x = 2 \end{cases}$ |
| -163 | $\left\lfloor\sqrt{\frac{163}{3}}\right\rfloor = 7$ | $x^2 - x + 41$ | 2: $x^2 + x + 1 = 1$ for $x = 0, 1$<br>3: $x^2 - x - 1 = \begin{cases} -1 & \text{for } x = 0, 1 \\ 1 & \text{for } x = 2 \end{cases}$<br>5: $x^2 - x + 1 = \begin{cases} 1 & \text{for } x = 0, 1 \\ 3 & \text{for } x = 4, 2 \\ 2 & \text{for } x = 3 \end{cases}$<br>7: $x^2 - x - 1 = \begin{cases} -1 & \text{for } x = 0, 1 \\ 1 & \text{for } x = 2, 6 \\ 5 & \text{for } x = 3, 5 \\ 4 & \text{for } x = 4 \end{cases}$ |

□

Change for consistent notation.

**Example 4.3:** We compute the class group of $\mathbb{Z}[\sqrt{-41}]$.

For $d = -41$, $\lfloor\mu\rfloor = \left\lfloor 2\sqrt{\frac{41}{3}}\right\rfloor = 7$. Modulo 2, 3, 5, and 7, -41 is congruent to 1, 1, 4, and

1, which are all squares. Factor

$$\begin{aligned}(2) &= A\overline{A}\\ (3) &= B\overline{B}\\ (5) &= C\overline{C}\\ (7) &= D\overline{D}\end{aligned}$$

Then the class group is generated by $\langle A\rangle, \langle B\rangle, \langle C\rangle, \langle D\rangle$. (Note that $\langle\overline{A}\rangle = \langle A\rangle^{-1}$, etc.) We have

$$(1+\delta)(\overline{1+\delta}) = (42) = (2)(3)(7) = A\overline{A}B\overline{B}D\overline{D}.$$

If a prime ideal $P$ divides $(1+\delta)$ then $\overline{P}$ divides $(\overline{1+\delta})$. Hence the conjugate factors are divided between $(1+\delta)$ and $(\overline{1+\delta})$. Without loss of generality, we can suppose

$$(1+\delta) = ABD.$$

The class of a principal ideal is the identity in the class group, so

$$\langle A\rangle\langle B\rangle\langle D\rangle = 1.e1 \tag{3.9}$$

Next consider

$$(2+\delta)(\overline{2+\delta}) = (45) = (3)^2(5) = B^2\overline{B}^2C\overline{C}.$$

Note that 3 does not divide $2+\delta$ so $B\overline{B} = (3)$ doesn't divide $(2+\delta)$. Thus $B^2$, $\overline{B}^2$ divide $(2+\delta)$, $(\overline{2+\delta})$ in some order. Since we haven't distinguished between $C$ and $\overline{C}$ yet, we may assume WLOG that $\langle B\rangle^2\langle\overline{C}\rangle$, $\langle\overline{B}\rangle^2\langle C\rangle$ are equal to $(2+\delta)$ and $(\overline{2+\delta})$ in some order, and

$$\langle B\rangle^2\langle\overline{C}\rangle = \langle B\rangle^2\langle C\rangle^{-1} = 1$$

or

$$\langle C\rangle = \langle B\rangle^2 .cb2 \tag{3.10}$$

Similarly, looking at

$$(3+\delta)(\overline{3+\delta}) = (50) = (2)(5)^2 = A\overline{A}C^2\overline{C}^2,$$

we get that

$$\langle A\rangle\langle\overline{C}\rangle^2 = 1 \text{ or } \langle\overline{A}\rangle\langle\overline{C}\rangle^2 = 1.$$

Noting that $A = \overline{A}$ (since $(2) = (2, 1+\delta)(2, 1-\delta)$ and $(2, 1+\delta) = (2, 1-\delta)$ when $d \equiv 3 \pmod 4$ by [Artin, 13.8.4]),

$$\langle A\rangle = \langle C\rangle^2 .ac2 \tag{3.11}$$

From (3.10) we may omit $\langle C\rangle$ from the list of generators for the group, from (3.11) we may omit $\langle A\rangle$, and from (3.9) we may omit $\langle D\rangle$. Thus the class group is the cyclic group generated by $\langle B\rangle$. From (3.10) and (3.11), we get

$$\langle A\rangle = \langle B\rangle^4 .ab4 \tag{3.12}$$

Since $A$ is not principal, $\langle B\rangle^4 \neq 1$. Note $\langle A\rangle = \left\langle \overline{A} \right\rangle = \langle A\rangle^{-1}$ implies $\langle A\rangle^2 = 1$. Combining this with (3.12) gives that $\langle B\rangle^8 = 1$. Since $\langle B\rangle^n \neq 1$ for any proper divisor $n$ of 8 (it sufficed to check $n = 4$), the class group is cyclic of order 8, $C_8$.

# Chapter 4
# The algebra of quadratic forms

quadratic-forms

We follow Cox [5], except for the proof of Gauss composition, when we follow Cassels (add reference). The last section is based on Bhargava's paper [1].

## §1 Quadratic forms

quadratic-forms1

**Definition 1.1:** Let $R$ be an integral domain. A **quadratic form** on $R$ is a function on $R^n$, in the form

$$f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j.$$

Supposing $R$ is a UFD, we say $f$ is **primitive** iff $\gcd_{1 \le i \le j \le n} a_{ij} = 1$.

A quadratic form may be represented by a matrix

$$Q = \begin{bmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \frac{a_{1,n-1}}{2} & \frac{a_{1,n}}{2} \\ \frac{a_{12}}{2} & a_{22} & \cdots & \frac{a_{2,n-1}}{2} & \frac{a_{2,n}}{2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{a_{1,n-1}}{2} & \frac{a_{2,n-1}}{2} & \cdots & a_{n-1,n-1} & \frac{a_{n-1,n}}{2} \\ \frac{a_{1,n}}{2} & \frac{a_{2,n}}{2} & \cdots & \frac{a_{n-1,n}}{2} & a_{nn} \end{bmatrix}$$

(working in $K = \mathrm{Frac}(R)$ as necessary to allow division by 2); we have

$$f(\mathbf{x}) = \mathbf{x} Q \mathbf{x}^T.$$

**Definition 1.2:** We say two forms $f$ and $g$ are **equivalent** if there are is an invertible matrix $A$ (i.e. a matrix with determinant a unit) such that

$$f(\mathbf{x}) = g(\mathbf{x} A^T).$$

We say $f$ and $g$ are **properly equivalent** if $\det(A) = 1$.

Note that the matrices corresponding to $f$ and $g$ are related by

$$Q_f = A^T Q_g A.$$

For the rest of this chapter, we will focus on integral binary quadratic forms, i.e. those in two variables over $\mathbb{Z}$.

# §2 Representing integers

**Definition 2.1:** We say that $f$ **represents** $n$ if there exists $\mathbf{x} = (x_1, \dots, x_n)$ such that $f(\mathbf{x}) = n$. We say that $f$ **properly represents** $n$ if we can choose $\mathbf{x}$ so that $\gcd(x_1, \dots, x_n) = 1$.

**Lemma 2.2:** pr-repA form $f(x, y)$ properly represents $n$ if and only if $f(x, y)$ is properly equivalent to the form $nx^2 + b'xy + c'y^2$ for some $b', c' \in \mathbb{Z}$.

*Proof.* If $f(p, q) = n$ with $(p, q)$ relatively prime, then by Bézout we can find $r, s$ such that $ps - qr = 1$. Let $f(x, y) = ax^2 + bxy + cy^2$. Then $f$ is equivalent to

$$f(px + ry, qx + sy) = \underbrace{f(p, q)}_{n} x^2 + (2apr + bps + brq + 2cqs)xy + f(r, s)y^2.$$

For the converse, note that $nx^2 + bxy + cy^2$ properly represents $n$ by taking $(x, y) = (1, 0)$. □

**Theorem 2.3:** represent-iff-square Let $n \neq 0$ and $d$ be integers. Then the following are equivalent.

1. There exists a binary quadratic form of discriminant $d$ which properly represents $n$.

2. $d$ is square modulo $4n$.

*Proof.* Suppose $f$ is a binary quadratic form of discriminant $d$ properly representing $n$. Then by Lemma 2.2, $f$ is equivalent to some form $nx^2 + bxy + cy^2$. Hence the discriminant is $d = b^2 - 4nc$, and $d \equiv b^2 \pmod{4n}$.

Conversely, suppose $b^2 \equiv d \pmod{4n}$, so $b^2 = d + 4nc$ for some integer $n$, i.e. $d = b^2 - 4nc$. Then

$$f(x, y) = nx^2 + bxy + cy^2$$

properly represents $n$, as $f(1, 0) = n$, and $\operatorname{disc}(f) = b^2 - 4nc = d$. □

**Corollary 2.4:** cor-represent-iff-square Let $n$ be an integer and $p$ an odd prime not representing $n$. Then $\left(\frac{-n}{p}\right) = 1$ iff $p$ is represented by a primitive form of discriminant $-4n$.

*Proof.* Note $\left(\frac{-n}{p}\right) = 1$ iff $\left(\frac{-4n}{p}\right) = 1$, and this is equivalent to the second statement by the theorem. □

The results in this section are particularly useful if there are few quadratic forms with determinant $d$. There is a method to list all these quadratic forms, as we will show in the next section.

# §3 Reduction of quadratic forms

We would like to have a canonical representative for every equivalence class of binary quadratic forms. We choose the one with "smallest" coefficients. This is made precise by the following definition.

**Definition 3.1:** A positive definite binary quadratic form $ax^2 + bxy + cy^2$ is **reduced** if it is primitive and

$$|b| \le a \le c$$

and

$$b \ge 0 \text{ if } |b| = a \text{ or } a = c.$$

**Theorem 3.2:** one-reduced Every equivalence class of primitive binary quadratic forms contains exactly one reduced form.

There's a more enlightening proof using the action of GL2 on the upper half plane.

*Proof.* Existence, Step 1: We first show there is a form in the class with $|b| \le a \le c$.

Take the form $f(x) = ax^2 + bxy + cy^2$ in the equivalence class such that $|b|$ is smallest. Note $a, c > 0$ because the form is positive definite. We claim that $a, c \ge |b|$. Indeed, we have

$$f(x + my, y) = ax^2 + (2am + b)xy + (am^2 + c)y^2,$$

so $-b \le 2am + b \le b$ for all $m \in \mathbb{Z}$, giving $a \ge |b|$. Similarly, $c \ge |b|$.

Next, if $a > c$, then replacing $(x, y)$ by $(-y, x)$ we get $c > a \ge |b|$.

Step 2: The form is reduced unless $b < 0$ and $a = -b$ or $a = c$. We tackle these cases next. In these cases $ax^2 - bxy + cy^2$ is reduced, so it suffices to show $ax^2 \pm bxy + cy^2$ are equivalent. In these two cases we make the following substitutions:

$$\begin{aligned} f(x,y) = ax^2 - axy + cy^2 &\implies & f(x+y,y) = ax^2 + axy + cy^2 \\ f(x,y) = ax^2 + bxy + ay^2 &\implies & f(-y,x) = ax^2 - bxy + ay^2. \end{aligned}$$

Uniqueness, Step 1: We claim that for $(x, y) \in \mathbb{Z}^2$ with $xy \ne 0$, and $f(x, y) = ax^2 + bxy + cy^2$ with $a, c \ge |b|$, we have

$$f(x, y) \ge (a - |b| + c) \min(x^2, y^2).$$

Indeed, without loss of generality assume $x \ge y$. Then

$$f(x, y) \ge (a - |b|)xy + cy^2 \ge (a - |b| + c)y^2.$$

As a corollary, for $xy \neq 0$,

$$ax^2 + bxy + cy^2 \geq a - |b| + c$$

with equality iff $x, y = \pm 1$, $xy = -\operatorname{sign}(b)$.

Step 2: To distinguish between reduced forms, we examine the smallest nonzero values attained by a them, and the number of primitive solutions to them. Note all solutions $(x, y)$ with $xy = 0$ and one of $|x|, |y| \geq 2$ are removed from consideration.

1. If $|b| < a < c$, then the smallest values attained by $f$ primitively are

   $$a < c < a - |b| + c$$

   with solutions $(\pm 1, 0)$, $(0 \pm 1)$ and $\pm(-1, \operatorname{sign}(b))$ respectively.

2. If $b \geq 0$ and $|b| = a < c$, then the smallest values attained by $f$ primitively are

   $$a < c = a - |b| + c;$$

   the first has 2 solutions and the latter has 4 primitive solutions.

3. If $b \geq 0$ and $|b| < a = c$, then the smallest values attained by $f$ primitively are

   $$a = c < a - |b| + c;$$

   the first has 4 solutions and the latter has 2 primitive solutions.

4. If $b \geq 0$ and $|b| = a = c$, then the smallest value attained by $f$ primitively is

   $$a = c = a - |b| + c$$

   which has 6 primitive solutions.

After examining this data, the only reduced forms that could be equivalent are those falling in the first category with opposite $b$'s, i.e. $ax^2 \pm bxy + cy^2$. But any change of variables sending one to the other must preserve the solutions $(\pm 1, 0)$ and $(0, \pm 1)$, so must have matrix $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$. If this matrix has determinant 1, then it must be $\pm I$ and cannot change between the two forms. $\square$

Suppose $d < 0$; note that there is an algorithm to list all reduced quadratic forms with discriminant $d$. The conditions $|b| \leq a \leq c$ and $b^2 - 4ac = d$ give

$$d = b^2 - 4ac \leq a^2 - 4a^2 = -3a^2.$$

Hence

$$a \leq \sqrt{-\frac{d}{3}}.$$

We simply check for solutions to $b^2 - 4ac = d$ for all $0 \leq |b| \leq a \leq \sqrt{-\frac{d}{3}}$.

## 3.1 Examples

**Example 3.3:** When $n = 1, 2, 3$, the above check gives that the only reduced form of discriminant $-4n$ is $x^2 + ny^2$.

Combining this fact with Theorem 2.3, we get that $f$ properly represents $m$ iff $d := -4n$ is a square modulo $4m$, i.e. $-1$ is a square modulo $m$. Thus we have the chain of equivalences:

1. $f$ represents $m$.
2. $f$ properly represents $\frac{m}{k^2}$ for some square factor $k^2 \mid m$.
3. $d$ is a square modulo $\frac{m}{k^2}$ for some $m$.
4. $d$ is a square modulo $\frac{m}{k^2}$ for the largest square factor $k^2 \mid m$.
5. $d$ is a square modulo $p$ for every $p \mid m$ with $\mathrm{ord}_p(m)$ odd.

By quadratic reciprocity, we have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1, 3 \pmod 8 \\ -1, & p \equiv 5, 7 \pmod 8 \end{cases}$$

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3 \\ -1, & p \equiv 2 \pmod 3. \end{cases}$$

Hence we have the following.

| $m$ represented by | iff every such prime has even exponent in $m$ |
|---|---|
| $x^2 + y^2$ | $p \equiv 3 \pmod 4$ |
| $x^2 + 2y^2$ | $p \equiv 5, 7 \pmod 8$ |
| $x^2 + 3y^2$ | $p \equiv 2 \pmod 3$ |

Compare this with the proof using factorization in $\mathbb{Z}[\sqrt{-d}]$.[1] In particular, note that $\mathbb{Z}[\sqrt{-d}]$ is a UFD when $d = 1, 2$, and in these cases, there is exactly one form of discriminant $-4d$. *This is not a coincidence!*

Next we show the following.

**Example 3.4:** x25y2 A positive integer $n$ is represented by $x^2 + 5y^2$ iff

1. Any prime $p \equiv 11, 13, 17, 19 \pmod{20}$ appears in $n$ with even exponent.
2. There are an even number of prime divisors that are $p \equiv 2, 3, 7 \pmod{20}$, counting multiplicity.

[1] When $d = 3$ we have to be slightly careful.

3. (No restriction on primes $p \equiv 1, 5, 9 \pmod{20}$.)

Note this condition is quite different from the ones before!

*Proof 1.* This time we have to check $a \le \sqrt{-\frac{20}{3}} < 3$. The reduced forms of discriminant $-20$ are

$$\begin{aligned} f(x) &:= x^2 + 5y^2 \\ g(x) &= 2x^2 + 2xy + 3y^2. \end{aligned}$$

We run into trouble already: Theorem 2.3 fails to distinguish between these. We still start with the same argument, though.

Step 1: By Corollary 2.3, a prime $p$ is represented by $f$ or $g$ iff $\left(\frac{-5}{p}\right) = 1$. By quadratic reciprocity,

$$\left(\frac{-5}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = \begin{cases} 1, & p \equiv 1, 3, 7, 9 \pmod{20} \\ -1, & p \equiv 11, 13, 17, 19 \pmod{20}. \end{cases}$$

Step 2: Now we distinguish between these two cases. By checking modulo 4, we see that $f$ only represents primes $p \equiv 1, 9 \pmod{20}$ (and 5) and $g$ only represents primes $p \equiv 3, 7 \pmod{20}$ (and 2).[2] By Step 1, $f$, $g$ must represent all of these respective primes.

Step 3: We have the desired result for primes. How to pass to products of primes? First note that primes $p \equiv 11, 13, 17, 19 \pmod{20}$ have to appear with even exponent (if $x^2 + 5y^2 \equiv 0 \pmod{p}$, since $\left(\frac{-5}{p}\right) = -1$, we must have $p \mid x, y$; now divide $x, y$ by $p$ and repeat).

Now consider the magical identity

$$x25y2 - magic(2x^2 + 2xy + 3y^2)(2z^2 + 2zw + 3w^2) = (2xy + xw + yz + 3yw)^2 + 5(xw - yz)^2, \tag{4.1}$$

which says that a product of numbers represented by $g$ is represented by $f$! This immediately gives the sufficiency condition.

For the necessary condition, note we may divide $x, y$ by 2 until they are not both even. Now take it modulo 8 to see that $n \equiv 1, 4, 5, 6 \pmod{8}$. This gives that item 2 is necessary. $\square$

Wait a minute. Where does the magical identity come from? Historically this was the way such problems were solved, and in fact the motivation for *composing* quadratic forms: for primitive quadratic forms $f, g, h$, we say $f \circ g = h$ iff there exist integral bilinear forms $B_1, B_2$ satisfying certain conditions such that

$$f(\mathbf{x})g(\mathbf{y}) = h(B_1(\mathbf{x}, \mathbf{y}), B_2(\mathbf{x}, \mathbf{y})).$$

[2]These sets are disjoint; we say $f, g$ are unique in their *genus*.

We won't go into the historical details, because the modern way of thinking of composition is cleaner (see Section 5). We know we had the "composition law"

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2.$$

We can view this as coming from the identity

$$fermat-id-explained\, \mathrm{Nm}_{K/\mathbb{Q}}(a+bi)\,\mathrm{Nm}_{K/\mathbb{Q}}(c+di) = \mathrm{Nm}_{K/\mathbb{Q}}((a+bi)(c+di)) \quad (4.2)$$

where $K=\mathbb{Q}(i)$, so $\mathrm{Nm}_{K/\mathbb{Q}}(z)=|z|^2$. We now look at a different proof of Example 3.4.

*Proof 2.* This time the complication comes from that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, nor PID; its ideal class group has order 2, with representatives

$$\begin{aligned}\mathfrak{a} &= 1\\ \mathfrak{b} &= (3, 1+\sqrt{-5}).\end{aligned}$$

Step 1: Let $p$ be prime. As in the proof of Theorem **??**.**??**, we factor the equation $x^2+5y^2=p$ in $\mathbb{Z}[\sqrt{-5}]$ to get

$$(x+\sqrt{-5}y)(x-\sqrt{-5}y)=p.$$

Now we know the ideal $(p)$ splits iff $x^2+5 \pmod p$ splits, i.e. $\left(\frac{-5}{p}\right)=1$. We calculated that this happens when $p\equiv 1,3,5,7,9 \pmod{20}$.

Step 2: So if $p$ is of the above form, we know that either $p$ is a product of two principal ideals, or two (conjugate) ideals similar to $\mathfrak{b}$. In the two cases, we have respectively

$$\begin{aligned}(p) &= (\lambda)(\overline{\lambda})\\ (p) &= \lambda(3,1+\sqrt{-5})\overline{\lambda}(3,1+\sqrt{-5})\end{aligned}$$

for some $\lambda\in\mathbb{Q}(\sqrt{-5})$. Then calculating the norm of the ideal in $K=\mathbb{Q}(\sqrt{-5})$ gives

$$\begin{aligned}p &= \mathrm{Nm}_{K/\mathbb{Q}}(\lambda)\\ p &= \underbrace{\mathfrak{N}((3,1+\sqrt{-5}))}_{3}\mathrm{Nm}_{K/\mathbb{Q}}(\lambda)^2.\end{aligned}$$

Let $\lambda = x+y\sqrt{-5}$. In the first case, we must have $p=x^2+5y^2$, so $p\equiv 1,5,9 \pmod{20}$, while in the second case, we must have $p=3(x^2+5y^2)$ ($x,y\in\mathbb{Q}$, here) so when $p$ is odd, $p\equiv 3\cdot 1, 3\cdot 9 \pmod{20}$. (We can check that $x,y$ do not have 2 or 5 in the denominator by an infinite descent argument, so we may consider $x,y\in\mathbb{Z}/20\mathbb{Z}$.) $p=2$ is possible as $(2,1+\sqrt{-5})^2=(2)$. Thus again we've distinguished between the two cases.

Step 3: A prime $p\equiv 1,5,9 \pmod{20}$ splits into two principal ideals, a prime $p\equiv 2,3,7 \pmod{20}$ splits into two ideals of type $\mathfrak{b}$, and a prime $p\equiv 11,13,17,19 \pmod{20}$ remains prime. In order for $(n)$ to split into two principal ideals, we must be able to write

$$(n)=\mathfrak{c}\overline{\mathfrak{c}}$$

where $\mathfrak{c}$ is a product of ideals, containing an *even* number of prime ideals of type $\mathfrak{b}$, and $\overline{\mathfrak{c}}$ contains the conjugates of those ideals. (Two ideals of type $\mathfrak{b}$ multiply to a principal ideal.) The result follows. $\square$

It seems like the quadratic forms in the first proof are related to the ideals in the second proof. This is indeed the case: we can explain (4.1) similarly to (4.2) by

$$\begin{aligned}&\frac{\mathrm{Nm}_{K/\mathbb{Q}}(2x+(1+\sqrt{-5})y)}{\mathfrak{N}(2,1+\sqrt{-5})}\cdot\frac{\mathrm{Nm}_{K/\mathbb{Q}}(2z+(1+\sqrt{-5})w)}{\mathfrak{N}(2,1+\sqrt{-5})}\\ =&\frac{\mathrm{Nm}_{K/\mathbb{Q}}((2x+(1+\sqrt{-5})y)(2z+(1+\sqrt{-5})w))}{\mathfrak{N}((2))}\end{aligned}$$

The two forms on the LHS are exactly those on the LHS of (4.1) while that on the RHS can be written in the form $B_1^2+5B_2^2$ because $\frac{1}{2}(2x+(1+\sqrt{-5})y)(2z+(1+\sqrt{-5})w)$ is an integral ideal. We will see that in this way the group law on ideal classes translates into a group law on quadratic forms.

After we establish Gauss composition, we will show the equivalence between a quadratic form $Q$ representing a prime $p$, and $(p)$ splitting into ideals of a certain form (Theorem 5.4). The above proof was a specific example of this.

# §4 Ideals on quadratic rings

**Definition 4.1:** We will be considering rings that are free $\mathbb{Z}$-modules of finite rank. We call such rings **quadratic**, **cubic**, **quartic**, and **quintic**, if the rank is 2, 3, 4, or 5, respectively.

The rings we are primarily interested are integral domains, which are exactly the rings that can be embedded in field extensions.

**Definition 4.2:** An **order** $\mathcal{O}$ in a finite extension $K/\mathbb{Q}$ is a subring of $K$ containing 1, that is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.

The maximal order of $K$ is simply $\mathcal{O}_K$, the ring of integers of $K$.

**Definition 4.3:** Let $R$ be a ring that is a free $\mathbb{Z}$-module of finite rank. The **conductor** of $R$ is the greatest integer $n$ for which there exists a ring $T$ such that

$$\mathcal{O}=\mathbb{Z}+nT.$$

(Necessarily, $T$ has the same rank.)

If $S$ is a quadratic ring then $S=\langle 1,\tau\rangle$ for some $\tau$ satisfying a quadratic equation $\tau^2+b\tau+c=0$. If this polynomial is irreducible over $\mathbb{Z}$, then $S$ can be embedded in a quadratic field extension. Otherwise, $S$ is not an integral domain. We make the following definitions. The first four are equivalent to our previous definitions when $S$ is integrally closed.

1. The discriminant of $S$ is the discriminant of the characteristic polynomial, $b^2 - 4c$.
2. Conjugation is the linear transformation that takes 1 to 1 and switches the zeros of $x^2 + bx + c$.
3. The norm of an element $\alpha \in S$ is $\alpha\overline{\alpha}$.
4. The numerical norm $\mathfrak{N}_R(\mathfrak{a})$ of an ideal $\mathfrak{a} \in R$ to be $[R : I] = |R/I|$.[3]
5. A basis $(\alpha, \beta)$ for $\mathfrak{a} \subseteq R$ is positively oriented if

$$\frac{\begin{vmatrix} \alpha & \overline{\alpha} \\ \beta & \overline{\beta} \end{vmatrix}}{\operatorname{disc}(S)} = \frac{\alpha\overline{\beta} - \beta\overline{\alpha}}{d} > 0.$$

We now describe all quadratic rings.

**Proposition 4.4:** There is a bijection between $D = \{d \in \mathbb{Z} : d \equiv 0, 1 \pmod 4\}$ and quadratic rings (up to isomorphism), given by

$$S : d \mapsto \mathbb{Z}[\tau_d]$$

where $\tau_d$ satisfies a monic quadratic equation with discriminant $d$.

Moreover,

$$d = f^2 d_K,$$

where $f$ is the conductor of $\mathbb{Z}[\tau_d]$ and, when $d$ is nonsquare, $d_K$ is the discriminant of $\mathbb{Q}(\tau_d)$ ($d_K \equiv 0, 1 \pmod 4$ and $16 \nmid d_K$).

1. An integer $d \in D$ corresponds to a integral domain if and only if $d$ is not a square.
2. If $d = 0$ then $S(d) = \mathbb{Z}[x]/(x^2)$.
3. If $d$ is a nonzero square then $S(d) = \mathbb{Z} \cdot (1, 1) + \sqrt{d}(\mathbb{Z} \oplus \mathbb{Z})$.
4. If $d_K \equiv 1 \pmod 4$, $d_K \neq 1$, then $S(d) = \mathbb{Z}[f\tau] = \langle 1, f\tau \rangle$ where $\tau = \frac{1+\sqrt{d_K}}{2}$.
5. If $d_K \equiv 0 \pmod 4$ then $S(d) = \mathbb{Z}[f\tau] = \langle 1, f\tau \rangle$ where $\tau = \frac{\sqrt{d_K}}{2}$—the root of the nonsquare part of $d$.

*Proof.* Note the map is well-defined, because any two quadratic equations with discriminant $d$, say $x^2 + b_j x + c_j$, $j = 1, 2$, have $b_1 \equiv b_2 \equiv d \pmod 2$ and hence are related by the change of variable $x \mapsto x + k$ for some $k$. The map is injective because the discriminant doesn't change under replacing $\tau$ with $\tau + k$.

[3]For fractional ideals $\mathfrak{a}$, i.e. $R$-submodules of $R \otimes_{\mathbb{Z}} \mathbb{Q}$, take a fractional ideal $\mathfrak{b}$ containing $\mathfrak{a}$ and $R$ and define $\mathfrak{N}_R(\mathfrak{a}) = \frac{[\mathfrak{b}:\mathfrak{a}]}{[\mathfrak{b}:R]}$.

For item 1, note $d$ is a square iff the characteristic polynomial factors. Item 2 is clear; for item 3 note that we have the homomorphism

$$\begin{aligned}\mathbb{Z}[\tau]/(\tau^2-d) &\hookrightarrow \mathbb{Z}[\tau]/(\tau-\sqrt{d})\times\mathbb{Z}[\tau]/(\tau+\sqrt{d})\cong\mathbb{Z}\times\mathbb{Z}\\ 1&\mapsto(1,1)\\ \tau&\mapsto(\sqrt{d},-\sqrt{d})\end{aligned}$$

with image $\mathbb{Z}\cdot(1,1)+\sqrt{d}(\mathbb{Z}\oplus\mathbb{Z})$.

Now write $d=f^2d_K$; we will show $f$ is the conductor. Choose $b=0$ or 1 with $b\equiv d\pmod 4$ and $c$ such that $b^2-4c=d$, and let

$$\begin{aligned}S(d_K)&=\mathbb{Z}[\tau]/(\tau^2+b\tau+c)=\mathbb{Z}\left[\frac{-b+\sqrt{d_K}}{2}\right]\\ S(d)&=\mathbb{Z}[\tau]/(\tau^2+fb\tau+fc)=\mathbb{Z}\left[\frac{-fb+f\sqrt{d_K}}{2}\right].\end{aligned}$$

Now $S(d_K)$ is the ring of integers of $S(d)$, so the largest quadratic ring containing $S(d)$; moreover the above representation gives

$$conductor-in-qring S(d)=\mathbb{Z}+fS(d_K), \tag{4.3}$$

so $f$ must be the conductor.

Items 4 and 5 come from (4.3) and the fact that $\mathbb{Z}\left[\frac{-b+\sqrt{d_K}}{2}\right]=\mathbb{Z}[\tau_K]$. □

## 4.1 Proper and invertible ideals

From now on, assume that $d$ is not a square. We create a bijection between the "ideal class group" of a quadratic ring of discriminant $d$ and quadratic forms of discriminant $d$. To do this we first have to define the "ideal class group" of a quadratic ring. This is more complicated than defining it for a ring of integers, because a general order is not a Dedekind domain. We find that we first have to restrict the ideals under consideration, in order for inverses to exist.[4] Later we restrict the ideals further so that we have unique factorization.

**Definition 4.5:** df:proper-ideal A **proper ideal** of $\mathcal{O}$ is an ideal such that

$$\mathcal{O}=\{\beta\in K:\beta\mathfrak{a}\subseteq\mathfrak{a}\}.$$

(In general we only have $\subseteq$.)

Note that for the maximal order $\mathcal{O}_K$, all ideals are proper, and for any order, all principal ideals are proper. Furthermore, any ideal is proper for exactly most one order, namely the order $\{\beta\in K:\beta\mathfrak{a}\subseteq\mathfrak{a}\}$. The following tells us exactly which order that is.

[4] Else we only get a semigroup.

**Lemma 4.6:** proper-ideal-of Suppose $\mathfrak{a} = (\alpha, \beta)$ is an ideal in a order of a quadratic field. Suppose $\tau = \frac{\beta}{\alpha}$ has degree 2 over $\mathbb{Q}$ and satisfies the equation

$$ax^2 + bx + c = 0$$

where $a > 0$, $b$, and $c$ are integers with $\gcd(a, b, c) = 1$. Let $K = \mathbb{Q}(\tau)$. Then $\mathfrak{a}$ is a proper ideal of $R := (1, a\tau)$, and

$$\mathfrak{N}_R(\mathfrak{a}) = \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}{a}.$$

As stated this only works for imaginary quadratic fields.

*Proof.* Let $\mathcal{O}$ be the order. Now $(1, \tau)$ is also a fractional ideal of $\mathcal{O} \subseteq \mathbb{Q}(\tau)$. We know $\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\}$. Now, $\beta$ is in this set iff

$$\begin{aligned} \beta &\in (1, \tau) \\ \beta\tau &\in (1, \tau), \end{aligned}$$

i.e.

$$\begin{aligned} \beta &= p + q\tau \text{ for some } p, q \in \mathbb{Z} \\ \beta\tau &= (p + q\tau)\tau = p\tau + q\left(-\frac{b}{a}\tau - \frac{c}{a}\right) \in (1, \tau); \end{aligned}$$

since $\gcd(a, b, c) = 1$, this is true iff $a \mid q$. Hence $\mathcal{O} = (1, a\tau)$.

For the second part, note

$$\mathfrak{N}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = \frac{[\mathcal{O} : (1, \tau)]}{[\mathfrak{a} : (1, \tau)]} = \frac{[\alpha(1, \tau) : (1, \tau)]}{[(1, a\tau) : (1, \tau)]} = \frac{\mathrm{Nm}(\alpha)}{a}.$$

□

**Proposition 4.7:** Let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper iff it is invertible. Hence the proper fractional ideals form a group $I(\mathcal{O})$ under multiplication.

*Proof.* If $\mathfrak{a}$ is invertible, then $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ for some $\mathfrak{b}$. If $\beta\mathfrak{a} \subseteq \mathfrak{a}$, then

$$\beta\mathcal{O} = \beta(\mathfrak{a}\mathfrak{b}) = (\beta\mathfrak{a})\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} = \mathcal{O}$$

so $\beta \in \mathcal{O}$. This shows $\mathfrak{a}$ is proper.

Conversely, suppose $\mathfrak{a}$ is proper. Write $\mathfrak{a} = \alpha(1, \tau)$. Letting $ax^2 + bx + c$ be the minimal polynomial of $\tau$ with integer coefficients, by Lemma 4.6, $\mathcal{O} = (1, a\tau)$. We show that

$$\mathfrak{a}\overline{\mathfrak{a}} = \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}{a}\mathcal{O};$$

it will follow that $\frac{a}{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}\overline{\mathfrak{a}}$ is the inverse of $\mathfrak{a}$.

First note $\mathcal{O} = \overline{\mathcal{O}}$, since $\mathcal{O} = (1, a\tau) = (1, a\overline{\tau})$ (on account of $a\tau + a\overline{\tau} = -b$). Hence $\overline{\mathfrak{a}}$ is actually an ideal of $\mathcal{O}$. Next, we calculate

$$\begin{aligned}
\mathfrak{a}\overline{\mathfrak{a}} &= \alpha(1,\tau)\overline{\alpha}(1,\overline{\tau}) \\
&= \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)(1,\tau,\overline{\tau},\tau\overline{\tau}) \\
&= \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\left(1,\tau+\overline{\tau},\tau,-\frac{c}{a}\right) \\
&= \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)\left(1,-\frac{b}{a},-\frac{c}{a},\tau\right) \\
&= \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}{a}(1,a\tau)
\end{aligned}$$

as needed (using $\gcd(a,b,c) = 1$ in the last step). □

Let $P(\mathcal{O})$ be the subgroup of principal ideals in $I(\mathcal{O})$. Define the **class group** of $\mathcal{O}$ to be

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

Let $P^+(\mathcal{O})$ be the subgroup of principal ideals in the form $(\alpha)$ where $\alpha$ is *totally positive*, i.e. positive under every real embedding. (This is an empty condition if $\mathcal{O}$ is imaginary.) Define the **narrow class group** of $\mathcal{O}$ to be

$$C^+(\mathcal{O}) = I(\mathcal{O})/P^+(\mathcal{O}).$$

(This is an example of what is called a ray class group in class field theory.)

# §5 Gauss composition

g-comp

**Theorem 5.1** (Correspondence between ideals and binary quadratic forms)**:** ideal-form-correspondence There is a bijection between

1. narrow ideals classes in quadratic rings with given orientation and

2. binary quadratic forms (up to proper equivalence),

given by

$$(\mathfrak{a} = (\alpha,\beta), R) \mapsto \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha x - \beta y)}{\mathfrak{N}_R(\mathfrak{a})}$$

$$\left(\left(1, \frac{-b+\sqrt{d}}{2a}\right), \mathbb{Z}\left[\frac{-b+\sqrt{d}}{2}\right]\right) \mapsfrom Q(x,y) = ax^2 + bxy + cy^2$$

where $K$ is the quadratic field containing $\mathfrak{a}$, $(\alpha, \beta)$ is a positively oriented basis for $\mathfrak{a}$, and $d = b^2 - 4ac$. This restricts to a bijection between *invertible* oriented ideal classes in the order of discriminant $d$ and *primitive* binary quadratic forms of discriminant $d$:

$$C^+(\mathcal{O}(d)) \overset{\cong}{\leftrightarrows} C(d).$$

**Corollary 5.2** (Gauss composition)**:** gauss-composition There exists a group structure on equivalence classes of binary quadratic forms, induced by the group structure on ideal classes.

*Proof.* Step 1: We show the forward map is well-defined. We need to check two things.

1. Change of basis gives an equivalent form: Temporarily write $Q_{a_1,a_2}(x,y) = \frac{\mathrm{Nm}_{K/\mathbb{Q}}(a_1x - a_2y)}{\mathfrak{N}\mathfrak{a}}$. Suppose $\mathfrak{a} = (a_1, a_2) = (b_1, b_2)$ where both bases are positively oriented. We can write

$$\begin{pmatrix} b_1 \\ -b_2 \end{pmatrix} = A \begin{pmatrix} a_1 \\ -a_2 \end{pmatrix}, \quad A \in \mathrm{SL}_2(\mathbb{Z}).$$

   Then

$$ideal-qform-change-basis Q_{b_1,b_2}(x,y) = \frac{\mathrm{Nm}_{K/\mathbb{Q}}\left((x,y)\begin{pmatrix} b_1 \\ -b_2 \end{pmatrix}\right)}{\mathfrak{N}_R(\mathfrak{a})} = \frac{\mathrm{Nm}_{K/\mathbb{Q}}\left((x,y)A\begin{pmatrix} a_1 \\ -a_2 \end{pmatrix}\right)}{\mathfrak{N}_R(\mathfrak{a})} = \tag{4.4}$$

   so the quadratic forms are equivalent.

2. Multiplying by a totally positive element gives an equivalent form: Suppose $\lambda$ is totally positive. Then $\mathrm{Nm}_{K/\mathbb{Q}}(\lambda) > 0$. First note that $(\lambda a_1, \lambda a_2)$ is also positively oriented:

$$\frac{\begin{vmatrix} \lambda a_1 & \overline{\lambda a_1} \\ \lambda b_1 & \overline{\lambda b_1} \end{vmatrix}}{d} = \mathrm{Nm}_{K/\mathbb{Q}}(\lambda) \frac{\begin{vmatrix} a_1 & \overline{a_1} \\ b_1 & \overline{b_1} \end{vmatrix}}{d} > 0.$$

   Then

$$\begin{aligned} Q_{\lambda a_1, \lambda a_2}(x,y) &= \frac{\mathrm{Nm}(\lambda a_1 x - \lambda a_2 y)}{\mathfrak{N}_R(\lambda \mathfrak{a})} \\ &= \frac{\mathrm{Nm}_{K/\mathbb{Q}}(a_1 x - a_2 y)}{\mathfrak{N}_R(\mathfrak{a})} \\ &= Q_{a_1,a_2}(x,y) \end{aligned}$$

   as needed.

Step 2: We show this map is injective. First note an alternate characterization for the forward map. Writing $(\alpha,\beta)=\alpha(1,\tau)$, we find that the quadratic form corresponding to $(\alpha,\beta)$ is

$$\begin{aligned} Q_{\alpha,\beta}(x,y) &= \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha x-\beta y)}{\mathfrak{N}_R(\mathfrak{a})} \\ &= \frac{(\alpha x-\beta y)(\overline{\alpha}x-\overline{\beta}y)}{\mathfrak{N}_R(\mathfrak{a})} \\ &= \frac{\alpha\overline{\alpha}x^2-(\alpha\overline{\beta}+\overline{\alpha}\beta)xy+\beta\overline{\beta}y^2}{\mathfrak{N}_R(\mathfrak{a})} \\ qform-factored &= \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}{\mathfrak{N}_R(\mathfrak{a})}(x-\tau y)(x-\overline{\tau}y), \qquad \tau=\frac{\beta}{\alpha}. \end{aligned} \tag{4.5}$$

Suppose $Q_{a_1,a_2}(x,y)\sim Q_{b_1,b_2}(x,y)$. By changing the basis of $\mathfrak{b}=(b_1,b_2)$, which by (4.4) corresponds to changing the basis of the quadratic form, we may assume $Q_{a_1,a_2}(x,y)=Q_{b_1,b_2}(x,y)$. The above factorization (4.5) says that one of the following holds:

1. $\frac{a_1}{a_2}=\frac{b_1}{b_2}$. Letting $\lambda=\frac{a_1}{b_1}=\frac{a_2}{b_2}$, we find $\mathfrak{a}=\lambda\mathfrak{b}$. Since both bases are positively oriented,

$$0<\frac{\begin{vmatrix} a_1 & \overline{a_1} \\ a_2 & \overline{a_2}\end{vmatrix}}{\begin{vmatrix} b_1 & \overline{b_1} \\ b_2 & \overline{b_2}\end{vmatrix}}=\mathrm{Nm}_{K/\mathbb{Q}}(\lambda),$$

   showing either $\lambda$ or $-\lambda$ is totally positive.

2. $\frac{a_1}{a_2}=\frac{\overline{b_1}}{\overline{b_2}}$. We show that this kind of "disorientation" is impossible. Let $\lambda=\frac{a_1}{\overline{b_1}}=\frac{a_2}{\overline{b_2}}$. Then

$$0<\frac{\begin{vmatrix} a_1 & \overline{a_1} \\ a_2 & \overline{a_2}\end{vmatrix}}{\begin{vmatrix} b_1 & \overline{b_1} \\ b_2 & \overline{b_2}\end{vmatrix}}=-\frac{\begin{vmatrix} a_1 & \overline{a_1} \\ a_2 & \overline{a_2}\end{vmatrix}}{\begin{vmatrix} \overline{b_1} & b_1 \\ \overline{b_2} & b_2\end{vmatrix}}=-\mathrm{Nm}_{K/\mathbb{Q}}(\lambda),$$

   giving $\mathrm{Nm}_{K/\mathbb{Q}}(\lambda)<0$. But

$$\begin{aligned} Q_{b_1,b_2}(x,y) &= \frac{(b_1x-b_2y)(\overline{b_1}x-\overline{b_2}y)}{\mathfrak{N}_R(\mathfrak{a})} \\ Q_{a_1,a_2}(x,y) &= \frac{(a_1x-a_2y)(\overline{a_1}x-\overline{a_2}y)}{\mathfrak{N}_R(\mathfrak{b})}=\lambda\overline{\lambda}\frac{(\overline{b_1}x-\overline{b_2}y)(b_1x-b_2y)}{\mathfrak{N}_R(\mathfrak{b})}; \end{aligned}$$

   equating gives $\mathrm{Nm}_{K/\mathbb{Q}}(\lambda)>0$, contradiction.

<u>Step 3:</u> Applying the reverse map and then the forward map gives the identity.

Given $Q(x,y)=ax^2+bxy+cy^2=a(x-\tau y)(x-\overline{\tau}y)$, the reverse map takes it to $\mathfrak{a}:=(1,\tau)$. Note $\{1,\tau:=\frac{-b+\sqrt{d}}{2a}\}$ is in fact a $\mathbb{Z}$-basis for $(1,\tau)$ over $R:=\mathbb{Z}[a\tau]=\mathbb{Z}\left[\frac{-b+\sqrt{d}}{2}\right]$

(not just a generating set over $\mathcal{O}$). Indeed, $a\tau(\tau) = (-b\tau - c) \in (1, \tau)$. In exactly the same way, $\{1, a\tau\}$ is a $\mathbb{Z}$-basis for $R$ over $R$.

By (4.5), the forward map then takes $(\mathfrak{a}, R)$ to

$$\frac{1}{\mathfrak{N}_R(\mathfrak{a})}(x-\tau y)(x-\overline{\tau}y) = [\mathfrak{a} : R](x-\tau y)(x-\overline{\tau}y) = a(x-\tau y)(x-\overline{\tau}y).$$

Step 4: Invertible classes correspond to primitive forms. Suppose $\mathfrak{a} = \alpha(1, \tau)$ is invertible and $\tau$ satisfies $ax^2 + bx + c = 0$, where $\gcd(a, b, c) = 1$. Then by Lemma 4.6, $a = \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}{\mathfrak{N}_R(\mathfrak{a})}$. Hence by (4.5), the quadratic form is $ax^2 + bxy + cy^2$, which is primitive.

Conversely suppose $Q$ is primitive. Then by Proposition 4.6, the corresponding ideal $(1, \tau)$ is proper in $R := (1, a\tau)$.

The fact that the discriminant is preserved can be seen from the reverse map. $\square$

**Example 5.3:** ex:id-qf We calculate the binary quadratic form corresponding to the order $\mathcal{O}$ of discriminant $d$. This will be the identity element in the form class group $C(D)$. We have $\mathcal{O} = (1, \tau)$ where

$$\tau = \begin{cases} \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4 \\ \frac{\sqrt{d}}{2}, & d \equiv 0 \pmod 4). \end{cases}.$$

Then

$$Q_{\mathcal{O}}(x, y) = \mathrm{Nm}_{K/\mathbb{Q}}(x + y\tau) = \begin{cases} x^2 - \frac{d}{4}y^2, & d \equiv 0 \pmod 4 \\ x^2 + xy - \frac{d-1}{4}y^2, & d \equiv 1 \pmod 4). \end{cases}$$

This is consistent with the fact that $x^2 - \frac{d}{4}$ and $x^2 + x - \frac{d-1}{4}$ are the minimal polynomials of $\tau$ in the two cases, respectively.

**Theorem 5.4:** pr:rep-iff-ideal Let $\mathfrak{a}$ be an invertible ideal in the quadratic ring $\mathcal{O}$ and $f$ its associated quadratic binary form. Let $m$ be a nonzero integer. Then the following are equivalent.

1. There exists $\mathfrak{a}'$ in the same ideal class as $\mathfrak{a}$ with
$$\mathfrak{a}'\overline{\mathfrak{a}'} = (m).$$
2. There exists $\mathfrak{a}'$ in the same ideal class as $\mathfrak{a}$ with $\mathfrak{N}_{\mathcal{O}}(\mathfrak{a}') = m$.
3. $f$ represents $m$.

As written this only works for imaginary quadratic fields. For real fields, $f$ may represent $-m$ instead.

*Proof.* Equivalence of the first two items is clear. We show (2) $\iff$ (3).

Suppose $f$ represents $m$. Suppose $m = d^2a$, and $f$ represents $a$ primitively. By Proposition 2.2, $f$ is equivalent to a form $ax^2 + bxy + cy^2$. By Gauss composition, this form corresponds to an ideal $\mathfrak{a}' = a(1,\tau)$ with $a\tau^2 + b\tau + c = 0$ inside $\mathcal{O} = (1, a\tau)$. Hence $\mathfrak{N}_{\mathcal{O}}(\mathfrak{a}') = a$. Then

$$\mathfrak{N}_{\mathcal{O}}(d\mathfrak{a}') = d^2 a,$$

as needed.

Conversely, suppose $\mathfrak{N}_{\mathcal{O}}(\mathfrak{a}) = m$. Write $\mathfrak{a} = \alpha(1,\tau)$ with $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) > 0$. Suppose $a\tau^2 + b\tau + c = 0$ with $\gcd(a,b,c) = 1$, so $\mathcal{O} = (1, a\tau)$ and $\mathfrak{N}_{\mathcal{O}}((1,\tau)) = \frac{1}{a}$. The corresponding quadratic form is

$$g(x,y) = \frac{\mathrm{Nm}_{K/\mathbb{Q}}(x - \tau y)}{\mathfrak{N}_{\mathcal{O}}((1,\tau))} = a\,\mathrm{Nm}_{K/\mathbb{Q}}(x - \tau y).$$

Since $\alpha \in \mathcal{O} = (1, a\tau)$, we have $\alpha = p - qa\tau$ for some $p, q \in \mathbb{Z}$. We have $\alpha\tau = p\tau - q(-b\tau - c) = (p + qb)\tau + cq$; since $\alpha\tau \in \mathcal{O} = (1, a\tau)$ as well, we get $\frac{p+qb}{a} \in \mathbb{Z}$. Now by Lemma 4.6,

$$\begin{aligned} m = \mathfrak{N}_{\mathcal{O}}(\mathfrak{a}) &= \frac{\mathrm{Nm}_{K/\mathbb{Q}}(\alpha)}{a} \\ &= \frac{1}{a^2} \cdot a\,\mathrm{Nm}_{K/\mathbb{Q}}(p - qa\tau) \\ &= \frac{1}{a^2} g(p, aq) \\ &= g\left(\frac{p}{a}, q\right) \\ &= g\left(\frac{-bq - p}{a}, q\right) \qquad\qquad g(x,y) = g\left(-\frac{b}{a}y - x, y\right). \end{aligned}$$

We showed above that $\frac{-bq-p}{a} \in \mathbb{Z}$, as needed. (Think of the last step as "root flipping.") $\square$

## §6 Ideal class group of an order

Suppose $\mathcal{O}$ is an order in the field $K$, and $\mathcal{O}_K$ is the ring of integers (the maximal order). We want to relate $C(\mathcal{O})$ to $C(\mathcal{O}_K)$, because the latter is the most "natural" class group for $K$. In reality, we will relate $C(\mathcal{O})$ to a quotient of a subgroup of $I(\mathcal{O}_K)$, a generalized ideal class group of $\mathcal{O}_K$.

After learning class field theory, which relates generalized class ideal class groups to extensions of $K$, we will see that the primes represented by the quadratic form corresponding to $\mathcal{O}$ can be characterized in terms of a certain field extensions $L/K$.

CHANGE NOTATION: Replace Id with $I$ and $C$ with $C$ in earlier chapters.

**Definition 6.1:** Define

$$\begin{aligned} I_K(f) &= \{\mathfrak{a} \in I_K : \mathfrak{a} \text{ relatively prime to } f\mathcal{O}_K\} \\ P_K(\mathbb{Z}, f) &= \{\alpha\mathcal{O}_K : \alpha \equiv a \pmod{f\mathcal{O}_K} \text{ for some } a \in \mathbb{Z}\} \\ I_K(\mathcal{O}, f) &= \{\mathfrak{a} \in I(\mathcal{O}) : \mathfrak{a} \text{ relatively prime to } f\mathcal{O}\}. \end{aligned}$$

**Theorem 6.2:** class-group-O Let $f$ be the conductor of $\mathcal{O}$, i.e. $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. There is an isomorphism

$$I_K(f)/P_K(\mathbb{Z}, f) \to I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O})$$

induced by the map $g : I_K(f) \to I(\mathcal{O})$,

$$g(\mathfrak{a}) = \mathfrak{a} \cap \mathcal{O}.$$

First, a preliminary lemma.

**Lemma 6.3:** Let $\mathcal{O}$ be an order of conductor $f$. Then every $\mathcal{O}$-ideal prime to $f$ is proper.

*Proof.* Cox, Prop. 7.20. Suppose $\mathfrak{a}$ is prime to $f$. Then $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$. Suppose $\beta\mathfrak{a} \subseteq \mathfrak{a}$. Then

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subseteq \mathfrak{a} + f\mathcal{O}_K \subseteq \mathcal{O}$$

so $\beta \in \mathcal{O}$. Thus $\mathfrak{a}$ is proper. □

*Proof of Theorem 6.2.* Step 1: We show there is a norm-preserving isomorphism

$$\begin{aligned} I_K(f) &\to I(\mathcal{O}, f) \\ \mathfrak{a} &\mapsto \mathfrak{a} \cap \mathcal{O} \\ \mathfrak{b}\mathcal{O}_K &\leftarrow\!\shortmid \mathfrak{b}. \end{aligned}$$

Step 2: The map above induces an isomorphism $I_K(f)/P_K(\mathbb{Z}, f) \to I(\mathcal{O}, f)/P(\mathcal{O}, f)$

Step 3: The inclusion $I(\mathcal{O}, f) \hookrightarrow I(\mathcal{O})$ induces an isomorphism $I(\mathcal{O}, f)/P(\mathcal{O}, f) \to I(\mathcal{O})/P(\mathcal{O})$. This follows from Theorem **??**.**??**. □

# §7 Cube law

We now derive quadratic composition in a different way. We will associate a "cube" of integers with three quadratic forms. In order to identify equivalent binary quadratic forms, we mod out by $\mathrm{SL}_2(\mathbb{Z})^3$. After decreeing that the sum of forms making up any cube is 0, we find that we have

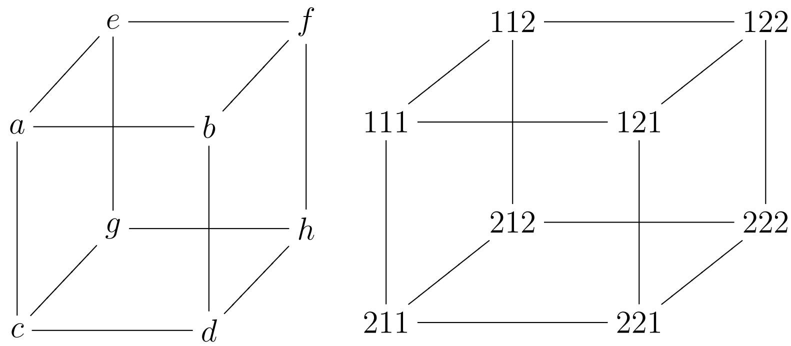
1. identified quadratic forms up to equivalence, and
2. recovered our original composition law.

Later we will see that these ideas generalize to composition laws for other polynomial forms and associated ideals/rings.

Let $\mathcal{C}_2 = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. Choosing a basis $(v_1, v_2)$ for $\mathbb{Z}^2$, every element of $\mathcal{C}^2$ can be written in the form

$$\begin{aligned} &av_1 \otimes v_1 \otimes v_1 + bv_1 \otimes v_2 \otimes v_1 + cv_2 \otimes v_1 \otimes v_1 + dv_2 \otimes v_2 \otimes v_1 \\ &+ ev_1 \otimes v_1 \otimes v_2 + fv_1 \otimes v_2 \otimes v_2 + gv_2 \otimes v_1 \otimes v_2 + hv_2 \otimes v_2 \otimes v_2. \end{aligned}$$

We represent this graphically as a **cube**.




Think of this as a higher-dimensional analogue of a matrix. Let $M_i, N_i$ for $i = 1, 2, 3$ be the two matrices obtained by slicing the cube along the 3 possible directions.

$$\begin{aligned} M_1 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \\ M_2 &= \begin{pmatrix} a & c \\ e & g \end{pmatrix}, \quad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix} \\ M_3 &= \begin{pmatrix} a & e \\ b & f \end{pmatrix}, \quad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}. \end{aligned}$$

Define an action of $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{C}_2$ by letting $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ in the $i$th factor of $\mathrm{SL}_2(\mathbb{Z})^3$ act on $A$ by sending

$$\begin{pmatrix} M_i \\ N_i \end{pmatrix} \mapsto \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} M_i \\ N_i \end{pmatrix} = \begin{pmatrix} rM_i + sN_i \\ tM_i + uN_i \end{pmatrix}.$$

Note that the actions of the 3 factors of $\mathrm{SL}_2(\mathbb{Z})$ commute, in the same way that row and column operations commute for a matrix.

Now associate a cube $A$ with three binary quadratic forms $Q_1^A, Q_2^A, Q_3^A$ by letting

$$Q_i^A(x, y) = -\det(M_i x - N_i y).$$

We call $A$ **projective** if $Q_1^A, Q_2^A, Q_3^A$ are all primitive.

Invariant theory gives the following result.

**Proposition 7.1:** The ring of invariants of $\mathcal{C}_2$ under $\mathrm{SL}_2(\mathbb{Z})^3$ is

$$(\mathcal{C}_2)^{\mathrm{SL}_2(\mathbb{Z})^3} = \mathbb{Z}[\mathrm{disc}(A)]$$

where

$$\begin{aligned} \mathrm{disc}(A) &:= \mathrm{disc}(Q_1) = \mathrm{disc}(Q_2) = \mathrm{disc}(Q_3) \\ &= \sum_{s,t \text{ long diagonal}} s^2t^2 - 2 \sum_{s,t,u,v \text{ face}} stuv + 4 \sum_{s,t,u,v \text{ regular tetrahedrom}} stuv. \end{aligned}$$

(The fact that disc$(A)$ is invariant is easy to see; we shall not need the opposite implication.)

We now prove the bijection in Theorem 5.1 and Gauss composition (Corollary 5.2) in a different way, using cubes. The idea is to associate triples of ideals multiplying to 1 with triples of quadratic forms in the same cube (which we will deem to add up to 0), and in this way transfer the group structure from narrow ideal classes to classes of quadratic forms.

**Definition 7.2:** We say that three oriented fractional ideals $I_1, I_2, I_3$ in a quadratic ring $S$ form a **balanced triple** if

$$\begin{aligned} I_1 I_2 I_3 &\subseteq S \text{ and} \\ \mathbb{N}(I_1)\mathbb{N}(I_2)\mathbb{N}(I_3) &= 1. \end{aligned}$$

We say two balanced triples $(I_1, I_2, I_3)$ and $(I_1', I_2', I_3')$ are equivalent if there are $\lambda_1, \lambda_2, \lambda_3$ such that

$$\begin{aligned} I_1 &= \lambda_1 I_1' \\ I_2 &= \lambda_2 I_2' \\ I_3 &= \lambda_3 I_3'. \end{aligned}$$

**Theorem 7.3:** There is a bijection between equivalence classes of cubes, and ordered pairs $(S, (I_1, I_2, I_3))$ where $S$ is a quadratic ring and $(I_1, I_2, I_3)$ is a balanced triple modulo equivalence.

$$\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2 / \operatorname{SL}_2(\mathbb{Z})^3 \leftrightarrow \{(S, (I_1, I_2, I_3))\}$$

If $(\alpha_1, \alpha_2)$, $(\beta_1, \beta_2)$ and $(\gamma_1, \gamma_2)$ are correctly oriented bases for $I_1$, $I_2$, and $I_3$, then the cube is given by $(a_{ijk})_{1 \le i,j,k \le 2}$ where

$$\alpha_i \beta_j \gamma_k = c_{ijk} + a_{ijk}\tau$$

and $\tau$ is such that

$$\begin{aligned} \tau^2 - \frac{d}{4} &= 0, & d &\equiv 0 \pmod 4 \\ \tau^2 - \tau - \frac{d-1}{4} &= 0, & d &\equiv 1 \pmod 4. \end{aligned}$$

# Chapter 5
# Units in number fields

units-in-nf

## §1 Units

Any finitely generated abelian group is isomorphic to $A_{\text{tors}} \oplus \mathbb{Z}^t$ where $A_{\text{tors}}$ consists of all torsion elements, i.e. elements of finite order. The number $t$ is called the **rank** of $A$.

The main theorem of this chapter is the following.

**Theorem 1.1** (Dirichlet's unit theorem)**:** dut Let $K$ be a number field with $r$ real embeddings and $2s$ nonreal complex embeddings. Then the group of units in $K$ is finitely generated with rank equal to $r + s - 1$.

The idea of the proof is as follows.

1. Following the idea of the proof that the class number is finite (Section 3.3), we embed the set of units as a lattice in $\mathbb{R}^r \times \mathbb{R}^s$. Since we want to send a group (under multiplication) to a lattice (under addition), we take logarithms of the norm to define our embedding. In actuality, the homomorphism $L$ is not injective, but the kernel will be finite, which is good enough. (See Proposition 2.2.)

2. Construct independent units from elements generating the same ideal. We do this by finding $\alpha, \gamma$ generating the same principal ideal and taking $\alpha\gamma^{-1}$. Consider a fixed large symmetric convex compact set $T$ of $\mathbb{R}^r \times \mathbb{C}^s$, which will contain elements $\sigma(\alpha)$ by Minkowski. For $\alpha$ such that $L(\alpha) \in T$, $(\alpha)$ is one of a finite number of principal ideals $(\gamma_k)$. Then $\alpha\gamma_k^{-1}$ is a unit.

   However, since we want independent units, we look not for points in the form $L(\alpha)$ but rather of the form $\mathbf{x}L(\alpha)$ where $x$ has norm 1. Think of this as "rotating" or "twisting" the unit that we get.

First, a basic criterion for being a unit.

**Proposition 1.2:** Let $K/\mathbb{Q}$ be a finite extension. An element $\alpha \in K$ is a unit if and only if $\mathrm{Nm}(\alpha) = \pm 1$.

*Proof.* Suppose $\alpha$ is a unit. Then $\alpha^{-1} \in K$ and

$$\mathrm{Nm}(\alpha)\,\mathrm{Nm}(\alpha^{-1}) = \mathrm{Nm}(\alpha\alpha^{-1}) = 1$$

so $\mathrm{Nm}(\alpha) = \pm 1$.

Conversely, suppose $\mathrm{Nm}(\alpha) = \pm 1$. Then by Theorem 2.3, letting $\sigma_1 = I, \ldots, \sigma_n$ be the distinct embeddings of $K$ to the Galois closure, we have

$$\alpha \cdot \prod_{k=2}^{n} \sigma_k(\alpha) = \mathrm{Nm}_{L/K}(\alpha) = \pm 1.$$

Hence $\alpha^{-1} = \pm \prod_{k=2}^{n} \sigma_k(\alpha) \in \mathcal{O}_K$. □

# §2 Dirichlet's unit theorem

We now prove Dirichlet's unit theorem.

**Lemma 2.1:** bound-degree-norm There are a finite number of algebraic integers $\alpha$ such that

$$\begin{aligned} [\mathbb{Q}(\alpha):\mathbb{Q}] &\le m \\ |\alpha'| &\le M \text{ for all conjugates } \alpha'. \end{aligned}$$

*Proof.* The second condition means that the coefficients of the minimal polynomial $f$ are bounded. Since the degree of $f$ is at most $m$, there are a finite number of possibilities for the $f$ and hence $\alpha$.[1] □

Let $\{\sigma_1, \ldots, \sigma_r\}$ be the real embeddings and $\{\sigma_{r+1}, \bar{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \bar{\sigma}_{r+s}\}$ be the complex embeddings of $K$. Since

$$\mathrm{Nm}(\alpha) = |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)| |\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2,$$

we define the homomorphism

$$\begin{aligned} &L : K^\times \to \mathbb{R}^{r+s} \\ &L(\alpha) = (\ln|\sigma_1(\alpha)|, \ldots, \ln|\sigma_r(\alpha)|, 2\ln|\sigma_{r+1}(\alpha)| \cdots, 2\ln|\sigma_{r+s}(\alpha)|). \end{aligned}$$

This is the composition of our previous embedding $\sigma$ with $f$:

$$\begin{aligned} &\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s & \sigma(\alpha) &= (\sigma_1(\alpha_1), \ldots, \sigma_r(\alpha_r)) \\ &f : \mathbb{R}^r \times \mathbb{R}^s \to \mathbb{R}^{r+s} & f(x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s}) &= (\ln|x_1|, \ldots, \ln|x_r|, 2\ln|z_{r+1}|, \ldots, 2\ln|z_{r+s}|). \end{aligned}$$

**Proposition 2.2:** luk-in-h The image $L(U_K)$ is a lattice contained in the hyperplane

$$H := \{(x_1, \ldots, x_{r+s}) : x_1 + \cdots + x_{r+s} = 0\}.$$

Moreover, $L$ has finite kernel.

[1]See Chapter **??** for...

*Proof.* If $L(u) = (x_1, \ldots, x_{r+s}) \in U_K$ then

$$\begin{aligned} x_1 + \cdots + x_{r+s} &= \ln|\sigma_1(\alpha)| + \cdots + \ln|\sigma_r(\alpha)| + 2\ln|\sigma_{r+1}(\alpha)| + \cdots + 2\ln|\sigma_{r+s}(\alpha)| \\ &= \ln|\operatorname{Nm}(\alpha)| = 0. \end{aligned}$$

To show $L(U_K)$ is a lattice it suffices to show it is discrete. To this end, we show the base elements

$$B(r) = \{(x_1, \ldots, x_{r+s}) : |x_j| \le C\}$$

centered at the origin contain finitely many points of $L(U_K)$. Indeed, if $\sigma(\alpha) \in B(r)$, then $|\sigma_k(\alpha)| < C$ for every embedding $\sigma_k$. By Proposition 2.1, there are a finite number of possibilities for $\alpha$.

If $\alpha \in \ker L$, then $|\sigma_k(\alpha)| = 1$ for all $k$. Again by Proposition 2.1 there are a finite number of possibilities for $\alpha$. □

Since $U_K$ is abelian, we now know

$$U_K \cong \underbrace{\ker(L)}_{U_K^{\text{tors}}} \oplus \underbrace{L(U_K)}_{\text{lattice of } H}.$$

It remains to show the following.

**Lemma 2.3:** $L(U_K)$ is a full lattice in $H$. Therefore it has rank $r + s - 1$.

*Proof.* Let $\mathbf{x} \in \mathbb{R}^r \times \mathbb{C}^s$. By Proposition 3.1, the volume of the fundamental parallelopiped of $\sigma(\mathfrak{a})$ is $2^{-s} \cdot \mathbb{N}\mathfrak{a} \cdot |\Delta_K|^{\frac{1}{2}}$. Note that multiplication by $\mathbf{x}$ multiplies the norm by $\operatorname{Nm}(x)$ (more precise here?) so the volume of the fundamental parallelopiped of $\sigma(\mathfrak{a})$ is $\operatorname{Nm}(\mathbf{x}) 2^{-s} \mathbb{N}\mathfrak{a} \cdot |\Delta_K|^{\frac{1}{2}}$.

Now suppose $\mathbf{x}$ is any element such that $\operatorname{Nm}(\mathbf{x}) = 1$. Let $V = 2^{-s}\mathbb{N}\mathfrak{a} \cdot |\Delta_K|^{\frac{1}{2}}$. Let $T$ be any compact convex symmetric set with volume at least $2^{r+s}V$. We note the following.

1. By Minkowski's Theorem, there is point of $T$ in the lattice $\mathbf{x} \cdot \sigma(\mathcal{O}_K)$.

2. Since $T$ is bounded, all elements of $T$ have norm bounded by a constant $C$. If $\sigma(\alpha) \in T$, then $\alpha$ has norm bounded by $C$. By Lemma 3.3.7 there are a finite number of principal ideals with norm bounded by $C$, say $(\gamma_1), \ldots, (\gamma_m)$. Then if $\sigma(\alpha) \in T$, we have $(\alpha) = (\gamma_k)$, i.e. $\alpha = u\gamma_k$ for some unit $u$, and some $k$.

In conclusion, for each $\mathbf{x}$ we find $\alpha$ such that

$$T \ni \mathbf{x}\sigma(\alpha) = \mathbf{x}\sigma(u\gamma_k) \text{ for some } k,$$

i.e.

$$x - sigma - u\mathbf{x}\sigma(u) \in \bigcup_{k=1}^{m} \sigma(\gamma_k^{-1})T. \tag{5.1}$$

Since $T$ is bounded, so is $\bigcup_{k=1}^{m} \sigma(\gamma_k^{-1})$. There exists $C'$ so that every coordinate of $\mathbf{x}\sigma(u)$ is less than $C'$:

$$x - sigma - u2(\mathbf{x}\sigma(u))_k < C'. \tag{5.2}$$

The idea is that this places a large constraint on the possibilities for $\varepsilon$, so as we vary $\mathbf{x}$ between "extreme" values, we will have to get linearly independent $u$.

Take

$$\mathbf{x}_k = \Big(C', \ldots, C', \underbrace{\frac{1}{C'^{r+s-1}}}_{k}, C', \ldots, C'\Big)$$

Then letting $u_k$ be such that (5.1) holds for $x_k, u_k$, we get by (5.2) that, componentwise,

$$\sigma(u_k) < (1, \ldots, 1, C'^{r+s}, 1, \ldots, 1),$$

i.e.

$$L(u_k) = f(\sigma(u_k)) < (0, \ldots, 0, \ln(C'^{r+s}), 0, \ldots, 0).$$

Note the following.

1. Every entry of $L(u_k)$ is negative except for the $k$th one, which must be positive because the entries sum up to 0.

2. The sum of entries of $L(u_k)$, omitting the last term, is positive.

The following lemma will show that $L(u_1), \ldots, L(u_{r+s-1})$ are linearly independent. It will follow that $u_1, \ldots, u_{r+s-1}$ generate a free abelian group. This means $\operatorname{rank}(U_K) \geq r + s - 1$; we have equality by Proposition 2.2 since $\dim H = r + s - 1$.

**Lemma 2.4:** Suppose that $A$ is a $n \times n$ matrix such that

1. $a_{i,j} < 0$ for $i \neq j$ and $a_{i,i} > 0$.

2. $\sum_{j=1}^{n} a_{i,j} > 0$.

Then $A$ is invertible.

*Proof.* Suppose $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ is a nonzero vector. Suppose $i$ is such that $|a_i|$ is greatest. Then looking at the $i$th component gives $\sum_{j=1}^{n} a_{ij} v_j = 0$. Then

$$\sum_{j=1}^{n} a_{ij} v_j > a_{ij} v_i + \sum_{j \neq i} a_{ij} v_i > 0,$$

so $Av \neq 0$. Thus $A$ is invertible. □

□

This finishes the proof of Dirichlet's Unit Theorem.

# §3 $S$-units

**Definition 3.1:** Let $S$ be a finite set of prime ideals of $K$. The **ring of $S$-integers** is

$$\mathcal{O}_K(S) = \bigcap_{\mathfrak{p} \notin S} (\mathcal{O}_K)_{\mathfrak{p}} = \{\alpha \in K : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

I.e. we allow dividing by elements whose "only prime factors" are in $S$. The group of $S$-units is the group of units in $\mathcal{O}_K(S)$:

$$U(S) = \mathcal{O}_K(S)^{\times} = \{\alpha \in K \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0 \text{ for all } \mathfrak{p} \notin S\}.$$

There are more units in $U(S)$ than in $U_K$; the following generalization of Dirichlet's theorem says that we get an "extra" unit for every prime in $S$.

**Theorem 3.2** (Dirichlet's S-unit theorem)**:** dsut The group of $S$-units is finitely generated with rank $r + s + |S| - 1$.

*Proof.* Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. Consider the maps

$$U_K \hookrightarrow U(S) \xrightarrow{\varphi} \mathbb{Z}^m$$

where

$$\varphi(x) = (\mathrm{ord}_{\mathfrak{p}_1}(x), \ldots, \mathrm{ord}_{\mathfrak{p}_m}(x)).$$

Its kernel is $U_K$, as the elements of $U_K$ are exactly those $x$ with order 0 for every prime $\mathfrak{p}$, and by definition $\mathrm{ord}_{\mathfrak{p}}(x) = 0$ for $x \in U(S)$ and $\mathfrak{p}$ outside of $S$. Let $h$ be the class number of $K$. Then $\mathfrak{p}_k^h = (\alpha_k)$ for some $\alpha_k$. We have

$$\varphi(x) = (0, \ldots, 0, \underbrace{h}_{k}, 0 \ldots, 0).$$

Hence $\varphi(U(S))$ is a full lattice in $\mathbb{Z}^m$. Since $U_K$ has rank $r + s - 1$ by Dirichlet's Unit Theorem (1.1), $U(S)$ has rank $r + s - 1 + m$. $\square$

# §4 Examples and algorithms

# §5 Regulator

# Chapter 6
# Cyclotomic fields

cyclotomic

## §1 Cyclotomic polynomials

**Definition 1.1:** A **cyclotomic extension** of $\mathbb{Q}$ is a field $\mathbb{Q}[\zeta]$ where $\zeta$ is a root of unity. We call $\zeta$ a primitive $n$th root of unity if $\zeta^n = 1$ but $\zeta^m \neq 1$ for $0 < m < n$.

We will use $\zeta_n$ to denote a primitive $n$th root of unity.
The $n$th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{0 \le j < n, \gcd(j,n)=1} (x - e^{\frac{2\pi i j}{n}})$$

Equivalently, it can be defined by the recurrence $\Phi_0(x) = 1$ and

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{m|n, m<n} \Phi_m(x)}.$$

Hence, it has integer coefficients.

**Theorem 1.2:** cyclotomic-irreducible The cyclotomic polynomials are irreducible over $\mathbb{Q}[x]$.

*Proof.* We need the following lemma:

Suppose $\omega$ is a primitive $n$th root of unity, and that its minimal polynomial is $g(x)$. Let $p$ be a prime not dividing $n$. Then $\omega^p$ is a root of $g(x) = 0$.

Since $\Phi_n(\omega) = 0$, we can write $\Phi_n = fg$. If $g(\omega^p) \neq 0$ then $f(\omega^p) = 0$. Since $\omega$ is a zero of $f(x^p)$, $f(x^p)$ factors as

$$f(x^p) = g(x)h(x)$$

for some polynomial $h \in \mathbb{Z}[x]$.

Now, in $\mathbb{Z}/p\mathbb{Z}[x]$ note $(f_1 + \ldots + f_k)^p = f_1^p + \ldots + f_k^p$ since the $p$th power map is an homomorphism. Hence

$$g(x)h(x) \equiv f(x^p) \equiv f(x)^p \pmod{p}.$$

Hence $f(x)$ and $g(x)$ share a factor modulo $p$. However, the derivative of $x^n - 1$ modulo $p$ is $nx^{n-1} \neq 0$, showing that $x^n - 1$ has no repeated irreducible factor modulo $p$; hence $\Phi_n$ has no repeated factor modulo $p$. Since $\Phi_n = fg$, this produces a contradiction.

Therefore $g(\omega^p) = 0$, as needed.

Any primitive $n$th root is in the form $\omega^k$ for $k$ relatively prime to $n$. Writing the prime factorization of $k$ as $p_1 \cdots p_m$, we get by the lemma that $\omega^{p_1}, \omega^{p_1 p_2}, \ldots, \omega^{p_1 \cdots p_m}$ are all roots of $g$. Hence $g$ contains all primitive $n$th roots of unity as roots, and $\Phi_n = g$ is irreducible. □

**Theorem 1.3:** cyclotomic-degree

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

*Proof.* The minimal polynomial of $\zeta_n$ equals the cyclotomic polynomial by Theorem 1.2; the latter has degree $\varphi(n)$. □

We use cyclotomic polynomials to prove a special case of Dirichlet's theorem.

**Theorem 1.4** (Dirichlet's theorem for $p \equiv 1 \pmod{n}$)**:** dirichlet1(†) Let $n$ be a positive integer. There are infinitely many primes $p$ with $p \equiv 1 \pmod{n}$.

**Lemma 1.5:** For any integer $m$, all divisors of $\Phi_n(m)$ either divide $n$ or are $1 \pmod{n}$.

*Proof.* Suppose $p$ is prime and $p \mid \Phi_n(m)$. Then $p \mid m^n - 1$, i.e.

$$m^n \equiv 1 \pmod{p}$$

so $r := \operatorname{ord}_p(m) \mid n$. Since $m^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem, $r \mid p - 1$.

If $r = n$, then $n \mid p - 1$, i.e. $p \equiv 1 \pmod{n}$. Suppose that $r < n$. Then

$$p \mid \Phi_n(m) \mid \frac{m^n - 1}{m^r - 1} = m^{r(\frac{n}{r}-1)} + \cdots + m^r + 1.$$

However, $m^r \equiv 1 \pmod{p}$ so

$$m^{r(\frac{n}{r}-1)} + \cdots + m^r + 1 \equiv \frac{n}{r} \pmod{p},$$

so $p \mid \frac{n}{r} \mid n$. □

*Proof of Theorem 1.4.* Suppose by way of contradiction that only finitely many primes are $1 \pmod{n}$. Let their product be $P$ (if there are no such primes, $P = 1$). Consider $\Phi_n(knP)$, $k \in \mathbb{Z}$. Since it divides $(nP)^n - 1$, it can't have prime divisors in common with $n$ or $P$. With appropriate choice of $k$ we can be sure $\Phi_n(knP) \neq 0, \pm 1$. By the claim all prime divisors of $\Phi_n(knP)$ are $1 \pmod{n}$, but they don't divide $P$, contradiction. □

# §2 Ring of integers

Our next two propositions will give us information about the ring of integers of $\mathbb{Q}[\zeta]$, as well as some other useful facts. In the process we will rederive Theorem 1.3.

**Proposition 2.1:** cyclotomic-unit Suppose $\zeta$ and $\zeta'$ are primitive $n$th roots of unity. Then $\frac{1-\zeta'}{1-\zeta}$ is a unit in $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']$.

*Proof.* Then we have $\zeta' = \zeta^s$ and $\zeta = \zeta'^t$ for some $s, t$, so $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']$ and

$$\frac{1-\zeta'}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{s-1} \in \mathbb{Z}[\zeta]$$
$$\frac{1-\zeta}{1-\zeta'} = 1 + \zeta' + \cdots + \zeta'^{t-1} \in \mathbb{Z}[\zeta].$$

Therefore $\frac{1-\zeta'}{1-\zeta}$ is a unit in $\mathbb{Z}[\zeta]$. □

**Proposition 2.2:** cyclotomic-p Let $p$ be prime and $r \in \mathbb{N}$. Suppose $p^r > 2$, let $\zeta_{p^r}$ be a primitive $p^r$-th root of unity, and let $K = \mathbb{Q}[\zeta_{p^r}]$. Then

1. $[\mathbb{Q}[\zeta_{p^r}] : \mathbb{Q}] = \varphi(p^r) = p^{r-1}(p-1)$.
2. The element $\pi = 1 - \zeta_{p^r}$ is prime in $\mathcal{O}_K$, and $(p) = (\pi)^{\varphi(p^r)}$.
3. $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.
4. $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = (-1)^{\frac{\varphi(p^r)}{2}} p^{p^{r-1}(pr-r-1)}$. Thus $p$ is the only prime ramifying in $\mathbb{Q}[\zeta_{p^r}]$.

*Proof.* By Proposition 4.1,

$$\begin{aligned}
p &= 1 + X^{p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}|_{X=1} \\
&= \Phi_{p^r}(1) \\
&= \prod_{\zeta' \text{ primitive } p^r\text{th root of unity}} (1-\zeta') \\
&= \prod_{\zeta' \text{ primitive } p^r\text{th root of unity}} \frac{1-\zeta'}{1-\zeta_{p^r}}(1-\zeta_{p^r}) \\
&= u(1-\zeta)^{\varphi(p^r)}
\end{aligned}$$

where $u = \prod_{\zeta' \text{ primitive } p^r\text{th root of unity}} \frac{1-\zeta'}{1-\zeta_{p^r}}$ is a unit by Proposition 2.1. Thus $(p) = (\pi)^{\varphi(p^r)}$.

From the degree equation (Theorem 2.5.2), we get that $[\mathbb{Q}[\zeta] : \mathbb{Q}] \geq \varphi(p^r)$ with strict inequality when $\pi$ factors further. On the other hand $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r)$ since the cyclotomic polynomial has degree $\varphi(p^r)$. Hence equality must hold, and $\pi$ must be prime, giving (1) and (2).

The degree equation for $(p) = (\pi)^{\varphi(p^r)}$ reads

$$\varphi(p^r) = f((\pi)/(p)) \cdot \varphi(p^r)$$

so we must have $f((\pi)/(p)) = 1$, i.e. the natural map

$$f - is - 1\mathbb{Z}/(p) \xrightarrow{\cong} \mathcal{O}_K/(\pi) \tag{6.1}$$

is an isomorphism.

We first calculate $\operatorname{disc}(\mathbb{Z}[\zeta_p]/\mathbb{Z})$. By Proposition 1.4.4,

$$\begin{aligned}
\operatorname{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z}) &= \pm \operatorname{Nm}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\Phi'_{p^r}(\zeta)) \\
\Phi'_{p^r}(\zeta) &= \left(\frac{X^{p^r}-1}{X^{p^{r-1}}-1}\right)'\Bigg|_{x=\zeta} \\
&= \frac{p^r X^{p^r-1}(X^{p^{r-1}}-1) - (X^{p^r}-1)p^{r-1}X^{p^{r-1}-1}}{(X^{p^{r-1}}-1)^2}\Bigg|_{X=\zeta_{p^r}} \\
&= \frac{p^r \zeta_{p^r}^{p^r-1}}{\zeta^{p^{r-1}}-1} = \frac{p^r \zeta_{p^r}^{-1}}{\zeta_p - 1}
\end{aligned}$$

where we set $\zeta_p = \zeta^{p^{r-1}}$; this is a primitive $p$th root of unity. We calculate the norm of each factor.

1. $\operatorname{Nm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(p^r) = (p^r)^{[\mathbb{Q}(\zeta_p):\mathbb{Q}]} = p^{rp^{r-1}(p-1)}$.
2. $\operatorname{Nm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_{p^r}^{-1}) = \pm 1$ since $\zeta_{p^r}^{-1}$ is a unit.
3. $\operatorname{Nm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = p^{p^{r-1}}$: The minimal polynomial of $\zeta_p - 1$ over $\mathbb{Q}$ is $\Phi_{p^r}(X+1)$, whose constant term is $\Phi_p(1) = X^{p^{r-1}(p-1)} + \cdots + X^{p^{r-1}} + 1|_{X=1} = p$. Hence by Proposition 1.2.3(1c), we have

$$\operatorname{Nm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = (\pm p)^{[\mathbb{Q}(\zeta_{p^r}):\mathbb{Q}(\zeta_p)]} = \pm p^{\frac{\varphi(p^r)}{\varphi(p)}} = \pm p^{p^{r-1}}.$$

Combining these we get

$$disc - cyclotomic - p\,\operatorname{disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z}) = \operatorname{Nm}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}} \frac{p^r \zeta_{p^r}^{-1}}{\zeta_p - 1} = \frac{p^{r(p-1)p^{r-1}} \cdot \pm 1}{\pm p^{p^{r-1}}} = \pm p^{p^{r-1}(pr-r-1)}. \tag{6.2}$$

By Proposition 1.3.2 (fix this a bit), we have

$$\pm p^{p^{r-1}(pr-r-1)} = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = (\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}])^2 \operatorname{disc}(\mathbb{Z}[\zeta]/\mathbb{Z}).$$

Hence both factors are powers of $p$ up to sign. Since $(\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}])$ is a power of $p$, the quotient module is annihilated by a power of $p$, i.e. then

$$power - p - ok p^m \mathcal{O}_K \subseteq \mathbb{Z}[\zeta_{p^r}] \tag{6.3}$$

for some $m$. Note surjectivity in (6.1) gives $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$ and hence

$$okz\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}] + \pi\mathcal{O}_K. \tag{6.4}$$

Suppose $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}] + \pi^n\mathcal{O}_K$. Then substitution into (6.4) gives

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}] + \pi\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}] + \pi(\mathbb{Z}[\zeta_{p^r}] + \pi^n\mathcal{O}_K) = \mathbb{Z}[\zeta_{p^r}] + \pi^{n+1}\mathcal{O}_K.$$

Hence by induction, $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}] + \pi^n\mathcal{O}_K$ for all $n$. However, $(p) = (\pi)^{\varphi(p^r)}$ so this means $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}] + p^n\mathcal{O}_K$ for all $n$. Taking $n = m$, (6.3) gives $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$, proving (3). Together with (6.2), this gives (4). The second part of (4) now follows from Theorem 2.6.1 (A prime ramifies if and only if it divides the discriminant).

All embeddings of $\mathbb{Q}(\zeta_n)$ are complex, and there are $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ of them. By Theorem 1.4.6(1), the sign is $(-1)^{\varphi(p^r)}$. $\square$

Now we prove the analogous result for $\mathbb{Q}(\zeta_n)$, for any $n \in \mathbb{N}$, by taking compositums of fields of the form $\mathbb{Q}(\zeta_{p^r})$.

**Theorem 2.3:** Let $n, r \in \mathbb{N}$ with $n \not\equiv 2 \pmod 4$[1]. Let $\zeta_n$ be a primitive $n$th root of unity.

1. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

2. $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

3. $$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = \frac{(-1)^{\frac{\varphi(n)}{2}} n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}.$$

Moreover,

1. If $p \neq 2$, then $p$ ramifies iff $p \mid n$.

2. If $p = 2$, then $p$ ramifies iff $4 \mid n$.

*Proof.* Let $K = \mathbb{Q}(\zeta_n)$. Along with the theorem statement, we will show that if $n = p^r m$, $p \nmid m$, then

$$cyclotomic-factorization-1(p) = \left(\prod \mathfrak{P}_i\right)^{\varphi(p^r)} \tag{6.5}$$

for distinct primes $\mathfrak{P}_i$.

We induct on the number of prime factors of $n$. The case when $n$ is a prime power is treated by Proposition 2.2. Suppose the theorem true for $m$ and $p \nmid m$; consider $n = p^r m$.

[1]If $n \equiv 2 \pmod 4$, note $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$.

Writing $\zeta_{p^r} = \zeta_n^m$ and $\zeta_m = \zeta_n^{p^r}$, we consider

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_{p^r m}) \arrow[dl, dash] \arrow[dr, dash, "\le\varphi(p^r)"] & \\
\mathbb{Q}(\zeta_{p^r}) \arrow[dr, dash, "\varphi(p^r)"'] & & \mathbb{Q}[\zeta_m] \arrow[dl, dash, "\varphi(n)"] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& (\mathfrak{p}\mathcal{O}_K)^{\varphi(p^r)} = \prod_i \mathfrak{p}_i\mathcal{O}_K \arrow[dl, dash] \arrow[dr, dash, "\ge\varphi(p^r)"] & \\
\mathfrak{p}^{\varphi(p^r)} \arrow[dr, dash, "\text{totally ramified}"'] & & \prod \mathfrak{p}_i \arrow[dl, dash, "\text{unramified}"] \\
& (p) &
\end{tikzcd}$$

By Proposition 2.2(2), $(p) = \mathfrak{p}^{\varphi(p^r)}$ in $\mathbb{Q}[\zeta_{p^r}]$, while by part 2, $p$ splits into disctinct factors. Matching factorizations in $\mathbb{Q}[\zeta_{p^r m}]$, we get that each $\mathfrak{p}_i\mathcal{O}_K$ must be a perfect $\varphi(p^r)$th power. Hence $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \ge \varphi(p^r)$, and equality must hold. Then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(p^r)\varphi(m) = \varphi(n)$ showing (1).

Item (2) follows from Proposition 1.4.8 since by (3), $\operatorname{disc}(\mathbb{Q}(\zeta_{p^r})/\mathbb{Q})$ and $\operatorname{disc}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ are relatively prime. Item (3) follows from Proposition 1.4.8 as well. The factorization comes from the fact that since $[\mathbb{Q}(\zeta_{p^r m}) : \mathbb{Q}(\zeta_m)] = \varphi(p^r)$ and each $\mathfrak{p}_i$ is the $\varphi(p^r)$th power of an ideal, the degree equation says each $\mathfrak{p}_i$ must actually be the $\varphi(p^r)$th power of a *prime* ideal. □

We now show a more precise version of (6.5), using Theorem 6.3.

**Theorem 2.4:** cyclotomic-factorization-p Suppose that $n = p^r m$, where $p \nmid m$. Let

$$f = \operatorname{ord}_m(p).$$

Then the prime factorization of $(p)$ in $\mathbb{Q}(\zeta_n)$ is

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{\varphi(p^r)}$$

where $\mathfrak{P}_j$ are distinct primes, each with residue degree $f$ over $\mathbb{Q}$, and $g = \frac{\varphi(m)}{f}$.

*Proof.* (†)[2] To use Theorem 6.3, we find the factorization of $\Phi_n(X)$ modulo $p$. We have

$$cyclotomic-factorization-p-eq1 \Phi_n(X) = \prod_{j \,(\mathrm{mod}^\times\, n)} (X - \zeta_n^j) = \prod_{j \,(\mathrm{mod}^\times\, m)} \prod k \,(\mathrm{mod}^\times\, p^r)(X - \zeta_m^j \zeta_{p^r}^k). \tag{6.6}$$

Now note that

$$X - \zeta_m^j \zeta_{p^r}^k \equiv X - \zeta_m^j \pmod{\zeta_{p^r} - 1}.$$

Hence (6.6) gives

$$\Phi_n(X) \equiv \prod_{j \,(\mathrm{mod}^\times\, m)} (X - \zeta_m^j)^{\varphi(p^r)} \equiv \Phi_m(X)^{\varphi(p^r)} \pmod{\zeta_{p^r} - 1}.$$

[2]For an alternate proof see Example 10.1.6.

But both sides are in $\mathbb{Z}[X]$ so this congruence holds modulo $(\zeta_{p^r}-1)\cap\mathbb{Z}=(p)$.

Now consider $\Phi_m(X) \pmod p$. Note that modulo $p$, $P(X):=X^m-1$ has no repeated factors since it is relatively prime to $P'(X)=mX^{m-1}\neq 0$; hence its divisor $\Phi_m(X)$ has no repeated factors either. Note $\mathbb{F}_{p^r}^\times$ consists exactly of elements with $x^{p^r-1}=1$, any root $\alpha$ of $\Phi_m(X)$ satisfies $\alpha^m=1$ (but not $\alpha^{m'}=1$ for $0<m'<m$). Thus the smallest field extension $\mathbb{F}_{p^r}$ containing $\alpha$ is hence the smallest $r$ such that $m\mid p^r-1$, i.e. $r=\mathrm{ord}_m(p)$. The irreducible factors of $\Phi_m(X)$ have degree $f$, so $f$ is the residue degree. The number of factors equals $\frac{\varphi(m)}{f}$, and this is the number of distinct prime divisors of $(p)$. $\square$

# §3 Subfields of cyclotomic extensions

**Proposition 3.1:** galois-cyclotomic The Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is

$$G(\mathbb{Q}(\zeta_n)/\mathbb{Q})=(\mathbb{Z}/n\mathbb{Z})^\times.$$

*Proof.* The conjugates of $\zeta_n$ over $\mathbb{Q}$ are $\zeta_n^k$ with $k\in(\mathbb{Z}/n\mathbb{Z})^\times$, the roots of $\Phi_n$. The Galois group acts transitively on the conjugates, so for every $k\in(\mathbb{Z}/n\mathbb{Z})^\times$, there is a automorphism $\sigma_k$ sending $\zeta_n\to\zeta_n^k$, and these are all the automorphisms (look at the degree). Since $\zeta_n$ generates $\mathbb{Q}(\zeta_n)$, the action of an automorphism on $\zeta_n$ determines it completely. It is clear that $k\to\sigma_k$ is an isomorphism $(\mathbb{Z}/n\mathbb{Z})^\times\to G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. $\square$

**Proposition 3.2:** The unique quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ is

$$\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right).$$

*Proof.* By the fundamental theorem of Galois theory, a quadratic extension corresponds to a subgroup of index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times\cong\mathbb{Z}/(p-1)\mathbb{Z}$, and there is exactly one such subgroup. If it equals $\mathbb{Q}(\sqrt{d})$, then the only primes ramifying are those dividing $d$; since the only prime ramifying in $\mathbb{Q}(\zeta_p)$ is $p$, we must have $d=\pm p$.

To determine the sign, we explicitly find express a generator for $\mathbb{Q}(\sqrt{d})$ in terms of $\zeta_p$. Define $\tau$ by the Gauss sum

$$\tau=\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^k.$$

An automorphism $\sigma\in G(L/K)$ is described by $\sigma(\zeta_p)=\zeta_p^j$ for some $j$; we have

$$\sigma\tau=\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta_p^{jk}=\sum_{k=1}^{p-1}\left(\frac{j^{-1}k}{p}\right)\zeta_p^k$$

so $\sigma\tau=\tau$ iff $\left(\frac{j}{k}\right)=1$, which happens for exactly half the elements of $G(L/K)$. Hence $\tau$ indeed generates a quadratic field.[3]

[3]This gives motivation for the Gauss sum appearing in the proof of quadratic reciprocity.

Now, if $p \equiv 1 \pmod 4$, we have $\left(\frac{-1}{p}\right) = 1$ and we can pair $\left(\frac{k}{p}\right)\zeta_p^k + \left(\frac{-k}{p}\right)\zeta_p^{-k} \in \mathbb{R}$, while if $p \equiv 3 \pmod 4$, we have $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{k}{p}\right)\zeta_p^k + \left(\frac{-k}{p}\right)\zeta_p^{-k} \in \mathbb{R}i$. This gives the sign of $d$.

Alternatively, we can calculate $\tau$ explicitly as in (BLAH). □

**Proposition 3.3:** For $n > 2$, $\mathbb{Q}(\zeta_n)$ is a CM-field with totally real subfield

$$\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}\left(\cos \frac{2\pi}{n}\right).$$

*Proof.* □

## §4 Fermat's last theorem: Regular primes

**Theorem 4.1:** cyclotomic-units Any unit $u \in \mathbb{Z}[\zeta_n]$ can be written in the form

$$u = \zeta_n^k v$$

where $v$ is totally positive, i.e. $\sigma(v) \in \mathbb{R}$ for any embedding $\sigma : \mathbb{Q}[\zeta_n] \to \mathbb{C}$.

**Definition 4.2:** A prime $p$ is **regular** if $p$ does not divide the class number of $\mathbb{Z}[\zeta_p]$.

**Theorem 4.3** (First case of Fermat's last theorem for regular primes)**:** Suppose that $p > 2$ is a regular prime. Then any integer solution to

$$x^p + y^p = z^p$$

satisfies $p \mid xyz$.

*Proof.* For $p = 3$, note that any cube must be congruent to 0 or $\pm 1$ modulo 9. Hence in order for $x^3 + y^3 \equiv z^3 \pmod 9$, one of $x, y, z$ is divisible by 3, as needed.

Now assume $p > 3$. By dividing by $\gcd(x, y, z)$ we may assume $x, y, z$ are relatively prime.
Step 1: Factor the equation as

$$fermat-factored \prod_{j=0}^{p-1} (x + \zeta_p^j y) = z^n. \tag{6.7}$$

(Note $p$ is odd.) We show that if $p \nmid xyz$, then the factors on the left are relatively prime. Take $j \neq k$ and consider $\mathfrak{a} := \gcd((x + \zeta_p^j y), ((x + \zeta_p^k y)))$. We have

$$\mathfrak{a} \mid (x + \zeta_p^j y - x - \zeta_p^k y) = (\zeta_p^j - \zeta_p^k)(y).$$

Now $x, y$ have no common factor in $\mathbb{Z}$, so $(x)$ and $(y)$ have no common factor in $\mathbb{Z}[\zeta_p]$, and $(x + \zeta_p^j y)$ and $(y)$ have no common factor. This shows

$$\mathfrak{a} \mid (\zeta_p^j - \zeta_p^k).$$

The RHS is prime, so either $\mathfrak{a} = (\zeta_p^j - \zeta_p^k) = (1 - \mathfrak{p})$ or $\mathfrak{a} = (1)$. In the first case, we get $(1-\mathfrak{p}) \mid \prod_{j=0}^{p-1}(x + \zeta_p^j y) = z^n$ so $p \mid z^n$, contradiction.

Step 2: By uniqueness of ideal factorization, each factor of (6.7) is a perfect $p$th power.

$$(x + \zeta_p^j y) = \mathfrak{a}_j^p$$

However, $p \nmid |C(\mathbb{Z}[\zeta_p])|$ so $C(\mathbb{Z}[\zeta_p])$ has no $p$-torsion. Since $(x + \zeta_p^j y)$ is a principal ideal, $\mathfrak{a}_j$ must also be a principal ideal $(a_j)$. By Theorem 4.1, we can write

$$a_j = \zeta_p^{r_j} v_j, \quad v_j \in \mathbb{Q}[\zeta_p]^+.$$

□

## §5 Exercises

### Problems

1.1 Let $p$ be a prime. Prove that any equiangular $p$-gon with rational side lengths is regular.

1.2 (Komal) Prove that there exists a positive integer $n$ so that any prime divisor of $2^n - 1$ is smaller that $2^{\frac{n}{1993}} - 1$.

1.3 Find all rational $p \in [0, 1]$ such that $\cos p\pi$ is...

(a) rational

(b) the root of a quadratic polynomial with rational coefficients

1.4 (China) Prove that there are no solutions to $2\cos p\pi = \sqrt{n+1} - \sqrt{n}$ for rational $p$ rational and positive integer $n$.

1.5 (TST 2007/3) Let $\theta$ be an angle in the interval $(0, \pi/2)$. Given that $\cos\theta$ is irrational and that $\cos k\theta$ and $\cos[(k+1)\theta]$ are both rational for some positive integer $k$, show that $\theta = \pi/6$.

2.1 Show that the ring of integers in $\mathbb{Q}(\cos\frac{2\pi}{n})$ is $\mathbb{Z}[\cos\frac{2\pi}{n}]$.

? Show that the class group of $\mathbb{Q}(\zeta_{23})$ (is this the right one?) is nontrivial.

# Chapter 7
# Valuations and completions

valuations-and-completions Here is some motivation for considering $\mathfrak{p}$-adic fields.

1. One useful tool in arithmetic geometry is the *local to global* principle, which says that the existence of solutions modulo all primes tells us something about the existence of solutions in the original field or ring, such as $\mathbb{Q}$ or $\mathbb{Z}$. For example, the Hasse-Minkowski Theorem. However, it is not enough to check for solutions modulo all powers of $p$ — because a solution modulo $p$ does not necessarily give a solution modulo powers of $p$. The solution is to look for solutions in a field which contains information *modulo all powers of* $p$, a $p$-adic field.

2. When we take a $\mathfrak{p}$-adic fields, the only prime ideal remaining is $\mathfrak{p}$; all others primes become units. This vastly simplifies algebraic number theory; we don't have to worry about primes that split. Then we can recover facts about the global field.

## §1 Case study: $p$-adic integers

padic-exs We first examine how $p$-adic rationals are defined, before generalizing to other number fields.

Often we look at the integers modulo higher and higher powers of a prime $p$; for example, when we were looking at the existence of primitive roots (Theorem **??**.**??**) or the structure of $\mathbb{Z}/p^n\mathbb{Z}$ (Theorem **??**.**??**). Hensel's lemma told us that under certain conditions we can lift solutions modulo higher and higher powers of $p$.

Rather than work with powers of $p$ piecemeal, we can devise a structure that holds information modulo all powers of $p$ at once. To do this, we define the ring $p$-adic integers $\mathbb{Z}_p$ and $p$-adic rationals $\mathbb{Q}_p$, which contain $\mathbb{Z}$ and $\mathbb{Q}$, respectively. We will do this in two ways:

1. Define $\mathbb{Z}_p$ as an *inverse limit* of the rings $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Q}_p$ as the fraction field.

2. Give $\mathbb{Q}$ a topology (or even better, a metric) related to divisibility by $p$, and complete $\mathbb{Q}$ with respect to this topology.

## 1.1 $p$-adics as an inverse limit

**Definition 1.1:** p-adic-comp-seq A $p$-adic integer is a compatible sequence

$$(x_n)_{n\geq 1}$$

where $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ and such that $x_{n+1} \equiv x_n \pmod{p^n}$ for all $n$, i.e. $x_{n+1}$ maps to $x_n$ under the projection map $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$.

The ring structure is defined by componentwise addition and multiplication. The ring of $p$-adic integers is denoted by $\mathbb{Z}_p$ and its fraction field is denoted by

$$\mathbb{Q}_p = \text{Frac}(\mathbb{Z}_p).$$

In light of Theorem **??**.**??**, we can phrase this definition in a more abstract way:

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

where there are maps $\varphi_n^m : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ given by projection whenever $m \geq n$.

## 1.2 $p$-adics as completions

We can give define a topology on $\mathbb{Z}$ by decreeing that it be invariant under translation and that a neighborhood base of 0 be $\{p^n\mathbb{Z}, n \geq 0\}$. This is the same as the topology induced by the norm

$$|a|_p = p^{-v} \text{ when } a = \frac{p^v b}{c},\ p \nmid b, c.$$

**Definition 1.2** (Alternate definition of $p$-adics)**:** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the $p$-adic norm.

We show the equivalence more generally in ().

## 1.3 Units in $\mathbb{Z}_p$

**Proposition 1.3:** The group of units in $\mathbb{Z}_p$ is

$$\mathbb{Z}_p^\times \cong \begin{cases} \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}, & p \neq 2 \\ \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & p = 2. \end{cases}$$

*Proof.* Note that

$$\mathbb{Z}_p^\times = \varprojlim_{n\geq 1} (\mathbb{Z}/p^n\mathbb{Z})^\times$$

because any inverse modulo $p^n$ can be lifted to an inverse modulo $p^{n+1}$.

The proposition follows from taking inverse limits in Theorem **??**.**??**. □

## 1.4 Monsky's Theorem*

We use the 2-adic valuation to prove the following theorem from combinatorial geometry. Surprisingly, no proof is known that does not use $p$-adics.

**Theorem 1.4:** A unit square cannot be cut into an odd number of triangles of equal area.

The idea of the proof is as follows.

1. Extend the 2-adic valuation to a nonarchimedean valuation on the real numbers.
2. Color each point in the plane one of three colors, based on the 2-adic valuation of the coordinates. We show that the sides of the square only have two colors, with the vertices alternating colors, and that a triangle of area $\frac{1}{m}$ where $m$ is odd, cannot contain vertices of al three colors. The last facts depends crucially on the fact that the area formula for a triangle has a factor of $\frac{1}{2}$ in it.
3. By Sperner's Lemma (from graph theory), the coloring in such a subdivision is inconsistent.

*Proof.* We postpone the proof of the first item.[1] Assuming it, color the points of the plane in three colors depending on which of the following conditions is satisfied.

(A) $|x|_2 < 1, |y|_2 < 1$

(B) $|x|_2 \geq 1, |x|_2 \geq |y|_2$

(C) $|y|_2 \geq 1, |y|_2 > |x|_2$

First, we show that if $(\Delta x, \Delta y)$ has color A, then translating by $(\Delta x, \Delta y)$ does not change the color of $A$. Indeed, consider 3 cases.

1. $(x, y)$ is of color A. By the nonarchimedean property, we have

$$|x + \Delta x|_2 \leq \max(|x|_2, |\Delta x|_2) \leq 1,\ |y + \Delta y|_2 \leq \max(|y|_2, |\Delta y|_2) \leq 1,$$

   so $(x + \Delta x, y + \Delta y)$ is again of color A.

2. $(x, y)$ is of color $B$. Since $|x|_2 \geq 1 > |\Delta x|_2$, we gave

$$|x + \Delta x|_2 = |x|_2 \geq 1.$$

   Since $|x|_2 \dot{\geq} |y|_2$ and $1 > |\Delta_y|_2$ we have

$$|y + \Delta y|_2 \leq \max(|y|_2, |\Delta_y|_2) \dot{\leq} |x|_2 = |x + \Delta x|_2.$$

   Hence $(x + \Delta x, y + \Delta y)$ is again of color B.

[1] There is a way around it; see Proofs from the Book.

3. $(x, y)$ is of color $C$. The proof is the same as above except $x, y$ are interchanged and there is strict inequality in the dotted inequalities above.

Now suppose that $A, B, C$ are three points of those respective colors. By translation we may assume that $A = O$. Let $B = (x, y)$ and $C = (x', y')$. We have

$$\begin{aligned} |x|_2 &\geq |y|_2 \\ |y'|_2 &> |x|_2 \\ \implies |xy'|_2 &> |x'y|_2. \end{aligned}$$

1. $A, B, C$ cannot be collinear, as that would imply $xy' = x'y$.

2. We show $A, B, C$ cannot form a triangle of area $\frac{1}{m}$ for $m$ odd. The area is $\pm\frac{1}{2}(xy' - x'y)$, and we have
$$|\frac{1}{2}(xy' - x'y)| = \left|\frac{1}{2}\right|_2 |x|_2 |y'|_2 > 1,$$
while $\left|\frac{1}{m}\right| = 1$.

Next we establish the following combinatorial lemma.

**Lemma 1.5** (Sperner's lemma)**:** Suppose $\mathcal{P}$ is a polygon that has been subdivided into triangles. Define a *vertex* or *segment* to be a vertex or edge of one of these triangles, and say a segment is of type $\mathcal{C}_1\mathcal{C}_2$ if the endpoints are colored $\mathcal{C}_1$ and $\mathcal{C}_2$. We say a triangle is *rainbow* if it has vertices of all 3 colors.

Suppose every vertex of the subdivision is colored with either $\mathcal{A}$, $\mathcal{B}$, or $\mathcal{C}$, such that the following hold.

1. No outer edge of $\mathcal{P}$ contains vertices of all three colors.

2. There are are an odd number of segments of type $\mathcal{AB}$ on the outer edges.

Then $\mathcal{P}$ contains a triangle whose vertices are all different colors.

*Proof.* We count the number of segments of type $\mathcal{AB}$. In a monochromatic triangle the count is 0, in a two-colored triangle the count is 0 or 2, and in a three-colored triangle the count is 1. Let $n$ be the sum of the counts over all triangle. Every interior segment of type $\mathcal{AB}$ is counted twice, as it is part of two triangles, so

$$n = 2i + e,$$

where $i$ and $e$ denote the number of interior and exterior segments of type $\mathcal{AB}$. Since $e$ is odd by assumption, $n$ is also odd. But this can only happen if there is a three-colored triangle. $\square$

Now the points $O = (0,0)$, $X = (1,0)$, $Y = (1,1)$, and $Z = (0,1)$ are colored with $\mathcal{A}$, $\mathcal{B}$, $\mathcal{B}$, $\mathcal{C}$, respectively. We've shown that each side contains segments of at most 2 colors; segments of type $\mathcal{AB}$ can only appear on side $OX$ and $XY$; in the former there must be an odd number (since $O, X$ are different colors) and in the latter there must be an even number. Thus the conditions of Sperner's Lemma are satisfied, and any subdivision must contain a rainbow triangle, which cannot have area $\frac{1}{m}$ for $m$ odd. □

## §2 Valuations

**Definition 2.1:** A **valuation** on a field $K$ is a function $|\cdot| : K \to \mathbb{R}$ such that

1. $|x| \ge 0$ with equality only when $x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \le |x| + |y|$.

If the stronger condition $|x + y| \le \max(|x|, |y|)$ holds, then $|\cdot|$ is **nonarchimedean**.

**Example 2.2:** For a number field $K$, any embedding $\sigma : K \hookrightarrow \mathbb{C}$ gives a valuation on $K$:

$$|a| := |\sigma a|.$$

**Example 2.3:** p-adic-val The **$\mathfrak{p}$-adic valuation** is

$$|a|_{\mathfrak{p}} = \left(\frac{1}{\mathfrak{N}\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)}.$$

In the special case $K = \mathbb{Q}$, $\mathfrak{p} = (p)$, we have

$$|a|_p = \left(\frac{1}{p}\right)^{v_{\mathfrak{p}}(a)}.$$

**Proposition 2.4:** nonarch-crit A valuation is nonarchimedean if and only if it is bounded on $\mathbb{Z}$. Hence if $\operatorname{char}(K) \ne 0$, then $K$ only has nonarchimedean valuations.

*Proof.* If $|\cdot|$ is archimedean, then $|1 + \cdots + 1| \le |1| = 1$, so $|n| \le 1$ for any $n \in \mathbb{Z}$.

Conversely, suppose that $|\cdot|$ is bounded on $\mathbb{Z}$, say by $C$. We have

$$\begin{aligned}
|(a+b)^n| &= \left|\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right| \\
&\le \sum_{k=0}^{n} C|a|^k|b|^{n-k} \\
&\le C(n+1)\max(|a|,|b|)^n.
\end{aligned}$$

Hence for all $n \ge 1$, $|a + b| \le (C(n+1))^{\frac{1}{n}} \max(|a|, |b|)$. Taking $n \to \infty$ gives the result. □

**Proposition 2.5** (Relationship between additive and multiplicative valuations)**:** Fix a base $b$. There is a correspondence between additive and multiplicative valuations, given by

$$|x| = b^{-v(x)}$$
$$v(x) = -\log_b(x).$$

Different values of $b$ give equivalent valuations. If $v(K^\times)$ is discrete in $\mathbb{R}$, then it is a multiple of a discrete valuation.

We say $|\cdot|$ is discrete when $|K^\times|$ is a discrete subgroup of $\mathbb{R}_{>0}$.
Using the above correspondence, we find

1. $A := \{a \in K : |a| \le 1\}$ is a subring of $K$, with
2. $U := \{a \in K : |a| = 1\}$ as its group of units, and
3. $\mathfrak{m} := \{a \in K : |a| < 1\}$ as its unique maximal ideal.

The valuation is discrete if and only if $\mathfrak{m}$ is principal; then $A$ is a DVR.

**Proposition 2.6** (Elementary properties of discrete valuations)**:** elem-prop-dv

1. $|a+b| \le \max(|a|, |b|)$ with equality if $|a| \ne |b|$.
2. ("All triangles are isosceles.") If $d(c,b) < d(c,a)$ then $d(a,c) = d(a,b)$. (The longer side is the repeated one.)
3. If $a_1 + \cdots + a_n = 0$, then the maximum valuation of the summands must be attained for at least two of them.

## 2.1 Equivalent valuations

A valuation on $K$ defines a metric (and hence a topology) on $K$ by

$$d(a,b) = |a-b|.$$

For example, high powers of $p$ have small $p$-adic valuation, so numbers differing by high powers of $p$ are close together in the $p$-adic valuation.

**Proposition 2.7:** val-equiv-crit Let $|\cdot|_1, |\cdot|_2$ be valuations on $K$, with the first being nontrivial. Then the following are equivalent.

1. $|\cdot|_1, |\cdot|_2$ determine the same topology on $K$.
2. If $|\alpha|_1 < 1$, then $|\alpha|_2 < 1$.
3. $|\cdot|_1 = |\cdot|_2^a$ for some $a > 0$.

We say that $|\cdot|_1$ and $|\cdot|_2$ are **equivalent** if the above conditions hold.

*Proof.*
(1) $\implies$ (2): Note $|\alpha|_j < 1$ if and only if $|\alpha^n|_j = |\alpha|_j^n \to 0$, i.e. $\alpha^n$ converges to 0 in the topology of $|\cdot|_j$. Since the topologies are the same,

$$|\alpha|_1 < 1 \iff \alpha^n \text{ converges to } 0 \iff |\alpha|_2 < 1.$$

(2) $\implies$ (3): Take $y$ so that $|y|_1 > 1$, and let $a = \frac{|y|_2}{|y|_1}$, so that $|y|_2 = |y|_1^a$. We show that $|x|_2 = |x|_1^a$ for all $x \in K$.

Suppose $|x|_1 = |y|_1^{b_1}$ and $|x|_2 = |y|_2^{b_2}$. We need to show $b_1 = b_2$, i.e. so the following commutes.

$$\begin{tikzcd}
|x|_1 \arrow[r, dotted, "\wedge a"] & |x|_2 \\
|y|_1 \arrow[u, "\wedge b_1"] \arrow[r, "\wedge a"] & |y|_2 \arrow[u, "\wedge b_2"']
\end{tikzcd}$$

We approximate $b_1$ with rational numbers $\frac{m}{n}$. First suppose $b_1 > \frac{m}{n}$. Then

$$\left|\frac{y^m}{x^n}\right|_1 = |y|^{m-b_1n} < 1$$

so by hypothesis

$$|y|_2^{m-b_2n} = \left|\frac{y^m}{x^n}\right|_2 < 1$$

giving $b_2 > \frac{m}{n}$. Similarly, if $b_1 < \frac{m}{n}$, then the above argument with $\frac{x^n}{y^m}$ shows $b_2 < \frac{m}{n}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we have $b_1 = b_2$.

(3) $\implies$ (1): The open ball of radius $r$ with respect to $|\cdot|_1$ is the same as the open ball of radius $r^a$ with respect to $|\cdot|_2$. $\square$

# §3 Places

**Definition 3.1:** A **place** is an equivalence class of nontrivial valuations on $K$.[2] We denote by $V_K$ the set of places of $K$, by $V_K^0$ the set of nonarchimedean places and $V_K^\infty$ the set of archimedean places.

We aim to classify all places in a number field $K$.

**Proposition 3.2:** nonarch-vals Let $K/\mathbb{Q}$ be an algebraic extension. Then the places on $K$ are exactly the $\mathfrak{p}$-adic valuations $|\cdot|_\mathfrak{p}$ for $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$.

[2] Some books use "prime" instead of "place." We use the latter term to avoid confusion.

*Proof.* Since $K$ is algebraic over $\mathbb{Q}$, an element $\alpha \in \mathcal{O}_K$ satisfies a monic polynomial equation with coefficients in $\mathbb{Z}$:

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

By Proposition 2.4, $a_j \in \mathbb{Z}$ gives $|a_j| \le 1$. By the nonarchimedean property,

$$|\alpha|^n = |a_{n-1}\alpha^{n-1} + \cdots + a_0| \le \max_{0\le m\le n-1} |a_m||\alpha^m| \le \max_{0\le m\le n-1} |\alpha|^m.$$

Hence $|\alpha| < 1$.

Let $B$ be the ring of integers of $|\cdot|$ and $\mathfrak{m}$ its maximal ideal. Since $\mathfrak{m}$ is prime in $B$, $\mathfrak{p} := \mathfrak{m} \cap A$ is prime in $A$. Note $\mathfrak{p} \ne (0)$ because if so $|\cdot|$ is trivial.

Now suppose $v_{\mathfrak{p}}(y) = n$. Let $\pi \in \mathfrak{p}\backslash\mathfrak{p}^2$ be a uniformizer. Then $(y\pi^{-n})$ is a fractional ideal; suppose ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ appear in its factorization with exponents at least $-k$. Take $b \in \bigcap_{j=1}^n \mathfrak{p}_j^k$. Then $(y\pi^{-n}b)$ is an integral ideal $(c)$ not divisible by $\mathfrak{p}$. We have $c \in A\backslash\mathfrak{p}$. Writing $|\pi| = \left(\frac{1}{\mathfrak{N}\mathfrak{p}}\right)^a$, we have

$$|y| = \left|\frac{c}{b}\right| |\pi^n| = \left|\frac{1}{\mathfrak{N}\mathfrak{p}}\right|^n = |y|_{\mathfrak{p}}^a.$$

Moreover, two equivalent nonarchimedean valuations would have the same maximal ideals and hence correspond to the same prime $\mathfrak{p}$. □

**Theorem 3.3** (Ostrowski)**:** ostrowski The following is a list of all places on $\mathbb{Q}$.

1. Archimedean: $|\cdot|_\infty$.[3]
2. Nonarchimedean: $|\cdot|_p$, where $p$ ranges over all primes.

*Proof.* Let $|\cdot|$ be a valuation on $\mathbb{Q}$ and $m, n$ be integers greater than 1. To compare $|m|$ and $|n|$, we write $m$ in base $n$:

$$m = a_r n^r + \cdots + a_0, \quad 0 \le a_k \le n-1,\ a_r > 0.$$

Let $N = \max\{1, |n|\}$. Then by the triangle inequality,

$$|m| \le \sum_{k=0}^r a_k N^k.$$

Since $r \le \frac{\ln m}{\ln n}$, we get

$$|m| \le \left(1 + \frac{1}{N} + \frac{1}{N^2} + \cdots\right) nN^{\frac{\ln m}{\ln n}} \le 2nN^{\frac{\ln m}{\ln n}}$$

[3]A stronger version of part 1 is as follows. Let $K$ be complete with respect to an archmimedean norm. Then $K = \mathbb{R}$ or $\mathbb{C}$, and the norm is the normal absolute value raised to a power in $(0, 1]$.

Replacing $m$ by $m^t$ and taking the $t$th root gives

$$|m| \le (2n)^{\frac{1}{t}} N^{\frac{\ln m}{\ln n}}.$$

Taking $t \to \infty$ gives

$$\text{ostrowski1} |m| \le N^{\frac{\ln m}{\ln n}}. \tag{7.1}$$

Consider two cases.

1. For all integers $n > 1$, $|n| > 1$. Then (7.1) gives $|m|^{\frac{1}{\ln m}} \le |n|^{\frac{1}{\ln n}}$. By symmetry, we get $|m|^{\frac{1}{\ln m}} = |n|^{\frac{1}{\ln n}}$. Since this is true for all $m$ and $n$, $|n|^{\frac{1}{\ln n}} = c$ is constant, i.e.

$$|n| = c^{\ln n} = n^{\frac{\ln n}{\ln c}}$$

   for all $n \in \mathbb{Z}$. Since $\mathbb{Z}$ generates $\mathbb{Q}$ as a group, we get that $|\cdot|$ is equivalent to the standard archimedean valuation.

2. For some $n > 1$, $|n| \le 1$. Then (7.1) shows that $|m| \le 1$ for all $m > 1$. Thus by Proposition 2.4, $|\cdot|$ is nonarchimedean. The nonarchimedean valuations are given by Proposition 3.2. □

Later on we will return to the question of finding all valuations on an extension of $\mathbb{Q}$ (Theorem **??**).

Generalize the nonarchimedean stuff to number fields.

## 3.1 Approximation

**Theorem 3.4** (Weak approximation theorem)**:** thm:weak-approx Let $v_1, \ldots, v_n$ be all the places of $K$, with valuations $|\cdot|_1, \ldots, |\cdot|_n$. The map

$$\phi : K \to \prod_{j=1}^{N} K_{v_j}$$

induced by the inclusions $K \hookrightarrow K_{v_j}$ has dense image.

In other words, given $a_1, \ldots, a_n \in K$, for any $\varepsilon > 0$, there exists $a \in K$ such that

$$|a - a_j|_j < \varepsilon \text{ for all } j.$$

*Proof.* Step 1: We show that there exists $a$ such that

$$weak - approx - 1 \, |a|_1 > 1. \tag{7.2}$$
$$|a|_j < 1, \quad i = 2, \ldots, n.$$

We induct on $n$. For $n = 2$, note that by Proposition 2.7(2), we can find $b, c$ so that

$$|b|_1 < 1, \qquad |b|_2 \ge 1$$
$$|c|_1 \ge 1, \qquad |c|_2 < 1.$$

Now take $a = \frac{c}{b}$.

For the induction step, suppose we've found $b$ so that (7.2) holds for $n-1$. Choose $c$ so that

$$|c|_1 > 1, \quad |c|_n < 1;$$

we will use it to "correct" $|b|_n$ as necessary. Consider three cases.

1. $|b|_n < 1$: We can let $a = b$.

2. $|b|_n = 1$: Let $a = b^r c$, for large enough $r$. This works because

$$\lim_{r\to\infty} |b^r c|_j = \begin{cases} \infty, & j = 1 \\ 0, & 2 \le j \le n-1 \\ |c|_n < 1, & j = n. \end{cases}$$

3. $|b|_n > 1$: First note that from $1 - |a^r| \le |1 + a^r| \le 1 + |a^r|$ we get

$$weak-approx-expr \lim_{r\to\infty} \left|\frac{x^r}{1+x^r}\right| = \begin{cases} 0, & |x| < 1 \\ 1, & |x| > 1. \end{cases} \tag{7.3}$$

   Let $a = \frac{cb^r}{1+b^r}$, for large enough $r$. This works because the above gives

$$\lim_{r\to\infty} \left|\frac{cb^r}{1+b^r}\right|_j = \begin{cases} |c|_1 > 1, & j = 1 \\ 0, & 2 \le j \le n-1 \\ |c|_n < 1, & j = n. \end{cases}$$

<u>Step 2:</u> Now we show that there are points in the image of $\phi$ arbitrarily close to $(1, 0, \ldots, 0)$. Indeed, choosing $a$ as in step 1, we have by (7.3) that

$$\lim_{r\to\infty} \varphi\left(\frac{a^r}{1+a^r}\right) = (1, 0, \ldots, 0).$$

<u>Step 3:</u> From step 2, choose $b_j$ sufficiently close to $(0, \ldots, 0, \underbrace{1}_{j}, 0, \ldots, 0)$. Let

$$a = \sum_{j=1}^{n} a_n b_n$$

to find $\varphi(a)$ can be arbitrarily close to $(a_1, \ldots, a_n)$. $\square$

Note that if we include only the finite places, then this follows from the Chinese remainder theorem.

# §4 Completion

**Definition 4.1:** Let $K$ be a field with valuation $|\cdot|$. The **completion** of $K$, denoted $\hat{K}$ is the field containing $K$ (i.e. there is a injection $K \hookrightarrow \hat{K}$ preserving valuation) satisfying the following properties.

1. $\hat{K}$ is complete in its topology.
2. (UMP) For any homomorphism $\varphi$ from $K$ to a complete field $L$, there exists a unique homomorphism $\hat{K} \to L$ making the following commute.

$$\begin{tikzcd} \hat{K} \arrow[r, dotted] & L \\ K \arrow[u, hook] \arrow[ur, hook] & \end{tikzcd}.$$

I.e., *$\hat{K}$ is the smallest complete field containing $K$.*

*Proof of existence.* For existence, let $\hat{K}$ be the set of equivalence classes of Cauchy sequences in $K$, and deem two sequences $\{a_n\}$ and $\{b_n\}$ equivalent if $\lim_{n\to\infty} |a_n - b_n| = 0$. Define $K \hookrightarrow \hat{K}$ by sending $a$ to $(a, a, \ldots)$. Extend the valuation by letting defining the norm of a $\{a_n\}$ to be $\lim_{n\to\infty} |a_n|$. See any book on real analysis for the details.

For the second part, given a sequence $\{a_n\} \in \hat{K}$, map it to $\lim_{n\to\infty} \varphi(a_n) \in L$. Uniqueness follows from the universal property. $\square$

## 4.1 Completions of archimedean fields

**Theorem 4.2** (Ostrowski)**:** ostrowski2vals-on-number-fields The only complete archimedean fields, up to isomorphism of valued fields and equivalence of valuation, are $\mathbb{R}$ and $\mathbb{C}$.

*Proof.* See Neukirch, p. 124. $\square$

We can now finish our classification of places on $K/\mathbb{Q}$.

**Theorem 4.3** (Classification of places of $K$)**:** Let $K$ be a number field. There is exactly one place of $K$ for each

1. prime ideal $\mathfrak{p}$,
2. real imbedding, and
3. conjugate pair of complex embeddings.

The valuations corresponding to prime ideals, i.e. $\mathfrak{p}$-adic valuations, are called **finite places**, while the those corresponding to real and complex embeddings are called **infinite (real or complex) places**.

*Proof.* The nonarchimedean valuations of $K$ are given by Proposition **??**, while each archimedean valuation $v$ corresponds to an embedding (respecting valuations)

$$K \hookrightarrow K_v \cong \mathbb{R} \text{ or } \mathbb{C},$$

the isomorphism coming from Theorem 4.2. Note that complex conjugate embeddings give the same valuation. $\square$

**Corollary 4.4:** Let $L/K$ be extensions of number fields. If $v$ is a place corresponding to a prime $\mathfrak{p}$ of $K$, then the places $w \mid v$ in $L$ correspond to primes $\mathfrak{P} \mid \mathfrak{p}$. If $v$ is a place of $K$ corresponding to an embedding $\sigma : K \to \mathbb{R}$ or $\mathbb{C}$, then the places $w \mid v$ correspond to of $\sigma$ to $L$.

## 4.2 Completions of nonarchimedean fields

Suppose $K$ is a field with a discrete nonarchimedean valuation $|\cdot|$. Let $\pi$ be a local uniformizing parameter, i.e. the largest element of $K$ with $|\pi| < 1$. Equivalently, $\pi$ generates the maximal ideal $\mathfrak{m}$ in the subring of $\pi$-integers.

Since $K$ is dense in $\hat{K}$ and

$$|K\backslash\{0\}| = \{|\pi|^m : m \in \mathbb{Z}\}$$

is discrete in $\hat{K}$, we get $|K| = |\hat{K}|$.

**Proposition 4.5:** pi-adic-expansion Let $S$ be a set of representatives for $A/\mathfrak{m}$. Then every element of $\hat{K}$ has a unique expression in the form

$$\sum_{n \geq N} a_n \pi^n.$$

(More precisely, the sum represents $\lim_{m\to\infty} \sum_{n=N}^{m} a_n \pi^n$.) The norm is given by

$$\left|\sum_{n \geq N} a_n \pi^n\right| = |\pi|^{-n_0}, \quad a_N \neq 0.$$

In other words, we can write elements of $\hat{K}$ as "numbers with infinite $\pi$-expansions going off to the left," as we saw in section 1.

*Proof.* Let $\{s_n\}_{n\geq 1}$ be a Cauchy sequence in $K$. Let

$$s_n = \sum_{m \gg -\infty} a_n(m) \pi^j;$$

where $a_n(m) \in S$; this sum is finite. We have

$$|s_{n_1} - s_{n_2}| = p^{-\min\left\{m : a_{n_1}(m) \neq a_{n_2}(m)\right\}}.$$

Hence for each $m$, $a_n(m)$ eventually stabilizes, say at $a_n$. Then

$$\lim_{n\to\infty} s_n = \sum_{n\gg -\infty} a_n\pi^n.$$

□

Thus we have two ways to think of a $\mathfrak{p}$-adic valuation.

**Proposition 4.6:**

$$\hat{K} = \mathrm{Frac}(\varprojlim A/\mathfrak{m}^n).$$

To connect up the analytic and algebraic definitions of the completion, note that the completion of a ring $A$ with respect to an ideal $\mathfrak{m}$ is defined as $\hat{A} = \varprojlim_{n\ge 0} A/\mathfrak{m}^n$, with the topology given by a neighborhood base at 0 being $\{\mathfrak{m}^n\}_{n\ge 0}$.

**Definition 4.7:** Define the exponential function as a power series

$$e^x = \sum_{n=1}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \cdots .$$

We investigate the convergence of $e^x$. Writing $a = a_r p^r + \cdots + a_0$ in base $p$, we find by Example **??**.**??** that

$$\mathrm{ord}_p(n!) = \frac{n - \sum_{i=0}^r a_i}{p-1}.$$

Hence

$$\mathrm{ord}_p\left(\frac{x^n}{n!}\right) = n\,\mathrm{ord}_p(x) - \frac{n - \sum_{i=0}^r a_i}{p-1} = n\left(\mathrm{ord}_p(x) - \frac{1}{p-1}\right) + o(n).$$

Since $e^x$ converges if and only if $\mathrm{ord}_p\left(\frac{x^n}{n!}\right) \to -\infty$, we get the following.

**Proposition 4.8:** $e^x$ converges for $\mathrm{ord}_p(x) > \frac{1}{p-1}$.

# §5 Hensel's lemma

The following is the first version of Hensel's lemma for $\pi$-adics. COMPARE TO ELEMENTARY STATEMENT IN TERMS OF MODS.

**Lemma 5.1** (Hensel's lemma, I)**:** hensel1 Let $f(X) \in A[X]$, and $a_0$ be a simple root of $f(X)$ modulo $\pi$, i.e. $f(a_0) \equiv 0 \pmod{\pi}$ and $f'(a_0) \not\equiv 0 \pmod{\pi}$. Then there exists a unique root $a$ of $f(X)$ with $a \equiv a_0 \pmod{\pi}$.

Note this can be generalized as follows: Suppose $f(a_0) \equiv 0 \pmod{\pi^n}$ and $v_\pi(f'(a_0)) = k < n$. Then there is a unique root $a$ of $f(X)$ with $a \equiv a_0 \pmod{\pi^{n-k}}$. The proof is the same, and is left to the reader!

*Proof.* We find zeros of $f(X)$ modulo higher and higher powers of $\pi$.

Using induction, we find $a_n$ satisfying

$$f(a_n) \equiv 0 \pmod{\pi^{n+1}}.$$

The base case holds by hypothesis. For the induction step, note that by Taylor expansion of polynomials,

$$\begin{aligned} f(a_n + h\pi^{n+1}) &= f(a_n) + h\pi^{n+1} f'(a_n) + \cdots \\ &\equiv f(a_n) + h\pi^{n+1} f'(a_n) \pmod{\pi^{n+2}}. \end{aligned}$$

Since $f'(a_n) \not\equiv 0 \pmod{\pi}$ and $f(a_n) \equiv 0 \pmod{\pi^{n+1}}$, we can choose $h$ so that this is 0 modulo $\pi^{n+1}$. (Explicitly, $h = -\frac{f(a_n)}{\pi^{n+1}} \cdot \frac{1}{f'(a_n)}$.) We let $a_{n+1} = a_n + h\pi^{n+1}$. By construction, the sequence $a_n$ converges; let $a$ be its limit. Since $a \equiv a_n \pmod{\pi^n}$, we get $f(a) \equiv f(a_n) \equiv 0 \pmod{\pi^{n+1}}$ for all $n$, and therefore $f(a) = 0$. □

The first form of Hensel's lemma tells us about lifting a root $a_0$ of $\overline{f}$ ($f$ modulo $\pi$) to a root $a$ of $f$ in $K$. We can think of this as lifting a linear factor $x - a_0$ of $\overline{f}$ to a linear factor $x - a$ of $f$. A stronger form of Hensel's lemma says that we can in fact lift any factor of $f$ to one of $\overline{f}$.

**Theorem 5.2** (Hensel's lemma, II)**:** hensel2 Let $k$ be the residue field of $A$ and $f$ be a monic polynomial. If $\overline{f} = g_0 h_0$ where $g_0$ and $h_0$ are monic and relatively prime, then $f = gh$ for some $g$ and $h$ such that $\overline{g} = g_0$ and $\overline{h} = h_0$. (uniqueness)

If $\overline{f} = g_1 \cdots g_n$ is the complete factorization of $\overline{f}$ in $k[X]$, then the complete factorization of $f$ in $K[X]$ is $f = f_1 \cdots f_n$ where $\overline{f_j} = g_j$.

*Proof.* First we need the following lemma, which tells us that if the reductions of polynomials are relatively prime, then so are the original polynomials.

**Lemma 5.3:** Let $A$ be a local ring with residue field $k$. If $g, h \in A[X]$ are such that $\overline{g}$ and $\overline{h}$ are relatively prime, then $g$ and $h$ are relatively prime in $A[X]$ and there exist polynomials $u, v$ with $\deg u < \deg h$ and $\deg v < \deg g$ such that

$$ug + vh = 1.$$

*Proof.* Since $\overline{g}$ and $\overline{h}$ are relatively prime in $k[X] = (A/\mathfrak{m})[X]$, $(\overline{g}, \overline{h}) = A[X]/\mathfrak{m}A[X]$ and $(g, h) + \mathfrak{m}A[X] = A[X]$. Since $A[X]/\mathfrak{m}A[X]$ is finitely generated (on account of $g, h$ being monic), by Nakayama's Lemma $(g, h) = A[X]$. We can choose $u, v$ such that $ug + vh = 1$; drop all terms with higher degree. □

We proceed as in the proof of Theorem 5.1. Suppose we have found $g_n$ and $h_n$ such that

$$f \equiv g_n h_n \pmod{\pi^{n+1}}.$$

We have

$$(g_n + v\pi^{n+1})(h_n + u\pi^{n+1}) \equiv g_n h_n + (ug_n + vh_n)\pi^{n+1} \pmod{\pi^{n+2}}.$$

By the lemma we can choose $u$ and $v$ such that the above is congruent to $f$ modulo $\pi^{n+2}$. Again let $g_{n+1} = g_n + v\pi^{n+1}$, $h_{n+1} = h_n + u\pi^{n+1}$, and take the limit as $n \to \infty$.

The second part follows from induction. Note $f = f_1 \cdots f_n$ is the complete factorization because any factorization of $f$ gives a factorization for $\overline{f}$. $\square$

**Definition 5.4:** A **henselian field** is a field with nonarchimedian valuation $v$ which satisfies Hensel's Lemma (with $\mathfrak{p}$ the maximal ideal corresponding to $v$).

Hensel's lemma says that a field that is complete with respect to a discrete valuation is henselian.

# §6 Extending valuations

**Theorem 6.1** (Extending discrete valuations)**:** extend-discrete-valuations Let $K$ be henselian and let $L/K$ be finite separable of degree $n$. Then $|\cdot|_K$ extends uniquely to a discrete valuation $|\cdot|_L$ on $L$, given by

$$|\beta|_L = |\operatorname{Nm}_{L/K}\beta|_K^{\frac{1}{n}}.$$

*Proof.* Neukirch, pg. 131-132. $\square$

**Definition 6.2:** Let $K$ be henselian. Let $\operatorname{ord} : K^\times \to \mathbb{Z}$ be the corresponding additive valuation, extended to $K^{\mathrm{al}\times} \to \mathbb{Q}$. Given a polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

define the **Newton polygon** of $f(X)$ to be the lower convex hull[4] of

$$P_i := (i, \operatorname{ord}(a_i)).$$

**Proposition 6.3:** Suppose the bottom of the Newton polygon has segments of $x$-length $n_i$ and slope $-s_i$. Then

1. $f(X)$ has exactly $n_i$ roots $\alpha \in K^{\mathrm{al}}$ with $\operatorname{ord}(\alpha) = s_i$, and
2. $f_i(X) = \prod_{\operatorname{ord}(\alpha_i)=s_i}(X - \alpha_i)$ has coefficients in $K$.

*Proof.* We prove the following statement by induction: if $f(X) = \prod(X - \alpha_j) \in \overline{K}[X]$ and exactly $n_i$ of the roots $\alpha_j$ have order equal to $s_i$, then the Newton's polygon of $f(X)$ has a segment of slope $-s_i$ and $x$-length $n_i$.

[4] draw the convex hull, and remove the segments joining $(0, \operatorname{ord} a_0)$ and $(n, 0)$ from the top

The case $n = 1$ follows since the only line segment on the bottom joins $(0, \operatorname{ord}(\alpha_i))$ and $(1, 0)$. Now suppose the claim proved for $n$. Consider

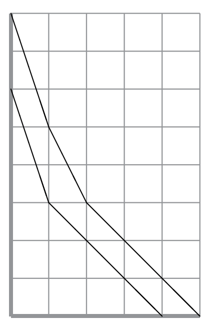
$$g(X) = (X - \alpha)f(X) = \sum_{k=0}^{n+1} (a_{k-1} - \alpha a_k)X^k$$

(where nonexistent coefficients are set to 0). Let $t = \operatorname{ord}(\alpha)$. Let $k_0$ be the point such that the slopes of the line segments of Newton's polygon $N$ for $k < k_0$ are $s \leq -t$, and such that the slopes of the line segments of $N$ for $k > k_0$ are greater than $s > -t$. Let

$$\begin{aligned}
d_k &= \operatorname{ord}(a_k) \\
\ell_k &= y\text{-value of intersection of } N \text{ with } x = k \\
d'_k &= \operatorname{ord}(a_{k-1} - \alpha a_k) \\
\ell'_k &= \begin{cases} \ell_k + t, & 0 \leq k \leq k_0 \\ \ell_{k-1} & k_0 < k \leq n. \end{cases}
\end{aligned}$$

Let $N'$ be the broken line formed by joining $(k, \ell'_k)$. $N'$ consists of segments of the same slopes as $N$, plus one more segment of slope $-t$ and $x$-length 1, in increasing order. It suffices to show that $N'$ is the lower convex hull of the points $(k, d'_k)$.

Here is an example with $p = 5$, $f(X) = (X - 5)(X - 10)(X - 15)(X - 125)$ and $\alpha = 25$.[5]



Consider 2 cases. We will use

$$d'_k = \operatorname{ord}(a_{k-1} - \alpha a_k) \geq \min(\operatorname{ord}(a_{k-1}), \operatorname{ord}(\alpha a_k)) = \min(d_{k-1}, d_k + t),$$

with equality holding if $d_{k-1} \neq d_k + t$.

1. $k \leq k_0$: We have

$$\begin{aligned}
d_{k-1} \geq \ell_{k-1} &\overset{(*)}{\geq} \ell_k + t = \ell'_k, \\
d_k + t \geq \ell_k + t &= \ell'_k
\end{aligned}$$

[5]Of course, $f$ does not have to split over $\mathbb{Q}[X]$ and the valuations don't have to be integers.

where in (*) we use the fact that the slope of the segment $(k-1,\ell_{k-1})(k,\ell_k)$ is at most $-t$. Hence $(k,d'_k)$ lies above $N'$. Now suppose $(k,d_k)$ lies on a corner of $L$ (excluding $k=k_0$). Then $d_k=\ell_k$ and inequality holds in (*):

$$d_{k-1}>\ell_k+t=\ell'_k=d_k+t$$

so $d'_k=\ell'_k$ and $(k,d'_k)$ lies on $N'$.

2. $k>k_0$: We have

$$\begin{aligned} d_{k-1}&\geq \ell_{k-1}=\ell'_k\\ d_k+t&\geq \ell_k+t\overset{(*)}{>}\ell_{k-1}=\ell'_k. \end{aligned}$$

where in (*) we use the fact that the slope of the segment $(k-1,\ell_{k-1})(k,\ell_k)$ is greater than $-t$. Hence $(k,d'_k)$ lies above $(k,\ell'_k)$. Now suppose $(k-1,d_{k-1})$ lies on a corner of $L$. Then $d_{k-1}=\ell_{k-1}$ so

$$d_k+t\geq\ell_k+t>d_{k-1}=\ell_{k-1}=\ell'_k,$$

showing $d'_k=\ell'_k$ and $(k,d'_k)$ lies on $N'$. □

# §7 Places as Galois orbits

Here is an alternate definition of a place.

**Definition 7.1:** Let $(K,v)$ be a field with valuation and $L/K$ be an extension. A **place** on $L$ over $v$ is a $G(\overline{K}_v/K_v)$-orbit on $\mathrm{Hom}_K(L,\overline{K}_v)$.

**Example 7.2:** Let $K=\mathbb{R}$, and $L$ a fiinite extension of $K$. Then the places of $L$ over $\mathbb{R}$ are just $\mathrm{Hom}_K(L,\mathbb{R})$, the real embeddings of $L$, and the complex places are just $G(\mathbb{C}/\mathbb{R})\backslash\mathrm{Hom}_K(L,\mathbb{C})$, i.e. pairs of complex conjugate embeddings.

We show this is equivalent to our previous definition.

**Theorem 7.3:** Assume... There is a bijective correspondence between equivalence classes of valuations $w\mid v$, $v$ on $K$, and $G(\overline{K}_v/K_v)$-orbits on $\mathrm{Hom}_K(L,\overline{K}_v)$:

$$\{w\mid v: w\in M_L\}\xrightarrow{\cong} G(\overline{K}_v/K_v)\backslash\mathrm{Hom}_K(L,\overline{K}_v).$$

Letting $\overline{v}$ be the unique extension of $v$ to $\overline{K}_v$, the embedding $\tau:L\hookrightarrow\overline{K}_v$ is associated to the valuation $|\cdot|_{\overline{v}}$ restricted to $L$.

# §8 Krasner's lemma and consequences

The following is a surprising result... Krasner's lemma

**Lemma 8.1** (Krasner's lemma)**:** krasner Let $K$ be complete with respect to a nonarchimedean valuation $|\cdot|$, and extend $|\cdot|$ to an algebraic closure $K^{\text{al}}$. Let $\alpha, \beta \in K^{\text{al}}$. If $\beta$ is separable over $K[\alpha]$, and

$$belong-ineq|\beta-\alpha| < |\beta'-\beta| \tag{7.4}$$

for any conjugate $\beta' \neq \beta$ of $\beta$ over $K$, then $\beta \in K[\alpha]$.

We say that $\alpha$ *belongs* to $\beta$ if inequality (7.4) holds.

*Proof.* By the fixed field theorem, it suffices to show that for all embeddings $\sigma : K(\alpha,\beta) \hookrightarrow K^{\text{al}}$ fixing $K(\alpha)$, that $\sigma(\beta)=\beta$. We have

$$|\sigma(\beta)-\alpha| = |\sigma(\beta)-\sigma(\alpha)| = |\beta-\alpha|$$

since $|\bullet| = |\sigma\bullet|$ and $\sigma(\alpha)=\alpha$. Hence

$$|\sigma(\beta)-\beta| = |(\sigma(\beta)-\alpha)+(\alpha-\beta)| \le |\beta-\alpha|,$$

the last following since $|\cdot|$ is nonarchimedean. By the minimality assumption we must have $\sigma(\beta)=\beta$. □

We define a norm on polynomials by setting

$$\left\|\sum_{k=0}^{n} c_k X^k\right\| = \max_{0\le k\le n} |c_k|.$$

Using Krasner's Lemma, we show that polynomials that are close together have roots that are closely related.

*Proof.* Choose $\delta$ so this last quantity is at most $\min_{i\neq j}|\alpha_i-\alpha_j|$. Then by Krasner's Lemma 8.1, $\alpha \in K[\beta]$. Since $\beta$ and $\alpha$ both have degree $n$ over $K$, $K(\alpha)=K(\beta)$. □

In fact, we have the following stronger result. Using Krasner's Lemma, we show that polynomials that are close together have roots generating the same extensions.

**Theorem 8.2:** krasner-poly Given $f$, there exists $\varepsilon > 0$ such that if $\|f-g\| < \varepsilon$, then there is an ordering of roots $\alpha_1,\dots,\alpha_n$ and $\beta_1,\dots,\beta_n$ of $f$ and $g$, respectively, counting multiplicities, such that $K(\alpha_j)=K(\beta_j)$.

*Proof.* Step 1: First we show that the roots of $g$ approach the roots of $f$, as $\|f-g\| \to 0$.

**Lemma 8.3:** root-continuity1 Keep the hypothesis of the theorem. Suppose $\varepsilon > 0$. Then there exists $\delta > 0$ such that if $\|f - g\| < \delta$, then for every root $\beta$ of $g$, there exists a root $\alpha$ of $f$ such that $|\beta - \alpha| < \varepsilon$.

*Proof.* First note that the roots of a monic polynomial $h$ are bounded in terms of $\|h\|$. Indeed, letting $h(X) = \sum_{k=0}^{n} c_k X^k$, if $\gamma$ is a root of $h$, then by Proposition 2.6(3), we must have $c_k \gamma^k \geq \gamma^n$ for some $0 \leq k < n$, and hence

$$\gamma \leq c_k^{\frac{1}{n-k}} \leq \max(1, \|h\|).$$

Suppose $\|f - g\| \leq \delta$ is small (say, less than 1). Then $\|g\| \leq \|f\| + \delta$, which is bounded. Hence the roots of $\|g\|$ are bounded, say by $C$. Let $\beta$ be a root of $g$. On the one hand, we have

$$function - continuity(f - g)(\beta) \leq \|f - g\| \max\{|\beta|^n, 1\} \leq \delta \max\{C^n, 1\} \tag{7.5}$$

and on the other,

$$(f - g)(\beta) = f(\beta) = \prod_{k=1}^{n} (\beta - \alpha_k).$$

Hence $|\beta - \alpha_k| \leq (\delta \max\{C^n, 1\})^{\frac{1}{n}}$ for some $n$. We can choose $\delta$ so this is less than $\varepsilon$. $\square$

Step 2: We strengthen the lemma to account for multiplicities.

**Lemma 8.4:** root-continuity2 Keep the hypotheses of the theorem. For every $\varepsilon > 0$ there exists $\delta > 0$ such that whenever $\|f - g\| < \delta$, there exist orderings $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ such that $|\beta_k - \alpha_k| < \varepsilon$ for all $k$.

*Proof.* By Lemma 8.3, as $\|f - g\| \to 0$, the distance from the roots of $g$ to the closest roots of $f$ approaches 0. Let $\beta_1(g), \ldots, \beta_n(g)$ be the roots of $g$. For each $k$ let $\alpha_k(g)$ be the root of $f$ closest to $\beta_k(g)$. We have $\max_k |\beta_k(g) - \alpha_k(g)| \to 0$ as $g \to f$. Suppose the distinct roots $\alpha'_1, \ldots, \alpha'_m$ of $f$ have multiplicities $r_1, \ldots, r_m$, and suppose that they occur with multiplicities $s_1, \ldots, s_m$ in the $\alpha_k(g)$. Suppose by way of contradiction that $(s_1(g), \ldots, s_m(g))$ is not constantly $(r_1, \ldots, r_m)$ for $g$ close enough to $f$. Then we can find a sequence $g_j \to f$ such that $(s_1(g_j), \ldots, s_m(g_j))$ is constant and not equal to $(r_1, \ldots, r_m)$. Then

$$g_j(X) = \prod_{k=1}^{n} (X - \beta_k(g_j)) \to \prod_{k=1}^{m} (X - \alpha'_k(g_j))^{s_k} \neq \prod_{k=1}^{m} (X - \alpha'_k)^{r_k} = f(X),$$

contradiction. $\square$

Step 3: Take $\varepsilon = \min_{i \neq j} |\alpha'_i - \alpha'_j|$ in Lemma 8.4. Then Krasner's Lemma 8.1 gives the conclusion. $\square$

From this we get that every field extension of $\mathbb{Q}_p$ can be described by a field extension of $\mathbb{Q}$, by choosing a close enough approximation to a minimal polynomial.

**Corollary 8.5:** Let $L/\mathbb{Q}_p$ be a finite extension. Then there is a finite extension $K/\mathbb{Q}$ such that $[K : \mathbb{Q}] = [L : \mathbb{Q}_p] = n$ and $K \cdot \mathbb{Q}_p = L$.

*Proof.* Using the primitive element theorem, choose $\alpha$ so that $\mathbb{Q}_p(\alpha) = L$. Let $g \in \mathbb{Q}_p[X]$ be the minimal polynomial of $\alpha$. By Theorem 8.2, for $g$ close enough to $f$, there is a root $\beta$ of $g$ such that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Take $g \in \mathbb{Q}[X]$ sufficiently close, and $L = K(\beta)$. Then

$$K \cdot \mathbb{Q}_p = K(\alpha) = K(\beta) = L. \qquad \square$$

# Chapter 8
# Local and global fields

lg-fields

## §1 Topology of local fields

**Definition 1.1:** A **local field** is a field $K$ with a nontrivial valuation $|\cdot|$ such that $K$ is locally compact.

Note this requires that $K$ is complete.

**Proposition 1.2:** ring-of-integers-compact Let $K$ be complete with respect to a discrete nonarchimedean valuation. Then $A$ is compact if and only if $k := A/\mathfrak{m}$ is finite.

*Proof.* Suppose $A$ is compact. Note $\mathfrak{m} = \{x : |x| < 1\}$ is open, and any translate of it is open. Note $A = \bigsqcup_{a \in A/\mathfrak{m}} a + \mathfrak{m}$ where the union is over representatives in $A/\mathfrak{m}$. A finite number of these cover $A$, so $k$ is finite.

Conversely, suppose $k := A/\mathfrak{m}$ is bounded. It suffices to show that $A$ is closed and totally bounded[1].

1. $A$ is closed since $A = \{x : |x| \le |\pi|\}$.
2. $A$ is totally bounded: Given $\varepsilon > 0$, choose $r$ so that $|\pi|^{r+1} < \varepsilon$. Now every element is in a ball of radius 1 centered at one of the finite number of points in the form $a_0 + a_1\pi + \cdots + a_r\pi^r$. $\square$

**Proposition 1.3:** compact-sets-in-lf If $K$ has finite residue field then $\mathcal{O}_K^\times$, $\mathfrak{p}^n$, and $1 + \mathfrak{p}^n$ are all compact.

*Proof.* From Proposition 1.2, $A$ is compact. The above are all closed subsets of $A$ so compact. $\square$

**Theorem 1.4:** The following is a complete classification of local fields, up to isomorphism.

[1] A set is *totally bounded* if for every $r$, $A$ can be covered by a finite number of sets with diameter at most $r$.

1. $\mathbb{R}$ and $\mathbb{C}$ with the usual metric.
2. Finite extensions of $\mathbb{Q}_p$.
3. Field of formal Laurent series $k((T))$ over finite field.

*Proof.* Neukirch, p. 135. □

Fill in: local fields vastly simplify things because...

## 1.1 Open sets and continuity

**Proposition 1.5:** power-open For any local field $K$ and any $n$, the $n$th power map is open on $K^\times$, i.e. it takes open subsets of $K^\times$ to open sets.

*Proof.* For $K = \mathbb{R}$ or $\mathbb{C}$, this is clear.

For $K$ $\pi$-adic, this is an easy consequence of Hensel's Lemma. Let $y \in K^{\times n}$. We may suppose $v(y) = 0$. Suppose $x_0^p - y = 0$. Let $k = v(p)$ and let $\varepsilon$ be such that $v(\varepsilon - y) \geq 2k+1$. Consider the polynomial $f(x) = x^n - y$. Now $f(x_0) \equiv 0 \pmod{\pi^{2k+1}}$ so by Hensel's Lemma $x_0$ lifts to a solution of $f$ in $K$. (The version of Hensel in ACIM, p. 14. Add this in.) □

**Proposition 1.6:** pr:nm-cont For any extension of local fields $L/K$, any $\sigma \in G(L/K)$ acts as a homeomorphism, and the norm map $\mathrm{Nm}_{L/K}$ is continuous and open on $K^\times$.

# §2 Unramified extensions

**Definition 2.1:** Let $K$ be a complete field with residue field $k$; let $L$ be a finite extension of $K$ with residue field $l$. We say $L/K$ is **unramified** if $l/k$ is separable and the prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ does not ramify in $L$.

$L/K$ is **totally ramified** if $\mathfrak{p}$ ramifies completely; by the degree equation this is equivalent to $l = k$.

Note from the residue equation that

$$doesnt-ramify\,\mathfrak{p} \text{ does not ramify} \iff [L:K] = [l:k]. \tag{8.1}$$

Our main theorem of this section is Theorem 2.4. We will show that if $L/K$ is unramified, then $l/k$ is separable. If $l/k$ is separable, though, we need an extra condition to make sure $L/K$ is unramified; namely that a minimal polynomial for $L/K$ stays a minimal polynomial for $l/k$, so that (8.1) holds.

**Proposition 2.2:** complete-unramified-criteria Let $K$ be a complete field with residue field $k$; let $L$ be a finite extension of $K$ with residue field $l$. Suppose $L = K(\alpha)$, and let $g(x) \in K[x]$. The following are equivalent.

1. $L/K$ is unramified, and $g$ is the minimal polynomial of $\alpha$.

2. $l/k$ is separable, with $l = k(\overline{\alpha})$, $g$ has $\alpha$ as a root, $\overline{g}$ is the minimal polynomial of $\overline{\alpha}$, and $\overline{g}$ has no repeated roots.

*Proof.* Suppose (1) holds. Then $\overline{g}$ has $\overline{\alpha}$ as a root. Note $L = K(\alpha)$ gives $l = k(\overline{\alpha})$. By (8.1), $\overline{\alpha}$ has degree $[l : k] = [L : K]$ over $k$. Since $\overline{g}$ has degree $[L : K]$, it must be the minimal polynomial of $\overline{\alpha}$, and have no repeated roots. This shows $l/k$ is separable.

Suppose (2) holds. We have

$$[L : K] \le \deg g = \deg \overline{g} = [l : k],$$

the last equality following since $\overline{g}$ is the minimal polynomial of $\overline{\alpha}$. But $[L : K] \ge [l : k]$, so equality holds and $\mathfrak{p}$ (the prime ideal of $\mathcal{O}_K$) is unramified by (8.1). Thus $L/K$ is unramified. $\square$

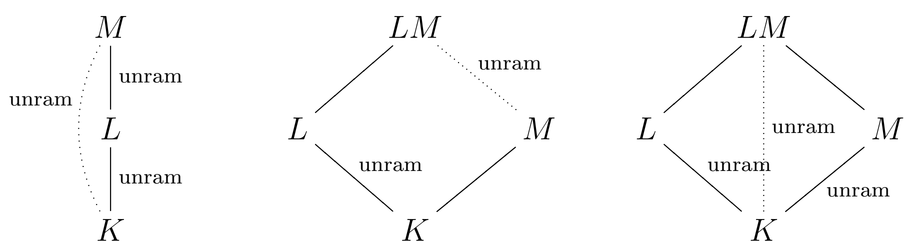
For local fields, the property of being unramified behaves well under extensions and products.

**Proposition 2.3:** unramified-props

1. Suppose that $K \subseteq L \subseteq M$ are finite extensions. If $M/L$ and $L/K$ are unramified, then $M/K$ is unramified.

2. Suppose that $K \subseteq L, M$ are finite extensions. If $L/K$ is unramified, then $LM/M$ is unramified.

3. Suppose that $K \subseteq L, M$ are finite extensions. If $L/K$ and $M/K$ are unramified, then $LM/K$ is unramified.




*Proof.* Let $k, l, m, n$ be the residue fields of $K, L, M, LM$, and $\mathfrak{p}$, $\mathfrak{P}$, and $\mathfrak{P}'$ be the prime ideals of $\mathcal{O}_K$, $\mathcal{O}_L$, $\mathcal{O}_M$, respectively.

1. We have $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}\mathcal{O}_L = \mathfrak{P}'$. Separability is transitive, so $M/K$ is unramified.

2. Write $L = K(\alpha)$. By Proposition 2.2, we can find $g$ with $\alpha$ as root such that $\overline{g}$ is the minimal polynomial of $l = k(\alpha)$ over $k$, and is separable. Then the minimal polynomial for $n = m(\alpha)$ over $m$ divides $\overline{g}$, hence is separable. By Proposition 2.2 again, $LM/M$ is unramified.

3. By part 2, $LM/M$ is unramified. Since $M/K$ is unramified, by part 1 $LM/K$ is unramified. $\square$

**Theorem 2.4:** unramified-is-separable Let $K$ be a field; fix an algebraic closure. There is an equivalence of categories between

- finite unramified extensions $L/K$, and
- finite separable extensions $l/k$.

$$\begin{tikzcd} L_1 \arrow[r] \arrow[d] & L_2 \arrow[d] \\ l_1 = L_1/\mathfrak{p}_1 \arrow[r] & l_2 = L_2/\mathfrak{p}_2. \end{tikzcd}$$

Moreover,

1. $L \subseteq M$ if and only if $l \subseteq m$.
2. The residue field of $LM$ is $lm$.
3. $L/K$ is Galois if and only if $l/k$ is Galois, and

$$G(L/K) \xrightarrow{\cong} G(l/k)$$

by restricting $\sigma \in G(L/K)$ to $B = \mathcal{O}_L$ and modding out by $\mathfrak{P}B$.

*Proof.* By Proposition 2.2, $L$ does get sent to a separable extension.

First we show the map is surjective. Given $l/k$ separable, choose $\beta$ so that $l = k(\beta)$ and choose $f$ so that $\overline{f}$ be the minimal polynomial of $\beta$. Since $\beta$ is a simple root of $\overline{f}$, by Hensel's Lemma 5.1 we can lift it to a root $\alpha$ of $f$. Then $K(\alpha)$ is mapped to $k(\beta)$.

Part (2) is clear. For (1), if $L \subseteq M$ then clearly $l \subseteq m$. Conversely, suppose $l \subseteq m$. Now $LM$ is also unramified (Proposition 2.3) and has residue field $l \cdot m = m$. Hence,

$$[M : K] = [m : k] = [lm : k] = [LM : K],$$

showing $L \subseteq M$.

If $l = m$, then the above shows that $L = M$. Hence the map is injective. The action on maps $L_1 \to L_2$ is self-explanatory.

For (3), note an extension is Galois iff it is the (minimal) splitting field of a separable polynomial $f$. Take $g$ to be the minimal polynomial of a primitive element $\alpha$; note $\overline{\alpha}$ generates $l/k$. Note by Proposition 2.2, $\overline{g}$ is separable. If $L/K$ is Galois, then $g$ splits over $L$ so $\overline{g}$ splits over $l$. Combining the previous two statements, $l/k$ is Galois. Conversely, suppose $l/k$ is Galois. Since $\overline{g}$ splits into nonrepeated linear factors, Hensel's Lemma 5.2 lifts it to a factorization of $g$. Hence $g$ splits over $K$ into distinct linear factors, showing $L/K$ is Galois. $\square$

Suppose $k$ is a finite field. In this case, the separable extensions $l/k$ are exactly the finite extensions. Moreover, we understand what these extensions are; there is one of each degree, and we can find the corresponding $L/K$ explicitly. Furthermore, by surjectivity in (3), $G(L/K)$ contains a unique element mapping to the Frobenius element in $G(l/k)$; see Definition 10.1.1.

**Lemma 2.5:** nroot-unram Let $\alpha$ be a root of

$$f(X) := X^n - a = 0$$

where $a$ is a unit and $p \nmid n$. Then $K(\alpha)/K$ is unramified.

*Proof.* Let $g(X) \mid f(X)$ be the minimal polynomial of $\alpha$. Let $L = K(\alpha)$ and $l$ be its residue field.

Note that $f'(X) = nX^{n-1} \neq 0$ has no common factor with $f(X) = X^n - a$, even when reduced modulo $\mathfrak{p}$, as $p \nmid n$ and $a \notin \mathfrak{p}$. Hence $f(X)$, and *a fortiori* $g(X)$, has no repeated root in $k$. Any factorization of $g(X)$ in $k$ gives a factorization of $g(X)$ in $K$ by Hensel's Lemma. Hence $g$ remains irreducible in $k[X]$. This shows $[l : k] = [L : K]$. By the degree equation, $L/K$ must be unramified. $\square$

**Theorem 2.6:** unram-ram Let $L/K$ be an extension of complete fields with finite residue fields. Then there exists a field $K \subseteq L_u \subseteq L$ such that $L_u/K$ is unramified and every unramified extension of $K$ contained in $L$ is contained in $L_u$. Moreover,

1. $L_u$ is obtained by adjoining to $K$ all roots of unity in $L$ whose order is relatively prime to $q := \mathrm{char}(K)$.

2. $L/L_u$ is totally ramified.

$$\begin{tikzcd} L \arrow[d, dash, "\text{totally ramified}"] \\ L_u \arrow[d, dash, "\text{unramified}"] \\ K \end{tikzcd}$$

We call $L_u$ the **maximal unramified extension** of $K$ contained in $L$. This is useful... Defining this when $L/K$ is infinite

*Proof.* Let $L_u$ be the compositum of all unramified extensions of $K$ contained in $L$. Then $L_u$ is unramified by Proposition 2.3, and it contains all unramified extensions of $K$ contained in $L$.

For each $n$ not a multiple of $p$, $K(\zeta_n)/K$ is unramified by Lemma 2.5. Letting $q = |k|$, the corresponding extension of residue fields is $k(\zeta_n)/k = \mathbb{F}_{q^{\mathrm{ord}_q(n)}}/\mathbb{F}_q$. We get all finite extensions $l/k$ in this way, thus all unramified extensions $L'/K$ in this way. Taking the roots of unity inside $L$ gives the result. $\square$

# §3 Ramified extensions

**Definition 3.1:** Let $L/K$ be a ramified extension of local fields, with $q := \text{char}(k) = p^n$. We say

1. $L/K$ is **tamely ramified** if $p \nmid [l : k]$.
2. $L/K$ is **wildly ramified** if $p \mid [l : k]$.

We seek analogues of Lemma 2.5 in for ramified extensions.

For a prime $\mathfrak{p}$ of a Dedekind domain $A$ (not necessarily corresponding to a local field) let $v_{\mathfrak{p}}$ denote the corresponding valuation. (That is, if $v_{\mathfrak{p}}(a)$ is defined such that $\mathfrak{p}^{v_{\mathfrak{p}}(a)}$ is the highest power of $\mathfrak{p}$ dividing $(a)$.) Note the following two facts.

1. If $\mathfrak{p}B = \mathfrak{P}^e$, then
$$v_{\mathfrak{p}}(a) = v_{\mathfrak{P}}(a)^e.$$
2. If $a_1 + \cdots + a_n = 0$, then the minimum value of $v_{\mathfrak{p}}(a_i)$ is attained for two indices.

**Definition 3.2:** eisenstein-df An **Eisenstein extension** relative to $\mathfrak{p}$ is an extension $K(\alpha)/K$ where the minimal polynomial of $\alpha$ is of the form

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

where $v_{\mathfrak{p}} a_i > 0$ and $v_{\mathfrak{p}} a_0 = 1$.

**Theorem 3.3:** eisenstein-ramification The prime ideal $\mathfrak{p}$ totally ramifies in any Eisenstein extension relative to $\mathfrak{p}$:

$$\mathfrak{p}B = \mathfrak{P}^e, \quad \mathfrak{P} = (f(\alpha), \mathfrak{P})^e.$$

*Proof.* Let $\mathfrak{P}^e || \mathfrak{p}$. Note $e \le n = [L : K]$. We calculate the valuation of $f(\alpha)$ with respect to $\mathfrak{P}$.

$$\begin{aligned} v_{\mathfrak{P}}(\alpha^n) &= n v_{\mathfrak{P}}(\alpha) \\ v_{\mathfrak{P}}(a_k \alpha^k) &= e + k \,\text{ord} > e, && 1 \le k \le n-1 \\ v_{\mathfrak{P}}(a_0) &= e. \end{aligned}$$

Since $f(\alpha) = \alpha^n + \cdots + a_0 = 0$, the minimum valuation must be attained for two terms. The only way this is possible is if $n \,\text{ord}_{\mathfrak{P}}(\alpha) = e$. Then $\text{ord}_{\mathfrak{P}}(\alpha) = 1$ and $n = e$, as needed. □

**Theorem 3.4:** Let $K$ be complete with respect to a nonarchimedean valuation. The totally ramified extensions of $K$ are exactly those of the form $K(\alpha)$ where $\alpha$ is the root of an Eisenstein polynomial.

*Proof.* The forward direction follows directly from Theorem 3.3.

Conversely, let $L/K$ be a totally ramified extension. Take $\alpha$ to be a generator of the maximal ideal $\mathfrak{P}$ of $\mathcal{O}_L$. Note $\operatorname{ord}(\alpha) = \frac{1}{n}$ since $(\alpha)^n = \mathfrak{p}$. Note that for any $a_{n-1}, \ldots, a_0$, we have

$$\operatorname{ord}(a_k\alpha^k) = \operatorname{ord}(a_k) + \frac{k}{n} \equiv \frac{k}{n} \pmod 1,$$

since $\operatorname{ord}(a_k)$ is an integer. Thus, the nonzero terms $a_k\alpha^k$, $0 \le k < n$, have different orders. Thus by Proposition 2.6, $a_{n-1}\alpha^{n-1} + \cdots + a_0 \neq 0$ unless all coefficients are 0. This shows that $\alpha$ must have degree $n$; suppose $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. Again by Proposition 2.6, the minimum order is attained for two terms. We have

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}}(\alpha^n) &= n \operatorname{ord}_{\mathfrak{p}}(\alpha) = 1 \\ \operatorname{ord}_{\mathfrak{p}}(a_k\alpha^k) &= k \operatorname{ord}(a_k) + \frac{k}{n}, \qquad\qquad 0 \le k \le n-1. \end{aligned}$$

The only way this can happen is if $\alpha^n$ and $\operatorname{ord}(a_0)$ are the nonzero terms with least order. This gives $\operatorname{ord}(a_0) = 1$, and $\operatorname{ord}(a_k) > 0$ for $1 \le k \le n$, i.e. the polynomial is Eisenstein. $\square$

**Theorem 3.5:** Suppose $L/K$ is a totally and tamely ramified extension of degree $n$. Then $L = K(\alpha)$ for some $\alpha$ a root of

$$X^n - \pi = 0$$

for $\pi \in \mathfrak{p}$.

*Proof.* Take $\beta \in \mathfrak{P}$. Since $L/K$ is totally ramified, $\operatorname{ord}_{\mathfrak{p}}(\beta^n) = 1$. Hence $\beta^n = u\pi$ for some $u \in B^\times$, and $\beta$ is a zero of

$$g(X) := X^n - u\pi.$$

Unfortunately, $u$ may not be in $A$. However, we show that this polynomial is close enough to

$$f(X) := X^n - u'\pi$$

for some $u' \in A$ and proceed as in Theorem 8.2 to show that the roots of these two polynomials generate the same extension.

Since $L/K$ is totally ramified, $l = k$, i.e. $A/\mathfrak{p}A \xrightarrow{\cong} B/\mathfrak{P}B$. Thus there exists $u' \equiv u \pmod{\mathfrak{P}}$ with $u' \in A$. This means $|u' - u| < 1$. Letting $\alpha_1, \ldots, \alpha_n$ be the roots of $f(X) = 0$,

$$|\beta - \alpha_1| \cdots |\beta - \alpha_n| = |f(\beta)| = |u\pi - u'\pi| < |\pi| = |\alpha_1| \cdots |\alpha_n|$$

so $|\beta - \alpha_j| < |\alpha_j|$ for some $j$; without loss of generality $j = 1$.

Since $L/K$ is tamely ramified, $p \nmid n$ and $f'(\alpha_1) = n\alpha_1^{n-1}$ has valuation $|\alpha_1|^{n-1}$. Hence

$$\textit{derivative} - \textit{valuation}|\alpha_1|^{n-1} = |f'(\alpha_1)| = |(\alpha_1 - \alpha_2) \cdots (\alpha_1 - \alpha_n)|. \tag{8.2}$$

Note $|\alpha_j| = |u'\pi|^{\frac{1}{n}} = |\alpha_1|$; hence $|\alpha_1 - \alpha_j| \le |\alpha_1|$. By (8.2), equality must hold. Hence $|\beta - \alpha_1| < |\alpha_1 - \alpha_j|$ for all $j \neq 1$, and by Krasner's Lemma 8.1, $K(\alpha_1) \subseteq K(\beta)$. Since both extensions are totally ramified of degree $n$, $L = K(\beta) = K(\alpha_1)$. $\square$

The analogues of Proposition 2.3 carry over exactly.

**Proposition 3.6:** ramified-props

1. Suppose that $K \subseteq L \subseteq M$ are finite extensions. If $M/L$ and $L/K$ are tamely ramified, then $M/K$ is tamely ramified.
2. Suppose that $K \subseteq L, M$ are finite extensions. If $L/K$ is tamely ramified, then $LM/M$ is tamely ramified.
3. Suppose that $K \subseteq L, M$ are finite extensions. If $L/K$ and $M/K$ are tamely ramified, then $LM/K$ is tamely ramified.

**Theorem 3.7:** Let $K$ be a field with characteristic 0 and finite residue field, and let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. Given $n$, there are only finitely many extensions of $K_{\mathfrak{p}}$ with degree at most $n$.

*Proof.* First we show that there are finitely many totally ramified extensions of degree $n$. Every such extension is realized by adjoining a root of an Eisenstein polynomial of degree $n$. By taking the coefficients, an Eisenstein polynomial can be identified with a point of

$$poly-compact\, \underbrace{\mathfrak{p}\times\cdots\times\mathfrak{p}}_{n-1}\times A^{\times}\pi. \tag{8.3}$$

The topology given by $\|\cdot\|$ is exactly the product topology here; this is compact by Proposition 1.3. Now for each polynomial $f$, by Theorem 8.2 there exists an open set $U_f$ such that any $g \in U_f$ has roots generating the same extensions as those of $f$. Since (8.3) is compact, a finite number of $U_f$ cover $f$. The roots corresponding to those $f$ generate all the totally ramified extensions of degree $n$.

By Theorem 2.6. Any finite extension $L$ of degree $n$ is an totally ramified extension of degree $\frac{n}{m}$ of an unramified extension $L_u$ of degree $m$ for some $m$. By the remark after Theorem 2.4, there is exactly one unramified extension of degree $m$; for each $L_u$ by the above there are a finite number of possibilities for $L$. □

# §4 Witt vectors*

We know from Proposition 4.5 that every element of $\hat{K}$ can be written as $\sum_{n\geq N} a_n\pi^n$ where the $a_n$ come from a fixed set of representatives for $A/\mathfrak{m}$. Although this allows us to write down any element, unless the set of representatives is closed under addition and multiplication (i.e. form a copy of $k$ in $A$), we cannot simply add and multiply the coefficients. Instead, we find that addition and multiplication are governed by *Witt vectors*. We will actually develop this theory in a more general context.

**Definition 4.1:** Let $p$ be a prime number. A ring $R$ is a **strict $p$-ring** if $R$ is complete and Hausdorff with respect to the $p$-adic topology, $p$ is not a zero-divisor in $R$, and the residue ring $R/(p)$ is perfect. (A ring of characteristic $p$ is **perfect** if the map $x \mapsto x^p$ is bijective.)

We will primarily be interested in the case where $R$ is an unramified extension of $\mathbb{Z}_p$.

**Theorem 4.2:** Let $K$ be a perfect ring of characteristic $p$.

1. There is a strict $p$-ring $R$ with residue ring $K$, unique up to canonical isomorphism.
2. There is a unique system of representatives $\tau : K \to R$, called the **Teichmüller representatives**, such that
$$\tau(xy) = \tau(x)\tau(y)$$
for all $x, y \in K$.

The main example of interest to us is the following.

**Example 4.3:** Fix $f$; then there is a unique unramified extension of $\mathbb{Z}_p$ with residue field $\mathbb{F}_q$, $q = p^f$, namely $\mathbb{Z}_p[\zeta_{p^f-1}]$. The Teichmuller representatives are the $(q-1)$th roots of unity $\mu_{q-1}$. They are multiplicative, but not additive. The following construction will tell us how to add them.

**Lemma 4.4:** witt-operations Given $X = (X_0, X_1, \ldots)$, define

$$W_n(X) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n, \quad n \geq 0.$$

Then there exist polynomials

$$S_0, S_1, \ldots; P_0, P_1, \ldots \in \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$$

such that

$$W_n(S) = W_n(X) + W_n(Y)$$
$$W_n(P) = W_n(X) \cdot W_n(Y).$$

where $X = (X_0, X_1, \ldots)$, $Y = (Y_0, Y_1, \ldots)$, $S = (S_0, S_1, \ldots)$, and $P = (P_0, P_1, \ldots)$.

The motivation for defining these polynomials is that they tell us how to add in strict $p$-rings using the base-$p$ represenation with Teichmüller representatives as coefficients.

**Theorem 4.5:** Let $R$ be a strict $p$-ring, $k$ its residue ring, and $\tau : k \to R$ be the system of Teichmüller representatives. Then

$$\sum_{n=0}^{\infty} \tau(x_n)p^n + \sum_{n=0}^{\infty} \tau(y_n)p^n = \sum_{n=0}^{\infty} \tau(S_n(x_0^{p^{-n}}, x_1^{p^{-(n-1)}}, \ldots, x_n; y_0^{p^{-n}}, y_1^{p^{-(n-1)}}, \ldots, y_n)p^n.$$

*Proof of Lemma 4.4.* We will abbreviate

$$W(X) = (W_0(X), W_1(X), \ldots)$$
$$R = \mathbb{Z}[X_0, X_1, \ldots; Y_0, Y_1, \ldots].$$

All comparisons between $X, Y$ will be done componentwise, and we define $X^n = (X_0^n, X_1^n, \ldots)$.

We find the $S_m, P_m$ inductively, with the additional condition that $S_m, P_m$ are polynomials in $X_0, \ldots, X_m, Y_0, \ldots, Y_m$. To begin, note $W_0(X) = X_0$ so we set

$$\begin{aligned} S_0(X,Y) &= X_0 + Y_0 \\ P_0(X,Y) &= X_0 Y_0. \end{aligned}$$

**Lemma 4.6:** If $F_m, G_m \in R$ and $F_m \equiv G_m \pmod{p}$ for every $m$, then

$$W_n(F) \equiv W_n(G) \pmod{p^{n+1}}.$$

*Proof.* First note that for any $f, g \in R$ such that $f \equiv g \pmod{p}$,

$$f^{p^j} \equiv g^{p^j} \pmod{p^{j+1}}.$$

The proof is by induction, with the induction step following by the binomial theorem: if $f^{p^{j-1}} = g^{p^{j-1}} + p^j h$ then

$$f^{p^j} = (g^{p^{j-1}} + p^j h)^p = g^{p^j} + \underbrace{\binom{p}{1} p^{j-1}}_{p^j} h g^{p^{j-1}(p-1)} + p^{j+1} k$$

for some $k \in R$.

This claim gives $f_j^{p^{n-j}} \equiv g_j^{p^{n-j}} \pmod{p^{n-j+1}}$ and hence

$$p^j f_j^{p^{n-j}} \equiv p^j g_j^{p^{n-j}} \pmod{p^{n+1}}.$$

Summing these up give the result. $\square$

Directly from the definitions, we have

$$W_n(X) = W_{n-1}(X^p) + p^n X_n.$$

Hence the equations

$$\begin{aligned} W_n(S) &= W_n(X) + W_n(Y) \\ W_n(P) &= W_n(X) W_n(Y) \end{aligned}$$

are equivalent to

$$\begin{aligned} W_{n-1}(S^p) + p^n S_n &= W_{n-1}(X^p) + p^n X_n + W_{n-1}(Y^p) + p^n Y_n \\ witt - add &= W_{n-1}(S(X^p, Y^p)) + p^n (X_n + Y_n) && (8.4) \\ W_{n-1}(P^p) + p^n P_n &= (W_{n-1}(X^p) + p^n X_n)(W_{n-1}(Y^p) + p^n Y_n) \\ witt - mult &= W_{n-1}(P(X^p, Y^p)) + p^n (X_n W_{n-1}(Y^p) + Y_n W_{n-1}(X^p) + p^n X_n Y_n) && (8.5) \end{aligned}$$

where (8.4) and (8.5) follow from the hypothesis for $n-1$. Solving for $S_n$ and $P_n$, these are equivalent to

$$S_n = X_n + Y_n + \frac{W_{n-1}(S(X^p, Y^p)) - W_{n-1}(S^p)}{p^n}$$
$$P_n = X_n W_{n-1}(Y^p) + Y_n W_{n-1}(X^p) + p^n X_n Y_n + \frac{W_{n-1}(P(X^p, Y^p)) - W_{n-1}(P^p)}{p^n}.$$

However, since taking $p$th powers is a homomorphism modulo $p$, for any $f \in R$ we have $f(X,Y)^p \equiv f(X^p, Y^p) \pmod p$. Applying this to $f = S_j, P_j$, we see the conditions of the lemma are satisfied, so the numerators are divisible by $p^n$, and we can successfully define $S_n$ and $P_n$. $\square$

**Theorem 4.7:** Let $A$ be a commutative ring. For

$$a = (a_0, a_1, \dots), \quad b = (b_0, b_1, \dots), \quad a_i, b_i \in A_i,$$

the operations

$$a \overset{W}{+} b = S(a,b), \quad a \overset{W}{\cdot} b = P(a,b).$$

turn the set $A^{\mathbb{N}_0}$ into a commutative ring $W(A)$.

This is called the **ring of Witt vectors** over $A$.

*Proof.* We first prove that associativity, commutativity, and distributivity hold as polynomial identities in the $a_j, b_j$. The result then follows by considering the substitution homomorphism $\mathbb{Z}[a_0, \dots; b_0, \dots] \to A$.

**Lemma 4.8:** The function $W : R^{\mathbb{N}} \to R^{\mathbb{N}}$, where $R := \mathbb{Z}[a_0, \dots; b_0, \dots]$, is injective.

*Proof.* Suppose $X = (X_0, X_1, \dots)$ and $W(X) = (Y_0, Y_1, \dots)$. We show the $X_j$ are determined by induction. We have $X_0 = W_0(X) = Y_0$. For the induction step, note

$$Y_n = W_n(X) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n;$$

since $X_0, \dots, X_{n-1}, Y_n$ are determined and multiplication by $p^n$ is injective in $R$, $X_n$ is determined. $\square$

Lemma 4.4 gives

$$W(X \overset{W}{+} Y) = W(S(X,Y)) = W(X) + W(Y)$$
$$W(X \overset{W}{\cdot} Y) = W(P(X,Y)) = W(X) \cdot W(Y).$$

Hence $W : W(A) \to R^{\mathbb{N}}$ is a map that preserves addition and multiplication; moreover, it is injective. Its image is a subalgebra of $R$, since it contains 0 and 1:

$$W(0, 0, \dots) = (0, 0, \dots)$$
$$W(1, 0, \dots) = (1, 1, \dots).$$

Hence $\overset{W}{+}$ and $\overset{W}{\cdot}$ turn $W(A)$ into a commutative algebra with unit (we are basically "pulling back" the algebra structure from $R^{\mathbb{N}}$ to $W(A)$ using $W$). ☐

### 4.1 Frobenius and Transfer maps

## §5 Extending valuations on global fields

**Theorem 5.1:** ext-val-irr Let $|\cdot|$ be a valuation on $K$ and let $\hat{K}$ be the completion of $K$ with respect to $|\cdot|$. Let $L = K(\alpha)$ be a finite separable extension of $K$, and let $f$ be the minimal polynomial of $\alpha$.

The completions of $L$ with respect to the extensions $|\cdot|'$ of $|\cdot|$ are exactly $\hat{K}[X]/(h)$ as $h$ ranges over irreducible factors of $f$ in $\hat{K}$.

*Proof.* Suppose we are given an extension $|\cdot|'$. Let $\hat{L}$ be the completion of $L$ with respect to $|\cdot|'$.

$$\begin{tikzcd} L = K[\alpha] \arrow[r, hook] \arrow[d, dash] & \hat{L} = \hat{K}[\alpha] \arrow[d, dash] \\ K \arrow[r] & \hat{K} \end{tikzcd}$$

Note $\hat{K}[\alpha]$ contains $\alpha$ and is complete (as it is a finite-dimensional vector space over a complete field), so $\hat{L} = \hat{K}[\alpha]$. Then considering the extension $\hat{L}/\hat{K}$, $\alpha$ is the root of one of the irreducible factors of $f$ in $\hat{K}[X]$.

Conversely, given an irreducible factor $g$ of $h$ in $\hat{K}[X]$, consider $\hat{K}[\alpha'] = \hat{K}[X]/(g)$.

$$\begin{tikzcd} L = K(\alpha) \arrow[r, hook] \arrow[d, dash] & \hat{L} = \hat{K}(\alpha') \arrow[d, dash] \\ K \arrow[r] & \hat{K} \end{tikzcd}$$

The valuation on $\hat{K}$ extends uniquely to $\hat{K}(\alpha')$ by Theorem 6.1. Then let $K(\alpha) \hookrightarrow \hat{K}(\alpha')$ be the map sending $\alpha$ to $\alpha'$. (This makes sense as the minimal polynomials of $\alpha, \alpha'$ over $K$ are both $f$.) By the same reason as before, $\hat{L} = \hat{K}(\alpha)$, as desired. ☐

**Theorem 5.2:** completion-tensor Let $\hat{K}$ be the completion of $K$ with respect to a archimedean or discrete nonarchimedean valuation $|\cdot|$. Let $L/K$ be a finite separable extension. There are finitely many extensions of $|\cdot|$ to $L$; denoting them by $|\cdot|_i$ and the respective completions of $L$ be $L_i$, we have the natural isomorphism

$$\hat{K} \otimes_K L \cong \prod_i L_i.$$

*Proof.* By the primitive element theorem, we can write $L = K(\alpha)$. Let $f$ be the minimal polynomial of $\alpha$. Let $f$ factor into irreducibles in $\hat{K}[X]$ as

$$f = f_1 \cdots f_n.$$

Then

$$\hat{K} \otimes_K L \cong \hat{K} \otimes_K K[x]/(f) \cong \hat{K}[x]/(f) \overset{\text{CRT}}{\cong} \prod_{i=1}^{n} \hat{K}[x]/(f_i) \overset{\text{Thm 5.1}}{\cong} \prod_{i=1}^{n} L_i.$$

□

Note the map in the theorem sends

$$a \otimes b \mapsto (a_1 b, \dots, a_n b),$$

where $a_i$ is the embedding of $a$ into $L_i$. We now have a way to calculate norms and traces in terms of completed fields.

**Corollary 5.3:** complete-ntr Keep the same notation as above. Then

1. $\mathrm{Nm}_{L/K}(\alpha) = \prod_{i=1}^n \mathrm{Nm}_{L_i/\hat{K}}(\alpha)$.
2. $\mathrm{Tr}_{L/K}(\alpha) = \prod_{i=1}^n \mathrm{Tr}_{L_i/\hat{K}}(\alpha)$.

*Proof.* Using Proposition 1.2.3(1) and Theorem 5.1, we see

$$\mathrm{Nm}_{L/K}(\alpha) = \prod_{\alpha' \text{ root of } f} \alpha' = \left(\prod_{\alpha' \text{ root of } f_1} \alpha'\right) \cdots \left(\prod_{\alpha' \text{ root of } f_n} \alpha'\right) = \prod_{i=1}^{n} \mathrm{Nm}_{L_i/\hat{K}}(\alpha)$$

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\alpha' \text{ root of } f} \alpha' = \left(\sum_{\alpha' \text{ root of } f_1} \alpha'\right) + \cdots + \left(\sum_{\alpha' \text{ root of } f_n} \alpha'\right) = \sum_{i=1}^{n} \mathrm{Tr}_{L_i/\hat{K}}(\alpha).$$

□

# §6 Product formula

**Lemma 6.1:** compare-normed-val Let $L/K$ be a finite extension of number fields, with normalized nonarchimedean valuations $w \mid v$, as in Example 2.3. Let $|\cdot|'_w$ be $w$ normalized so it extends $v$. Then

$$|\cdot|_w = |\cdot|_w'^{[L_w:K_v]}.$$

*Proof.* Easy, see Milne pg. 132. □

**Theorem 6.2** (Product formula)**:** product-formula For any nonzero $\alpha \in K$,

$$\prod_{v \in V_K} |\alpha|_v = 1.$$

*Proof.*
Step 1: We first show the result for $K = \mathbb{Q}$. Given $n \in \mathbb{Q}$, factor it as $n = \pm \prod_{i=1}^{\infty} p_i^{a_i}$ where $p_i$ are all the prime numbers; note only a finite number of the $a_i$ are nonzero. Then

$$|\alpha| = \left(\prod_{i=1}^{\infty} |\alpha|_{p_i}\right) |a|_\infty = \left(\prod_{i=1}^{\infty} p_i^{-a_i}\right)\left(\prod_{i=1}^{\infty} p_i^{a_i}\right) = 1.$$

Step 2: We pass to field extensions of $\mathbb{Q}$ using the following lemma.

**Lemma 6.3** (Extension formula)**:** extension-formula Let $K \subseteq L$ be number fields and let $v$ be a place of $K$. Then

$$\prod_{w|v} |\alpha|_w = \left|\operatorname{Nm}_{L/K} \alpha\right|_v .$$

*Proof.* For a place on $L$ let $|\cdot|'_w$ be the valuation normalized so that it extends $v$. We have

$$\begin{aligned}
\left|\operatorname{Nm}_{L/K} \alpha\right|_v &= \prod_{w|v} \left|\operatorname{Nm}_{L_w/K_v}(\alpha)\right|_v \\
&= \prod_{w|v} \left|\operatorname{Nm}_{L_w/K_v}(\alpha)\right|'_w \\
&= \prod_{w|v} \left|\operatorname{Nm}_{L_w/K_v}(\alpha)\right|_w^{\frac{1}{[L:K]}} && \text{by Lemma 6.1} \\
&= \prod_{w|v} |\alpha|_w && \text{by Theorem 7.6} \quad \square
\end{aligned}$$

Step 3: Since every place on $K$ restricts to a unique place on $\mathbb{Q}$,

$$\prod_{w \in V_K} |\alpha|_w = \prod_{v \in V} \prod_{w|v} |\alpha|_w = \prod_{v \in V} |\operatorname{Nm}_{L/K}(\alpha)|_v \overset{\text{Step 1}}{=} 1,$$

where we apply step 1 to $\operatorname{Nm}_{L/K}(\alpha)$. $\square$

The product formula will be useful when defining a measure of size independent of scaling (see Chapter **??**).

## §7 Problems

1. Let $K$ be a complete nonarchimedean field whose residue field has characteristic $p$. Prove that the maximal tamely ramified (separable) extension of $K$ is

$$K_{\text{tr}} = K_u\left(\left\{\pi^{\frac{1}{m}} : p \nmid m\right\}\right).$$

# Chapter 9
# Ramification

ramification We seek to generalize the definition of discriminant over Dedekind domains $A$ which are not PID's. To do this we will first define the *different*, which measure how much we can enlarge $B$ so that the image of the trace map is still in $A$, then define the discriminant as the discrepancy between $B$ and the enlarged $B$, using $\chi_A$. We will find that the different is the (ideal) norm of the discriminant.

We will see that our definition coincides with our previous definition when $A$ is a PID. Fortunately, we don't have to prove everything from scratch again: by localization we can always reduce to the DVR/PID case.

The main use of the discriminant is to measure ramification: The primes dividing the discriminant are those that ramify. On a deeper level, the exponents measure the degree of ramification.

## §1 Lattices and $\chi$

**Definition 1.1:** Let $A$ be a Dedekind domain, $K = \text{Frac}(A)$, and $V$ a finite dimensional $K$-vector space. An $A$-submodule $X \subseteq V$ is a **lattice** if it is finitely generated $A$-module and $\text{span}_K(X) = V$.

The most basic example of a latice is a fractional ideal of $K$.

We would like to measure the discrepancy between two lattices—like the norm, but measured by an *ideal* instead. To do this, we first need some facts from commutative algebra.

### 1.1 Filtrations of modules

**Definition 1.2:** A module is **simple** if it is nonzero and has no nonzero proper submodule. A composition series of length $m$ is a chain of submodules

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = 0$$

where $M_{i-1}/M_i$ is simple for each $i$. $M$ has **finite length** if it has a finite composition series.

**Proposition 1.3:** The simple modules are exactly those in the form $R/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal of $R$. If $M$ is simple, $M = R/\mathfrak{m}$ where $\mathfrak{m} = \text{Ann}(M)$.

The main theorem on filtrations is the following.

**Theorem 1.4** (Jordan-Hölder)**:** Suppose $M$ has a composition series.

1. (Existence) Any chain of submodules of $M$ can be refined to a composition series.
2. (Uniqueness) Any composition series of $M$ has the same length; moreover the number of times $R/\mathfrak{m}$ appears as a quotient $M_{i-1}/M_i$ in the filtration is invariant.

We will be applying this when $R$ is a Dedekind domain, so the maximal ideals are simply the nonzero prime ideals.

We also need the following.

**Proposition 1.5:** If $M/M'$ and $M'$ have finite length, then so does $M$.

## 1.2 The function $\chi_A$

**Definition 1.6:** Let $A$ be a Dedekind domain. Define

$$\chi_A : \{A\text{-module of finite length}\} \to \{\text{ideals of } A\}$$

as follows: Given $M$ of finite length, with composition series

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = 0$$

and $A/\mathfrak{p}_i \cong M_{i-1}/M_i$, define

$$\chi_A(M) = \prod_{i=1}^{m} \mathfrak{p}_i.$$

**Example 1.7:** The primes appearing in the filtration of an ideal $\mathfrak{a} \subset A$ are just the primes dividing $\mathfrak{a}$ with multiplicity, so

$$\chi_A(\mathfrak{a}) = (\mathfrak{a}).$$

**Proposition 1.8:** chi-exact If $M'$ and $M''$ have finite length and $0 \to M' \to M \to M'' \to 0$ exact sequence of $A$-modules, then

$$\chi_A(M) = \chi_A(M')\chi_A(M'').$$

**Definition 1.9:** Let $A$ be a Dedekind domain, $K = \mathrm{Frac}(A)$, and $X_1, X_2 \subseteq V$ be $A$-lattices. Choose $X_3 \subseteq X_1 \cap X_2$ any $A$-lattice and define

$$\chi_A(X_1, X_2) := \chi_A(X_1/X_3)\chi_A(X_2/X_3)^{-1}$$

as fractional ideals of $K$.

*Proof of well-definedness.* We show this is independent of choice of $X_3$.

Observe $\chi_A(X_1, X_2)\chi_A(X_2, X_1) = (1)$. Note this is independent of choice of $X_3$. It suffices to show that

$$\chi_A(X_1/X_3)\chi_A(X_2/X_3)^{-1} = \chi_A(X_1/X_4)\chi_A(X_2/X_4)^{-1}$$

when $X_4 \subseteq X_3$. This follows by the exact sequence

$$0 \to X_3/X_4 \to X_1/X_4 \to X_1/X_3.$$

and Proposition 1.8. □

### 1.3 $\chi$ and localization

It is easier to study $\chi_A$ when $A$ is local; in this case $\chi_A(X)$ is simply a power of the maximal ideal. To understand $\chi_A$ (and hence the discriminant) for general $A$, we thus consider the localization of $A$ at all primes. The following says that $\chi_A$ is well-behaved under localization.

**Proposition 1.10:** chi-exponent Let $A$ be a Dedekind domain and $\mathfrak{p} \subset A$ be a nonzero prime. Then

$$v_{\mathfrak{p}}(\chi_A(\chi_1, \chi_2)) = v_{\mathfrak{p}A_{\mathfrak{p}}}(\chi_{A_{\mathfrak{p}}}((X_1)_{\mathfrak{p}}, (X_2)_{\mathfrak{p}})).$$

*Proof.* Note $X_{\mathfrak{p}} = A_{\mathfrak{p}} \cdot X = A_{\mathfrak{p}} \otimes_A X$ is an $A_{\mathfrak{p}}$-lattice of $V$.

Localization is exact, so preserves quotients. Suppose $M \supseteq N$ are adjacent terms in the filtration of $A$. If $M/N = A/\mathfrak{p}$ then

$$M_{\mathfrak{p}}/N_{\mathfrak{p}} = (M/N)_{\mathfrak{p}} = (A/\mathfrak{p})_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$$

while if $M/N = A/\mathfrak{q}$, $\mathfrak{q} \neq \mathfrak{p}$, then $M_{\mathfrak{p}}/N_{\mathfrak{p}} = 0$. Only the quotients with $A/\mathfrak{p}$ remain; the result follows. □

**Proposition 1.11:** Let $A$ be a Dedekind domain with fraction field $K$, $X$ an $A$-lattice in $V$, and $\sigma \in \mathrm{Aut}_K(V)$. Then

$$\chi_A(X, \sigma X) = (\det \sigma).$$

*Proof.* It suffices to check both sides have the same $\mathfrak{p}$-valuation for every prime $\mathfrak{p}$ of $A$; by Proposition 1.10 this is equivalent to

$$\chi_{A_{\mathfrak{p}}}(X_{\mathfrak{p}}, \sigma_{\mathfrak{p}} X_{\mathfrak{p}}) = (\det \sigma_{\mathfrak{p}}).$$

Thus we only need to check the proposition for the case where $A$ is a DVR, hence a PID. For all nonzero $\alpha \in A$,

$$\chi(X, \alpha\sigma X) = \alpha^n \chi(X, \sigma X) = \det[\alpha] \cdot \chi(X, \sigma X);$$

note we used $\chi(uX, \alpha uX) = \alpha^n$ since $X$ is free over $A$, and that the matrix of the transformation $[\alpha]$ is simply $\alpha I$. Thus by choosing $\alpha$ such that $\alpha\sigma X \subseteq X$ we may assume $\sigma(X) \subseteq X$.

By the structure theorem for modules, $X/\sigma X \cong A/\alpha_1 \times \cdots \times A/\alpha_n$ for some $\alpha_j$, giving

$$\chi_A(X, \sigma X) = (\alpha_1 \cdots \alpha_n) = (\det \sigma).$$

$\square$

## 1.4 Discriminant of bilinear forms

In this section we will define the discriminant of a bilinear form $T$ on a lattice $X$ over $K$, the fraction field of a Dedekind domain $A$. When we specialize to the case that $X$ is a extension of $A$ and $T = \mathrm{Tr}$, then we get a generalization of our original definition 1.3.1, in the case where $X$ is not necessarily free over $A$.

**Definition 1.12:** Keep the above assumptions. Let $V$ be a finite-dimensional $K$-vector space and $T : (V, V) \to K$ be a nondegenerate $K$-bilinear form. Thinking of $T$ as a map $V \otimes_K V \to K$, we get a map

$$\wedge^n T : \wedge^n V \otimes_K \wedge^n V \to K$$

defined by

$$wedge-T-def \wedge^n T(v_1 \wedge \cdots \wedge v_n, w_1 \wedge \cdots \wedge w_n) = \sum_{\pi \in S_n} (-1)^{\mathrm{sign}(\pi)} T(v_1 \wedge w_{\pi(1)}) \cdots T(v_n \wedge w_{\pi(n)}). \tag{9.1}$$

Note $\wedge^n T \otimes \wedge^n T$ is a 1-dimensional vector space over $K$, with lattice $\wedge^n X \otimes_K \wedge^n X$. Define the **discriminant** of $T$ on $X$ to be

$$\mathfrak{d}_{X,T} := \chi_A(\wedge^n T, \wedge^n X \otimes \wedge^n X).$$

The main reason for defining the discriminant as above is because the "$\wedge$" construction is natural and makes it easy to prove a few basic properties.

**Proposition 1.13:** chi-det If $X$ is free over $A$ with basis $(e_1, \ldots, e_n)$, then

$$\mathfrak{d}_{X,T} = (\det(T(e_i, e_j))).$$

*Proof.* Note that $X \otimes_K X$ is generated by $\wedge^n T(e_1 \wedge \cdots \wedge e_n, e_1 \wedge \cdots \wedge e_n)$. By (9.1), this is exactly $(\det(T(e_i, e_j)))$. $\square$

We now give an alternative characterization of the discriminant, in terms of the *dual lattice*.

**Definition 1.14:** Define the **dual** of $X$ with respect to $T$ by

$$X_T^* := \{y \in V : T(x, y) \in A \text{ for all } x \in X\}.$$

This is an $A$-lattice of $V$.

We first need the following.

**Proposition 1.15:** dual-basis If $e_1, \ldots, e_n$ is a basis for $X$ over $A$, and $e_1^*, \ldots, e_n^*$ is a *dual basis*, i.e. $T(e_i, e_j^*) = \delta_{ij}$ for each $j$, then $e_1^*, \ldots, e_n^*$ is a basis for $X^*$ over $A$.

*Proof.* Note $y \in X^*$ iff $T(e_j, y) \in A$ for each $j$. Writing $y = \sum_{j=1}^n a_j e_j^*$, we find $T(e_j, y) = a_j$, so $y \in X^*$ iff $a_j \in A$ for each $j$, i.e. $y \in \operatorname{span}_A(e_1^*, \ldots, e_n^*)$. □

**Proposition 1.16:** We have

$$\chi_A(X_T^*, X) = \mathfrak{d}_{X,T}.$$

*Proof.* We use the fact that a fractional ideal is determined by its localizations at all primes (this follows since the exponent of $\mathfrak{p}$ in $\mathfrak{a}$ is the same as that of $\mathfrak{p}A_\mathfrak{p}$ in $\mathfrak{a}A_\mathfrak{p}$, Proposition 2.2.5).

By using Proposition 1.10, we may localize at nonzero $\mathfrak{p} \subset A$. Hence it suffices to prove may assume $A$ is DVR, i.e. free over $A$.

Write

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = B \begin{pmatrix} e_1^* \\ \vdots \\ e_n^* \end{pmatrix}$$

where $B = (b_{i,j})$ is a $n \times n$ matrix. Then by Proposition 1.13,

$$\mathfrak{d}_{X,T} = (\det(T(e_i, e_j))) = (\det(b_{i,j})) = \chi(X_T^*, BX_T^*) = \chi(X_T^*, X),$$

as needed. □

## §2 Discriminant and different

For the AKLB setup with $L/K$ finite separable, consider the nondegenerate $K$-bilinear map

$$\begin{aligned} \operatorname{Tr} : L \times L &\to K \\ (x, y) &\mapsto \operatorname{Tr}_{L/K}(xy). \end{aligned}$$

**Definition 2.1:** Define the **codifferent**

$$B^* := B^*_{\operatorname{Tr}} = \{y \in L : \operatorname{Tr}(xy) \in A \text{ for all } x \in B\}$$

and the **different** and **discriminant** by

$$\begin{aligned} \mathfrak{D}_{B/A} = \mathfrak{D}_{L/K} &:= (B^*)^{-1} \\ \mathfrak{d}_{B/A} = \mathfrak{d}_{L/K} &:= \mathfrak{d}_{B,\operatorname{Tr}}. \end{aligned}$$

(These are fractional ideals of $K$.)

Observe that $B \subseteq B^*$ (in light of $\operatorname{Tr}_{L/K}(B) \subseteq A$) so $B \supseteq \mathfrak{d}_{B/A}$.

The following gives the precise relationship between the discriminant and different.

**Proposition 2.2:** $\mathrm{Nm}_{L/K}(\mathfrak{D}_{B/A}) = \mathfrak{d}_{B/A}$.

*Proof.* We have

$$\mathfrak{d}_{B/A} = \chi_A(B^*, B) = \chi_A(B^*/B)$$

and

$$\mathfrak{D}_{B/A} = (B^*)^{-1} = \chi_B(B^*/B).$$

The result thus follows from commutativity of the following diagram.

$$\begin{tikzcd}
\{\text{finite length } B\text{-module}\} \arrow[r, "\chi_B"] \arrow[dr, "\chi_A"'] & I_B \arrow[d, "\mathrm{Nm}_{L/K}"] \\
& I_K.
\end{tikzcd}$$

We have commutativity since if $B/\mathfrak{P}$ is a quotient of adjacent terms in the $B$-filtration of $M$, then when we refine it to a $A$-filtration, since $B/\mathfrak{P} = (A/\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}$ as vector spaces, we get $f(\mathfrak{P}/\mathfrak{p})$ copies of $A/\mathfrak{p}$. □

Note: Grothendieck group.

## 2.1 Basic properties

First, a slightly cleaner characterization of the codifferent.

**Lemma 2.3:** codiff-lem $\mathfrak{a} \in I_K$ and $\mathfrak{b} \in I_L$. Then

$$\mathrm{Tr}_{L/K}(\mathfrak{b}) \subseteq \mathfrak{a} \iff \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{D}_{B/A}^{-1}.$$

*Proof.* We check $\mathrm{Tr}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq A$ iff $\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{D}_{L/K}^{-1}$.

The reverse direction is clear. For the forward direction, note that if $x \in \mathfrak{a}^{-1}\mathfrak{b}$ and $y \in B$, then $xy \in \mathfrak{a}^{-1}\mathfrak{b}$ and hence $\mathrm{Tr}(xy) \in A$. This shows $x \in \mathfrak{D}_{B/A}^{-1}$. □

**Proposition 2.4:**

1. (Transitivity) Let $M/L$ be a finite separable extension, with $C$ the integral closure of $A$ in $M$. Then
$$\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}.$$
2. (Localization) For $S \subseteq A$ a multiplicative subset,
$$S^{-1}\mathfrak{D}_{B/A} = \mathfrak{D}_{S^{-1}B/S^{-1}A}.$$
3. (Completion)
$$\mathfrak{D}_{B/A} \cdot \hat{B}_{\mathfrak{P}} = \mathfrak{D}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}}.$$

*Proof.* 1. We have

$$\begin{aligned}
&e \in \mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1} \\
\iff &\mathfrak{D}_{B/A} e \subseteq \mathfrak{D}_{C/B}^{-1} \\
\iff &\mathrm{Tr}_{M/L}(\mathfrak{D}_{B/A} e) \subseteq B && \text{Lemma 2.3 with } M/L \\
\iff &\mathfrak{D}_{B/A}\mathrm{Tr}_{M/L}(e) \subseteq B \\
\iff &\mathrm{Tr}_{M/L}(e) \in \mathfrak{D}_{B/A}^{-1} \\
\iff &\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(e)) \subseteq A && \text{Lemma 2.3 with } L/K \\
\iff &e \in \mathfrak{D}_{C/A}^{-1}.
\end{aligned}$$

2. Omit.

3. Localize at $\mathfrak{p}$. May assume $A$ is a DVR. ($B$ may not be a DVR.) Consider

$$\begin{tikzcd}
\prod_{\mathfrak{P}|\mathfrak{p}} \hat{B}_{\mathfrak{P}} \arrow[r, hook] \arrow[d, "\cong"] & \prod_{\mathfrak{P}|\mathfrak{p}} \hat{L}_{\mathfrak{P}} \arrow[d, "\cong"] \\
B \otimes_A \hat{A}_{\mathfrak{p}} \arrow[r, hook] \arrow[d, dash] & L \otimes_K \hat{K}_{\mathfrak{p}} \arrow[d, "\mathrm{Tr}_{L/K} \otimes_K \hat{K}_{\mathfrak{p}}"] \\
\hat{A}_{\mathfrak{p}} \arrow[r, hook] & \hat{K}_{\mathfrak{p}}
\end{tikzcd}$$

The top-to-bottom map on the right is $\sum \mathrm{Tr}_{\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{p}}}$. Then

$$\begin{aligned}
\mathfrak{d}_{B/A}^{-1} \otimes_A \hat{A}_{\mathfrak{p}} &\cong \mathfrak{D}^{-1}_{B\otimes_A \hat{A}_{\mathfrak{p}}/\hat{A}_{\mathfrak{p}}} \\
&\cong \mathfrak{D}^{-1}_{\prod_{\mathfrak{P}|\mathfrak{p}} \hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}} \\
&\cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{D}^{-1}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}} \\
&\cong \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{d}^{-1}_{B/A} \otimes_B \hat{B}_{\mathfrak{P}}
\end{aligned}$$

□

# §3 Discriminant and ramification

Recall $\mathrm{ord}_{\hat{\mathfrak{P}}}(\mathfrak{D}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}} = \mathrm{ord}_{\mathfrak{P}}(\mathfrak{d}_{B/A})$. Our goal is to show that $e_{\mathfrak{P}/\mathfrak{p}} = 1$ and $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separable (i.e. $\mathfrak{P}$ is unramified over $K$, iff $\mathfrak{P} \nmid \mathfrak{d}_{B/A}$.

In the CDVR case,

$$\begin{tikzcd}
\mathfrak{P} \arrow[r, hook] \arrow[d, dash] & B \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash] \\
\mathfrak{p} \arrow[r, hook] & A \arrow[r, dash] & K
\end{tikzcd}$$

we have $B/\mathfrak{p}B = B/\mathfrak{P}^e$.

**Lemma 3.1:**

$$\mathrm{Tr}_{L/K}(b) \bmod p = e\mathrm{Tr}_{l/k}(\bar{b}).$$

*Proof.* For all $b \in B$,

$$0 = \mathfrak{P}^e/\mathfrak{P}^e \subseteq \mathfrak{P}^{e-1}/\mathfrak{P}^e \subseteq \cdots \subseteq \mathfrak{P}/\mathfrak{P}^e \subseteq B/\mathfrak{P}^e.$$

Each adjacent quotient is 1 dimensional over $l$ and hence $f$-dimensional over $k$. Choose a basis $\{\overline{w}_i\}_{i=1}^n$ $(n = ef)$ for $B/\mathfrak{P}^e$ as $k$-vector space, such that

$$\mathrm{span}_k(\{w_i\}_{i=(e-j)f+1}^{ef}) = \mathfrak{P}^{e-j}/\mathfrak{P}^e.$$

(The last $jf$ vectors span $\mathfrak{P}^{e-j}/\mathfrak{P}^e$.) Lift $\{\overline{w}_i\}$ to $w_i \in B$ such that $w_i \bmod \mathfrak{P}^e = \overline{w}_i$. The $w_i$ are a basis of $B$ over $A$. Now

$$\begin{aligned} \mathrm{Tr}_{L/K}(b) &= \mathrm{Tr}_K(m_b) \\ bw_i &= (b_{i,j})(w_j)_{j=1}^n \\ \bar{b}\overline{w}_i &= (\bar{b}_{i,j})(\overline{w}_j). \end{aligned}$$

We have

$$\mathrm{Tr}_{L/K}(b) = \sum_{i=1}^n b_{ii} \bmod \mathfrak{p}.$$

Now $(b_{i,j} \bmod \mathfrak{p})_{fk+1 \le i,j \le f(k+1)}$ represents the linear map (multiplication by $\bar{b}$)

$$\frac{\mathfrak{P}^k/\mathfrak{P}^e}{\mathfrak{P}^{k+1}/\mathfrak{P}^e} \to \frac{\mathfrak{P}^k/\mathfrak{P}^e}{\mathfrak{P}^{k+1}/\mathfrak{P}^e}.$$

The trace as a $k$-linear map is $\mathrm{Tr}_{l/k}(\bar{b})$. There are $e$ such $f \times f$ blocks. □

**Corollary 3.2:**

$$\mathrm{ord}_{\mathfrak{P}}(\mathfrak{d}_{B/A}) \ge e - 1.$$

*Proof.* It suffices to show

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}_{B/A}) \ge (e-1)f.$$

This is since $\mathfrak{D}_{B/A} = \mathfrak{P}^c$ implies $\mathfrak{d}_{B/A} = \mathrm{Nm}_{L/K}(\mathfrak{P}^c) = \mathfrak{P}^{cf}$.

Now

$$\mathfrak{d}_{B/A} = (\det \mathrm{Tr}_{L/K}(w_i w_j))$$

same as in the previous proof. Now $w_i \in \mathfrak{P}$ if $f+1 \le i \le n = ef$, therefore $\overline{w}_i \in \mathfrak{P}/\mathfrak{P}^e$. For all $j$, $\mathrm{Tr}_{L/K}(w_i w_j) \in \mathfrak{P} \cap K = \mathfrak{p}$, giving the result. □

Now consider the general case.

**Theorem 3.3:** Suppose $A, B$ are Dedekind. Then

1. $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{D}_{B/A}) \geq e_{\mathfrak{P}/\mathfrak{p}} - 1$.
2. $\mathfrak{P}$ is unramified over $K$ iff $\mathfrak{P} \nmid \mathfrak{D}_{L/K}$.

Serre does this by Eisenstein polys.

*Proof.* 1. $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{D}_{B/A}) = \mathrm{ord}_{\hat{\mathfrak{P}}}(\mathfrak{D}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}})$. and $e_{\mathfrak{P}/\mathfrak{p}} = e_{\hat{\mathfrak{P}}/\hat{\mathfrak{p}}}$. Use the CDVR case.

2. For "$\Leftarrow$", note $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{D}_{L/K})$ implies $0 \geq e_{\mathfrak{P}/\mathfrak{p}} - 1$ i.e. $e_{\mathfrak{P}/\mathfrak{p}} = 1$.
   For "$\implies$", it suffices to prove $p \nmid \mathfrak{d}_{B/A}$. Reduce to the CDVR case. Now
   $$\det(\mathrm{Tr}_{L/K}(w_i w_j)) \bmod \mathfrak{p} = e_{\mathfrak{P}/\mathfrak{p}} \mathrm{Tr}_{l/k}(\overline{w_i w_j}) \neq 0$$
   if $l/k$ is separable (Neukirch I.2).

□

## 3.1 Types of ramification

**Definition 3.4:** $\mathfrak{P}$ is unramified if $e_{\mathfrak{P}/\mathfrak{p}}$ and $l/k$ separable. For $\mathfrak{P}$ ramified,

1. $\mathfrak{P}$ is **tamely ramified** if either $\mathrm{char}\, k = 0$ or $\mathrm{char}\, k \nmid e_{\mathfrak{P}/\mathfrak{p}}$.
2. $\mathfrak{P}$ is **wildly ramified** otherwise.

**Theorem 3.5:** $\mathfrak{P}$ is tamely ramified over $K$ iff

$$\mathrm{ord}_{\mathfrak{P}}(\mathfrak{d}_{L/K}) = e_{\mathfrak{P}/\mathfrak{p}} - 1.$$

*Proof.* Reduce to the CDVR case.

Step 1: We show that $\mathfrak{P}$ is tamely ramified iff $\mathrm{Tr}_{L/K}(B) = A$. Observe that $\mathrm{Tr}_{L/K}(B)$ is an ideal of $A$, so the latter is equivalent to $\mathrm{Tr}_{L/K}(B) \pmod{\mathfrak{p}} \neq 0$. But we know

$$\mathrm{Tr}_{L/K}(b) \bmod \mathfrak{p} = e_{\mathfrak{P}/\mathfrak{p}} \mathrm{Tr}_{l/k}(\bar{b}),$$

and $\mathrm{Tr}_{l/k}(\bar{b}) \neq 0$ (not identically 0). Hence $e_{\mathfrak{P}/\mathfrak{p}} \not\equiv 0 \pmod{\mathfrak{p}}$ iff $\mathrm{Tr}_{L/K}(b) \not\equiv 0 \pmod{\mathfrak{p}}$.

Step 2: $\mathrm{Tr}_{L/K}(B) = A \iff \mathrm{ord}_{\mathfrak{P}}(\mathfrak{D}_{L/K}) = e_{\mathfrak{P}/\mathfrak{p}} - 1$.
We've seen

$$\mathrm{Tr}_{L/K}(\mathfrak{b}) \subseteq \mathfrak{a} \iff \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{D}_{B/A}^{-1}.$$

Plug in $\mathfrak{b} = B$ to get, as ideals of $B$,

$$\begin{aligned} A' := \mathrm{Tr}(B) \subseteq \mathfrak{a} &\iff B \subseteq \mathfrak{a}\mathfrak{D}_{L/K}^{-1} \\ &\iff \mathfrak{D}_{L/K} \subseteq \mathfrak{a}B \end{aligned}$$

Write $A' = \mathfrak{p}^a$. We have $\mathfrak{p}^a \mid \mathfrak{D}$ iff $\mathfrak{p}^a \mid A'$ for $a \in \mathbb{Z}$. (Power can be rational.)

For $a \in \mathbb{Z}$, $\operatorname{ord}_{\mathfrak{p}}(A') \ge a$ iff $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{D}) \ge a$.

Thus we get

$$\operatorname{ord}_{\mathfrak{p}}(A') \le \underbrace{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{D}_{L/K})}_{\frac{\operatorname{ord}_{\mathfrak{P}}(\mathfrak{D})}{e_{\mathfrak{P}/\mathfrak{p}}}} < \operatorname{ord}_{\mathfrak{p}}(A') + 1.$$

Thus $\operatorname{Tr}_{L/K}(B) = A$ iff $a = 0$ iff $\operatorname{ord}_{\mathfrak{P}}(\mathfrak{D}) = e - 1$.

Thus $\mathfrak{P}$ is tamely ramified iff $v(\mathfrak{D}) = e - 1$. □

## 3.2 Computation of different

**Proposition 3.6:** monogenous When $A$ and $B$ are CDVR's, $B$ is generated by one element over $A$ as an $A$-algebra:

$$B = A[\beta].$$

(We say that $B$ is *monogenous* over $A$.)

Let $L := \operatorname{Frac}(A)$, $K := \operatorname{Frac}(B)$. When $L/K$ is totally ramified, then we can choose $\beta$ to be any uniformizer $\pi_L$.

*Proof.* Any element of $B$ can be written as $\sum_{k\ge 0} a_k \pi_k$ where $a_k$ are fixed representatives of $l = B/(\pi_L)$. But we can choose the $a_k$ to be representatives of $k = A/(\pi_K)$, since $k = l$. □

**Theorem 3.7:** (Residue field extension separable.) $\mathfrak{d}_{B/A} = (f'_\beta(\beta))$ where $f_\beta(x) \in A[x]$ is the minimal polynomial of $\beta$ over $K$.

*Proof.*

**Lemma 3.8:**

$$\operatorname{Tr}_{L/K}\left(\frac{\beta^k}{f'(\beta)}\right) = \begin{cases} 0, & 0 \le i \le n-2 \\ 1, & i = n-1. \end{cases}$$

*Proof.* The eigenvalues of multiplication by $\beta$ are just the roots $\beta_1, \ldots, \beta_n$ of the characteristic polynomial. Note that if $A$ is a linear operator with eigenvalues $\lambda_i$ and $P$ is a polynomial then $P(A)$ has eigenvalues $P(\lambda_i)$. Hence

$$\operatorname{tr}\left(\frac{\beta^k}{f'(\beta)}\right) = \sum_{i=1}^n \frac{\beta_i^k}{f'(\beta_i)}$$

Let $D(x_1, \ldots, x_n) = \sum_{i<j}(x_i - x_j)$. Noting $f'(\beta_i) = \prod_{j\ne i}(\beta_i - \beta_j)$, the above equals

$$\frac{1}{D(x_1, \ldots, x_n)} \underbrace{\sum_{i=1}^n \frac{x_i^k D(x_1, \ldots, x_n)}{\prod_{j\ne i}(x_i - x_j)}}_{P(x_1, \ldots, x_n)}$$

evaluated at $(x_1, \dots, x_n) = (\beta_1, \dots, \beta_n)$. Consider $P$. Note $P$ is zero whenever $x_i = x_j$ for some $i \neq j$ (All except two terms are 0; those two cancel.). So $x_i - x_j \mid P$, and $D \mid P$. However, $P$ has degree less than $\frac{(n-1)n}{2}$ when $k < n-1$, so must be 0. If $k = n-1$ then we know $P$ is a constant multiple of $D$, look at the coefficient of any term to see that in fact $P = D$. $\square$

It suffices to prove

$$(f'_\beta(\beta)^{-1}) = B^* := \left\{ b \in L : \mathrm{Tr}_{L/K}(bb') \in A \text{ for all } b' \in B \right\}.$$

The condition inside is equivalent to

$$\mathrm{Tr}(b\beta^j) \in A, \quad 0 \le j \le n-1.$$

(because $B = \bigoplus A\beta^i$.) But by the lemma,

$$\mathrm{Tr}\left( \sum_{i=0}^{n-1} a_i \frac{\beta^{i+j}}{f'(\beta)} \right) = a_{n-1-j} + \cdots (>).$$

"Triangular." Therefore

$$B^* = \bigoplus A \cdot \frac{\beta^i}{f'_\beta(\beta)} = \left( \frac{1}{f'_\beta(\beta)} \right).$$

$\square$

Good exercise: Compute $\mathfrak{D}_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}$. This is tamely ramified only at $n = 1$. Totally ramified tower. The first step is $(\mathbb{Z}/p)^\times$, tame, everything else is $p$, wild.

(Note $G(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ because $D_p \cong G(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$.

# §4 Ramification groups

Local, CDVR setup.

**Definition 4.1:** Let $i \ge -1$. The $i$th **ramification group** is

$$\begin{aligned} G_i &= \{\sigma \in G : b \in \mathcal{O}_L,\, v_L(\sigma(b) - b) \ge i+1\} \\ &= \{\sigma \in G : v_L(\sigma(\beta) - \beta) \ge i+1\}. \end{aligned}$$

Observe $G_{-1} = G$, that $G_i \supseteq G_j$ for $i \le j$ and $\bigcap_{i \ge -1} G_i = \{1\}$. Also note for all $i$, $G_i$ is a normal subgroup of $G$ because

$$G_i = \ker(G \to \mathrm{Aut}(\mathcal{O}_L/(\pi_L^{i+1})).$$

In particular, $G_i/G_{i+1}$ is a group. Furthermore $G_i$ is defined even when $i$ is not an integer; we have $G_i = G_{\lceil i \rceil}$.

We will study $\{G_i\}_{i \ge -1}$. We want

1. A formula for $v_L(\mathfrak{D}_{L/K})$. If at most tame, equals $e-1$, else greater.
2. Look at quotients $G_i/G_{i+1}$. Abelian, cyclic, $p$-group, prime-to-$p$?

## 4.1 $\mathfrak{D}_{L/K}$ and $i_G$

**Definition 4.2:** Let $\sigma \in G(L/K)$. Define $i_G : G \to \mathbb{N}_0 \cup \{\infty\}$ by

$$i_G(\sigma) = \min\{v_L(\sigma(\beta) - \beta) : \beta \in B\}.$$

Note that if $B = A[\beta]$, then

$$i_G(\sigma) = v_L(\sigma(\beta) - \beta).$$

Observe

- $i_G(\sigma) = \infty$ iff $\sigma = 1$.
- $G_i = \{\sigma \in G : i_G(\sigma) \geq i+1\}$, so $\sigma \in G_i$ iff $i_G(\sigma) \geq i+1$, so doesn't depend on choice of generator.

Note

$$i_G(\tau\sigma\tau^{-1}) = i_G(\sigma), \quad \sigma, \tau \in G.$$

Because $G_i \trianglelefteq G$. Note

$$i_G(\sigma\tau) \geq \min(i_G(\sigma), i_G(\tau)).$$

Because

$$\begin{aligned} i_G(\sigma\tau) &= v_L(\sigma\tau\beta - \beta) \\ &\geq \min(v_L(\sigma\tau(\beta) - \tau(\beta)), v_L(\tau(\beta) - \beta)) \\ &= \min(i_G(\sigma), i_G(\tau)). \end{aligned}$$

since $\mathcal{O}_L = \mathcal{O}_K[\beta] = \mathcal{O}_K[\tau\beta]$.

**Proposition 4.3:**

$$v(\mathfrak{D}_{L/K}) = \sum_{\sigma \neq 1} i_G(\sigma) = \sum_{i \geq 0} (|G_i| - 1).$$

$(\mathfrak{a} = (\pi_L^i) \implies v_L(a) = i.)$

*Proof.* Let $f(x)$ be the minimal polynomial for $\beta$. Letting $n = [L : K]$,

$$f(x) = \prod_{i=1}^{n} (X - \beta_i).$$

Now

$$\begin{aligned} \mathfrak{D}_{L/K} &= (f'(\beta)) \\ &= \prod_{i>1} (\beta - \beta_i) \\ &= \prod_{\sigma \neq 1} (\beta - \sigma(\beta)). \end{aligned}$$

Take $v_L$ for (1).

$$v_L(\mathfrak{D}_{L/K}) = \sum_{\sigma\neq 1} \underbrace{v_L(\beta - \sigma(\beta))}_{i_G(\sigma)}.$$

For (2), consider multiset

$$\bigsqcup_{i\geq 0}(G_i\backslash\{1\}).$$

finite. Note $\sigma \in G$ appears in $G_0, G_1, \ldots, G_{i_G(\sigma)-1}$, there's $i_G(\sigma)$. Compute the size of the multiset in two different ways

$$\sum_{i\geq 0}(|G_i| - 1) = \sum_{\sigma\neq 1} i_G(\sigma).$$

□

Remark: $v_L(\mathfrak{D}_{L/K}) = e - 1$ iff $G_1 = \{1\}$ (because $|G_0| = e$, iff $L/K$ is at most tame.
Let's understand $\mathfrak{D}_{L/K}$, $i_G$ under sub and quotient group. Consider $L/L^H/K$.
First, sub.

**Proposition 4.4:** ram-grp-sub

$$\begin{aligned} i_H(\sigma) &= i_G(\sigma) \text{ for all } \sigma \in H \\ H_i &= H \cap G_i. \end{aligned}$$

*Proof.* Same generator works for larger ring. $\mathcal{O}_L = \mathcal{O}_K[\beta] \implies \mathcal{O}_L = \mathcal{O}_{K'}[\beta]$. Then true by def. □

**Corollary 4.5:**

$$v_L(\mathfrak{D}_{L/K'}) = \sum_{\sigma\neq 1, \sigma\in H} \underbrace{i_G(\sigma)}_{i_H(\sigma)}.$$

For quotient.

**Proposition 4.6:** igh-ig For $H \trianglelefteq G$, $\overline{G} \neq 1 \in G/H$,

$$i_{G/H}(\overline{\sigma}) = \frac{1}{e_{L/K'}} \sum_{\sigma\in G,\, \sigma \bmod H = \overline{\sigma}} i_G(\sigma).$$

**Corollary 4.7:**

$$v_{K'/K}(\mathfrak{D}_{K'/K}) = \frac{1}{e'_{L/K}} \sum_{\sigma\notin H, \sigma\in G} i_G(\sigma).$$

Because by prev. $\sum_{\overline{\sigma}\neq 1} i_{G/H}(\overline{\sigma})$ equals RHS by prop.

*Proof.* Choose $\alpha \in \mathcal{O}_{K'}$ and $\beta \in \mathcal{O}_L$ such that $\mathcal{O}_{K'} = \mathcal{O}_K[\alpha']$ and $\mathcal{O}_L = \mathcal{O}_K[\beta]$. Then

$$\begin{aligned} e_{L/K'} i_{G/H}(\overline{\sigma}) &= e_{L/K'} v_{K'}(\overline{\sigma}\alpha' - \alpha') \\ &= v_L(\overline{\sigma}\alpha' - \alpha'). \\ \sum_{\sigma \in G} &= i_G(\sigma) \\ &= \sum_{\tau \in H} \underbrace{i_G(\sigma\tau)}_{v_L(\sigma\tau\beta - \beta)} \\ &= v_L\left(\prod_{\tau \in H} (\sigma\tau(\beta) - \beta)\right) = before. \end{aligned}$$

fixing $\sigma$.

It suffices to prove $(\sigma\overline{\alpha'} - \alpha') = \prod_{\tau \in H}(\sigma\tau(\beta) - \beta)$. Call LHS, RHS $\mathfrak{a}, \mathfrak{b}$.

1. $\mathfrak{a} \mid \mathfrak{b}$: Consider
$$g(X) = \prod_{\tau \in H} (X - \tau(\beta)) \in \mathcal{O}_{K'}[x].$$
minimal polynomial of $\beta/K'$.
$$\sigma g(X) = \prod_{\tau \in H} (X - \sigma\tau(\beta)).$$
Observe $\sigma\alpha' - \alpha'$ divides coefficients of $\sigma g(X) - g(X)$. Because for all $a \in \mathcal{O}_{K'}$, $a = a_0 + a_1\alpha'$, $\sigma\alpha = a_0 + a_1\sigma\alpha' + \cdots$. Note $\sigma\alpha' - \alpha' \mid \sigma\alpha'^i - \alpha'^i$. Note $g(\beta) = 0$. Take $x = \beta$ to get
$$\sigma\alpha' - \alpha' \mid \sigma g(\beta) - \underbrace{g(\beta)}_{0}.$$

2. $\mathfrak{b} \mid \mathfrak{a}$. SWITCH $f$ and $g$ below. Cook up a minimal polynomial to show divisibility. $\alpha' = \mathcal{O}_K[\beta] = \mathcal{O}_L$. Write
$$\alpha' = \sum_{i=0}^{n-1} a_i \beta^i =: g(\beta).$$
$a_i \in \mathcal{O}_K$. $g(X) \in \mathcal{O}_K[X]$. Consider $g(X) - \alpha' \in \mathcal{O}_{K'}[X]$. By construction has $\beta$ as a root.

   Hence plugging in $x = \beta$,
$$\begin{aligned} f(X) &\mid g(X) - \alpha \\ \sigma f(X) &\mid \sigma(f(X)) - \sigma(\alpha') \\ \sigma f(\beta) &\mid f(\beta) - \sigma(\alpha') \end{aligned}$$
giving $\pm b \mid \pm a$.

□

End of unedited stuff.

## 4.2 Filtration of ramification groups

sec:ram-filt We know from (??) that

$$G_{-1}/G_0 \cong G/I_{L/K} \cong G(l/k).$$

In particular, if $k$ is finite then $G_{-1}/G_0$ is finite cyclic and if $k = \overline{k}$ then $G_{-1}/G_0$ is trivial. From now on assume $i \geq 0$.

We aim to study the filtration

$$ramification-filtration-eq G \supseteq G_0 \supseteq G_1 \supseteq \cdots. \tag{9.2}$$

To do this, we first study the filtration

$$units-filtration-eq L^\times \supseteq U_L^0 \supseteq U_L^1 \supseteq \cdots \tag{9.3}$$

where

$$U_L^i = \begin{cases} \mathcal{O}_L^\times, & i = 0 \\ 1 + \pi_L^i \mathcal{O}_L, & i \geq 1. \end{cases}$$

The quotient groups in (9.3) can be understood explicitly (Proposition 4.8). We will relate the two filtrations by Proposition 4.10.[1] From this we get several important corollaries about the structure of the groups $G_s$. Understanding conjugates and commutators of elements in the $G_s$ gives us several more important properties.

**Proposition 4.8:** units-filtration Let $K$ be a complete field with discrete valuation (for instance, a local field), $k$ its residue field, and $\mathfrak{m}$ the associated maximal ideal. Then we have isomorphisms

$$\begin{aligned} U_K/U_K^{(1)} &\xrightarrow{\cong} k^\times \\ u &\mapsto u \pmod{\mathfrak{m}} \end{aligned} \qquad\qquad \begin{aligned} U_K^{(m)}/U_K^{(m+1)} &\xrightarrow{\cong} k^+ \\ 1 + a\pi^m &\mapsto a \pmod{\mathfrak{m}}. \end{aligned}$$

*Proof.* For the first just note that $1 + \mathfrak{m}$ is the multiplicative unit of $A/\mathfrak{m}$. For the second, note $(1 + a\pi^m)(1 + b\pi^m) = 1 + (a + b)\pi^m + \cdots$. $\square$

To construct a map $G_i/G_{i+1} \to U_L^i/U_L^{i+1}$, we first need the following characterization of $G_i$.

**Lemma 4.9:** gi-quotient-crit Suppose $L/K$ is a finite Galois extension of local fields, $\pi$ is a uniformizer of $L$, and $G = G(L/K)$. For $i \in \mathbb{N}_0$ and $\sigma \in G_0$,

$$gi-quotient-crit-eq \sigma \in G_i \iff \frac{\sigma(\pi)}{\pi} \equiv 1 \pmod{\pi_L^i}. \tag{9.4}$$

[1] This will be important in local class field theory, which says there is a canonical isomorphism $K^\times/\mathrm{Nm}_{L/K}(L^\times) \cong G(L/K)$ if $L/K$ is finite abelian.

*Proof.* The RHS is equivalent to

$$gi-quotient-crit1 \sigma(\pi)-\pi \equiv 0 \pmod{\pi_L^{i+1}}. \tag{9.5}$$

We need to show this is equivalent to

$$gi-quotient-crit2 \sigma(\beta)-\beta \equiv 0 \pmod{\pi_L^{i+1}} \text{ for all } \beta \in L. \tag{9.6}$$

It is clear that (9.6) implies (9.5).

First suppose $L/K$ is totally ramified. Then $\mathcal{O}_L = \mathcal{O}_K[\pi]$ by Proposition 3.6, giving that (9.5) implies (9.6).

Now consider the general case. We know $L/L^{I_{L/K}}$ is totally ramified (Theorem 2.7.2), so the theorem holds for $L/L^{I_{L/K}}$. Now, by Proposition 4.4, $G_i(L/L^{I_{L/K}}) = G_i \cap I_{L/K} = G_i$. Furthermore, since $\pi_L$ is the same for $L/K$ and $L/L^{I_{L/K}}$, the right hand-side of (9.4) does not change whether we are talking about $L/K$ or $L/L^{I_{L/K}}$. Hence the theorem for $L/L^{I_{L/K}}$ implies the theorem for $L/K$. $\square$

**Proposition 4.10:** ramification-to-unit-group There is a well-defined injective group homomorphism

$$\begin{aligned} \theta_i : G_i/G_{i+1} &\hookrightarrow U_L^i/U_L^{i+1} \\ \sigma &\mapsto \frac{\sigma(\pi)}{\pi} \end{aligned}$$

that is independent of the choice of uniformizer $\pi$.

*Proof.* Note that

$$ram-unit1 u \in \mathcal{O}_L,\, \sigma \in G_i \implies \sigma(u) \equiv u \pmod{\pi^{i+1}} \implies \frac{\sigma(u)}{u} \in U_L^{i+1}. \tag{9.7}$$

First we show $\theta_i$ is a group homomorphism $G_i \to U_L^i/U_L^{i+1}$. We have

$$\frac{\sigma\tau(\pi)}{\pi} = \frac{\sigma(\pi)}{\pi} \cdot \frac{\tau(\pi)}{\pi} \cdot \frac{\sigma\left(\frac{\tau(\pi)}{\pi}\right)}{\frac{\tau(\pi)}{\pi}}.$$

Since $\frac{\tau(\pi)}{\pi} \in \mathcal{O}_L$ and $\tau \in G_i$, (9.7) gives $\frac{\sigma\left(\frac{\tau(\pi)}{\pi}\right)}{\frac{\tau(\pi)}{\pi}} \in U_L^{i+1}$.

Lemma 4.9 gives that the kernel is exactly $G_{i+1}$, so $\theta_i$ induces an injective map $G_i/G_{i+1} \to U_L^i/U_L^{i+1}$.

Now suppose $\pi'$ is another uniformizer. Write $\pi' = u\pi$ with $u \in \mathcal{O}_L^\times$. Then $\sigma \in G_i$ and (4.9) give

$$\frac{\sigma(\pi')}{\pi'} = \frac{\sigma(\pi)}{\pi} \cdot \underbrace{\frac{\sigma(u)}{u}}_{\in U_L^{i+1}}.$$

$\square$

**Corollary 4.11:** 1. $G_0/G_1$ is finite cyclic.

2. If $\mathrm{char}(l) = 0$ then $G_1 = \{1\}$; if $\mathrm{char}(l) = p \neq 0$, then for each $i \geq 1$,

$$G_i/G_{i+1} = (\mathbb{Z}/p\mathbb{Z})^{n_i}$$

for some $n_i$.

*Proof.* 1. Proposition 4.10 and 4.8 give $G_0/G_1 \hookrightarrow U_L/U_L^1 \cong l^\times$. But any finite subgroup of a finite field must be cyclic.

2. For $\mathrm{char}(l) = 0$, $l^+$ has no finite nontrivial subgroup. For $\mathrm{char}(l) = p$, we have $G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1} \cong l^+$. Just note $l^+$ is a an abelian $p$-group. □

**Corollary 4.12:** cor:G(local)=solvable $G_0 = I_{L/K}$ is solvable. If $G(l/k) = G_{-1}/G_0$ is solvable (in particular, if $k$ is finite) then $G$ is solvable.

*Proof.* The series

$$G_0 \supseteq G_1 \supseteq \cdots$$

is a solvable series for $G$. □

## 4.3 First ramification group

Recall that we defined $G_0 = I_{L/K}$ so that we can split $L/K$ into two parts: $L/L^{I_{L/K}}$ is totally ramified while $L^{I_{L/K}}/L$ is unramified. We can further split the extension $L/L^{I_{L/K}}$ into a wildly ramified and tamely ramified part.

**Definition 4.13:** Define the **wild inertia group** and **tame inertia group** to be

$$\begin{aligned} G_1 &= I_{L/K}^{\text{wild}} \\ G_0/G_1 &= I_{L/K}^{\text{tame}}. \end{aligned}$$

**Theorem 4.14:** The extension $L/L^{I_{L/K}^{\text{wild}}}$ is wildly ramified with Galois group $G_1 = I_{L/K}^{\text{wild}}$ and the extension $L^{I_{L/K}^{\text{wild}}}/L^{I_{L/K}^{\text{tame}}}$ is tamely ramified with Galois group $G_1/G_0$.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{wild ramification}"', "I_{L/K}^{\text{wild}}"] \\
L^{I_{L/K}^{\text{wild}}} \arrow[d, dash, "\text{tame ramification}"', "I_{L/K}^{\text{tame}}"] \\
L^{I_{L/K}} \arrow[d, dash, "\text{unramified}"', "G/I_{L/K}=G(l/k)"] \\
K
\end{tikzcd}$$

Moreover, $G_1$ is the unique p-Sylow subgroup of $G_0$, and

$$G_0 = G_1 \rtimes G_0/G_1.$$

*Proof.* Note $G_0/G_1 \hookrightarrow k^\times$ while $G_j/G_{j+1} \hookrightarrow k^+$ for $j \ge 1$; we have $p \nmid |k^\times|$ while $|k|$ is a power of $p$; and $|G_1| = \prod_{1 \le j \ll \infty} |G_j/G_{j+1}|$. Hence $G_1$ is a p-SSG of $G_0$; it is unique since it is normal and all $p$-SSGs are conjugate. Since the indices of the field extensions are the orders of the Galois groups, the result on tame and wild ramification follow.

Now we prove the semidirect product. This follows directly from the Schur-Zassenhaus Lemma: If $H$ is a normal Hall subgroup of a finite group $G$, then $H$ has a complement, and hence $G = H \rtimes G/H$. (A Hall subgroup $H \subseteq G$ is a group such that $\gcd(|H|, [G : H]) = 1$.)

The following is an alternate proof. We show the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & G_1 \arrow[r] \arrow[d, equal] & G_0 \arrow[r] \arrow[d, equal] & G_0/G_1 \arrow[r] \arrow[d, equal] & 1 \\ & I_{L/K}^{\mathrm{wild}} & I_{L/K} & I_{L/K}^{\mathrm{tame}} & \end{tikzcd}$$

splits by showing there exists a right inverse $G_0/G_1 \to G_0$ of the projection $G_0 \to G_1$.[2] Since $G_0/G_1$ is cyclic of order $r := |l^\times|$, it suffices to find a lift $\sigma \in G_0$ of the generator $\overline{\sigma} \in G_0/G_1$ with order $r$. Write $|G_0| = p^s r$. Let

$$\sigma = \sigma'^{p^{\varphi(r)t}}$$

where $t$ is such that $\varphi(r)t \ge s$. Note $r \nmid p$ implies $p^{\varphi(r)t} \equiv 1 \pmod{r}$. Since $\sigma'^r \in G_1$, this implies $\sigma$ is still a lift of $\overline{\sigma}$. Moreover $\varphi(r)t \ge s$ gives that its order is $r$, so it is the desired lift. □

**Proposition 4.15:** conjugate-rg For $i \ge 1$, $\sigma \in G_0$, $\tau \in G_i/G_{i+1}$,

$$\theta_i(\sigma\tau\sigma^{-1}) = \theta_0(\sigma)^i \theta_i(\tau).$$

(Here $\theta_0(\sigma)^i$ is thought of as in $U_L/U_L^1 \cong l^\times$, and $\theta_i(\tau) \in U_L^i/U_L^{i+1} \cong l^+$.)

*Proof.* It is slightly more convenient to work additively rather than multiplicatively, so we consider

$$\theta_i' : G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1} \cong (\pi^i)/(\pi^{i+1})$$
$$\sigma \mapsto \frac{\sigma(\pi)}{\pi} \mapsto \begin{cases} \frac{\sigma(\pi)}{\pi}, & i = 0 \\ \frac{\sigma(\pi)}{\pi} - 1, & i \ge 1, \end{cases}$$

where $\pi$ is any uniformizer.

Define

$$\pi' = \sigma^{-1}(\pi)$$

[2] The image of $G_0/G_1$ is a *complement* $Q$ of $G_1$ in $G_0$; the elements of $Q$ act on $G_1$ by conjugation—this is what the semidirect product means.

and let $a \in \mathcal{O}_L^\times$ be such that

$$\tau(\pi') = \pi' + a\pi'\pi^i.$$

Note that

$$\theta_i'(\tau) = \frac{\tau(\pi')}{\pi'} = a\pi^i.$$

Now we calculate, modulo $(\pi)^{i+1}$, that

$$\begin{aligned}
\theta_i'(\sigma\tau\sigma^{-1}) &= \frac{\sigma\tau\sigma^{-1}(\pi)}{\pi} - 1 \\
&= \frac{\sigma\tau(\pi')}{\pi} - 1 \\
&= \frac{\sigma(\pi' + a\pi'\pi^i)}{\pi} - 1 \\
&= \frac{\pi + \sigma(a\pi'\pi^i)}{\pi} - 1 \\
&= \frac{a\sigma(\pi'\pi^i)}{\sigma(\pi')} && \text{since } \sigma(a) \equiv a \pmod{\pi^{i+1}} \\
&= \left(\frac{\sigma(\pi)}{\pi}\right)^i a\pi^i \\
&= \theta_0'(\sigma)^i \theta_i'(\tau).
\end{aligned}$$

□

**Proposition 4.16:** If $\sigma \in G_i$ and $\tau \in G_j$, $i, j \geq 1$, then

$$\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+j+1}.$$

*Proof.* □

**Corollary 4.17:** For $i \geq 1$,

$$\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+1} \iff \sigma^i \in G_1 \text{ or } \tau \in G_{i+1}.$$

*Proof.* We have

$$\begin{aligned}
\sigma\tau\sigma^{-1}\tau^{-1} \in G_{i+1} &\iff \sigma\tau\sigma^{-1} = \tau && \text{in } G_i/G_{i+1} \\
&\iff \theta_i'(\sigma\tau\sigma^{-1}) = \theta_i'(\tau) && \text{in } (\pi^i)/(\pi^{i+1}) \\
&\iff \theta_i'(\tau)(\theta_0'(\sigma)^i - 1) = 0 && \text{by Proposition 4.15} \\
&\iff \theta_i'(\tau) = 0 \text{ or } \theta_0'(\sigma^1) = 1 \\
&\iff \tau \in G_{i+1} \text{ or } \sigma^i \in G_1.
\end{aligned}$$

□

**Corollary 4.18:** jump-multiple-go/g1 Suppose $G$ is abelian and $|G_0/G_1| \nmid i$. Then $G_i = G_{i+1}$.

*Proof.* Write $G_0/G_1 = \langle\overline{\sigma}\rangle$ where $r = |G_0/G_1|$. Since $r \nmid i$, $\overline{\sigma}^i \neq 1$; for any lift $\sigma \in G_0$ of $\overline{\sigma}$, $\sigma^i \notin G_1$. Since $G$ is abelian, we get for all $\tau \in G_i$, $\sigma\tau\sigma^{-1}\tau^{-1} = 1$. By the previous corollary, noting $\sigma^i \notin G_1$, we must have $\tau \in G_{i+1}$. □

**Definition 4.19:** A **jump** for $L/K$ is an integer $i$ such that

$$G_i \neq G_{i+1}.$$

Corollary 4.18 tells us that jumps are divisible by $|G_0/G_1|$.

# §5 Herbrand's Theorem

## 5.1 Functions $\varphi$ and $\psi$

Note that ramification groups behave nicely under taking subgroups (i.e. passing from $M/K$ to $M/L$), by Proposition 4.4. However, the indices are screwed up when passing to quotient groups (i.e. passing from $M/K$ to $M/L$). We calculate exactly how the index changes (Herbrand's Theorem 12.1), and use it to define a different numbering scheme that is invariant under passing to quotient groups.

It is important to know how ramification groups behave under quotients because this gives a compatible system that allows us to look at larger and larger field extensions, i.e. pass to the inverse limit.

**Definition 5.1:** Define $\varphi_{L/K} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ by

$$\varphi_{L/K}(u) = \int_0^u \frac{1}{[G_0 : G_t]} dt$$

(recall $G_u = G_{\lceil u \rceil}$) and extend $\varphi_{L/K}$ to $\mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$ by

$$\varphi(u) = u, \quad -1 \leq u \leq 0.$$

This is a piecewise linear increasing function with $\varphi_{L/K}(-1) = -1$ and with derivative at least $\frac{1}{|G_0|}$, so it is a bijection.

**Definition 5.2:** Define $\psi_{L/K} : \mathbb{R}_{-1} \to \mathbb{R}_{-1}$ by $\psi_{L/K} = \varphi_{L/K}^{-1}$. Define the **upper numbering** filtration by

$$G^v := G_{\psi_{L/K}(v)}, \quad v \geq -1.$$

## 5.2 Transitivity of $\varphi$ and $\psi$

The function $\varphi_{L/K}$ gives the reindexing when we pass to the quotient Galois group.

**Theorem 5.3** (Herbrand's Theorem)**:** herbrand-thm Let $L/K'/K$ be finite Galois extension with separable residue field extension. For all $u \geq -1$,

$$G_u H/H = (G/H)_{\varphi_{L/K'}(u)}.$$

Here, $G_u$ is the ramification group of $L/K$ and $(G/H)_{\varphi_{L/K'}(u)}$ is the ramification group of $K'/K$.

We will need several lemmas. First we relate the function $i_{G/H}(\overline{\sigma})$ and $i_G$ evaluated at the lifts of $\overline{\sigma}$ in $G$.

**Lemma 5.4:** igh-ig2 For $\overline{\sigma} \in G/H$, $j(\overline{\sigma}) = \max_{\sigma \in \overline{\sigma} H} i_G(\sigma)$,

$$i_{G/H}(\overline{\sigma}) - 1 = \varphi_{L/K'}(j(\overline{\sigma}) - 1).$$

Thus applying $\varphi_{L/K}$ has the effect of "turning" $i_G$ into $i_{G/H}$. By writing out the criterion for $\sigma \in G_u$ or $(G/H)_u$ in terms of $i_G$ and $i_{G/H}$, respectively, we will get Herbrand's Theorem.

*Proof.* Pick $\sigma_0 \in G$ mapping to $\overline{\sigma}$ such that $i_G(\sigma_0) = j(\overline{\sigma})$. Then by Proposition 4.6,

$$herbrand-pf1 i_{G/H}(\overline{\sigma}) = \frac{1}{e_{L/K'}} \sum_{\sigma \in \overline{\sigma} H} i_G(\sigma) = \frac{1}{e_{L/K'}} \sum_{\tau \in H} i_G(\sigma_0 \tau). \tag{9.8}$$

We claim that

$$i_G(\sigma_0 \tau) = \min(i_G(\sigma_0), i_G(\tau)) = \min(j(\overline{\sigma}), i_G(\tau))$$

for all $\tau \in H$. Indeed, by the nonarchimedean inequality,

$$i_G(\sigma_0 \tau) = v_L(\sigma_0 \tau(\beta) - \beta) \geq \min(v_L(\sigma_0 \tau(\beta) - \tau(\beta)), v_L(\tau(\beta) - \beta)) = \min(i_G(\sigma_0), i_G(\tau)).$$

Consider two cases.

1. $i_G(\tau) = i_H(\tau) \geq i_G(\sigma_0)$. The above gives

   $$i_G(\sigma_0 \tau) \geq \min(i_G(\sigma_0), i_G(\tau)) \geq i_G(\sigma_0).$$

   Equality holds by the maximality assumption on $\sigma_0$.

2. $i_G(\tau) < i_G(\sigma_0)$. Then

   $$i_G(\sigma_0 \tau) = \min(i_G(\sigma_0), i_G(\tau)) = i_G(\tau).$$

The RHS of (9.8) then equals $\frac{1}{e_{L/K'}} \sum_{\tau \in H} \min(i_G(\sigma_0), i_G(\tau))$; the result then follows from the next lemma. □

**Lemma 5.5:**

$$\varphi_{L/K}(u) = \frac{1}{e_{L/K}} \sum_{\sigma \in G} \min(j(\overline{\sigma}), u + 1) - 1.$$

*Proof.* Since both sides are piecewise linear functions, and both sides equal $u$ for $-1 \le u \le 0$, it suffices to show their derivatives (slopes) are equal for $u > 0$.

If $i - 1 < u < i$ where $i \in \mathbb{N}$, then the slope of the LHS is $\frac{1}{[G:G_i]}$. For the RHS, since $i_G(\sigma)$ is an integer, each term is either $i_G(\sigma)$ or $u+1$; each term where $u+1$ is the minimum contributes to the slope. Hence the slope on the RHS is

$$\frac{1}{e_{L/K}} \left|\{\sigma \in G : u+1 < i_G(\sigma)\}\right| = \frac{1}{e_{L/K}} \left|\{\sigma \in G : i_G(\sigma) \ge i+1\}\right| = \frac{|G_i|}{e_{L/K}} = \frac{1}{[G_0 : G_i]},$$

as needed. □

*Proof of Theorem 5.3.* We have the following string of equivalences.

1. $\overline{\sigma} \in G_u H/H = G_u/G_u \cap H$
2. There is $\sigma \in G$ lifting $\overline{\sigma}$ so that $\sigma \in G_u$.
3. $j_G(\overline{\sigma}) - 1 \ge u$.
4. $\varphi_{L/K'}(j_G(\overline{\sigma}) - 1) \ge \varphi_{L/K'}(u)$.
5. $i_{G/H}(\overline{\sigma}) - 1 \ge \varphi_{L/K'}(u)$.
6. $\overline{\sigma} \in (G/H)_{\varphi_{L/K'}(u)}$.

We have (3) $\iff$ (4) because $\varphi_{L/K'}$ is monotonically increasing and (4) $\iff$ (5) by Lemma 5.4. □

Now we prove transitivity for $\varphi$ and $\psi$.

**Proposition 5.6:** phi-psi-trans

$$\begin{aligned} \varphi_{L/K} &= \varphi_{K'/K} \circ \varphi_{L/K'} \\ \psi_{L/K} &= \psi_{L/K'} \circ \psi_{K'/K}. \end{aligned}$$

*Proof.* It suffices to prove the first equation; the first implies the second since $\varphi$ and $\psi$ are inverse. For $-1 \le u \le 0$ both sides equal $u$. Thus it suffices to show the derivatives of both sides are equal for $u \ge 0$. For $u \notin \mathbb{Z}$, the derivative on the LHS is

$$\varphi'_{L/K}(u) = \frac{1}{[G_0 : G_u]}.$$

By the chain rule, the slope on the RHS is

$$\begin{aligned}
\varphi'_{K'/K}(\varphi_{L/K'}(u))\varphi'_{L/K'}(u) &= \frac{|(G/H)_{\varphi_{L/K'}(u)}|}{|(G/H)_0|}\frac{|H_u|}{|H_0|} \\
&= \frac{|G_uH/H||H_u|}{e_{K'/K}e_{L/K'}} && \text{by Herbrand's Theorem 12.1} \\
&= \frac{|G_u/H\cap G_u||H_u|}{e_{L/K}} \\
&= \frac{|G_u|}{|G_0|}
\end{aligned}$$

using $H\cap G_u = H_u$ (Proposition 4.4) and multiplicativity of ramification index. The derivatives are equal, as needed. □

Finally, we prove the most important consequence of Herbrand's Theorem: namely, by using the upper numbering (i.e. numbering using the inverse of $\varphi_{L/K}$), quotients of ramification groups are preserved.

**Proposition 5.7:** For all $v \geq -1$,

$$G^vH/H = (G/H)^v.$$

*Proof.* By Herbrand's Theorem 12.1 and transitivity of $\psi$ (Proposition 5.6) ($\psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}$), we get

$$\begin{aligned}
G^vH/H &= G_{\psi_{L/K}(v)}H/H \\
&= (G/H)_{\varphi_{L/K'}(\psi_{L/K}(v))} && = (G/H)_{\psi_{K'/K}(v)} = (G/H)^v
\end{aligned}$$ □

We can now define upper numbering for infinite algebraic extensions $L/K$.

**Definition 5.8:** Define

$$G(L/K)^v := \varprojlim_{K'/K \text{ finite Galois}} G(K'/K)^v.$$

# §6 Hasse-Arf Theorem

We have two different filtrations, the lower numbering filtration $\{G_u\}_{u\geq -1}$ and $\{G^v\}_{v\geq -1}$.

**Definition 6.1:** A **jump** is $u$ such that $G_u \neq G_{u+\varepsilon}$ or $v$ such that $G^v \neq G^{v+\varepsilon}$.

They are the $x$ and $y$-coordinates of jump points, i.e. where the slope of $\varphi$ changes.

Note a jump $u \in \mathbb{Z}$ since $G_u = G_{\lceil u \rceil}$. Moreover, $u$ is a jump for the lower numbering iff $v = \varphi_L/K(u)$ is a upper numbering, because $\varphi, \psi$ are monotonically increasing.

**Theorem 6.2** (Hasse-Arf Theorem)**:** If $G$ is finite abelian, then the jumps $v$ are integers.

In the cyclotomic case, $G$ was abelian.

**Remark:** There is a nonabelian example where $v \notin \mathbb{Z}$. (See HW.)

We postpone the proof. Applications.

1. Used in local class field theory.
2. "Conductor of Galois representations" are in $\mathbb{Z}$, not just in $\mathbb{Q}$. Finite $L/K$, $G(L/K) \to \mathrm{GL}_n(\mathbb{C})$.

# Part II

# Class Field Theory

# Chapter 10
# Class Field Theory: Introduction

intro-cft We give the main theorems of class field theory, deferring the proofs to the next five chapters. In this chapter we'll focus on the motivation and intuition behind the theorems. The reader may find it helpful to read this chapter along with Chapter 15, Applications.

In Section 1 we'll introduce the Frobenius map, which we need before we can state the theorems of class field theory. In Section 2 we state the theorems of local class field theory. We state two formulations of global class field theory: using ideals in Section 4 and using ideles in Section 6, after giving the relevant background on ray class groups and ideles. The formulation using ideals is less sophisticated to understand, but the formulation using ideles is more useful theoretically. We'll compare the two formulations in Section 6.1. Finally, we'll present a proof of the Kronecker-Weber Theorem using class field theory in Section 7. Throughout, we'll refer back to the cyclotomic case, because class field theory is easy to understand in this case, and it already shows much of what's at play.

## §1 Frobenius elements

sec:frobenius-elements In order to define the Artin map and state the main theorems of class field theory, we first need to understand the Frobenius map. This map takes prime ideals inside a field $K$ to automorphisms in a Galois group $G(L/K)$. One reason for studying the Frobenius map is that $\mathrm{Frob}_{L/K}(\mathfrak{p})$ gives information on how the prime ideal $\mathfrak{p}$ splits in a Galois extension. First, we'll define the Frobenius element and explain what it tells us about the splitting of primes. Next, we'll look at the example of a cyclotomic extension, which suggests that something deeper is going on with the Frobenius map, which we'll attempt to explain with class field theory.

The reader may wish to review Section 2.7, on the decomposition and inertia groups.

The results in this section will apply to both local and global fields.

**Definition 1.1:** frobenius-element Let $L/K$ be a Galois extension with Galois group $G$, and assume that the residue field $k$ is finite.

1. Let $\mathfrak{P}$ be an unramified prime of $L$. Define the **Frobenius element**

$$\mathrm{Frob}_{L/K}(\mathfrak{P}) = (\mathfrak{P}, L/K)$$

to be the element $\sigma \in D_{L/K}(\mathfrak{P}) \subseteq G(L/K)$ that acts as the Frobenius automorphism on the residue field $l = \mathcal{O}_L/\mathfrak{P}$ fixing $k = \mathcal{O}_K/\mathfrak{p}$. In other words, letting $k = \mathbb{F}_q$,

$$\sigma\alpha = \alpha^q \text{ for all } \alpha \in l.$$

2. Let $\mathfrak{p}$ be an unramified prime of $K$. Let $\mathfrak{P}$ be any prime dividing $\mathfrak{p}$, and define $\mathrm{Frob}_{L/K}(\mathfrak{p}) = (\mathfrak{p}, L/K)$ to be the conjugacy class of $(\mathfrak{P}, L/K)$. Equivalently (see lemma 1.2),
$$\mathrm{Frob}_{L/K}(\mathfrak{p}) = (\mathfrak{p}, L/K) := \{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}.$$

In the local case, when there is only one prime, we will simply write $\mathrm{Frob}_{L/K}$.

*Proof of existence of* $(\mathfrak{P}, L/K)$. When $\mathfrak{p}$ is unramified in $L$, $I(\mathfrak{P}) = 1$ so from Corollary 2.7.5, the map $D_{L/K}(\mathfrak{P}) \to G(l/k)$ is an isomorphism. Thus there is a unique element of $D_{L/K}(\mathfrak{P})$ whose image is the Frobenius element. □

To show the above definition is valid, we need to show that changing the prime above $\mathfrak{p}$ corresponds to conjugating the Frobenius element.

**Lemma 1.2:** lem:frob-lem Let $\tau \in G(L/K)$. Then

$$D(\tau\mathfrak{P}) = \tau D(\mathfrak{P})\tau^{-1}$$
$$(\tau\mathfrak{P}, L/K) = \tau(\mathfrak{P}, L/K)\tau^{-1}.$$

Therefore (since $G(L/K)$ operates transitively on the primes dividing $\mathfrak{p}$), the conjugacy class of $(\mathfrak{P}, L/K)$ is equal to $\{(\mathfrak{P}, L/K) \mid \mathfrak{P}|\mathfrak{p}\}$.

*Proof.* The first statement follows from the fact that if $G$ acts on $S$ and $G$ is the stabilizer of $s \in S$, then $tGt^{-1}$ is the stabilizer of $ts$. Recall that the decomposition group $D(\mathfrak{P})$ is defined as the stabilizer of $\mathfrak{P}$.

For the second statement, let $q = |k|$ and note that $\tau$, as an automorphism, preserves $q$th powers. Hence for all $b \in \mathcal{O}_L$,

$$(\tau(\mathfrak{P}, L/K)\tau^{-1})(b) \equiv \tau(\tau^{-1}(a)^q) \equiv a^q \pmod{\tau(\mathfrak{P})}.$$ □

Note that if $G$ is abelian, then the conjugacy classes are just elements, so we can think of $(\mathfrak{P}, L/K)$ as an element of $G(L/K)$.

One of the most basic applications of the Frobenius map is to the splitting of primes in an extension.

**Proposition 1.3:** frob-1-split-completely Let $L/K$ be an extension of degree $n$, unramified at $\mathfrak{P} \mid \mathfrak{p}$. Then $\mathfrak{p}$ splits into $\frac{n}{|\langle(\mathfrak{P}, L/K)\rangle|}$ factors, where $\langle(\mathfrak{P}, L/K)\rangle$ is the subgroup of $G$ generated by $(\mathfrak{P}, L/K)$.

In particular, $\mathfrak{p}$ splits completely iff $(\mathfrak{p}, L/K) = 1$.

*Proof.* Let $l$ and $k$ be the residue fields.

The Frobenius element generates the decomposition group $D(\mathfrak{P})$, since it acts as the Frobenius automorphism on $l/k$ and $D(\mathfrak{P}) \cong G(l/k)$. Hence $|D(\mathfrak{P})| = |\langle(\mathfrak{p}, L/K)\rangle|$. Since $\mathfrak{p}$ is unramified in $L$, $e(\mathfrak{P}/\mathfrak{p}) = 1$ and $f(\mathfrak{P}/\mathfrak{p}) = |D(\mathfrak{P})| = |\langle(\mathfrak{p}, L/K)\rangle|$. Hence, letting $g$ be the number of primes above $\mathfrak{p}$, we have

$$n = [L : K] = \underbrace{e(\mathfrak{P}/\mathfrak{p})}_{1} \underbrace{f(\mathfrak{P}/\mathfrak{p})}_{|\langle(\mathfrak{P}, L/K)\rangle|} g.$$

Then

$$g = \frac{n}{|\langle(\mathfrak{P}, L/K)\rangle|},$$

as needed.

In particular, $\mathfrak{p}$ splits completely iff $g = n$, iff $|\langle(\mathfrak{P}, L/K)\rangle| = 1$, iff $|\langle(\mathfrak{p}, L/K)\rangle| = 1$, i.e. the Frobenius element $(\mathfrak{p}, L/K)$ is trivial. □

Next, we'll need a result of how the Frobenius element changes as we change the base field.

**Proposition 1.4:** pr:frob-base-ext Suppose that $L/K$ is an unramified Galois extension, $K \subseteq K' \subseteq L$, and $\mathfrak{p}$ is a prime of $K'$. Let $k, k'$ be the residue fields of $K$ and $K'$. Then

$$\mathrm{Frob}_{L/K'}(\mathfrak{p}) = \mathrm{Frob}_{L/K}(\mathfrak{p})^{[k':k]}$$

Note by taking the $[k' : k]$th power we mean that if $\mathrm{Frob}_{L/K}(\mathfrak{p})$ is the conjugacy class of $\sigma$, then $\mathrm{Frob}_{L/K}(\mathfrak{p})^{[k':k]}$ is the conjugacy class of $\sigma^{[k':k]}$.

*Proof.* By definition, the left hand side induces the $|k'|$th power map on $l$, while the right hand side induces the $|k| \cdot [k' : k]$th power map on $l$. Hence they are equal. □

## 1.1 Examples

We calculate the Frobenius map explicitly in two examples. First, a warm-up.

**Example 1.5:** For the field extension $\mathbb{Q}(i)/\mathbb{Q}$,

$$(p, \mathbb{Q}(i)/\mathbb{Q}) = \begin{cases} \text{complex conjugation}, & p \equiv 3 \pmod 4, \\ 1, & p \equiv 1 \pmod 4. \end{cases}$$

*Proof.* If $p \equiv 3 \pmod 4$, then $p$ remains prime in $\mathbb{Q}(i)$. Reference The residue fields are

$$\begin{array}{c} l = \mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{F}_{p^2} \\ \Big| \\ k = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p. \end{array}$$

Now $(p, \mathbb{Q}(i)/\mathbb{Q})$ must induce the $p$th power map on $\ell = \mathbb{F}_{p^2}$. Since this is not the identity, it must be the only element of $G(\mathbb{Q}(i)/\mathbb{Q})$ that is not the identity, i.e. complex conjugation. (This does act as the $p$th power, since recalling $p \equiv 3 \pmod 4$, $(a+bi)^p \equiv a^p + b^p i^p \equiv a - bi \pmod p$.)

If $p \equiv 1 \pmod 4$, then $p$ splits in $\mathbb{Q}[i]$, say into $\mathfrak{P}_1$ and $\mathfrak{P}_2$ where $\mathfrak{P}_1, \mathfrak{P}_2$ are complex conjugate. Then $\mathbb{Z}[i]/\mathfrak{P}_1 = \mathbb{Z}[i]/\mathfrak{P}_2 = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ so the extension of residue fields is trivial and the Frobenius automorphism is trivial. It is induced by the identity map, so $(p, \mathbb{Q}(i)/\mathbb{Q}) = 1$. (Note that in this case the decomposition group is trivial and does not contain complex conjugation.) □

We generalize the above example to cyclotomic extensions.

**Example 1.6:** cyclotomic-frobenius Let $K = \mathbb{Q}(\zeta_n)$ where $\zeta_n$ is a primitive $n$th root of unity. Then $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ by identifying $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ with the automorphism sending $\zeta_n$ to $\zeta_n^k$ (Proposition 3.1).

Suppose $\sigma := (p, L/K)$ is the map $\zeta_n \mapsto \zeta_n^k$. By definition $\sigma$ reduces to the $p$th power map on the residue fields, so $\sigma(\zeta_n) \equiv \zeta_n^p \pmod{p\mathcal{O}_K}$. Hence

$$\zeta_n^p \equiv \zeta_n^k \pmod{p\mathcal{O}_K}.$$

But since $p \nmid n$, the $n$th roots of unity are distinct modulo $p$. (More precisely, they are distinct elements of $\mathbb{F}_{p^m}$ where $m$ is such that $p^m \equiv 1 \pmod n$.) Hence we must have $p \equiv k \pmod n$, i.e. $\sigma$ is the $p$th power map.

This shows that for a prime $p \nmid n$, under the identification $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, we have

$$(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = p \bmod n.$$

This calculation of the Frobenius elements gives a complete characterization of how primes split in cyclotomic extensions. We obtain a simple proof of Theorem 6.2.4, which we restate here.

**Theorem 1.7:** thm:cyclotomic-factorization-p-2 Suppose that $n = p^r m$, where $p \nmid m$. Let

$$f = \mathrm{ord}_m(p).$$

Then the prime factorization of $(p)$ in $\mathbb{Q}(\zeta_n)$ is

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{\varphi(p^r)}$$

where $\mathfrak{P}_j$ are distinct primes, each with residue degree $f$ over $\mathbb{Q}$, and $g = \frac{\varphi(m)}{f}$.

In particular,

$$(p) \text{ splits completely in } \mathbb{Q}(\zeta_n) \text{ iff } p \equiv 1 \pmod n.$$

*Proof.* For $r = 0$, i.e. $n = m$, the automorphism $\zeta_n \mapsto \zeta_n^p$ has order $\mathrm{ord}_m(p)$, so the result follows from Example 1.6 and Proposition 1.3. For $r > 0$, note that $(p)$ totally ramifies in $\mathbb{Q}(\zeta_{p^r})$ by Proposition 6.2.2, and $\mathbb{Q}(\zeta_n)$ is the compositum $\mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m)$. □

### 1.2 The Frobenius map is a nice homomorphism

sec:frob-map-nice Because we've defined the Frobenius map on prime ideals $\mathfrak{p}$ unramified in $L$, and the prime ideals are a free basis for the ideal group, we can extend the Frobenius map to the subgroup of ideals generated by unramified primes. Denoting this subgroup by $I_K^S$, we have a map

$$eq:frob-extend\,\mathrm{Frob}_{L/K} : I_K^S \to G(L/K). \tag{10.1}$$

What is nice about this map? Look back to the cyclotomic case, Example 1.6. The Frobenius map didn't map the primes arbitrarily; it sent $p$ to $p \pmod n$. What's to note here is that $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ *only depends on* $p \pmod n$*, information about* $p$ *intrinsic to* $\mathbb{Q}$, even though $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ tells us about the field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Thus (10.1) factors:

$$eq:frob-for-cyclo \qquad \begin{tikzcd} I_{\mathbb{Q}}^S \arrow[r, "\mathrm{Frob}_{L/\mathbb{Q}}"] \arrow[d] & G(L/\mathbb{Q}) \\ I_{\mathbb{Q}}^S/I_{\mathbb{Q}}(1,\infty n). \arrow[ur, "\cong"] & \end{tikzcd} \tag{10.2}$$

Here, $I_{\mathbb{Q}}^S$ denotes the prime ideals relatively prime to $n$ and $I_{\mathbb{Q}}(1,\infty n)$ denotes the subgroup of ideals generated by $(p)$ with $p \equiv 1 \pmod n$ and *positive*.

Something like this in fact happens in general: global class field theory tells us that for all abelian extensions, the Frobenius map "factors through a modulus," that $(\mathfrak{p}, L/K)$ depends only on what $\mathfrak{p}$ is modulo a nice subgroup of ideals in $K$. Our example essentially proves class field theory for cyclotomic extensions of $\mathbb{Q}$, by using the roots of unity to "keep book" on the action of Frobenius. Don't be deceived, though, the general case is much harder.

Before we look at global class field theory, we first study local class field theory. Since there's only one prime in a local field, rather than consider a map from the (rather boring) ideal group, we consider a map from the field itself.

## §2 Local reciprocity

sec:local-reciprocity When $K$ is a nonarchimedean local field, there is a single prime ideal $\mathfrak{p} = (\pi)$. For every abelian unramified extension, the previous section gives an element of $G(L/K)$ corresponding to $\mathfrak{p}$, which we can think of as corresponding to $\pi$.

The main theorem of local class field theory is that we can extend this map to all elements of $K^\times$, and get elements in $\varprojlim_{\text{finite abelian } L/K} G(L/K) = G(K^{\text{ab}}/K)$. We will also show that this map behaves well under restricting to subextensions $L/K$.

**Theorem 2.1** (Local reciprocity law)**:** local-reciprocity For any nonarchimedean local field $K$, there exists a unique homomorphism

$$\phi_K : K^\times \to G(K^{\text{ab}}/K),$$

called the **local Artin (reciprocity) map** with the following properties.

1. (Relationship with Frobenius map) For any prime element $\pi$ of $K$ and any finite unramified extension $L$ of $K$, $\phi_K(\pi)$ acts on $L$ as $\mathrm{Frob}_{L/K}(\pi)$.

2. (Isomorphism) Let $p_L$ be the projection $G(K^{\mathrm{ab}}/K) \to G(L/K)$. For any finite abelian extension $L/K$, $\phi_K$ induces an isomorphism $\phi_{L/K} : K^\times/\,\mathrm{Nm}_{L/K}(L^\times) \to G(L/K)$ making the following commute:

$$\begin{tikzcd} K^\times \arrow[r, "\phi_K"] \arrow[d] & G(K^{\mathrm{ab}}/K) \arrow[d, "p_L"] \\ K^\times/\,\mathrm{Nm}_{L/K}(L^\times) \arrow[r, "\phi_{L/K}", "\cong"'] & G(L/K). \end{tikzcd}$$

3. (Compatibility with norm map) For any $K \subseteq K'$, the following diagram commutes.

$$\begin{tikzcd} K'^\times \arrow[r, "\phi_{K'}"] \arrow[d, "\mathrm{Nm}_{K'/K}"] & G(K'^{\mathrm{ab}}/K') \arrow[d, "\bullet|_{K^{\mathrm{ab}}}"] \\ K^\times \arrow[r, "\phi_K"] & G(K^{\mathrm{ab}}/K) \end{tikzcd}$$

We can also say something about this map topologically.

**Definition 2.2:** A **norm group** is a subgroup of $K^\times$ of the form $\mathrm{Nm}_{L/K}(L^\times)$ for some finite extension $L/K$.

Let Frob denote the Frobenius element of $l/k$. The **Weil group** $W(L/K)$ of an extension $L/K$ is equal to the inverse image of $\mathrm{Frob}^{\mathbb{Z}}$ under the map $G(L/K) \to G(l/k)$. The topology on $W(L/K)$ is the topology from considering it as a disjoint union of cosets $I(L/K)\sigma_n$, where $\sigma_n$ is any lift of $\mathrm{Frob}^n$.

Note that the topology on $W(K^{\mathrm{ab}}/K)$ as defined above is strictly finer than the topology it inherits from $G(K^{\mathrm{ab}}/K)$ (see exercise 2.1).

**Theorem 2.3** (Local existence theorem)**:** local-existence Let $K$ be a nonarchimedean local field. The norm groups of $K$ are exactly the open subgroups of finite index.

**Theorem 2.4** (Topological isomorphism for LCFT)**:** thm:lcft-topology The image of the Artin map is the Weil group $W(L/K)$, and $\phi_K$ gives an isomorphism of topological groups $K^\times \to W(L/K)$. It restricts to an isomorphism $U_K \to I(L/K)$.

Combining Theorems 2.1 and 2.3 gives the following bijective correspondence.

**Theorem 2.5:** lcft-correspondence Let $K$ be a nonarchimedean local field. Then there is a bijective correspondence between finite abelian extensions of $K$ and the set of open subgroups of finite index of $K^\times$, given by

$$L \mapsto \mathrm{Nm}_{L/K}(L^\times).$$

Furthermore, this is an inclusion-reserving bijection that takes intersections to products and products to intersections:

$$\begin{aligned} L \subseteq M &\iff \operatorname{Nm}_{L/K}(L^\times) \supseteq \operatorname{Nm}_{M/K}(M^\times) \\ \operatorname{Nm}_{L\cdot L'/K}((L\cdot L')^\times) &= \operatorname{Nm}_{L/K}(L^\times) \cap \operatorname{Nm}_{L'/K}(L'^\times) \\ \operatorname{Nm}_{L\cap L'/K}((L\cap L')^\times) &= \operatorname{Nm}_{L/K}(L^\times) \cdot \operatorname{Nm}_{L'/K}(L'^\times). \end{aligned}$$

Finally, every subgroup of $K^\times$ containing a norm group is a norm group.

The following gives a sort-of converse statement: nonabelian extensions cannot be described by norm groups.

**Theorem 2.6** (Norm limitation theorem)**:** thm:lcft-norm-limitation Let $L$ be a finite extension of a local field $K$, and $K'$ be the largest abelian extension of $K$ contained in $L$. Then

$$\operatorname{Nm}_{L/K}(L^\times) = \operatorname{Nm}_{K'/K}(K'^\times).$$

# §3 Ray class groups

sec:ray-class-groups In order to define the Frobenius element of a prime we need the extension to be unramified. However, when $K$ is a global field, we cannot as easily say an extension $L/K$ is “unramified,” because $\mathcal{O}_K$ has many prime ideals. Requiring that $L/K$ to be unramified at all primes of $K$ is too restrictive, because most fields $L$ do not satisfy this condition.

Thus, we instead focus on a set of primes $S$ and consider extensions $L/K$ that are unramified outside of $S$. When we define Frobenius elements, we have to exclude $S$, and when we define a reciprocity map we have to exclude the subgroup that these primes generate. (Note that unlike in local reciprocity, we will not define $\phi_K$ with domain $K^\times$, but rather with domain a subgroup of the ideal group $I_K$.)

Letting $S$ range over all finite subsets, we will account for all finite abelian extensions $L/K$, because each extension is ramified at only finitely many primes (Theorem 2.6.1).

This motivates the following definition.

**Definition 3.1:** i-k-s Let $I_K$ be the group of fractional ideals of $K$. Define $I_K^S$ to be the subgroup of $I_K$ generated by prime ideals not in $S$.

Let $L/K$ be an extension of $K$. Define $I_L^S := I_L^{S'}$, where $S'$ is the set of prime ideals lying above a prime ideal in $S$.

Note that if $S \subseteq T$ then $I_K^S \supseteq I_K^T$.

Similar to Theorem 2.1, global class field theory will tell us there is a map

$$I_K^S / \operatorname{Nm}_{L/K}(I_L^S) \to G(L/K)$$

when $S$ contains the primes that ramify in $L$. However, this is not an isomorphism until we take a further quotient, namely, the quotient with a subgroup of principal ideals $P_K(1, \mathfrak{m})$, which we will define. First we need the following.

**Definition 3.2:** A **modulus** $\mathfrak{m}$ is a formal product of places of $K$, where

1. Finite primes have exponents in $\mathbb{N}_0$, and only finitely many exponents are nonzero.
2. Infinite real places have exponents 0 or 1.
3. Infinite complex places do not appear.

We say a place divides $\mathfrak{m}$ if it appears with positive exponent. We write

$$\mathfrak{m} = \underbrace{\prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{m(\mathfrak{p})}}_{\mathfrak{m}_0} \underbrace{\prod_{v \text{ real}} v^{m(v)}}_{\mathfrak{m}_\infty}.$$

In other words, a modulus is the product of a proper ideal with some number of real places.

**Definition 3.3:** Let $S(\mathfrak{m})$ denote the set of finite primes dividing $\mathfrak{m}$.

Define $K(1, \mathfrak{m})$ ("elements of $K$ that are 1 modulo $\mathfrak{m}$") to be the subgroup of elements of $K^\times$ satisfying the following.

$$\begin{cases} \operatorname{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}), & \text{finite } \mathfrak{p} \mid \mathfrak{m} \\ a_v > 0, & \text{real } v \mid \mathfrak{m}. \end{cases}$$

Let $i : K^\times \to I_K$ be the map sending $a$ to $(a)$, and let

$$P_K(1, \mathfrak{m}) := i(K(1, \mathfrak{m})).$$

Define the **ray class group** of $\mathfrak{m}$ to be

$$C_K(\mathfrak{m}) = I_K^{S(\mathfrak{m})} / P_K(1, \mathfrak{m}).$$

Note that $P_K(1, \mathfrak{m}) \in I_K^{S(\mathfrak{m})}$ because if $a \in K(1, \mathfrak{m})$ and $\mathfrak{p} \in S(\mathfrak{m})$, then $\operatorname{ord}_{\mathfrak{p}}(a-1) \geq 1$ and $\operatorname{ord}_{\mathfrak{p}}(a) = 0$, i.e. $\mathfrak{p} \nmid (a)$. We will often abbreviate $I^{S(\mathfrak{m})}$ as $I^{\mathfrak{m}}$.

**Example 3.4:** ex:ray-class-groups If $\mathfrak{m} = 1$ then $P_K(1, \mathfrak{m})$ is the subgroup of principal ideals and $C_K(\mathfrak{m})$ is just the ideal class group.

If $\mathfrak{m} = \prod_{v \text{ real}} v$, then

$$C_K(\mathfrak{m}) = I_K / \{(a) \in I_K : a_v > 0 \text{ for all real } v\}$$

is called the **narrow class group**. We are only modding out by the "totally positive" principal ideals, so it is larger than the class group.

**Definition 3.5:** A **congruence subgroup** for $K$ modulo $\mathfrak{m}$ is a subgroup $H$ such that

$$P_K(1,\mathfrak{m}) \subseteq H \subseteq I_K^{S(\mathfrak{m})}.$$

The corresponding **generalized ideal class group** is $I_K^{S(\mathfrak{m})}/H$.

We will show that generalized ideal class groups are exactly the Galois groups of abelian extensions of $K$.

Finally, in preparation for the global reciprocity theorem, we say what it means exactly for a map to only depend on modulo conditions, like the Frobenius map we considered in Section 1.2.

**Definition 3.6:** A homomorphism $\psi : I^S \to G$ **admits a modulus** if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = \mathfrak{m}$ such that $\psi$ factors through $I^S/P_K(1,\mathfrak{m})$. In other words, there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ such that

$$\psi(P_K(1,\mathfrak{m})) = 0.$$

# §4 Global reciprocity

sec:global-reciprocity In this section $K$ is a global field.

**Theorem 4.1** (Global reciprocity theorem)**:** global-reciprocity Let $L/K$ be a finite abelian extension. Let $S$ be the set of primes ramifying in $L$. There is a unique map $\psi_{L/K}$ such that for a prime ideal $\mathfrak{p} \notin S$, $\psi_{L/K}(\mathfrak{p})$ acts on $L$ as $\mathrm{Frob}_{L/K}(\mathfrak{p})$. Moreover, $\psi_{L/K}$ satisfies the following properties.

1. (Isomorphism) $\psi_{L/K}$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ and $\psi_{L/K}$ induces an isomorphism

$$\psi_{L/K} : I_K^S/(P_K(1,\mathfrak{m}) \cdot \mathrm{Nm}_{L/K}(I_L^S)) \xrightarrow{\cong} G(L/K).$$

2. (Compatibility over all extensions) Suppose $S \subseteq T$, and $L/K$, $M/K$ are finite abelian extensions such that $L \subseteq M$ and such that the set of primes ramifying in $L, M$ are contained in $S, T$, respectively. Then the following commutes, where $p_L$ is the projection map.

$$\begin{tikzcd} I_K^T \arrow[r, "\psi_{M/K}"] \arrow[d, hook] & G(M/K) \arrow[d, "p_L"] \\ I_K^S \arrow[r, "\psi_{L/K}"] & G(L/K). \end{tikzcd}$$

3. (Compatibility with norm map) For $K \subseteq K' \subseteq L$, the following diagram commutes.

$$\begin{tikzcd} I_{K'}^S \arrow[r, "\psi_{L/K'}"] \arrow[d, "\mathrm{Nm}_{K'/K}"] & G(L/K') \arrow[d, hook] \\ I_K^S \arrow[r, "\psi_{L/K}"] & G(L/K) \end{tikzcd}$$

**Remark:** rem:gcft-ideals The uniqueness of $\psi_{L/K}$ is clear from the fact that $I_K^S$ is freely generated by prime ideals. Part 2 follows immediately from the definition of $\psi_{L/K}$ and $\psi_{M/K}$, and part 3 follows immediately from the existence of $\psi_{L/K}$ and $\psi_{L/K'}$, as we show below. The crux of the theorem is part 1.

For part 2, since primes generate $I_K^S$, it suffices to show that for any prime $\mathfrak{p} \in I_K^S$,

$$\psi_{L/K}(\mathfrak{p}) = p_L(\psi_{M/K}(\mathfrak{p})).$$

But by definition, the left-hand side is $\mathrm{Frob}_{L/K}(\mathfrak{p})$ and the right-hand side is $p_L(\mathrm{Frob}_{M/K}(\mathfrak{p}))$. Now $p_L$ induces the map $G(m/k) \to G(l/k)$, so both sides act on $k$ as the $|k|$th power Frobenius, and are equal.

For part 3, we need to show for any prime $\mathfrak{p} \in I_{K'}^S$,

$$\psi_{L/K'}(\mathfrak{p}) = \psi_{L/K}(\mathrm{Nm}_{K'/K}(\mathfrak{p})).$$

But by definition, the left-hand side is $\mathrm{Frob}_{L/K'}(\mathfrak{p})$ and the right-hand side is $\psi_{L/K}(\mathfrak{p}^{[k':k]}) = \mathrm{Frob}_{L/K}(\mathfrak{p})^{[k':k]}$. The result now follows from Proposition 1.4.

**Example 4.2** (Cyclotomic extensions)**:** ex:cyclotomic-gcft In Section 1.2, we showed that the global reciprocity theorem (part 1 above) holds for a cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Indeed, letting $\mathfrak{m}$ be $n\infty$, we have that $I_K^{\mathfrak{m}}/P_K(1,\mathfrak{m}) \xrightarrow{\cong} G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ as in (10.2). (Note that $\mathrm{Nm}_{L/K}(I_L^S) \subseteq P_K(1,\mathfrak{m})$ will follow from the first inequality 14.2.1.)

Note the modulus in Theorem 4.1 has to be divisible by all primes ramifying in $L$, and the primes have to have large enough exponents for $\ker(\psi_{L/K})$ to be a congruence subgroup modulo $\mathfrak{m}$. There is a canonical choice for $\mathfrak{m}$, namely the modulus with least exponents. It is called the **conductor** of the extension $L/K$, and denoted by $\mathfrak{f}(L/K)$.

We have the following analogue of Theorem 2.3.

**Theorem 4.3** (Existence theorem)**:** global-existence Let $H$ be a congruence subgroup modulo $\mathfrak{m}$. Then there exists an abelian extension $L/K$ such that

$$H = P_K(1,\mathfrak{m}) \cdot \mathrm{Nm}_{L/K}(I_L^{\mathfrak{m}}) = \ker(\psi_{L/K}).$$

In particular, this applies when $H = P_K(1,\mathfrak{m})$.

**Definition 4.4:** df:ray-class-field For each modulus $\mathfrak{m}$ there is a field $K_{\mathfrak{m}}$, called the **ray class field** of $K$ modulo $\mathfrak{m}$ such that $\psi_{K_{\mathfrak{m}}/K}$ defines an isomorphism

$$C_K(\mathfrak{m}) \xrightarrow{\cong} G(K_{\mathfrak{m}}/K).$$

**Example 4.5:** Since $\infty(n)$ is the smallest modulus such that $\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ factors through $I_K^{\mathfrak{m}}/P_K(1,\mathfrak{m})$, $\infty(n)$ is the conductor of $\mathbb{Q}(\zeta_n)$. Since we actually have an isomorphism

$$C_K(\infty n) = I_K^{\infty n}/P_K(1,\infty n) \xrightarrow{\cong} G(\mathbb{Q}(\zeta_n)/\mathbb{Q}),$$

$\mathbb{Q}(\zeta_n)$ is in fact the ray class field of $\infty(n)$.

We have that $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ is the ray class field of $(n)$ (see exercise 1.2).

Putting this all together, if we fix a modulus $\mathfrak{m}$ we have the following bijection between extensions and subgroups.

**Theorem 4.6:** thm:ray-class-bijection Fix a modulus $\mathfrak{m}$ and a global field $K$. The map $L \mapsto \mathrm{Nm}_{L/K}(C_L(\mathfrak{m}))$ is a bijection between

1. the set of abelian extensions of $K$ in the ray class field $K_{\mathfrak{m}}$ and
2. the set of subgroups of $C_K(\mathfrak{m})$.

Moreover, it reverses inclusions and switches products and intersections:

$$\begin{aligned} L \subseteq M &\iff \mathrm{Nm}_{L/K}(C_L(\mathfrak{m})) \supseteq \mathrm{Nm}_{M/K}(C_M(\mathfrak{m})) \\ \mathrm{Nm}_{L_1\cdot L_2/K}(C_{L_1\cdot L_2,\mathfrak{m}}) &= \mathrm{Nm}_{L_1/K}(C_{L_1}(\mathfrak{m})) \cap \mathrm{Nm}_{L_2/K}(C_{L_2}(\mathfrak{m})) \\ \mathrm{Nm}_{L_1\cap L_2/K}(C_{L_1\cap L_2}(\mathfrak{m})) &= \mathrm{Nm}_{L_1/K}(C_{L_1}(\mathfrak{m}))\cdot \mathrm{Nm}(C_{L_2}(\mathfrak{m})). \end{aligned}$$

Note Theorem 4.1 is like Theorem 2.1 except that we're only working with finite extensions $L/K$ instead of putting them together into $K^{\mathrm{ab}}/K$. We cannot combine the maps $\psi_{L/K}$ because they are defined on different groups. Hence we now take a different approach, using ideles.

# §5 Ideles

sec:ideles In this section we give an alternate statement of the main theorems of global class field theory.

In local class field theory, we had isomorphisms $K^\times/\mathrm{Nm}_{L/K}(L^\times) \cong G(L/K)$. For this to be true, $\mathrm{Nm}_{L/K}(L^\times)$ must have finite index in $K^\times$. However, this is no longer true when $K$ is a global field. (If $K$ is local, it is complete with respect to a valuation, and $\mathrm{Nm}_{L/K}(x) = y$ has solutions in $y$ for many $x$, in the same way that Hensel's lemma often gives solutions over complete fields.)

We want to work with complete fields but $K$ comes with a bunch of different places. The solution is to complete $K$ at *every place at once* and combine the information into the adele ring and idele group. Then we will get statements for global class field theory that resemble local class field theory, with $K^\times$ replaced by $\mathbf{C}_K$, a group related to the idele group (to be defined).

**Definition 5.1:** Abbreviate $\mathcal{O}_v = \mathcal{O}_{K_v}$. The **adele ring** of $K$ is

$$\mathbb{A}_K = \left\{ (a_v) \in \prod_{v \in V_K} K_v : a_v \in \mathcal{O}_v \text{ for all but finitely many } v \right\}.$$

We write this as $\prod'_{v\in V_K}(K_v, \mathcal{O}_v)$. Equip it with a topology by letting a basis for open sets be $\prod_v U_v$, where $U_v$ is open in $K_v$ for all $v$ and $U_v = \mathcal{O}_v$ for almost all $v$. In other words, it is the unique topology from which $\prod_v \mathcal{O}_v$ inherits the product topology and is open.

The **idele group** of $K$ is the group of units of the above:

$$\mathbb{I}_K = \mathbb{A}_K^\times = \prod_{v \in V_K}{}' (K_v^\times, \mathcal{O}_v^\times) = \left\{ (a_v) \in \prod_{v \in V_K} K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

Equip it with a topology by letting a basis for open sets be $\prod_v U_v$, where $U_v$ is open in $K_v^\times$ for all $v$ and $U_v = \mathcal{O}_v^\times$ for almost all $v$. In other words, it is the unique topology from which $\prod_v \mathcal{O}_v^\times$ inherits the product topology and is open.

Be careful: the topology of the idele group is not the subspace topology induced from the adele ring.

**Definition 5.2:** For a finite set $S$ containing all infinite places, let $\mathbb{I}_K^S = \prod_{v\in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$. In other words, $\mathbb{I}_K^S$ contains those ideles that are units away from $S$. Give $\mathbb{I}_K^S$ the subspace topology inherited from $\mathbb{I}_K$.

Note the topology on $\mathbb{I}_K^S$ is just the product topology, and that $\mathbb{I} = \bigcup_S \mathbb{I}_K^S$.

**Proposition 5.3:** $\mathbb{I}_K^S$ is locally compact.

*Proof.* $\prod_{v\in S} K_v^\times$ is a finite product of locally compact spaces; $\prod_{v\notin S} \mathcal{O}_v^\times$ is a product of compact spaces (Proposition 8.1.3) so compact by Tychonoff's Theorem. Since a finite product of locally compact spaces is compact, the result follows. □

Think of the ideles as a thickening of ideals: it includes factors for infinite places, and includes units at finite primes. We can embed $K^\times$ via the diagonal map, and $K_v^\times$ via the inclusion map.

**Definition 5.4:** Define $i : K \hookrightarrow \mathbb{A}_K$ by the diagonal map $i(a) = (a, a, \ldots)$ and $i_v : K_v \hookrightarrow \mathbb{A}_K$ by the inclusion map $i_v(a) = (1, \ldots, 1, \underbrace{a_v}_{v}, 1, \ldots, 1)$. Also denote by $i, i_v$ the maps restricted to $K^\times \hookrightarrow \mathbb{I}_K$ and $i_v : K_v \hookrightarrow \mathbb{I}_K$.

**Proposition 5.5:** pr:k-discrete $i(K^\times)$ is discrete in $\mathbb{I}_K$.

*Proof.* Given $a \in K^\times$, let $S$ be set of places contining the infinite places and the finite places where $v(a) \neq 0$. Consider the open set

$$U = \{\mathbf{x} \in \mathbb{I}_K : |x_v - a|_v < \varepsilon \text{ for } v \in S,\ x_v \in U_v \text{ for } v \notin S\}$$

containing $i(a)$. If $i(b) \in U$ with $a \neq b$, then

$$\prod_v |b - a|_v < \varepsilon^{|S|} < 1,$$

contradicting the product formula 8.6.2. Hence $i(K^\times) \cap U = \{i(a)\}$. □

**Definition 5.6:** The **idele class group** is defined to be

$$\mathbf{C}_K = \mathbb{I}_K / K^\times,$$

where $K^\times$ is thought of as a subgroup of $\mathbb{I}_K$ by the diagonal map $i$.

We define a norm on adeles by defining it componentwise.

**Definition 5.7:** The **norm**, from $L$ to $K$ is the function $\mathrm{Nm}_{L/K} : \mathbb{A}_L \to \mathbb{A}_K$ defined by

$$\mathrm{Nm}_{L/K}\left((x_w)_{w \in V_L}\right) = \left(\prod_{w|v} \mathrm{Nm}_{L_w/K_v}(x_w)\right)_{v \in V_K}.$$

This descends to a function $\mathrm{Nm}_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$.

## 5.1 Ray class groups vs. ideles

We will need the following to go between the interpretations of global class field theory via ray class groups and via ideles. The statement in terms of ray class groups is easier for concrete applications, but the statement in terms of ideles is better abstractly, and more convenient to prove. (But to complicate things more, certain parts of the proof will be easier to think of in terms of ray class groups.)

We can go from $\mathbb{I}_K \to I_K$ easily, via the map

$$eq : idele - to - ideal p(\mathbf{a}) = \prod_{v = v_\mathfrak{p} \text{ finite}} \mathfrak{p}^{v(a_v)} \tag{10.3}$$

(also denoted simply $(\mathbf{a})$). However, if we want the image to be in $I_K^{S(\mathfrak{m})}$, we need to focus our attention on a subset of ideles $\mathbb{I}_K(1, \mathfrak{m})$ (defined below). Taking the map $\mathbb{I}_K(1, \mathfrak{m}) \to I_K^{S(\mathfrak{m})}$ and modding out by appropriate groups then makes it a bijection. We also need to check that we don't lose anything when we consider only ideles of the form $\mathbb{I}_K(1, \mathfrak{m})$; that is, that the inclusion $\mathbb{I}_K(1, \mathfrak{m}) \hookrightarrow \mathbb{I}_K$ is a bijection, again after modding out by appropriate groups. This is Proposition 5.9 below.

**Definition 5.8:** df:more-idele-dfs For a place $v \mid \mathfrak{m}$, define

$$I(\mathfrak{m})_v = \begin{cases} \mathbb{R}_{>0}, & v \text{ real} \\ 1+\mathfrak{p}^{m(\mathfrak{p})}, & v = v_{\mathfrak{p}} \text{ finite.} \end{cases}$$

Let $\mathcal{O}_v^\times$ be the group of units of $K_v$. (For $v$ infinite, $\mathcal{O}_v^\times := K_v^\times$). Define

$$eq: ik1m \mathbb{I}_K(1,\mathfrak{m}) = \prod_{v\mid\mathfrak{m}} I(\mathfrak{m})_v \times {\prod_{v\nmid\mathfrak{m}}}' (K_v^\times, \mathcal{O}_v^\times) \tag{10.4}$$

$$\mathbb{U}_K(1,\mathfrak{m}) = \prod_{v\mid\mathfrak{m}} I(\mathfrak{m})_v \times \prod_{v\nmid\mathfrak{m}} \mathcal{O}_v^\times$$

$$K(1,\mathfrak{m}) = i(K^\times) \cap \mathbb{I}_K(1,\mathfrak{m}).$$

Let $\mathbb{U}_K := \mathbb{U}_K(1,1)$.

Compare (10.4) to the definition of $P_K(1,\mathfrak{m})$.

**Proposition 5.9:** pr:idele-ray-class We have the following maps.

$$\begin{tikzcd} \mathbb{I}_K(1,\mathfrak{m})/K(1,\mathfrak{m}) \arrow[r, "\cong"] \arrow[d] & \mathbb{I}_K/K^\times = \mathbf{C}_K \\ \mathbb{I}_K(1,\mathfrak{m})/K(1,\mathfrak{m})\mathbb{U}_K(1,\mathfrak{m}) \arrow[r, "\cong"] & C_K(\mathfrak{m}). \end{tikzcd}$$

The bottom map is induced by the map $p : \mathbb{I}_K \to I_K^{\mathfrak{m}}$ and the top map is induced by inclusion.

Moreover, for any finite Galois $L/K$ such that

$$\mathbb{U}_K(1,\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K}(\mathbb{I}_L),$$

this diagram induces isomorphisms

$$\begin{tikzcd} \mathbb{I}_K(1,\mathfrak{m})/[K^\times \mathrm{Nm}_{L/K}\mathbb{I}_L \cap \mathbb{I}_K(1,\mathfrak{m})] \arrow[r, "\cong"] \arrow[dr, "\cong"] & \mathbb{I}_K/K^\times \mathrm{Nm}_{L/K}\mathbb{I}_L \\ & I_K^{\mathfrak{m}}/(P_K(1,\mathfrak{m}) \cdot \mathrm{Nm}_{L/K}(I_L^{\mathfrak{m}})). \end{tikzcd}$$

*Proof.* For the bottom map, consider the exact sequence

$$0 \to K^\times \cap \mathbb{I}_K(1,\mathfrak{m}) = K(1,\mathfrak{m}) \xrightarrow{i} \mathbb{I}_K(1,\mathfrak{m}) \xrightarrow{p} I^{S(\mathfrak{m})} \to 0.$$

We have that $\mathbb{I}_K(1,\mathfrak{m})/K(1,\mathfrak{m}) = \operatorname{coker} i$, so we use the kernel-cokernel sequence.[1] We have $\ker p = \mathbb{U}_K(1,\mathfrak{m})$, and $\operatorname{coker} p \circ i = I^{S(\mathfrak{m})}/p(K(1,\mathfrak{m})) = I^{S(\mathfrak{m})}/P_K(1,\mathfrak{m}) = C_K(\mathfrak{m})$, so this

[1]Given $A \xrightarrow{f} B \xrightarrow{g} C$, there is an exact sequence

$$0 \to \ker f \to \ker g\circ f \to \ker g \to \operatorname{coker} f \to \operatorname{coker} g \circ f \to \operatorname{coker} g \to 0.$$

This is proven using the snake lemma.

gives the exact sequence

$$\mathbb{U}_K(1,\mathfrak{m}) \to \mathbb{I}_K(1,\mathfrak{m})/K(1,\mathfrak{m}) \to C_K(\mathfrak{m}) \to 1,$$

which gives the bottom isomorphism.

The top map is clearly injective. For surjectivity, take $a \in \mathbb{I}_K$. By the weak approximation theorem 7.3.4, there exists $b$ so that $\frac{a_v}{b_v} \in \mathfrak{p}^{m(\mathfrak{p})}+1$ for every $v = v_{\mathfrak{p}}$ dividing $\mathfrak{m}$. Then $\frac{a}{b} \in \mathbb{I}_K(1,\mathfrak{m})$, and its image varies in $\mathbb{I}_K$ from $a$ by the constant factor $b \in K^\times$.

Now we show the second diagram. (Warning: this proof is not very enlightening.) Let $p$ and $p'$ denote the maps $\mathbb{I}_K \to I_K$ and $\mathbb{I}_K(1,\mathfrak{m}) \to I_K^S$, respectively. Note that the first diagram gives isomorphisms

$$\begin{tikzcd}
\mathbb{I}_K(1,\mathfrak{m})/((K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L)\cap \mathbb{I}_K(1,\mathfrak{m})) \arrow[r, "\cong"] \arrow[d] & \mathbb{I}_K/K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L \\
\mathbb{I}_K(1,\mathfrak{m})/K(1,\mathfrak{m})\mathbb{U}_K(1,\mathfrak{m})p'^{-1}(\operatorname{Nm}_{L/K}(I_L^{\mathfrak{m}})) \arrow[r, "\cong"] & I_K^{\mathfrak{m}}/(P_K(1,\mathfrak{m})\cdot \operatorname{Nm}_{L/K}(I_L^{\mathfrak{m}})).
\end{tikzcd}$$

We have that

$$K(1,\mathfrak{m})\mathbb{U}_K(1,\mathfrak{m})p'^{-1}(\operatorname{Nm}_{L/K}(I_L^S)) \tag{10.5}$$

$$eq:irc1 = K(1,\mathfrak{m})\mathbb{U}_K(1,\mathfrak{m})p'^{-1}(\langle \mathfrak{p}^{f(w/v)} \mid w \mid v \notin S\rangle), \qquad f_v = \text{residue degree} \tag{10.6}$$

$$eq:irc2 = K(1,\mathfrak{m})\mathbb{U}_K(1,\mathfrak{m})(\mathbb{I}_K(1,\mathfrak{m})\cap \mathbb{U}_K \operatorname{Nm}_{L/K}(\mathbb{I}_L)) \tag{10.7}$$

$$eq:irc3 = \mathbb{U}_K(1,\mathfrak{m})(\mathbb{I}_K(1,\mathfrak{m})\cap (K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L)) \tag{10.8}$$

$$eq:irc4 = (K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L)\cap \mathbb{I}_K(1,\mathfrak{m}). \tag{10.9}$$

(10.6) follows from the fact that if $\mathfrak{P} \mid \mathfrak{p}$, then $\operatorname{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$. To go between (10.6) and (10.7), note that $\mathfrak{p}^{f(w/v)} = p(\operatorname{Nm}_{L/K}(1,\ldots,1,\underbrace{\pi_w}_{w},1,\ldots,1))$, and that $\ker(p) = \mathbb{U}_K$.

Now we go between (10.7) and (10.8). For "$\subseteq$," suppose $a \in \mathbb{U}_K$ and $b \in \operatorname{Nm}_{L/K}(\mathbb{I}_L)$ such that $a\operatorname{Nm}_{L/K} b \in \mathbb{I}_K(1,\mathfrak{m})$. Suppose $c$ agrees with $a$ for every $v \mid \mathfrak{m}$, and is 1 everywhere else. Then $ac^{-1} \in \mathbb{U}_K(1,\mathfrak{m}) \subseteq \mathbb{I}_K(1,\mathfrak{m})$. Since $a\operatorname{Nm}_{L/K} b \in \mathbb{I}_K(1,\mathfrak{m})$ as well and $\mathbb{I}_K(1,\mathfrak{m})$ is a group, we must have $c\operatorname{Nm}_{L/K} b \in \mathbb{I}_K(1,\mathfrak{m})$. Hence

$$a\operatorname{Nm}_{L/K} b = \underbrace{ac^{-1}}_{\in \mathbb{U}_K(1,\mathfrak{m})} \underbrace{c\operatorname{Nm}_{L/K} b}_{\in \mathbb{I}_K(1,\mathfrak{m})\cap(K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L)},$$

as needed. Furthermore note $K(1,\mathfrak{m}) \subseteq \mathbb{I}_K(1,\mathfrak{m})\cap K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L$. For "$\supseteq$," suppose $a \in K^\times$ and $b \in \operatorname{Nm}_{L/K}(\mathbb{I}_L)$ such that $a\operatorname{Nm}_{L/K} b \in \mathbb{I}_K(1,\mathfrak{m})$. By weak approximation, take $c \in K^\times$ sufficiently close to $\frac{1}{b_v}$ with respect to $v$, for every $v \in \mathfrak{m}$, so that $\operatorname{Nm}_{L/K}(cb) \in \mathbb{I}_K(1,\mathfrak{m})$. Then $a\operatorname{Nm}_{L/K}(c^{-1}) \in \mathbb{I}_K(1,\mathfrak{m})$ as well, and in fact in $K(1,\mathfrak{m})$. Then

$$a\operatorname{Nm}_{L/K} b = \underbrace{a\operatorname{Nm}_{L/K}(c^{-1})}_{\in K(1,\mathfrak{m})} \underbrace{\operatorname{Nm}_{L/K} cb}_{\in \mathbb{I}_K(1,\mathfrak{m})\cap \operatorname{Nm}_{L/K}\mathbb{I}_L},$$

as needed.

The last step (10.9) follows from the assumption on $\mathfrak{m}$. ∎

**Example 5.10:** ex:class-group-idele-quotient Recall how we realized the class group and narrow class group as ray class groups in Example 3.4. We now realize them as quotients of the idele class group.

Take $\mathfrak{m}$ to be 1. Then the bottom map gives an isomorphism

$$\mathbb{I}_K/K^\times\mathbb{U}_K \cong C_K$$

where $C_K$ is just the class group of $K$. *This realizes the class group of $K$ as a quotient of the idele class group.*

In general, for any modulus $\mathfrak{m}$,

$$\mathbb{I}_K/K^\times\mathbb{U}_K(1,\mathfrak{m}) \cong \mathbb{I}_K(1,\mathfrak{m})/K(1,\mathfrak{m})\mathbb{U}_K(1,\mathfrak{m}) \cong C_K(\mathfrak{m}).$$

This realizes the ray class group modulo $\mathfrak{m}$ as a quotient of the idele class group.

In particular, $\mathfrak{m} = 1$ was the case above. Taking $\mathfrak{m} = \prod_{v \text{ real}} v$, $P_K(1,\mathfrak{m})$ is the group of principal ideals generated by totally positive elements (also written $P_K^+$) and $\mathbb{U}_K(1,\mathfrak{m}) = \prod_{v \text{ real}} \mathbb{R}_{>0} \times \prod_v \mathcal{O}_v^\times$. *This realizes the narrow class group of $K$ as a quotient of the idele class group.*

**Remark:** rem:S-ramify The condition on $\mathfrak{m}$ in Proposition 5.9 was that $\mathbb{U}_K(1,\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K}(\mathbb{I}_L)$. We claim that we can always choose such $\mathfrak{m}$, such that $S(\mathfrak{m})$ consists of exactly the primes ramifying in $L/K$.

The condition $\mathbb{U}_K(1,\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K}(\mathbb{I}_L)$ says that $\mathcal{O}_v^\times \subseteq \mathrm{Nm}_{L^v/K_v}(L^v)$ for all $v \nmid \mathfrak{m}$ and $I(\mathfrak{m})_v \subseteq \mathrm{Nm}_{L^v/K_v}(L^v)$ for all $v \mid \mathfrak{m}$. Now note the following.

1. If $L/K$ is unramified at $v$, i.e. $L^v/K_v$ is unramified, then

   $$\mathrm{Nm}_{L^v/K_v}(L^{v\times}) = \pi_v^{[L^v:K_v]\mathbb{Z}}\mathcal{O}_v^\times \supseteq \mathcal{O}_v^\times.$$

   This is a consequence of local class field theory (Example 13.5.1).

2. $\mathrm{Nm}_{L^v/K_v}(L^v)$ is an open subgroup of $K_v$ (this is the easy direction in Theorem 2.3) and $U_v^{(n)} := 1 + \pi_v^n\mathcal{O}_v$ is a neighborhood base of 1 in $K_v$.

By item 1, $\mathfrak{m}$ doesn't need to include the places where $L/K$ is unramified, and by item 2, for all ramified $v$ we can choose the power of $v$ in $\mathfrak{m}$ large enough to force $U_v^{(n)} \subseteq \mathrm{Nm}_{L^v/K_v}(L^{v\times})$. Then we will have $\mathbb{U}_K(1,\mathfrak{m}) \subseteq \mathrm{Nm}_{L/K}(\mathbb{I}_L)$.

# §6 Global reciprocity via ideles

sec:global-reciprocity-via-ideles We now state global reciprocity in terms of ideles.

**Theorem 6.1** (Global reciprocity, ideles)**:** thm:global-reciprocity-ideles Given a finite abelian extension $L/K$, there is a unique continuous[2] homomorphism $\phi_{L/K}$ that is compatible with the local Artin maps, i.e. the following diagram commutes[3]:

$$\begin{tikzcd} \mathbb{I}_K \arrow[r, "\phi_{L/K}"] & G(L/K) \\ K_v^\times \arrow[u, hook, "i_v"] \arrow[r, two heads, "\phi_v"] & G(L^v/K_v). \arrow[u, hook] \end{tikzcd}$$

Moreover, $\phi_{L/K}$ satisfies the following properties.

1. (Isomorphism) For every finite abelian extension $L/K$, $\phi_K$ defines an isomorphism

$$\phi_{L/K} : \mathbf{C}_K / \operatorname{Nm}_{L/K}(\mathbf{C}_L) = \mathbb{I}_K/(K^\times \cdot \operatorname{Nm}_{L/K}(\mathbb{I}_L)) \xrightarrow{\cong} G(L/K).$$

2. (Compatibility over all extensions) For $L \subseteq M$, $L, M$ both finite abelian extensions of $K$, the following commutes:

$$\begin{tikzcd} & G(M/K) \arrow[d, "p_L"] \\ \mathbb{I}_K \arrow[ur, "\phi_{M/K}"] \arrow[r, "\phi_{L/K}"] & G(L/K) \end{tikzcd}$$

   Thus we can define $\phi_K := \varprojlim_{L/K \text{ abelian}} \phi_{L/K}$ as a map $\mathbb{I}_K \to G(K^{\text{ab}}/K)$.

3. (Compatibility with norm map) $\phi_K$ is a continuous homomorphism $\mathbb{I}_K \to G(K^{\text{ab}}/K)$, and the following commutes.

$$\begin{tikzcd} \mathbb{I}_L \arrow[r, "\phi_L"] \arrow[d, "\operatorname{Nm}_{L/K}"] & G(L^{\text{ab}}/L) \arrow[d, "\bullet|_{K^{\text{ab}}}"] \\ \mathbb{I}_K \arrow[r, "\phi_K"] & G(K^{\text{ab}}/K) \end{tikzcd}$$

Note that in the local reciprocity theorem 2.1, the "compatibility over all extensions" was automatic when we declared the existence of $\phi_K : K^\times \to G(K^{\text{ab}}/K)$. We stated the global reciprocity theorem a bit differently, in the above fashion for easy comparison with global reciprocity in terms of ideals 4.1.

**Remark:** rem:gcft Uniqueness and existence of $\phi_{L/K}$ is easy, and parts 2 and 3 are easy given the existence of $\phi_L$. The crux of the theorem is again part 1.

[2] $G(L/K)$ is given the discrete topology.

[3] This implies that if $v = v_{\mathfrak{p}}$ is unramified in $L$, then $\phi_{L/K}(i_v(\pi_v)) = \operatorname{Frob}_{L/K}(\mathfrak{p})$. Global reciprocity is sometimes phrased in this way, though the phrasing using the local map gives a bit more information.

For uniqueness, note that the $\phi_{L/K}$ is determined by its action on $K_v^\times$, since for $\mathbf{x} = (x_v)$, we must have
$$\phi_{L/K}(\mathbf{x}) = \prod_{v \in V_K} \phi_v(x_v).$$
(The product is Cauchy in the topology of $\mathbb{I}_K$.) This does define a continuous map on $\mathbb{I}_K$ because $\phi_v(x_v) = 1$ whenever $x_v \in \mathcal{O}_v^\times$ and $v$ is unramified, and this happens for all but finitely many $v$.

Parts 2 and 3 follow from the corresponding statements for local class field theory (see Theorem 2.1 and the paragraph above this remark), by how $\phi$ is defined to be compatible with the local maps.

The idele version of global reciprocity allows us to recast the Existence Theorem 4.3 in a format more similar to the Existence Theorem in 2.3.

**Theorem 6.2** (Existence theorem)**:** thm:global-et-ideles For every subgroup $N \subseteq \mathbf{C}_K$ of finite index, there exists a unique abelian extension $L/K$ such that $\mathrm{Nm}_{L/K}\, \mathbf{C}_L = N$.

Combining the two theorems, we can recast the bijective correspondence in Theorem 4.6 in a format more similar to local class field theory 2.5.

**Theorem 6.3:** thm:gcft-bijection The map $L \mapsto \mathrm{Nm}_{L/K}(\mathbf{C}_L)$ is an inclusion-reversing bijection between the set of finite abelian extensions of $K$ and the open subgroups of finite index in $\mathbf{C}_K$, that switches intersections and products:
$$\begin{aligned} L \subseteq M &\iff \mathrm{Nm}_{L/K}(\mathbf{C}_L) \supseteq \mathrm{Nm}_{M/K}(\mathbf{C}_M) \\ \mathrm{Nm}_{L_1L_2/K}(\mathbf{C}_{L_1L_2}) &= \mathrm{Nm}_{L_1/K}(\mathbf{C}_{L_1}) \cap \mathrm{Nm}_{L_2/K}(\mathbf{C}_{L_2}) \\ \mathrm{Nm}_{L_1\cap L_2/K}(\mathbf{C}_{L_1\cap L_2}) &= \mathrm{Nm}_{L_1/K}(\mathbf{C}_{L_1}) \cdot \mathrm{Nm}_{L_2/K}(\mathbf{C}_{L_2}). \end{aligned}$$

Similar to Theorem 2.4, we have the following topological isomorphism for global class field theory.

**Theorem 6.4** (Topological isomorphism for GCFT)**:** thm:gcft-topology Let $K$ be a number field. Let
$$(K_\infty^\times)^0 := \prod_{v \text{ real}} \mathbb{R}_{>0} \times \prod_{v \text{ complex}} \mathbb{C} \times \prod_{v \in V_K^0} 1.$$
The Artin map $\phi_K$ is surjective and induces a topological isomorphism
$$\mathbb{I}_K / \overline{K^\times (K_\infty^\times)^0} \cong G(K^{\mathrm{ab}}/K).$$

## 6.1 Connecting the two formulations

sec:connecting-formulations We now show that the two formulations of global class field theory are equivalent, in the following sense.

**Theorem 6.5:** thm:gcft-equivalent We have the following implications.

1. (Global reciprocity, ideles $\Longrightarrow$ ideals) If Theorem 6.1(1) holds for a given $L/K$, then Theorem 4.1(1) holds for $L/K$. If Theorem 6.1 holds for all $L/K$ over a specified basefield (e.g. $\mathbb{Q}$), then Theorem 4.1 holds for all such $L/K$.

2. (Global reciprocity, ideals $\Longrightarrow$ (ideles)$-\varepsilon$) If Theorem 6.1(1)-(2) holds for a fixed $K$ and a family $\{L/K\}$ such that the compositum of the $L^v$ contains $K_v^{\mathrm{ur}}$ for every finite place $v$, then Theorem 6.1(1)-(2) holds for the same $K$ and $\{L/K\}$, except that the resulting map $\phi_{L/K}$ may not be compatible with $\phi_v$ when $v$ is archimedean.

3. (Global existence) Given Theorem 6.1, Theorems 4.3 and 6.2 are equivalent.

4. (Bijective correspondence) Given Theorem 6.1, Theorems 4.6 and 6.3 are equivalent.

*Proof.* For parts 1 and 2, we note that by Proposition 5.9,

$$eq:gcft-equivalent\mathbf{C}_K/\operatorname{Nm}_{L/K}\mathbf{C}_L=\mathbb{I}_K/K^\times\operatorname{Nm}_{L/K}\mathbb{I}_L\cong I_K^S/P_K(1,\mathfrak{m})\operatorname{Nm}_{L/K}(I_L^S), \tag{10.10}$$

where by Remark 5.1, we can choose $\mathfrak{m}$ to some modulus containing only ramified primes, and $S=S(\mathfrak{m})$. Thus any one of the dotted isomophisms below gives the other isomorphism.

$$gcft-equivalent2 \quad \begin{tikzcd} \mathbb{I}_K/K^\times\operatorname{Nm}_{L/K}(\mathbb{I}_L) \arrow[dd, "p"', "\cong"] \arrow[dr, dotted, "\cong", "\phi_{L/K}"'] & \\ & G(L/K) \\ I_K^S/P_K(1,\mathfrak{m})\operatorname{Nm}_{L/K}(I_L^S) \arrow[ur, dotted, "\psi_{L/K}", "\cong"'] & \end{tikzcd} \tag{10.11}$$

For part 1, given $\phi_{L/K}$, we define $\psi_{L/K}$ with the above diagram. Then, supposing $\mathfrak{p}$ corresponds to the uniformizer $\pi_v\in K_{\mathfrak{p}}$,

$$\psi_{L/K}(\mathfrak{p})=\psi_{L/K}(p(i(\pi_v)))=\phi_{L/K}(i(\pi_v))=\phi_v(\pi_v)=\operatorname{Frob}_{L^v/K_v}((\pi_v))=\operatorname{Frob}_{L/K}(\mathfrak{p}),$$

as needed. Part 2 is a more complicated; we'll give the proof below after a lemma. The "$-\varepsilon$" comes from the fact that the formulation in Theorem 6.1 says nothing about archimedean primes.

Parts 3 and 4 now result directly from the fact that (10.10) gives a bijective correspondence between subgroups of two groups. $\square$

**Lemma 6.6:** lem:local-uniqueness Suppose that $K$ is a nonarchimedean local field, $K^{\mathrm{ur}}$ is the maximal abelian unramified extension of $K$, and $L$ is an abelian extension containing $K^{\mathrm{ur}}$. Let $f:K^\times\to G(L/K)$ be a homomorphism satisfying (1) and either (2) or (2)′:

1. The composition $K^\times\xrightarrow{f}G(L/K)\to G(K^{\mathrm{ur}}/K)$ takes $\alpha$ to $\operatorname{Frob}_{K^{\mathrm{ur}}/K}(\pi)^{v(\alpha)}$.

2. For any uniformizer $\pi \in K$, $f(\pi)|_{K_\pi} = 1$, where
$$K_\pi := L^{\phi_K(\pi)}.$$

2'. For any finite subextension $K'/K$ of $K_\pi$, we have
$$f(\mathrm{Nm}_{K'/K}(K'^\times))|_{K'} = \{1\}.$$

Then $f$ equals the reciprocity map $\phi_K$.

For the proof, see Section 13.8.1.

*Proof of Theorem 6.5, Part 2.* Given $\psi_{L/K}$ we define $\phi_{L/K}$ using (10.11). The $\psi_{L/K}$ are compatible by Remark (4), so the $\phi_{L/K}$ are compatible (details omitted) and we can define $\phi_K = \varprojlim_{L/K} \phi_{L/K}$ where the limit is over $L/K$ in the given family. Let $L'$ be the compositum of the fields $L$.

We check the hypotheses 1 and $2'$ of Lemma 6.6. Let
$$f_v = \phi_K \circ i_v : K_v^\times \to G(L'^v/K_v).$$
Item 1 is clear as (10.11) gives letting $v = v_\mathfrak{p}$, we have
$$\phi_K(i_v(\alpha))|_{K_v^{\mathrm{ur}}} = \psi_K(\mathfrak{p}^{v(\alpha)})|_{K_v^{\mathrm{ur}}} = \mathrm{Frob}_{K_v^{\mathrm{ur}}/K_v}(\alpha)^{v(\alpha)}.$$
Item $2'$ follows from part 3 of Theorem 4.1 applied to $K'/K$ (see Remark 4): we get $\psi_{L/K}(\mathrm{Nm}_{K'/K}(I_{K'}^S))|_{K'} = 1$ which translates into $\phi_K(i_v(\mathrm{Nm}_{K_v'/K_v}(K_v'^\times)))|_{K_v'} = 1$. Thus $f_v = \phi_v$ for all finite places, as needed. □

We have proved the ideal version of global class field theory for cyclotomic extensions of $\mathbb{Q}$. Our plan of attack will be to show transfer this to the idele version for cyclotomic extension of $\mathbb{Q}$, then work on proving the idele version. Then we will be done by Theorem 6.5.

# §7 Kronecker-Weber Theorem

kw As a first application of class field theory, we explicitly describe the maximal abelian extensions of $\mathbb{Q}_p$ and $\mathbb{Q}$.

**Theorem 7.1** (Local Kronecker-Weber theorem)**:** lkwt Every abelian extension of $\mathbb{Q}_p$ is included in a cyclotomic extension, i.e. an extension $\mathbb{Q}_p(\zeta_n)$, $\zeta_n$ a primitive $n$th root of unity, for some $n$. In other words,
$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\zeta_n \mid n \in \mathbb{N}).$$

**Theorem 7.2** (Kronecker-Weber theorem)**:** kwt Every abelian extension of $\mathbb{Q}$ is included in a cyclotomic extension $\mathbb{Q}(\zeta_n)$. In other words,
$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_n \mid n \in \mathbb{N}).$$

*Proof of Theorem 7.1.* Consider $\mathbb{Q}_p(\zeta_k)$ where $p \nmid k$. Let $U$ denote the group of units. As $\mathbb{Q}_p(\zeta_k)$ is unramified, local class field theory tells us

$$\mathrm{Nm}_{\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_k)^\times) \cong \pi^{[\mathbb{Q}_p(\zeta_k):\mathbb{Q}_p]\mathbb{Z}}U.$$

Consider $\mathbb{Q}_p(\zeta_{p^m})$, which is totally ramified of degree $p^{m-1}(p-1)$ over $\mathbb{Q}_p$. Local reciprocity gives

$$\mathbb{Q}_p^\times / \mathrm{Nm}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_{p^m})^\times) \xrightarrow{\cong} G(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p).$$

Thus both sides have the same order, $p^{m-1}(p-1)$, and we must have

$$\mathrm{Nm}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_{p^m})^\times) = U^{(m)} := p^{\mathbb{Z}}(1+(p^m)).$$

Suppose $L/\mathbb{Q}_p$ is an abelian extension. Its corresponding norm group $N$ is open of finite index in $\mathbb{Q}_p$, so contains

$$p^{n\mathbb{Z}}(1+(p^m))$$

for some $n, m$. Choosing $k$ large enough we may suppose $n \mid [\mathbb{Q}_p(\zeta_k) : \mathbb{Q}_p]$. Then using Theorem 2.5[4],

$$N \supseteq \mathrm{Nm}(\mathbb{Q}_p(\zeta_n)^\times) \cap \mathrm{Nm}(\mathbb{Q}_p(\zeta_{p^m})^\times) = \mathrm{Nm}(\mathbb{Q}_p(\zeta_{np^m})^\times).$$

By Theorem 2.5, we get that $\mathbb{Q}_p(\zeta_{np^m}) \supseteq L$. □

*Proof of Theorem 7.2.* Given an abelian extension $K/\mathbb{Q}$, choose a modulus $\mathfrak{m}$ so that the Artin map is defined. Every modulus for $\mathbb{Q}$ divides $\infty(n)$ for some integer $n$. The ray class field of $\infty(n)$ is $\mathbb{Q}(\zeta_n)$. If $\mathfrak{m}$ divides $\infty(n)$, then $K$ is contained in $\mathbb{Q}(\zeta_n)$. Hence the maximal abelian extension is the union of all the $\mathbb{Q}(\zeta_n)$. □

We can similarly ask how to characterize abelian extensions of other number fields $K$. This is Hilbert's Twelfth Problem and Kronecker's Jugendtraum. Note that another way to phrase this theorem is the following:

1. $\mathbb{Q}^{\mathrm{ab}}$ is generated by the *torsion points* of $\mathbb{Q}^\times$ under multiplication.

2. Let $f(z) = e^{2\pi i z}$. Then $\mathbb{Q}^{\mathrm{ab}}$ is generated by $f(\mathbb{Q})$:

$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(f(\mathbb{Q})).$$

We can ask: for given $K$, can we get $K^{\mathrm{ab}}$ by adjoining torsion points of some algebraic variety, and does there exist a nice function $g(z)$ parameterizing this variety, so that

$$K^{\mathrm{ab}} \approx K(g(K))?$$

It turns out that the answer is affirmative for quadratic extensions: roughly speaking, the maximal abelian extension is generated by torsion points of elliptic curves with complex multiplication. We will give a complete solution to this problem in Chapter 16.

[4] omitting the subscripts on norms to avoid clutter

# §8 Problems

1.1 Why can't we define $\text{Frob}_\mathfrak{p} \in G(L/K)$ when $\mathfrak{p}$ is a prime in $K$ that is ramified in $L$?

1.2 Fix $n \in \mathbb{N}$.

(a) For which primes $p \in \mathbb{Z}$ does $(p)$ split completely in $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$? (Be careful with $p = 2$.)

(b) Show that the ray class field of $(n)$ is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

1.3 (IberoAmerican Olympiad for University Students, 2010/6) Prove that, for all integers $a > 1$, the prime divisors of $5a^4 - 5a^2 + 1$ have the form $20k \pm 1$.

1.4 Consider the field extension $\mathbb{Q}(\sqrt[3]{d}, \zeta_3)/\mathbb{Q}$ where $d \in \mathbb{Z}$ is not a perfect cube. Let $p$ be a prime relatively prime to $3d$. Prove that a prime $p$ splits into $n$ factors in $\mathbb{Q}(\sqrt[3]{d}, \zeta_3)$, where

$$n = \begin{cases} 2, & p \equiv 1 \pmod 3 \text{ and } d \text{ is a cube modulo } p \\ 3, & p \equiv 1 \pmod 3 \text{ and } d \text{ is not a cube modulo } p \\ 6, & p \equiv 2 \pmod 3. \end{cases}$$

2.1 Recall that $G(\overline{K}/K)$ has profinite (Krull) topology. Topologically $W(\overline{K}/K)$ is a $\mathbb{Z}$-disjoint union of $G(\overline{K}/K)_0$-cosets $G(\overline{K}/K)_0\sigma_n$, where $\sigma_n$ is any lift of $\text{Frob}_q^n$, $n \in \mathbb{Z}$, where each $G(\overline{K}/K)_0\sigma_n$ is given the same topology as the profinite topology on $G(\overline{K}/K)_0$ via translation by $\sigma_n$.

(a) Show that the natural inclusion $\iota : W(\overline{K}/K) \to G(\overline{K}/K)$ is continuous and has dense image.

(b) Show that $\iota$ is not a topological isomorphism onto $\iota(W(\overline{K}/K))$, where the latter is equipped with the topology induced by that of $G(\overline{K}/K)$.

4.1 There is a correspondence between quadratic characters (homomorphisms $\chi : (\mathbb{Z}/m)^\times \to \mathbb{C}$ such that $\chi^2 = 1, \chi \not\equiv 1$, where characters are naturally identified by restriction) and quadratic extensions,

(a) Prove this without using the statement of class field theory.

(b) How does CFT give the result?

(c) Using CFT for quadratic extensions, prove quadratic reciprocity.

4.2 Characterize all quadratic extensions $K/\mathbb{Q}$ that are contained in a $\mathbb{Z}/4$-extension. (Ben Blum-Smith, from http://math.stackexchange.com/questions/596195/ conceptual-reason-why-a-quadratic-field-has-1-as-a-norm-if-and-only-if

# Chapter 11
# Group homology and cohomology

group-hom-cohom In this chapter we introduce the theory of group homology and cohomology. In the next chapter we'll specialize to the case of Galois groups, and then we'll use Galois cohomology to prove the theorems of class field theory. Some results in this chapter will be given without proof; for detailed proofs see Rotman [12]. We assume knowledge of some basic terminology and facts from category theory and commutative algebra (covariant and contravariant functors, natural transformations, left and right exactness).

The idea of homology and cohomology—used in many different areas of mathematics—is that after applying a functor, a short exact sequence of modules may no longer be exact. Instead, we get the *long exact sequence in (co)homology*, with the (co)homology groups measuring the deviation from exactness.

Exactly what functors are we applying? In group cohomology (Section 6), we apply $\mathrm{Hom}_G(\mathbb{Z}, \bullet)$, turning a short exact sequence of $G$-modules

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

into

$$les - intro 0 \to A^G \to B^G \to C^G \to H^1(G, A) \to \cdots \tag{11.1}$$

where $A^G$ is the submodule of $A$ fixed by $G$. In the next chapter we will take $A, B, C$ to be a multiplicative or additive subgroup of a field $L$, and $G = G(L/K)$. Then $A^G$ is just $A \cap K$. Thus we see that the sequence (11.1) gives information about the relationship between a field $K$ and an extension field. For example, in Kummer Theory 12.2, we take $C = L^{\times n}$; then $C^G = L^{\times n} \cap K$, and we can characterize $G(L/K)$ and hence $L/K$ in terms of the $n$th powers of $L$ appearing in $K$. This is representative a general trend in class field theory: characterize extensions of $K$ in terms of information intrinsic to $K$.

We also get a sequence in group homology (Section 8), and we can splice the sequences for homology and cohomology together to get the Tate groups (Section 9). Norm groups will make their appearance here—which is how, in class field theory, we get a correspondence between norm groups and field extensions.

Finally, we assemble a toolbox of other constructions from group cohomology and homology, including cup products (Section 10), changes of group (Section 11), the corestriction map (Section 11.5), results on cyclic groups and the Herbrand quotient (Section 12), and Tate's theorem (Section 13). We include generalizations of cohomology to profinite groups (Section 14) and nonabelian groups (Section 15).

# §1 Projectives and injectives

Let $\mathcal{A}$ be an abelian category.[1] The reader unfamiliar with category theory may assume that $\mathcal{A}$ is the class of $R$-modules, since we will be primarily working with modules throughout.

**Definition 1.1:** Let $\mathcal{A}$ be an abelian category.

1. An object $P \in \mathcal{A}$ is **projective** if for every surjection $p : M \twoheadrightarrow N$ and morphism $f : P \to N$, there exists a unique morphism $g : P \to M$ such that $f = p \circ g$:

$$\begin{tikzcd} & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] \\ M \arrow[r, two heads, "p"'] & N \end{tikzcd}$$

   Equivalently, $\mathrm{Hom}(P, \bullet)$ is exact (or equivalently, right exact as it is always left exact).[2]

2. An object $I \in \mathcal{A}$ is **injective** if for every injection $i : M \hookrightarrow N$ and morphism $f : M \to I$, there exists a unique morphism $g : N \to I$, such that $f = g \circ i$:

$$\begin{tikzcd} M \arrow[r, hook, "i"] \arrow[d, "f"] & N \arrow[dl, dashed, "g"] \\ I & \end{tikzcd}$$

   Equivalently, $\mathrm{Hom}(\bullet, I)$ is exact (or equivalently, just right exact).

**Example 1.2:** A free $R$-module (a direct sum of copies of $R$) is projective.

**Definition 1.3:** An abelian category $\mathcal{A}$ . . .

1. **has enough injectives** if for every object $A \in \mathcal{A}$ there exists an injective object $E$ with a monic (injective) morphism $A \hookrightarrow E$.

2. **has enough projectives** if for every object $A \in \mathcal{A}$ there exists a projective object $P$ with an epic (surjective) morphism $P \twoheadrightarrow A$.

**Definition 1.4:** A **projective resolution** of $A$ is an exact sequence

$$\mathbf{P} : \cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} A \to 0$$

[1] A category is an **abelian category** if it is an additive category such that every morphism has a kernel and cokernel, every monomorphism (injection) is a kernel, and every epimorphism (surjection) is a cokernel.

[2] The diagram is equivalent to saying that if $p : M \twoheadrightarrow N$ is surjective, then so is the map $\mathrm{Hom}(P, M) \xrightarrow{\mathrm{Hom}(\bullet, p)} \mathrm{Hom}(P, N)$, i.e. $\mathrm{Hom}(P, \bullet)$ is right exact.

where each $P_n$ is projective.

An **injective resolution** of $A$ is an exact sequence

$$\mathbf{E} : 0 \to A \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \to \cdots$$

where each $E^n$ is injective.

**Proposition 1.5:** If $\mathcal{A}$ is an abelian category with enough projectives (injectives), then every object has a projective (injective) resolution. In particular, every $R$-module has a projective (injective) resolution.

*Proof.* Build the resolution step-by-step. See Rotman [12], Proposition 6.2-5. For the second part, note that the category of $R$-modules has enough projectives and enough injectives. □

# §2 Complexes

**Definition 2.1:** A **complex** in an abelian category (for example, the category of $R$-modules or abelian groups) is a sequence of morphisms

$$\mathbf{C} : \cdots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \to \cdots$$

such that the composition of any two adjacent morphisms is 0:

$$d_n d_{n+1} = 0.$$

We often work with complexes only going off to the left or right (positive and negative complexes, respectively), and label them

$$\cdots \to C_n \xrightarrow{d_n} C_{n-1} \to \cdots \to C_0 \to 0$$
$$0 \to C^0 \to \cdots \to C^{n-1} \xrightarrow{d^{n-1}} C^n \to \cdots$$

We will want to work with complexes like they are single objects.

**Theorem 2.2:** The class of complexes in $\mathcal{A}$ can be made into an abelian category, $\mathrm{Comp}(\mathcal{A})$ as follows: The objects are the complexes and the morphisms are **chain maps** $f = (f_n) : \mathbf{C} \to \mathbf{C}'$, i.e. a sequence of maps making the following commute.

$$\begin{tikzcd}
{} \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[d, "f_n"] & C_{n-1} \arrow[r, "d_{n-1}"] \arrow[d, "f_{n-1}"] & {} \\
{} \arrow[r] & C'_{n+1} \arrow[r, "d'_{n+1}"] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r, "d'_{n-1}"] & {}
\end{tikzcd}$$

*Proof.* See Rotman [12], Proposition 5.100. □

We will be interested in cohomology and homology modules associated to chain complexes. For this, we have the following notion of what it means for chain maps to be "the same" (See Theorem 3.2).

**Definition 2.3:** Two chain maps $f, g : \mathbf{C} \to \mathbf{C}'$ are **homotopic** if there exist a family of morphisms $s_n : C_n \to C'_{n+1}$ such that

$$f_n - g_n = d'_{n+1} s_n + s_{n-1} d_n.$$

In Section 4 we will define the homology modules and cohomology modules from projective and injective resolutions. To show this does not depend on the choice of projective or injective resolution, we need the following theorem.

**Theorem 2.4** (Comparison Theorem)**:** thm:comparison Let $\mathcal{A}$ be an abelian category, and suppose we have two complexes $\mathbf{C} : \cdots \to P_1 \to P_0 \to A \to 0$ and $\mathbf{C}' : \cdots P'_1 \to P'_0 \to A' \to 0$ and a map $g : A \to A'$. Then there exists a chain map $f$ extending $g$:

$$\begin{tikzcd}
\cdots \arrow[r] & P_1 \arrow[r] \arrow[d, "f_1"] & P_0 \arrow[r] \arrow[d, "f_0"] & A \arrow[r] \arrow[d, dotted, "g"] & 0 \\
\cdots \arrow[r] & P'_1 \arrow[r] & P'_0 \arrow[r] & A' \arrow[r] & 0.
\end{tikzcd}$$

Moreover, $f$ is unique up to homotopy.

The same is true of complexes going off to the right (reverse the arrows above).

*Proof.* Rotman [12], Theorem 6.16. □

# §3 Homology and cohomology

**Definition 3.1:** Given a complex $\mathbf{C}$, define

$$\begin{aligned}
Z_n(\mathbf{C}) &= \ker(d_n) \\
B_n(\mathbf{C}) &= \operatorname{im}(d_{n+1}) \\
H_n(\mathbf{C}) &= Z_n(\mathbf{C})/B_n(\mathbf{C}).
\end{aligned}$$

$H_n$ is called the $n$th **homology module**. For upper indexing, we let $Z^n(\mathbf{C}) = \ker(d^n)$, $B^n(\mathbf{C}) = \operatorname{im}(d^{n-1})$, and $H^n(\mathbf{C}) = Z^n(\mathbf{C})/B^n(\mathbf{C})$, and call $H^n$ the $n$th **cohomology module**.

Think of $H_n$ as measuring how far the complex is from being exact at $C_n$.

**Theorem 3.2:** thm:hn-functor Let $\mathcal{A}$ be an abelian category. For every integer $n$, $H_n$ is an additive functor from $\mathrm{Comp}(\mathcal{A}) \to \mathcal{A}$. Moreover, homotopic chain maps induce the same map in homology.

*Proof.* See Rotman [12], Proposition 6.8. □

**Theorem 3.3** (Long exact sequence)**:** les A short exact sequence of chain complexes

$$0 \longrightarrow \mathbf{C}' \xrightarrow{i} \mathbf{C} \xrightarrow{p} \mathbf{C}'' \longrightarrow 0$$

induces a long exact sequence of homology modules

$$\cdots \longrightarrow H'_n \xrightarrow{i_n} H_n \xrightarrow{p_n} H''_n \xrightarrow{\partial_n} H'_{n-1} \longrightarrow \cdots$$

The map $\partial_n$ is defined by

$$\partial_n[c''_n] = [i_{n-1}^{-1} d_{n-1} p_n^{-1} c''_n] \in C'_{n-1}.$$

*Proof.* Let $H_n = H_n(\mathbf{C})$, $B_n = \operatorname{im}(d^{n+1})$, and $Z_n = \ker(d^n)$ for the complex $\mathbf{C}$, and define $H'_n$, $H''_n$, and so forth similarly. By the Snake Lemma, the gray sequence below is exact.

$$\begin{tikzcd}
 & H'_n \arrow[r] \arrow[d] & H_n \arrow[r] \arrow[d] & H''_n \arrow[d] \arrow[dddll, rounded corners, "\partial_n"] & \\
 & C'_n/B'_n \arrow[r, "i_n"] \arrow[d, "d'_{n-1}"] & C_n/B_n \arrow[r, "p_n"] \arrow[d, "d_{n-1}"] & C''_n/B''_n \arrow[r] \arrow[d, "d''_{n-1}"] & 0 \\
0 \arrow[r] & Z'_{n-1} \arrow[r, "i_{n-1}"] \arrow[d] & Z_{n-1} \arrow[r, "p_{n-1}"] \arrow[d] & Z''_{n-1} \arrow[d] & \\
 & H'_{n-1} \arrow[r] & H_{n-1} \arrow[r] & H''_{n-1} &
\end{tikzcd}$$

Note that the connecting homomorphism is exactly that in the Snake Lemma. □

# §4 Derived functors

sec:derived-functors

## 4.1 Right derived functors and Ext

### 4.1.1 Covariant case

Given an injective resolution of $B$,

$$E^B : \quad 0 \to B \xrightarrow{\eta} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E_2 \xrightarrow{d^2} \cdots,$$

applying a (covariant) functor $T$ gives (after deleting $TB$)

$$eq:TEB 0 \to TE^0 \xrightarrow{Td^0} TE^1 \xrightarrow{Td^1} TE_2 \xrightarrow{Td^2} \cdots . \tag{11.2}$$

We will primarily be concerned with the case where $T = \mathrm{Hom}_R(A, \bullet)$, so the above becomes

$$eq:THom 0 \to \mathrm{Hom}(A, E^0) \xrightarrow{\mathrm{Hom}(A,d^0)} \mathrm{Hom}(A, E^1) \xrightarrow{\mathrm{Hom}(A,d^1)} \mathrm{Hom}(A, E^2) \xrightarrow{\mathrm{Hom}(A,d^2)} \cdots . \tag{11.3}$$

**Definition 4.1:** Let $T$ be a covariant functor. The $n$th **(covariant) right derived functor** of $T$ is

$$(R^nT)B := H^n(TE^B) = \frac{\ker(Td^n)}{\mathrm{im}(Td^{n-1})},$$

i.e. it is the $n$th cohomology module of (11.2).

For a $R$-module $E$, define

$$\mathrm{Ext}^n_R(A, B) := (R^n \mathrm{Hom}_R(A, \bullet))B = H^n(\mathrm{Hom}_R(A, E^B)),$$

i.e. it is the $n$th cohomology module of (11.3).

Here $d^{-1}$ is the trivial map $0 \to E^0$. We need to show that this definition does not depend on the injective resolution chosen.

*Proof of well-definedness.* Suppose we have two injective resolutions of $B$:

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "\eta"] \arrow[d, equal] & E^0 \arrow[r, "d^0"] \arrow[d, dotted, "f_0"] & E^1 \arrow[r, "d^1"] \arrow[d, dotted, "f_1"] & \cdots \\
0 \arrow[r] & B \arrow[r, "\eta'"] & E'^0 \arrow[r, "d'^0"] & E'^1 \arrow[r, "d'^1"] & \cdots
\end{tikzcd}$$

Let $(R^nT)B = \frac{\ker(Td^n)}{\mathrm{im}(Td^{n-1})}$ and $(R'^nT)B = \frac{\ker(Td'^n)}{\mathrm{im}(Td'^{n-1})}$.

By the Comparison Theorem 2.4, there is a unique chain map $f$ between the two resolutions, up to homotopy (the dotted lines above). Apply $T$ to this diagram to get a chain map $Tf_n : TE^n \to TE'^n$. As $H_n$ is a functor by Theorem 3.2, $Tf$ induces a map on the cohomology modules $(R^nT)B \to (R'^nT)B$. Since we can construct a chain map $g$ from the second to the first resolution as well, $(R^nT)B \to (R'^nT)B$ must be an isomorphism.

For the details, see [12], Proposition 6.20. (The argument there is written for left derived functors, but the idea is the same.) □

### 4.1.2 Contravariant case

We can define a companion functor $\mathrm{ext}^n_R$ that is contravariant instead of covariant. Given an projective resolution of $A$

$$P_A : \quad \cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\varepsilon} A \to 0,$$

applying a contravariant functor $T$ gives

$$eq:TPB0 \xrightarrow{Td_{-1}=0} TP_0 \xrightarrow{Td_0} TP_1 \xrightarrow{Td_1} TP_2 \xrightarrow{Td_2} \cdots . \tag{11.4}$$

To define ext, let $T = \mathrm{Hom}_R(\bullet, B)$.

**Definition 4.2:** Let $T$ be a contravariant functor. The $n$th **(contravariant) right derived functor** of $T$ is

$$(R^n T)A := H^n(TP_A) = \frac{\ker(Td^n)}{\mathrm{im}(Td^{n-1})},$$

i.e. it is the $n$th cohomology module of (11.4).

For $R$-modules $A, B$, define

$$\mathrm{ext}^n_R(A,B) := (R^n \mathrm{Hom}_R(\bullet, B))A = H^n(\mathrm{Hom}_R(P_A, B))$$

**Theorem 4.3:** Extisext For $R$-modules $A, B$,

$$\mathrm{Ext}^n_R(A,B) = \mathrm{ext}^n_R(A,B).$$

This theorem says that we have two choices when we need to calculate $\mathrm{Ext}^n_R(A,B)$, namely,

1. Find a injective resolution of $B$ and apply $\mathrm{Hom}(A, \bullet)$ (the Ext perspective), or
2. Find a projective (e.g. free) resolution of $A$ and apply $\mathrm{Hom}(\bullet, B)$ (the ext perspective).

*Proof.* See Rotman [12], Theorem 6.67. □

## 4.2 Left derived functors and Tor

Next we define left derived functors and Tor analogously. Given a projective resolution of $A$

$$P_A: \quad \cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\varepsilon} A \to 0,$$

applying a covariant functor $T$ gives

$$\cdots \xrightarrow{Td_2} TP_2 \xrightarrow{Td_1} TP_1 \xrightarrow{Td_0} TP_0 \xrightarrow{Td_{-1}} 0.$$

To define Tor, let $T = \bullet \otimes_R B$.

**Definition 4.4:** The $n$th **left derived functor** of $T$ is

$$(L_n T)B := H_n(TP_A) = \frac{\ker(Td_{n-1})}{\mathrm{im}(Td_n)}.$$

For $A$ an $R$-module, define

$$\begin{aligned} \mathrm{Tor}^R_n(A,B) &:= (L_n(\bullet \otimes_R B))A = H^n(P_A \otimes_R B) \\ \mathrm{tor}^R_n(A,B) &:= (L_n(A \otimes_R \bullet))A = H^n(A \otimes_R P_B). \end{aligned}$$

(Note $\mathrm{Tor}^R_n(A,B) = \mathrm{tor}^R_n(B,A)$.)

Note unlike the case with Ext, we need only consider covariant derived functors: $\mathrm{Hom}_R$ is contravariant in the first entry and covariant in the second, while $\otimes_R$ is covariant in both entries. Similar to Theorem 4.3, we have the following.

**Theorem 4.5:** Toristor For $A, B$ $R$-modules,

$$\mathrm{Tor}_n^R(A, B) = \mathrm{tor}_n^R(A, B).$$

*Proof.* See Rotman [12], Theorem 6.32. □

## 4.3 Long exact sequences

The most important property of the derived functors is that they repair "loss of exactness" after applying the functor.

**Theorem 4.6** (Long exact sequence)**:** les-ext Let $0 \to A \to B \to C \to 0$ be a short exact sequence of $G$-modules.

1. Let $T$ be a left exact covariant functor. Then there is a long exact sequence

$$\begin{tikzcd} 0 \arrow[r] & (R^0T)A \arrow[r] \arrow[d, equal] & (R^0T)B \arrow[r] \arrow[d, equal] & (R^0T)C \arrow[r, "\partial^0"] \arrow[d, equal] & (R^1T)A \arrow[r] & \cdots \\ & TA & TB & TC & & \end{tikzcd}$$

2. Let $T$ be a right exact covariant functor. Then there is a long exact sequence

$$\begin{tikzcd} \cdots \arrow[r] & (L_1T)C \arrow[r, "\partial_1"] & (L_0T)A \arrow[r] \arrow[d, equal] & (L_0T)B \arrow[r] \arrow[d, equal] & (L_0T)C \arrow[r] \arrow[d, equal] & 0 \\ & & TA & TB & TC & \end{tikzcd}$$

The maps $\partial^n$ are given by the snake lemma.

*Proof.* The long exact sequences exist by Theorem 3.3. (Note that the complexes only go off to the right/left in the two cases, respectively.) It remains to show the equalities. Take a projective resolution of $A$,

$$\cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\varepsilon} A \to 0.$$

By right exactness of $T$, the following is exact:

$$TP_1 \xrightarrow{Td_1} TP_0 \xrightarrow{T\varepsilon} TA \longrightarrow 0.$$

Hence $(L_0T)A = TP_0/\mathrm{im}(TP_1) \cong TA$.

The second part is similar. □

**Corollary 4.7:** les-ext-tor We have the long exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ext}^0_R(M,A) \arrow[r] \arrow[d, equal] & \mathrm{Ext}^0_R(M,B) \arrow[r] \arrow[d, equal] & \mathrm{Ext}^0_R(M,C) \arrow[r, "\partial^0"] \arrow[d, equal] & \mathrm{Ext}^1_R(M,A) \arrow[r] & \cdots \\
& \mathrm{Hom}_R(M,A) & \mathrm{Hom}_R(M,B) & \mathrm{Hom}_R(M,C) & &
\end{tikzcd}$$

and

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{Tor}^R_1(C,M) \arrow[r, "\partial_1"] & \mathrm{Tor}^R_0(A,M) \arrow[r] \arrow[d, equal] & \mathrm{Tor}^R_0(B,M) \arrow[r] \arrow[d, equal] & \mathrm{Tor}^R_0(C,M) \arrow[r] \arrow[d, equal] & 0 \\
& & M \otimes_R A & M \otimes_R B & M \otimes_R C &
\end{tikzcd}$$

*Proof.* $\mathrm{Hom}_R(A, \bullet)$ is left exact and $\bullet \otimes_R B$ is right exact. □

**Example 4.8:** ex:ext-inj We have the following.

$$\begin{aligned}
B \text{ injective} &\implies \mathrm{Ext}^n_R(A,B) = 0 \text{ for all } A,\ n \geq 1 \\
A \text{ projective} &\implies \mathrm{Tor}^n_R(A,B) = 0 \text{ for all } B,\ n \geq 1.
\end{aligned}$$

Indeed, recall that Ext is defined by taking an injective resolution of $B$ and Tor is defined by taking a projective resolution of $A$, and in these cases we can take the trivial resolutions $0 \to B \to B \to 0$ and $0 \to A \to A \to 0$.

**Example 4.9:** ex:abelian-tor2=0 Take $R = \mathbb{Z}$. Then a $R$-module is just an abelian group. Every group $H$ has a free resolution of length 2:

$$0 \to F_1 \to F_0 \to H \to 0.$$

Thus $\mathrm{ext}^n_{\mathbb{Z}}(H,G) = 0$ and $\mathrm{Tor}^{\mathbb{Z}}_n(H,G) = 0$ for $n \geq 2$.

# §5 Homological and cohomological functors

sec:cohom-functor This section is more abstract and may be skipped.

As we saw in Corollary 4.7 and Example 4.8, the key properties of $\mathrm{Ext}^n_R$ are roughly the following:

1. $\mathrm{Ext}^n_R(A,B) = 0$ when $B$ is injective and $n \geq 1$.

2. Short exact sequences give rise to long exact sequences.

3. In dimension 0, $\mathrm{Ext}^0_R(A,B) = \mathrm{Hom}_R(A,B)$.

We have a similar description for $\mathrm{Tor}_n^R$.

We abstract the definition for Ext and Tor, by defining homological and cohomological functors. There are several reasons for doing this:

1. We want to talk about *natural transformations* between cohomological functors.

2. In the last section we showed the existence of Ext satisfying the above properties (and similarly for Tor). It turns out that these properties characterize it uniquely. Thus we can just "remember" these properties and forget the details of the construction.

   There are similarly other (co)homological functors, and we sometimes want to show they are equal. To do this, it turns out we can just construct an isomorphism in dimension 0, and the rest works out by abstract nonsense. (See Theorem 5.2.)

Note in the above characterization of Ext we said $\mathrm{Ext}_n^R(A,B)=0$ for $n\geq 1$ when $B$ is injective. This is useful because every $R$-module has an injective resolution. In general, though, we may want to work with a general class of objects, say $\chi$ (which in our case is the class of injective modules). The key property is that for every module $A$ there is an injective module $E$ and an injective morphism $A\to E$, i.e. the category of $R$-modules has enough injectives.

**Definition 5.1:** Let $(T^n:\mathcal{A}\to\mathcal{B})_{n\geq 0}$ be a set of additive functors on abelian categories, and let $\chi$ be a class of objects in $A$. We say $A$ has **enough $\chi$-objects** is every object in $\mathcal{A}$ can be embedded in an object in $\chi$.

Supposing $A$ has enough $\chi$-objects, $(T^n)_{n\geq 0}$ is a **cohomological $\partial$-functor** if the following hold.

1. $(T^n)_{n\geq 0}$ is $\chi$-**coeffaceable**: $T^n(X)=0$ for all $X\in\chi$ and $n\geq 1$.

2. For every short exact sequence $0\to A\to B\to C\to 0$ there is a long exact sequence

   $$0\to T^0(A)\to\cdots\to T^n(A)\to T^n(B)\to T^n(C)\xrightarrow{\partial^n}T^{n+1}(A)\to\cdots$$

   such that the diagonal morphisms $\partial^n$ are natural (with respect to maps between two short exact sequences).

A morphism of cohomological $\partial$-functors is a natural transformation $\tau^n: T^n\to H^n$ commuting with the diagonal maps $\partial^n$.

There is a similar definition for effaceability and homological $\partial$-functors. We can also consider $(T^n)_{n\in\mathbb{Z}}$, that is $\partial$-functors extending infinitely in both directions, replacing the long exact sequence with an infinite exact sequence extending in both directions.

The following theorem gives existence and uniqueness of (co)homological $\partial$-functors.

**Theorem 5.2:** thm:hom-functor-uniqueness

1. Suppose $\tau^0 : T^0 \to T'^0$ is a natural transformation of cohomological $\partial$-functors in degree 0. Then there exists a unique morphism of cohomological $\partial$-functors $\tau : T \to T'$ extending $\tau^0$.

2. Suppose $T^n, T'^n : \mathcal{A} \to \mathcal{B}$ are two cohomological functors, and there is a natural isomorphism $T^0 \cong T'^0$. Then $T^n \cong T'^n$.

The same is true of homological $\partial$-functors, and $\partial$-functors extending in both directions.

*Proof.* See Rotman [12], 6.35. □

For example, $\mathrm{Ext}_R$ is characterized completely by the 3 properties we gave: it is a cohomological $\partial$-functor by items 1 and 2, and uniqueness comes from knowing it in dimension 0 (item 3). Ditto for $\mathrm{Tor}_R$.

# §6 Group cohomology

group-cohomology To apply homology to groups, we will turn a group $G$ into a ring, and consider modules over that ring.

**Definition 6.1:** Let $R$ be a ring. The **group ring** $R[G]$ or $RG$ is the ring

$$R^{\oplus G} = \left\{ \sum_{g \in G} a_g g : a_g \in R \right\}$$

with multiplication given by

$$\left( \sum_{g \in G} a_g g \right) \left( \sum_{h \in G} b_h h \right) = \sum_{g,h \in G} a_g b_h gh.$$

We will always work with $R = \mathbb{Z}$.

Note that any action of $G$ on a $\mathbb{Z}$-module makes the module into a $\mathbb{Z}G$-module. We often just abbreviate "$\mathbb{Z}G$-module" as "$G$-module."

**Definition 6.2:** Let $G$ be a group and $A, B$ be left $\mathbb{Z}G$-modules.

1. The **diagonal action** of $G$ on $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ is given by

$$(g\varphi)(a) = g(\varphi(g^{-1}a)).$$

2. The **diagonal action** of $G$ on $A \otimes_{\mathbb{Z}G} B$ is given by

$$g(a \otimes b) = (ga) \otimes (gb).$$

We now apply cohomology as follows.

**Definition 6.3:** Let $M$ be a $G$-module. Equip $\mathbb{Z}$ with the trivial $G$-module structure. The **cohomology groups** of $G$ with coefficients in $M$ are defined by

$$\begin{aligned} H^n(G,M) &= \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z},M) = H^n(\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},E^M)) \\ &= \operatorname{ext}^n_{\mathbb{Z}G}(\mathbb{Z},M) = H^n(\operatorname{Hom}_{\mathbb{Z}G}(P_{\mathbb{Z}},M)). \end{aligned}$$

Note from Theorem 4.3, we have two choices in finding $H^n(G,M)$: find a $\mathbb{Z}G$-injective resolution of $M$, or a $\mathbb{Z}G$-projective resolution of $\mathbb{Z}$.

There is a nice interpretation of $H^0(G,M)$.

**Definition 6.4:** Let $L, M$ be $G$-modules and $\varphi$ be a map $L \to M$. Define the **fixed point functor** by the following.

1. Action on modules:

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

2. Action on maps: Since $\varphi(L^G) \subseteq M^G$ we can define

$$\varphi^G = \varphi|_{L^G}.$$

**Proposition 6.5:** cohom1 As functors,

$$H^0(G,\bullet) = \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},\bullet) = \bullet^G.$$

In particular, the fixed point functor is left exact since $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},\bullet)$ is.

*Proof.* $\mathbb{Z}$ is equipped with the trivial $G$-action. A $G$-homomorphism $\varphi$ from $\mathbb{Z}$ to $M$ is determined by $\varphi(1)$, and $\varphi(1)$ must be a fixed point. Hence $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},M) = M^G$ via the map $\varphi \mapsto \varphi(1)$. □

**Remark:** This gives us another way to think about group cohomology. Given $M$, take an injective resolution $0 \to M \to E^0 \to E^1 \to \cdots$. Applying $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},\bullet)$ to this resolution is the same as applying $\bullet^G$, so we get $0 \to (E^0)^G \to (E^1)^G \to \cdots$. Then $H^n(G,M)$ is the $n$th cohomology group of this complex.

We will need the fact that cohomology preserves products.

**Proposition 6.6:** cohom-preserve-prod Let $G$ be a group and $M_i$ be $G$-modules. Then

$$H^n\left(G, \prod_{i\in I} M_i\right) \cong \prod_{i\in I} H^n(G,M_i).$$

*Proof.* First note that the product of injective modules is an injective module: By definition a $R$-module $I$ is injective iff $\operatorname{Hom}_R(\bullet, I)$ is exact. Thus, the statement follows from the fact that $\mathrm{Hom}_R(\bullet, \prod_i I_i) = \prod_i \mathrm{Hom}_R(\bullet, I_i)$, and the fact that a product of exact sequences is exact.

Thus if $E^{M_i}$ is an injective resolution for $M_i$, then $\prod_i E^{M_i}$ is an injective resolution for $\prod_i M_i$, and we get

$$H^n\left(G, \prod_{i\in I} M_i\right) = H^n\left(\mathrm{Hom}_{\mathbb{Z}G}\left(\mathbb{Z}, E^{\prod_{i\in I} M_i}\right)\right) = H^n\left(\mathrm{Hom}_{\mathbb{Z}G}\left(\mathbb{Z}, \prod_{i\in I} E^{M_i}\right)\right) = \prod_{i\in I} H^n(G, M_i).$$

□

## §7 Bar resolutions

sec:bar-res We now describe the cohomology groups, by working with an explicit presentation of $\mathbb{Z}$. (We use the ext approach.) This will give practical interpretations of $H^1(G,M)$ and $H^2(G,M)$. For proofs, see Rotman [12], Section 9.3.

**Definition 7.1:** Define the **bar resolution** $B(G)$ to be the exact sequence

$$\cdots \xrightarrow{d_3} B_2 \xrightarrow{d_2} B_1 \xrightarrow{d_1} B_0 \xrightarrow{d_0=\varepsilon} \mathbb{Z} \longrightarrow 0$$

where

$$B_n \cong \mathbb{Z}G^{\oplus G^n}$$

is the free abelian group with basis elements denoted by $[x_1|\cdots|x_n]$, and

$$eq:bar-d\, d_n([x_1|\cdots|x_n]) = x_1[x_2|\cdots|x_n] + \sum_{i=1}^{n-1}(-1)^i[x_1|\cdots|\underbrace{x_ix_{i+1}}_{i}|\cdots|x_n] + (-1)^n[x_1|\cdots|x_{n-1}]. \quad (11.5)$$

Let $U_n \subseteq B_n$ be the submodule generated by $[x_1|\cdots|x_n]$ where at least one of the $x_i$ equals 1, and define the **normalized bar resolution** to be the quotient complex $B^*(G) := B(G)/U(G)$.

Note in particular

$$\begin{aligned} d_3[x|y|z] &= x[y|z] - [xy|z] + [x|yz] - [x|y] \\ d_2[x|y] &= x[y] - [xy] + [x] \\ d_1[x] &= x[] - [] \\ d_0[] &= 1. \end{aligned}$$

We have $\mathrm{Hom}_G(B_n, M) = \mathrm{Hom}_G(\mathbb{Z}G^{\bigoplus G^n}, M)$, so it can be identified with the set of functions $G^n \to M$. Working out the kernels and images, we get the following.

**Theorem 7.2:** explicit-h1 We have the following descriptions of $H^1(G,M)$ and $H^2(G,M)$.

1. Define a **derivation** (or crossed homomorphism) of $G$ to be a function $G \to M$ such that
$$d(xy) = d(x) + xd(y)$$
and a **principal derivation** to be one in the form
$$d(x) = a - xa, \text{ for some } a \in M.$$
Denote the set of derivations and principal derivations by $\operatorname{Der}(G, M)$ and $\operatorname{PDer}(G, M)$. Then
$$H^1(G, M) \cong \operatorname{Der}(G, M)/\operatorname{PDer}(G, M).$$

2. We have
$$H^2(G, M) \cong \frac{\{f : G \times G \to M : f(x, y) + f(xy, z) = xf(y, z) + f(x, yz),\ f(x, 1) = f(1, y) = 0\}}{\{g : G \times G \to M : g(x, y) = xh(y) - h(xy) + h(x) \text{ for some } h : G \to M\}}.$$
The elements in the top set are called **factor sets**.

A particularly important case is the following.

**Corollary 7.3:** h1-is-hom Suppose $G$ acts trivially on $M$. Then
$$H^1(G, M) \cong \operatorname{Hom}_{\mathbb{Z}}(G, M).$$
(On the RHS, $G$ and $M$ are thought of as groups.)

*Proof.* Because the action is trivial, a derivation is just a function with $d(xy) = d(x)+d(y)$, i.e. a homomorphism. Moreover, any principal derivation is trivial. □

# §8 Group homology

group-homology

**Definition 8.1:** Let $A$ be a $G$-module. Equip $\mathbb{Z}$ with the trivial $G$-module structure. The **homology groups** of $G$ with coefficients in $\mathbb{Z}$ are defined by
$$\begin{aligned} H_n(G, A) &= \operatorname{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A) = H_n(P_{\mathbb{Z}} \otimes_{\mathbb{Z}G} A) \\ &= \operatorname{tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A) = H_n(\mathbb{Z} \otimes_{\mathbb{Z}G} P_A). \end{aligned}$$

There is similarly a nice interpretation of $H_0(G, M)$, as well as of $H_1(G, \mathbb{Z})$. Given a group $G$, define the map $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ by $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$, and define
$$I_G := \ker(\varepsilon) = \left\{ \sum_{g\in G} a_g g : \sum_{g\in G} a_g = 0 \right\}.$$

**Proposition 8.2:** hom1 As functors,

$$H_0(G, \bullet) = \bullet / I_G \bullet;$$

i.e. there is a natural isomorphism

$$\begin{aligned} H_0(G, A) = \mathbb{Z} \otimes_G A &\to A/I_G A \\ m \otimes a &\mapsto ma + I_G A. \end{aligned}$$

*Proof.* The short exact sequence $0 \to I_G \to \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z}$ gives exactness of

$$I_G \otimes_G A \to \mathbb{Z}G \otimes_G A \to \mathbb{Z} \otimes_G A \to 0$$

since tensoring is right exact. ($G$ acts trivially on the $\mathbb{Z}$ on the right.) Thus,

$$H_0(G, A) = \mathbb{Z} \otimes_G A = (\mathbb{Z}G \otimes_G A)/(I_G \otimes_G A) = A/I_G A.$$

□

**Proposition 8.3:** h1-is-gab There are canonical homomorphisms $H_1(G, \mathbb{Z}) \cong I_G/I_G^2 \cong G^{\mathrm{ab}}$.

Here $G^{\mathrm{ab}}$ denotes the *abelianization* of $G$, i.e. $G/G'$, where $G'$ is the derived subgroup, the (normal) subgroup generated by the commutators $aba^{-1}b^{-1}$.

*Proof.* The long exact sequence in homology for $0 \to I_G \to \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ is

$$\begin{tikzcd} H_1(G,\mathbb{Z}G) \arrow[r] \arrow[d, equal] & H_1(G,\mathbb{Z}) \arrow[r, "\partial_1"] & H_0(G,I_G) \arrow[r] \arrow[d, equal] & H_0(G,\mathbb{Z}G) \arrow[r, two heads] \arrow[d, equal] & H_0(G,\mathbb{Z}) \arrow[r] \arrow[d, equal] & 0 \\ 0 & & I_G/I_G^2 & \mathbb{Z} & \mathbb{Z} & \end{tikzcd}$$

The left term is 0 by Example 4.8 since $\mathbb{Z}G$ is free, hence projective. Thus $\partial_1$ is injective. From Proposition 8.2, we get the middle two inequalities (since $H_0(G, \mathbb{Z}G) = \mathbb{Z}G/I_G\mathbb{Z}G = \mathbb{Z}$). Surjectivity of the map $\mathbb{Z} \to \mathbb{Z}$ gives that it is actually an isomorphism, so exactness gives $\partial_1$ is an isomorphism. It remains to show

$$iggg I_G/I_G^2 \cong G/G'. \tag{11.6}$$

Define a map $f : G \to I_G/I_G^2$ by letting $f(x) = (x-1) \bmod I_G^2$. This is a homomorphism because

$$\begin{aligned} f(xy) &= xy - 1 \bmod I_G^2 \\ &= (x-1) + (y-1) \bmod I_G^2 && (x-1)(y-1) \in I_G^2 \\ &= f(x)f(y). \end{aligned}$$

Now $G' \in \ker f$ since $I_G/I_G^2$ is abelian ($\mathbb{Z}G$, as an additive group, is abelian), so we get a map $f : G/G' \to I_G/I_G^2$.

Now define $g : I_G \to G/G'$ by $g(x-1) = xG'$. (Note $x-1, x \in G\backslash\{1\}$, is a free basis for $G$.) We have

$$g\left(\sum_{x\in G\backslash\{1\}} m_x(x-1) \sum_{y\in G\backslash\{1\}} m_y(y-1)\right) = g\left(\sum_{x,y\in G\backslash\{1\}} m_x n_y((xy-1)-(x-1)-(y-1))\right)$$
$$= \prod_{x,y\in G\backslash\{1\}} (xyx^{-1}y^{-1})^{m_x n_x} G' = G'$$

so $g$ induces $g : I_G/I_G^2 \to G/G'$.

Now $f$ and $g$ are inverse, showing (11.6). $\square$

## 8.1 Shapiro's lemma

shapiro Shapiro's lemma will be helpful in computing (co)homology groups, especially in the guise of Corollary 8.7.

**Definition 8.4:** Let $S \subseteq G$ be a subgroup of finite index. Define the **induced** and **coinduced modules** to be[3]

$$\mathrm{Ind}_S^G(A) = A \otimes_{\mathbb{Z}S} \mathbb{Z}G.$$
$$\mathrm{Coind}_S^G(A) = \mathrm{Hom}_{\mathbb{Z}S}(\mathbb{Z}G, A).$$

If $S = \{1\}$ we simply write $\mathrm{Ind}^G(A)$ or $\mathrm{Coind}^G(A)$. An **induced module** of $G$ is a module in the form $\mathrm{Ind}^G(A)$; a **coinduced module** of $G$ is a module in the form $\mathrm{Coind}^G(A)$.

**Remark:** rem:finite-induced If $G$ is finite, the induced and coinduced modules are canonically isomorphic via the below map, so there is no need to distinguish between them.

$$\mathrm{Hom}_S(\mathbb{Z}G, A) \to A \otimes_{\mathbb{Z}S} \mathbb{Z}G$$
$$\varphi \mapsto \sum_{g\in G/S} \varphi(g^{-1}) \otimes_{\mathbb{Z}S} g.$$

**Proposition 8.5:** pr:coinduced-subgroup If $M$ is a coinduced $G$-module, and $H \subseteq G$ is a subgroup, then $M$ is a coinduced $H$-module.

*Proof.* Write $M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$; we can write $\mathbb{Z}[G] = \mathbb{Z}[H] \otimes B$; then we have by adjoint associativity[4] that $M = \mathrm{Hom}(\mathbb{Z}[H] \otimes M, A) = \mathrm{Hom}(\mathbb{Z}[H], \mathrm{Hom}(M, A))$. $\square$

[3] Be careful; in some books the definitions are reversed. We follow Serre's definition, which is the opposite of Milne's definitions.

[4] If $R, R'$ are rings, $M$ is a $R$-module, $N$ is a $(R, R')$-bimodule, and $P$ is a $R'$-module, then there is a canonical $(R, R')$-isomorphism $\mathrm{Hom}_R(M, \mathrm{Hom}_{R'}(N, P)) \cong \mathrm{Hom}_{R'}(M \otimes_R N, P)$.

The cohomology of coinduced modules and the homology of induced modules are easy to calculate.

**Lemma 8.6** (Shapiro's lemma)**:** shapiro-lemma The following hold.

$$H^n(G, \mathrm{Coind}_S^G(A)) = H^n(S, A)$$
$$H_n(G, \mathrm{Ind}_S^G(A)) = H_n(S, A).$$

*Proof.* Let $P_{\mathbb{Z}}$ be a $\mathbb{Z}G$-projective resolution of $\mathbb{Z}$. Note it is also a $\mathbb{Z}S$-projective resolution, as any $\mathbb{Z}G$-projective module is $\mathbb{Z}S$-projective.

By definition of cohomology group,

$$\begin{aligned} H^n(G, \mathrm{Coind}_S^G(A)) &= H^n(\mathrm{Hom}_{\mathbb{Z}G}(P_{\mathbb{Z}}, \mathrm{Hom}_{\mathbb{Z}S}(\mathbb{Z}G, A))) \\ &\overset{(*)}{=} H^n(\mathrm{Hom}_{\mathbb{Z}S}(P_{\mathbb{Z}} \otimes_{\mathbb{Z}G} \mathbb{Z}G, A)) = H^n(\mathrm{Hom}_{\mathbb{Z}S}(P_{\mathbb{Z}}, A)) = H^n(S, A). \end{aligned}$$

In $(*)$ we used adjoint associativity.

By the definition of homology group,

$$H_n(G, \mathrm{Ind}_S^G(A)) = H_n(P_{\mathbb{Z}} \otimes_{\mathbb{Z}G} (\mathbb{Z}G \otimes_{\mathbb{Z}S} A)) = H_n(P_{\mathbb{Z}} \otimes_{\mathbb{Z}S} A) = H_n(S, A).$$ □

**Corollary 8.7:** shapiro-cor Suppose that $A = \bigoplus_{i \in I} A_i$, $S = \mathrm{Stab}(A_j)$ (defined as $\{g \in G : gA_j = A_j\}$), and $G$ permutes the submodules $A_i$ transitively. Then

$$H_n(G, A) = H_n(S, A_j).$$

If $G$ is finite, then

$$H^n(G, A) = H^n(S, A_j).$$

*Proof.* We have $A = \mathrm{Ind}_S^G A_j$. If $G$ is finite then $A \cong \mathrm{Coind}_S^G A_j$ as well. □

**Corollary 8.8:** cor:ind-0 If $M$ is an coinduced $G$-module, then $H^n(G, M) = 0$ for all $n \geq 1$.

If $M$ is an induced $G$-module, then $H_n(G, M) = 0$ for all $n \geq 1$.

*Proof.* By Shapiro's lemma 8.6,

$$\begin{aligned} M = \mathrm{Coind}^G(A) &\implies H^n(G, M) = H^n(1, M) = 0 \\ M = \mathrm{Ind}^G(A) &\implies H_n(G, M) = H_n(1, M) = 0. \end{aligned}$$

We used the fact that $\mathbb{Z}$ is $\mathbb{Z}[\{1\}]$-projective. □

# §9 Tate groups

tate-groups By Corollary 4.7, given a short exact sequence of $G$-modules we get a long exact sequence in homology and cohomology. We splice these sequences together using the Snake Lemma to obtain a long exact sequence extending in both directions.

**Definition 9.1:** df:ngs Let $G$ be a group, $S$ be a subgroup of finite index, and $A$ be a $G$-module. Define the **norm** $N_{G/S} : A^S \to A^G$ by

$$N_{G/S}(a) = \sum_{j=1}^{n} t_j a,$$

where $\{t_1, \ldots, t_n\}$ is a left transversal (i.e. coset representatives) of $S$ in $G$. In particular, for $S = \{1\}$ the norm map is

$$N_G(a) = N(a) = \left( \sum_{g \in G} g \right) a.$$

**Definition 9.2:** tate-df Suppose $G$ is a finite group and $A$ is a $G$-module. Define the **Tate groups** by

$$H_T^q(G, A) = \begin{cases} H^q(G, A), & q \geq 1 \\ A^G/NA, & q = 0 \\ {}_N A/I_G A, & q = -1 \\ H_{-q-1}(G, A), & q \leq -2. \end{cases}$$

Here ${}_N A$ denotes $\{a \in A : Na = 0\}$.

**Theorem 9.3:** double-les If $G$ is a finite group and $0 \to A \to B \to C \to 0$ is an exact sequence of $G$-modules, then there is a long exact sequence

$$\cdots \to H_T^q(G, A) \to H_T^q(G, B) \to H_T^q(G, C) \to H_T^{q-1}(G, A) \to \cdots$$

*Proof.* It suffices to prove exactness for $q = -1$ and $q = 0$. We apply to the snake lemma to obtain the following (the top and bottom rows in the middle are the long exact sequence in homology and cohomology, respectively).

$$\begin{tikzcd}
 & \ker N_A \arrow[r] \arrow[d] & \ker N_B \arrow[r] \arrow[d] & \ker N_C \arrow[d] \arrow[dddll, rounded corners] & \\
H_1(G,C) \arrow[r, "\partial_1"] \arrow[ur] & H_0(G,A) \arrow[r] \arrow[d, "N_A"] & H_0(G,B) \arrow[r] \arrow[d, "N_B"] & H_0(G,C) \arrow[r] \arrow[d, "N_C"] & 0 \\
0 \arrow[r] & H^0(G,A) \arrow[r] \arrow[d] & H^0(G,B) \arrow[r] \arrow[d] & H^0(G,C) \arrow[r, "\partial^0"] \arrow[d] & H^1(G,A) \\
 & \operatorname{coker}(N_A) \arrow[r] & \operatorname{coker}(N_B) \arrow[r] & \operatorname{coker}(N_C) \arrow[ur] &
\end{tikzcd}$$

The maps $N_A$, $N_B$, $N_C$ are the norm maps on $A$, $B$, and $C$ after associating $H_0$ and $H^0$ with their descriptions in Propositions 6.5 and 8.2:

$$\begin{tikzcd}
& {}_N A/I_G A \arrow[r] \arrow[d] & {}_N B/I_G B \arrow[r] \arrow[d] & {}_N C/I_G C \arrow[d] \arrow[dddll, rounded corners] & \\
H_1(G,C) \arrow[ur] \arrow[r, "\partial_1"] & A/I_G A \arrow[r] \arrow[d, "N_A"] & B/I_G B \arrow[r] \arrow[d, "N_B"] & C/I_G C \arrow[r] \arrow[d, "N_C"] & 0 \\
0 \arrow[r] & A^G \arrow[r] \arrow[d] & B^G \arrow[r] \arrow[d] & C^G \arrow[r, "\partial^0"] \arrow[d] & H^1(G,A) \\
& A^G/NA \arrow[r] & B^G/NB \arrow[r] & C_G/NC \arrow[ur] &
\end{tikzcd}$$

□

## 9.1 Complete resolution*

[5] The description of Tate groups in the last section is somewhat unwieldy (because you can see the glue marks...). We give a different interpretation here, where the Tate groups at 0 and $-1$ are less distinguished. Then we use the technique of "dimension shifting" to extend results for cohomology (or homology) groups to results for Tate groups.

**Definition 9.4:** A **complete resolution** of a group $G$ is an exact sequence $\mathbf{X}$

$$\begin{tikzcd}
\cdots \arrow[r] & X_1 \arrow[r] & X_0 \arrow[rr, "d_0"] \arrow[dr, two heads, "\varepsilon"'] & & X_{-1} \arrow[r] & X_{-2} \arrow[r] & \cdots \\
& & & \mathbb{Z} \arrow[ur, hook, "\eta"'] & & &
\end{tikzcd}$$

where each $X_q$ is a finitely generated $G$-free module, $\varepsilon$ is surjective, and $\eta$ is injective.

**Proposition 9.5:** complete-resolution Every finite group $G$ has a complete resolution $\mathbf{X}$.

*Proof.* Take a $G$-free resolution of $\mathbb{Z}$ and its dual ($A^* = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z})$), and splice them together.

$$\begin{tikzcd}
\cdots \arrow[r] & P_1 \arrow[r] & P_0 \arrow[r, two heads] \arrow[drr] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 & & \\
& & 0 \arrow[r] & \mathbb{Z} \arrow[r, hook] & P_0^* \arrow[r] & P_1^* \arrow[r] & \cdots
\end{tikzcd}$$

[5]This section will not be used and can be omitted.

$\square$

**Proposition 9.6:** Let $G$ be a finite group, $A$ a $G$-module, and $\mathbf{X}$ a complete resolution. Then the Tate groups are exactly the cohomology groups

$$H_T^n(G,A) = H^n(\mathrm{Hom}_G(\mathbf{X},A)).$$

*Proof.* Since any two resolutions are chain-homotopic (going both ways) by the Comparison Theorem 2.4, it suffices to prove this for one resolution. We take a resolution as in Proposition 9.5 and apply $\mathrm{Hom}_G(\bullet, A)$ to it. We obtain the following.

$$\begin{tikzcd}
 & -2 & -1 & 0 & 1 & \\
\cdots \arrow[r] & \mathrm{Hom}_G(P_1^*,A) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_G(P_0^*,A) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_G(P_0,A) \arrow[r] \arrow[d, equal] & \mathrm{Hom}_G(P_1,A) \arrow[r] \arrow[d, equal] & \cdots \\
{} \arrow[r] & P_1 \otimes_{\mathbb{Z}G} A \arrow[r, "d^{-2}"] \arrow[dr] & P_0 \otimes_{\mathbb{Z}G} A \arrow[r, "d^{-1}"] \arrow[d, two heads, "\varepsilon\otimes\bullet"] & \mathrm{Hom}_G(P_0,A) \arrow[r, "d^0"] & \mathrm{Hom}_G(P_1,A) \arrow[r] & {} \\
 & & \mathbb{Z} \otimes_G A \arrow[r, "N_A"] \arrow[d, equal] & \mathrm{Hom}_G(\mathbb{Z},A) \arrow[u, hook, "\varepsilon^*"] \arrow[ur] \arrow[d, equal] & & \\
 & & A/I_G A & A^G & &
\end{tikzcd}$$

The isomorphisms on the left are given by the natural isomorphism

$$\begin{aligned} M \otimes_{\mathbb{Z}G} A &\to \mathrm{Hom}_G(M^*, A) \\ m \otimes a &\mapsto (f \mapsto f(m)a). \end{aligned}$$

The bent complex along the bottom is the complex for Tate cohomology; some diagram chasing gives that these groups are isomorphic to the cohomology groups in the middle complex. $\square$

## 9.2 Dimension shifting

Given a result or construction in dimension $n$, we can get the result in dimensions $n \pm 1$ by utilizing the long exact sequence 9.3 and the two propositions.

**Proposition 9.7:** induced-tate-0 Let $G$ be a finite group. If $M$ is an induced module then

$$H_T^n(G,M) = 0$$

for all $n$.

*Proof.* Since $G$ is finite, induced and coinduced modules are the same. The statement for homology and cohomology is Corollary 8.8; this takes care of all $n \neq 0, -1$. For $n = 0, -1$ we calculate $H_T^n(G, M)$ directly. Writing $M = A \otimes_{\mathbb{Z}} \mathbb{Z}G$, we see that every element of $m$ can be uniquely written as $\sum_{g \in G} a_g \otimes g$. We find that

$$M^G = \left\{ a \otimes \sum_{g \in G} g : a \in A \right\} = N(M)$$
$${}_N M = \left\{ \sum_{g \in G} a_g \otimes g : \sum_{g \in G} a_g = 0 \right\} = I_G M$$

so $H_T^0(G, M) = H_T^{-1}(G, M) = 0$. □

**Proposition 9.8:** in-induced Let $M$ be a module. Then there exist (canonical) short exact sequences

$$0 \to M \to M^* \to M^*/M \to 0$$
$$0 \to M' \to M_* \to M \to 0$$

such that $M^*$ is coinduced and $M_*$ is induced, and these sequences are split as abelian groups (i.e. as $\mathbb{Z}$-modules, but not necessarily as $\mathbb{Z}G$-modules).

*Proof.* The desired maps are

$$M \hookrightarrow \mathrm{Coind}_{\{1\}}^G(M)$$
$$m \to \varphi_m(g) = gm.$$
$$\mathbb{Z}[G] \otimes_{\mathbb{Z}} M \twoheadrightarrow M$$
$$g \otimes m \mapsto gm$$

Splitness follows from the fact that these maps have left and right inverses, respectively: $\varphi \mapsto \varphi(1)$ and $m \mapsto 1 \otimes m$. (They are only $\mathbb{Z}$-homomorphisms, not necessarily $\mathbb{Z}G$-homomorphisms.) □

Now suppose $G$ is finite; then coinduced and induced modules coincide. Taking the long exact sequence 9.3 of the above short exact sequences and using Proposition 9.7 gives

$$H_T^n(G, M) \cong H_T^{n-1}(G, M^*/M)$$
$$H_T^n(G, M) \cong H_T^{n+1}(G, M').$$

Thus we reduce a problem about cohomology in degree $n$ to a problem about cohomology in degree $n + 1$ or degree $n - 1$.

# §10 Cup products

cup-products There is a natural product defined in Tate cohomology.

Define $A \otimes B$ to be $A \otimes_{\mathbb{Z}} B$ with the structure of a $G$-module given by $g(a \otimes b) = ga \otimes gb$ (the diagonal action).

**Theorem 10.1:** thm:cup-product Let $G$ be a finite group and $A, B$ be $G$-modules. There exists a unique family of bilinear maps indexed by $(p, q) \in \mathbb{Z}^2$, together called the **cup product**,

$$\cup : H_T^p(G, A) \times H_T^q(G, B) \to H_T^{p+q}(G, A \otimes B),$$

satisfying the following four properties.

1. The homomorphisms are functorial in $A$ and $B$.
2. For $p = q = 0$, the cup product is induced by the map
$$A^G \otimes B^G \to (A \otimes B)^G.$$
3. If
$$0 \to A' \to A \to A'' \to 0$$
$$0 \to A' \otimes B \to A \otimes B \to A'' \otimes B \to 0$$
are exact[6], and $a'' \in H_T^p(G, A''), b \in H_T^q(G, B)$, then
$$(\delta a'') \cup b = \delta(a'' \cup b)$$
in $H_T^{p+q+1}(G, A' \otimes B)$. ($\delta$ is the map in the corresponding long exact sequence.)
4. If
$$0 \to B' \to B \to B'' \to 0$$
$$0 \to A \otimes B' \to A \otimes B \to A \otimes B'' \to 0$$
are exact, and $a \in H_T^p(G, A), b'' \in H_T^q(G, B'')$, then
$$a \cup (\delta b'') = (-1)^p \delta(a \cup b'')$$
in $H_T^{p+q+1}(G, A \otimes B')$.

*Proof.* We first define the cup product for cohomology groups and then use dimension shifting to define it for Tate groups.

[6] Recall $\bullet \otimes B$ is right exact, so the content is in left exactness.

We use the bar resolution[7], so that $n$-chains are functions $G^n \to A$. For $p, q \geq 0$, define

$$\cup : C^p(G, A) \times C^q(G, B) \to C^{p+q}(G, A \otimes B)$$

by

$$(f \cup g)[x_1|\cdots|x_{p+q}] = f([x_1|\cdots|x_p]) \otimes g([x_{p+1}|\cdots|x_{p+q}]).$$

For $n = 0$, we have $(f \cup g)[] = f[] \otimes g[]$ which shows property 2 is satisfied. We[8] can laboriously verify with (11.5) that

$$d(f \cup g) = (df) \cup g + (-1)^p f \cup (dg).$$

From this we get a well-defined map

$$\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B).$$

We can verify properties 3 and 4 by calculation.

Now we extend this definition by dimension shifting. Suppose the product is defined for $(p+1, q)$, we define it for $(p, q)$ as follows. Write $A$ (canonically) as a quotient of a induced module as in Proposition 9.8, $0 \to A' \to A_* \to A \to 0$. Since this is split, so is

$$0 \to A' \otimes B \to A_* \otimes B \to A \otimes B \to 0.$$

Since $A_*$ is induced, so is $A_* \otimes B$ (be slightly careful about the $G$-action here). Thus by Theorem 9.3, we get $H^p_T(A) \cong H^{p+1}_T(A')$ and $H^{p+q}_T(A) \cong H^{p+q+1}_T(A' \otimes B)$ (naturally), and thus we can define the cup product

$$\begin{tikzcd}
H^p_T(A) \times H^q_T(B) \arrow[r, dotted, "\cup"] \arrow[d, "\cong"] & H^{p+q}_T(A \otimes B) \\
H^{p+1}_T(A') \times H^q_T(B) \arrow[r, "\cup"] & H^{p+q+1}_T(A' \otimes B) \arrow[u, "\cong"']
\end{tikzcd}$$

Similarly define it for $(p, q)$ given $(p, q+1)$, but this time introduce a factor of $(-1)^p$ (in order to make the second condition hold). Note this is consistent with our defintions for $p, q \geq 0$, by conditions 3 and 4. It is not hard to verify that these maps are well-defined, and that conditions 3 and 4 continue to be satisfied. By the way we defined the maps, it also doesn't matter what order we define the maps in (so going from $(p+1, q+1) \to (p, q+1) \to (p, q)$ is the same as going from $(p+1, q+1) \to (p+1, q) \to (p, q)$, for instance).

Given the map for $(p, q)$, conditions 3 and 4 basically force us to define the map for $(p-1, q)$ and $(p, q-1)$ as above. Similarly we can dimension-shift in the opposite direction, and we get uniqueness for all $(p, q)$. □

[7] We can also use the standard resolution (not defined here); in that case the map is $(f \cup g)(x_0, \ldots, x_{p+q}) = f(x_0, \ldots, x_p) \otimes g(x_p, \ldots, x_{p+q})$.

[8] i.e. you

Cup products are rather nasty to work with when they aren't purely in cohomology, so if we need to do cup product computation, we work in cohomology whenever possible.

**Proposition 10.2:** The following hold:

1. Cup product is associative: For $x \in H^m(G,M)$, $y \in H^n(G,N)$, and $z \in H^p(G,P)$, $(x \cup y) \cup z = x \cup (y \cup z)$ (viewing the equation in $H^{m+n+p}(G, M \otimes N \otimes P)$.
2. Cup product is anticommutative: For $x \in H^m(G,M)$ and $y \in H^n(G,N)$, $x \cup y = (-1)^{mn} y \cup x$.

*Proof.* Omitted. The idea is to verify the formula in degree 0 and then dimension-shift to get the general case. □

## 10.1 Cup product calculations

To compute the Artin map in class field theory, we will need to calculate the cup product of things in dimensions $-2$ and 2. We will get there incrementally using dimension shifting and properties 3–4 of the cup product, first calculating the cup product on dimensions $(0,n)$ (especially $(0,1)$), then on $(-1,1)$, and then finally on $(-2,1)$.

**Theorem 10.3:** thm:cup-prod-calc Let $G$ be a finite group and $A, B$ $G$-modules. If $a \in A^G$, let $\overline{a}^0$ denote its image in $H_T^0(G,A)$, and if $Na = 0$, let $\overline{a}_0$ denote its image in $H_T^{-1}(G,A)$. For $g \in G$ let $\overline{g}$ denote its image in $G/G' = H_T^{-2}(G,\mathbb{Z})$.

1. $(0,n)$. Suppose $n \ge 0$, $a \in A^G$, and $x \in H_T^n(G,B)$. Let $f_a : B \to A \otimes B$ be the map sending $y$ to $a \otimes y$; it induces a map $H_T^n(G,A) \to H_T^n(G, A \otimes B)$. Then
$$\underbrace{\overline{a}^0}_{\in H_T^0(G,A)} \cup \underbrace{x}_{\in H_T^n(G,B)} = f_a(x) \in H_T^n(G, A \otimes B).$$
2. $(-1,1)$. Suppose $Na = 0$, and $[f] \in H^1(G,B)$ is represented by a cocycle $f : G \to B$. Then
$$\underbrace{\overline{a}_0}_{\in H_T^{-1}(G,B)} \cup \underbrace{[f]}_{\in H_T^1(G,B)} = \overline{\left(-\sum_{t\in G} ta \otimes f(t)\right)}^0.$$
3. $(-2,1)$. Let $s \in G$ and $[f] \in H^1(G,B)$. Then
$$\underbrace{\overline{s}}_{\in H_T^{-2}(G,\mathbb{Z})} \cup \underbrace{\overline{f}}_{\in H_T^1(G,B)} = \overline{f(s)}_0 \in H_T^{-1}(G,B).$$

*Proof.* We omit details of the calculations. See Serre [14], pg. 176-178.

1. For $n = 0$, this follows from definition of cup product. Now use dimension shifting, with the exact sequence $0 \to B \to B^* \to B^*/B \to 0$, $B^*$ coinduced.

2. Dimension shift from part 1 with $0 \to B \to B^* \to B^*/B \to 0$: suppose $b'' \in (B^*/B)^G$ is sent to $f$ under the diagonal morphism. Write $\overline{a}_0 \cup \overline{f} = \overline{a}_0 \cup d(\overline{b''}^0) = -d(\overline{a}_0 \cup \overline{b''}^0)$ and use part 1.

3. Show that
$$d(\overline{s} \cup [f]) = d(\overline{f}(s)_0).$$
Evaluate the LHS using property 3 and part 2.

$\square$

# §11 Change of group

change-of-group We would like to be able to connect (co)homology groups corresponding to different groups $G$, $G'$ and different modules over $G$, $G'$. This will allow us, for example, to define maps

$$\begin{aligned} \mathrm{Res}^n : & H^n(G, A) \to H^n(S, A) \\ \mathrm{Cor}_n : & H_n(S, A) \to H_n(G, A) \\ \mathrm{Inf}^n : & H^n(G/S, A^S) \to H^n(G, A) \qquad\qquad S \trianglelefteq G. \end{aligned}$$

## 11.1 Construction of maps

For there to be a map $H^n(G, A) \to H^n(G', A')$ we need there to be a map $G' \to G$, with some compatibility condition on the modules $A$, $A'$.

**Definition 11.1:** Let $G, G'$ be groups, let $A$ be a $G$-module and $A'$ be a $G'$-module. A **cocompatible pair** is a pair $(\alpha, f)$ where $\alpha : G' \to G$ is a group homomorphism and $f : A \to A'$ is a $\mathbb{Z}$-homomorphism such that

$$f((\alpha x')a) = x' f(a)$$

for all $x' \in G'$ and $a \in A$.

$$\begin{tikzcd} G' \arrow[r, "\alpha"] \arrow[d, squiggly, dash] & G \arrow[d, squiggly, dash] \\ A' & A \arrow[l, "f"] \end{tikzcd}$$

Let ((Pairs*)) denote the category whose objects are pairs $(G, A)$ and whose morphisms are cocompatible $(\alpha, f)$.

Define a **compatible pair** to be a pair $(\alpha, f)$ where $\alpha : G \to G'$ is a group homomorphism and $g : A \to A'$ is a $\mathbb{Z}$-homomorphism such that

$$f(xa) = (\alpha x) f(a)$$

for all $x \in G$.

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, squiggly, dash] & G' \arrow[d, squiggly, dash] \\ A \arrow[r, "f"] & A' \end{tikzcd}$$

Let ((Pairs)) denote the category whose objects are ordered pairs $(G, A)$ and whose morphisms are compatible $(\alpha, f)$.

Given a cocompatible pair, let $P'$ be a $G'$-projective resolution of $\mathbb{Z}$ and $P$ be a $G$-projective resolution of $\mathbb{Z}$. By the Comparison Theorem 2.4 there is a chain map $\tau(\alpha) : P' \to P$ induced by the map $1_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ and $\alpha$, unique up to homotopy. Define

$$\begin{aligned} C^n(G, A) = \operatorname{Hom}_{\mathbb{Z}G}(P_n, A) &\to \operatorname{Hom}_{\mathbb{Z}G}(P'_n, A') = C^n(G', A') \\ \varphi &\mapsto f \circ \varphi \circ \tau(\alpha)^n. \end{aligned}$$

Similarly, for a compatible pair, there is a chain map $\tau(\alpha) : P \to P'$ induced by $1_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ and $\alpha$; we get a map

$$\tau(\alpha)_n \otimes f : C_n(G, A) = P_n \otimes_{\mathbb{Z}G} A \to P'_n \otimes_{\mathbb{Z}G'} A' = C_n(G', A')$$

These maps descend to cohomology and homology, respectively.

**Definition 11.2:** Define the maps below using the (co)compatible pairs shown.

| Name | Map on $G$ | Map on $M$ | Map |
|---|---|---|---|
| Restriction | $i : S \to G$ | $M \xleftarrow{\cong} M$ | $\operatorname{Res}^n_{G/S} : H^n(G, M) \to H^n(S, M)$ |
| Corestriction | $i : S \to G$ | $M \xrightarrow{\cong} M$ | $\operatorname{Cor}^n_{S/G} : H_n(S, M) \to H_n(G, M)$ |
| Inflation | $q : G \to G/S$ | $M \hookleftarrow M^S$ | $\operatorname{Inf}^n_{S/G} : H^n(G/S, M^S) \to H^n(G, M)$ |
| Conjugation | $\sigma \mapsto g\sigma g^{-1}$ | $g^{-1}m \mapsfrom m$ | $H^n(G, M) \to H^n(G, M)$ |

For inflation, we require that $S \trianglelefteq G$ ($S$ be a normal subgroup of $G$).

**Proposition 11.3:** change-group-conjugation The conjugation map $H^n(G, M) \to H^n(G, M)$ is the identity.

This is important because when we are defining maps between different cohomology groups, we can be assured that conjugation won't change it, i.e. we have a canonical map.

*Proof.* For $n = 0$ this is the identity map $M^G \to M^G$. Since the conjugation $H^n(G, M) \to H^n(G, M)$ is a map of cohomological functors, and the identity map $H^n(G, M) \to H^n(G, M)$ is also a map of cohomological functors, and they agree for $n = 0$, by Theorem 5.2(2) they must be equal for all $n$.

Alternatively, use dimension shifting. $\square$

## 11.2 Extending maps to Tate cohomology

corestriction Right now $\operatorname{Res}^n$ is only defined on cohomology and $\operatorname{Cor}_n$ is only defined on homology. We would like to define them on Tate cohomology.

**Proposition 11.4:** pr:extend-to-tate Let $G$ be a finite group. The maps $\operatorname{Res}^n$ and $\operatorname{Cor}_n$ can be defined on Tate cohomology, such that the definitions for $H_T^n$ agree with the original definitions on cohomology and homology for $n \geq 0$ and $n \leq -1$, respectively, and such that Res and Cor are natural transformations compatible with forming the long exact sequence in homology and cohomology from a short exact sequence. Moreover, $\operatorname{Res}^n$ and $\operatorname{Cor}_n$ satisfy the following properties.

1. $\operatorname{Cor}^0_{S/G} : H_T^0(S,M) \to H_T^0(G,M)$ is the map $N_{G/S} : M^S/N_S M \to M^G/N_G M$.
2. $\operatorname{Res}^{-1}_{G/S} : H_T^{-1}(G,M) \to H_T^{-1}(S,M)$ is the map $C_{G/S} : {}_{N_G}M/I_G M \to {}_{N_S}M/I_S M$, where $C_{G/S}$ is the **conorm** map defined by
$$C_{G/S}(a) := \sum_i t_i^{-1} a$$
where $\{t_i\}$ is a left transversal of $G/S$. (Equivalently, let $\{t_i\}$ be a *right* transversal and let $C_{G/S}(a) := \sum_i t_i a$.[9])
3. $\operatorname{Cor}^{-2}_{S/G} : H_T^{-2}(S,M) \to H_T^{-2}(G,M)$ is the natural map $S^{\text{ab}} \to G^{\text{ab}}$. (See Proposition 8.3.)

*Proof.* First, the construction. We will use Theorem 5.2. Let $\chi$ be the class of coinduced $\mathbb{Z}G$-modules. Note that the category of $\mathbb{Z}G$-modules has enough coinduced $\mathbb{Z}G$-modules, by Proposition 9.8. Note that $\{H_T^n(S, \bullet_S)\}$ and $\{H_T^n(G,\bullet)\}$ are cohomological $\partial$-functors on the category of $\mathbb{Z}G$-modules, with respect to $\chi$ (by $M_S$, we mean think of $M$ as a $S$-module). Indeed, any coinduced module for $G$ is coinduced for $S$ by Proposition 8.5.[10] Since
$$\operatorname{Res}^0_{G/S} : M^G/N_G M \to M^S/N_S M, \quad \operatorname{Cor}_0^{S/G} : {}_{N_S}M/I_S M \to {}_{N_G}M/I_G M$$
are natural transformations, Theorem 5.2(1) applies to give unique morphisms Res and Cor extending $N_{G/S}$. (They agree in cohomology and homology with the original definitions by uniqueness in Theorem 5.2(1)).

Alternatively, we can extend the definitions of Res and Cor using dimension shifting (which is simpler, really).[11]

[9] To see this, note $t_1 S = t_2 S$ iff $t_1^{-1} t_2 \in S$, iff $St_1^{-1} = St_2^{-1}$.

[10] Note this would fail if we take $\chi$ to be the class of $\mathbb{Z}G$-injective modules, as $\mathbb{Z}G$-injective modules are not necessarily $\mathbb{Z}S$-injective.

[11] Alternatively, we can construct $\operatorname{Cor}^n$ explicitly as the map
$$H^n(S,M) \overset{\text{Shapiro}}{\cong} H^n(G, \operatorname{Coind}_S^G M) \to H^n(G,M)$$
where the last map is the change of group map induced by $G \cong G$ and $\operatorname{Coind}_S^G M \to M$ given by $\phi \mapsto \sum_i t_i \varphi(t_i^{-1})$, for some transversal $\{t_i\}$ for $S$ in $G$. This is just the norm map in dimension 0.

We now calculate the maps using dimension shifting.

1. Use the short exact sequence $0 \to M' \to M^* = \mathbb{Z}G \otimes_{\mathbb{Z}} M \to M \to 0$ from Proposition 9.8 to get the vertical isomorphisms in the diagram on the left below. (Note as before that $M^*$ is both $G$ and $S$-(co)induced.)

$$\begin{tikzcd} H_T^{-1}(S,M) \arrow[r, "\mathrm{Cor}_{S/G}^{-1}"] \arrow[d, "\delta"', "\cong"] & H_T^{-1}(G,M) \arrow[d, "\delta"', "\cong"] \\ H_T^0(S,M') \arrow[r, "\mathrm{Cor}_{S/G}^0"] & H_T^0(G,M). \end{tikzcd} \qquad \begin{tikzcd} {}_{N_S}M/I_SM \arrow[r] \arrow[d, "N_S(1\otimes\bullet)"', "\cong"] & {}_{N_G}M/I_GM \arrow[d, "N_G(1\otimes\bullet)"', "\cong"] \\ H_T^0(S,M') \arrow[r, "?"] & H_T^0(G,M). \end{tikzcd}$$

The left-hand diagram gives the right-hand diagram, after noting that $\delta$ is the map in the snake lemma in the proof of Theorem 9.3. From the right-hand diagram it is clear that the bottom map has to be $N_{G/S}$, because $N_{G/S} \circ N_S = N_G$.

2. From $0 \to M \to M^* \xrightarrow{f} M^*/M \to 0$ we get the commutative diagrams

$$\begin{tikzcd} H_T^{-1}(G,M^*/M) \arrow[r, "\mathrm{Res}_{G/S}^{-1}"] \arrow[d, "\delta"', "\cong"] & H_T^{-1}(S,M^*/M) \arrow[d, "\delta"', "\cong"] \\ H_T^0(G,M) \arrow[r, "\mathrm{Res}_{G/S}^0"] & H_T^0(S,M). \end{tikzcd} \qquad \begin{tikzcd} H_T^{-1}(G,M^*/M) \arrow[r, "?"] \arrow[d, "N_G\circ f^{-1}"', "\cong"] & H_T^{-1}(S,M^*/M) \arrow[d, "N_S\circ f^{-1}"', "\cong"] \\ M^G/N_GM \arrow[r] & M^S/N_SM. \end{tikzcd}$$

From $N_G = N_S \circ C_{G/S}$, the top map has to be $C_{G/S}$.

3. Recall the isomorphism $H_1(G^{\mathrm{ab}},\mathbb{Z}) \cong G^{\mathrm{ab}}$ was defined using the horizontal maps below.

$$\begin{tikzcd} H_1(S,\mathbb{Z}) \arrow[r, "\partial_1", "\cong"'] \arrow[d, "\mathrm{Cor}_1"] & H_0(S,I_S) \arrow[r, equal] \arrow[d, "\mathrm{Cor}_0"] & I_S/I_S^2 \arrow[r] & S/S' \arrow[d] \\ H_1(G,\mathbb{Z}) \arrow[r, "\partial_1", "\cong"'] & H_0(G,I_G) \arrow[r, equal] & I_G/I_G^2 \arrow[r] & G/G' \end{tikzcd}$$

The left square commutes by functoriality of Cor and the right rectangle commutes by tracing the map in Proposition 8.3. $\square$

## 11.3 Further properties

**Theorem 11.5:** corres Suppose $H$ is a subgroup of $G$ of finite index. Then $\mathrm{Cor}^n \circ \mathrm{Res}^n$ is multiplication by $[G:H]$.

*Proof.* In degree 0, we have $\mathrm{Cor}^0 \circ \mathrm{Res}^0 = [G:H]$ because $N_{G/H}$ is just multiplication by $[G:H]$ on $M^G$. As in the proof of Proposition 11.3, the general case then follows from either Theorem 5.2 or dimension shifting. $\square$

**Corollary 11.6:** hn-torsion

1. If $G$ is finite, then $|G|H^n(G, M) = 1$ for any $n > 0$.
2. If $G$ is finite and $M$ is finitely generated as an abelian group, then $H^n(G, M)$ is finite.

*Proof.*

1. By Theorem 11.5,
$$H^n(G, M) \xrightarrow{\text{Res}} H^n(1, M) \xrightarrow{\text{Cor}} H^n(G, M)$$
is multiplication by $|G|$. But $H^n(1, M) = 0$.
2. By the explicit description of $H^n(G, M)$ using the bar resolution, $H^n(G, M)$ is finitely generated. By item 1 it has finite exponent, so it must be finite.

□

**Corollary 11.7:** res-inj-p-prim Let $G$ be a finite group and $G_p$ its $p$-SSG. For any $G$-module $M$, the map
$$\text{Res}^n : H^n(G, M) \to H^n(G_p, M)$$
is injective on the $p$-primary component.

*Proof.* Suppose that $x \in \ker(\text{Res})$. Then $[G : G_p]x = \text{Cor} \circ \text{Res}(x) = 0$. Since the order of $x$ is a power of $p$ but $p \nmid [G : G_p]$, we get that $x = 0$. □

**Corollary 11.8:** cor:all-gp-0 If $H_T^n(G_p, A) = 0$ for all primes $p$ then $H_T^n(G, A) = 0$.

We will also need to know how restriction and corestriction affect cup products.

**Proposition 11.9:** res-cup The following hold.

1. $\text{Res}(x \cup y) = \text{Res}(x) \cup \text{Res}(y)$.
2. $\text{Cor}(x \cup \text{Res}(y)) = \text{Cor}(x) \cup y$.

*Proof.* See Cartan-Eilenberg [2], Chapter 12, or Atiyah-Wall in Cassels-Frohlich [3], p. 107. □

## 11.4 Inflation-restriction exact sequence

**Proposition 11.10:** inflate-restrict Suppose $H \trianglelefteq G$, $A$ is a $G$-module, and $n > 0$. If $H^i(H, A) = 0$ for all $i$ with $0 < i < r$, then

$$0 \to H^r(G/H, A^H) \xrightarrow{\text{Inf}} H^r(G, A) \xrightarrow{\text{Res}} H^r(H, A)$$

is exact.

*Proof.* We first prove the case $r = 1$. We show the following.

1. $\text{Res} \circ \text{Inf} = 0$: Change of group is functorial (easy to see from the definition), so $\text{Res} \circ \text{Inf}$ is induced by the maps $G/H \leftarrow G \hookleftarrow H$ and $M^H \hookrightarrow M \cong M$. The first map is 0 so $\text{Res} \circ \text{Inf} = 0$.

2. Inf is injective: Suppose $f : G/H \to A^H$ is a cocycle such that $\text{Inf}([f]) = 0$. Note $\text{Inf}([f]) = [f \circ p]$ where $p : G \to G/H$ is the projection. $\text{Inf}([f]) = 0$ means $f(s) = sa - a$ for some $a \in A$. Since $f$ is constant on cosets, $sa - a = sta - a$ for all $t \in H$, giving $ta = a$, and $a \in A^H$. Thus $[f] = 0$ in $H^1(G/H, A^H) = 0$.

3. $\ker(\text{Res}) \subseteq \text{im}(\text{Inf})$: Suppose $f : G \to A$ is a cocycle such that $[f] \in \ker(\text{Res})$. Since $\text{Res}[f] = [f \circ i]$, this means $f(t) = ta - a$ for some $a \in A$ and all $t \in H$. Define the coboundary $g : G \to A$ by $g(s) = sa - a$ for all $s \in G$; let $f_1 = f - g$; we have $[f_1] = [f]$.

   Now $f_1 = 0$ on $H$, and by definition of cocycle,
   $$f_1(st) = f_1(s) + sf_1(t).$$
   Letting $t$ range over $H$, we get that $f_1(st) = f_1(s)$, i.e. $f$ is constant on cosets of $H$. Letting $s \in H$ we have $f(st) = sf(t)$, so $\text{im}(f)$ is invariant under $H$. Thus $f$ descends to $f : G/H \to A^H$, i.e. $f \in \text{im}(\text{Inf})$.

Now we proceed by induction. Suppose the proposition holds for $r-1$. By dimension-shifting (Proposition 9.8), the exact sequence

$$eq:inf-res-shift 0 \to A \to A^* \to A^*/A \to 0 \tag{11.7}$$

with $A^*$ coinduced gives $\partial^{n-1} : H_T^{r-1}(G, A^*/A) \xrightarrow{\cong} H_T^r(G, A)$. We now show there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^{r-1}(G/H, (A^*/A)^H) \arrow[r, "\text{Inf}^{r-1}"] \arrow[d, "\partial^{n-1}"] & H^{r-1}(G, A^*/A) \arrow[r, "\text{Res}^{r-1}"] \arrow[d, "\partial^{n-1}"] & H^{r-1}(H, A^*/A) \arrow[d, "\partial^{n-1}"] \\
0 \arrow[r] & H^r(G/H, A^H) \arrow[r, "\text{Inf}^r"] & H^r(G, A) \arrow[r, "\text{Res}^r"] & H^r(H, A).
\end{tikzcd}$$

where all the vertical arrows are isomorphisms. We already know this for the middle arrow.

Since $A^*$ is $G$-coinduced, it is $H$-coinduced (Proposition 8.5), so the right vertical arrow is an isomorphism.

Since $H^1(H, A) = 0$, taking cohomology of (11.7) gives the exact sequence

$$0 \to A^H \to (A^*)^H \to (A^*/A)^H \to 0.$$

Recall $A^* = \text{Hom}(\mathbb{Z}[G], A)$, so $(A^*)^H = \text{Hom}(\mathbb{Z}[G/H], A)$ is $G/H$-coinduced. Thus we get the left vertical arrow is an isomorphism.

By (cohomological) functoriality of Inf and Res, the diagram commutes. $\square$

## 11.5 Transfer

hom-transfer Especially important for our purposes will be the restriction map on the first homology group.

**Definition 11.11:** The map $V_{G\to S}$ defined by the diagram below

$$\begin{tikzcd}
H_1(G,\mathbb{Z}) \arrow[r, equal] \arrow[d, "\mathrm{Res}_1"] & G/G' \arrow[d, "V_{G\to S}"] \\
H_1(S,\mathbb{Z}) \arrow[r, equal] & S/S'
\end{tikzcd}$$

is called the **transfer** or **Verlagerung**.

(The map Res defined on Tate cohomology in Section 11.2 also gives a map on homology.)

**Proposition 11.12:** pr:compute-transfer Let $G$ be a group and $S$ be a subgroup of finite index. The transfer is given by the following: Let $\{l_1,\ldots,l_n\}$ be a left transversal of $S$ in $G$. Then

$$\mathrm{Res}_1(g)=\prod_{i=1}^n g_iS'$$

where the $g_i\in S$ are such that $gl_i=l_{\pi(i)}g_{\pi(i)}$ for some permutation $\pi\in S_n$.

*Proof.* By functoriality of Res we have the commutative diagram (cf. Proposition 8.3)

$$\begin{tikzcd}
H_1(G,\mathbb{Z}) \arrow[r, "\partial_1", "\cong"'] \arrow[d, "\mathrm{Res}_1"] & H_0(G,I_G) \arrow[r, equal] \arrow[d, "\mathrm{Res}_0=C_{G/S}"] & I_G/I_G^2 \arrow[d, "C_{G/S}"] \\
H_1(S,\mathbb{Z}) \arrow[r, "\partial_1"] \arrow[dr, "\partial_1", "\cong"'] & H_0(S,I_G) \arrow[r, equal] & I_G/I_SI_G \\
& H_0(S,I_S) \arrow[r, equal] \arrow[u] & I_S/I_S^2 \arrow[u, hook]
\end{tikzcd}$$

where the top two $\partial_1$'s are from the exact sequence $0\to I_G\to\mathbb{Z}G\to\mathbb{Z}\to 0$, the bottom $\partial_1$ is from the exact sequence $0\to I_H\to\mathbb{Z}H\to\mathbb{Z}\to 0$, and the lower right square is induced by the inclusion $I_H\hookrightarrow I_G$. Replacing $H_1$ with $G^{\mathrm{ab}}$, we get

$$\begin{tikzcd}
G/G' \arrow[r, "\cong"] \arrow[d, "V_{G\to S}"] & I_G/I_G^2 \arrow[d, "C_{G/S}"] \\
S/S' \arrow[r] \arrow[dr, "\cong"] & I_G/I_SI_G \\
& I_S/I_S^2 \arrow[u, hook]
\end{tikzcd}$$

Given $g \in G/G'$, it maps to $g-1$ in $I_G/I_G^2$. We have

$$C_{G/S}(g-1) = \sum_{i=1}^{n} l_i^{-1}(g-1) = \sum_{i=1}^{n} g_i l_{\pi^{-1}(i)}^{-1} - l_i^{-1} = \sum_{i=1}^{n} i(g_i-1) l_{\pi^{-1}(i)}^{-1} \equiv \sum_{i=1}^{n}(g_i-1) \pmod{I_S I_G}.$$

The inverse image of this in $S/S'$ is $\prod_{i=1}^{n} g_i S'$, as needed. □

**Theorem 11.13:** transfer0 Let $G$ be a finite group. Then the transfer map

$$V : G^{\mathrm{ab}} \to (G')^{\mathrm{ab}}$$

is zero.

*Proof.* See Neukirch, [11, VI.7.6]. The proof uses the computation in Proposition 11.12. □

This will be important when we study the Hilbert class field.

# §12 Cohomology of cyclic groups

cyclic-groups The cohomology of cyclic groups is especially easy to understand, and will be very useful to us: when $L/K$ is an unramified extension of local fields, the Galois group $G(L/K) = G(l/k)$ is cyclic.

**Theorem 12.1:** iso+2 Let $G$ be a cyclic group and $x$ a generator. Let $\chi_x \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H_T^1(G, \mathbb{Q}/\mathbb{Z})$ be the homomorphism sending $x$ to $\frac{1}{|G|}$. Let $\delta : H_T^1(G, \mathbb{Q}/\mathbb{Z}) \to H_T^2(G, \mathbb{Z})$ be the diagonal map from the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. The map $\bullet \cup \delta\chi_x$ gives an isomorphism

$$H_T^r(G, M) \xrightarrow{\cong} H_T^{r+2}(G, M)$$

for all $G$-modules $M$ and $r \in \mathbb{Z}$.

Hence for all $n \in \mathbb{Z}$,

$$\begin{aligned} H_T^{2n-1}(G, A) &= {}_N A/DA \\ H_T^{2n}(G, A) &= A^G/NA. \end{aligned}$$

where $D$ is multiplication by $x-1$ .

*Proof.* Since $\mathbb{Q}$ is a divisible group, so is $H^n(G, \mathbb{Q})$, by looking at the description of $H^n$ in terms of cocycles (Section 7). Hence $\delta : H_T^1(G, \mathbb{Q}/\mathbb{Z}) \to H_T^2(G, \mathbb{Z})$ is an isomorphism and $\delta\chi_x$ is a generator of $H_T^2(G, \mathbb{Z})$.

The short exact sequence $0 \to I_G \to \mathbb{Z}G \to \mathbb{Z} \to 0$ splits because $G$ is cyclic:

$$\begin{tikzcd} 0 \arrow[r, shift left] & I_G \arrow[l, shift left] \arrow[r, shift left] & \mathbb{Z}G \arrow[l, shift left, "D"] \arrow[r, shift left, "\varepsilon"] & \mathbb{Z} \arrow[l, shift left] \arrow[r, shift left] & 0 \arrow[l, shift left] \end{tikzcd}$$

where $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$. Now $\mathbb{Z}G$ has trivial Tate cohomology by Proposition 9.7, so the diagonal maps in either direction are isomorphisms:

$$H^0_T(G,\mathbb{Z}) \xrightarrow[\cong]{\delta^0} H^1_T(G,I_G) \xrightarrow[\cong]{\delta^1} H^2_T(G,\mathbb{Z}).$$

Thus we can write $\delta\chi_x = \delta^0\delta^1 c$ for a generator $c$ of $H^0_T(G,\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$. Then by Theorem 10.1(4),

$$b \cup \delta\chi_x = b \cup \delta^0\delta^1 c = \delta^0\delta^1(b\cup c).$$

It suffices to show that the map $H^r_T(G,M) \xrightarrow{\bullet\cup c} H^r_T(G,M)$ is an isomorphism. But this map is just multiplication by $c$ for $r=0$, so it is multiplication by $c$ for all $r$. Now by Proposition 11.6 (true for $r>0$ and hence true for all $r$ by dimension-shifting) $|G|H^r_T(G,M)=0$. As $c$ is a generator of $\mathbb{Z}/|G|\mathbb{Z}$ it is relatively prime to $|G|$; hence multiplication by $c$ is an isomorphism on $H^r_T(G,M)$. This shows the isomorphism $H^r_T(G,M) \xrightarrow{\cong} H^{r+2}_T(G,M)$.

For the second part, note $H^{-1}_T(G,A) = {}_NA/DA$ and $H^0_T(G,A) = A^G/NA$. $\square$

**Corollary 12.2:** cor:exact-hex Let $G$ be a finite cyclic group. Suppose that $1\to A\to B\to C\to 1$ is an exact sequence of $G$-modules. Then there is an exact hexagon

*exact − hexagon*

$$\begin{tikzcd}
 & H^0_T(G,A) \arrow[r, "f_1"] & H^0_T(G,B) \arrow[dr, "f_2"] & \\
H^1_T(G,C) \arrow[ur, "f_6"] & & & H^0_T(G,C) \arrow[dl, "f_3"] \\
 & H^1_T(G,B) \arrow[ul, "f_5"] & H^1_T(G,A) \arrow[l, "f_4"] &
\end{tikzcd} \tag{11.8}$$

*Proof.* We have $H^2_T(G,A)\cong H^0_T(G,A)$. $\square$

## 12.1 Herbrand quotient

herbrand

**Definition 12.3:** Let $G$ be a finite cyclic group and $A$ a finite $G$-module. Define the **Herbrand quotient** to be

$$h(A) = h(G,A) = \frac{|H^{2n}_T(G,A)|}{|H^{2n-1}_T(G,A)|}$$

for any $n$.

This is well-defined by Theorem 12.1.

The following key properties of the Herbrand quotient will help us in computations.

**Proposition 12.4:** herbrand-1 Let $G$ be a finite cyclic group. The Herbrand quotient satisfies the following.

1. If $A$ is a finite $G$-module, then $h(G, A) = 1$.

2. ($h$ is an Euler-Poincaré function) If $1 \to A \to B \to C \to 1$ is an exact sequence of $G$-modules, then
$$h(G, B) = h(G, A)h(G, C).$$
(If two of these are defined then the other is defined.)

3. If $G$ acts trivially on $\mathbb{Z}$, then $h(G, \mathbb{Z}) = |G|$.

4. If $f : A \to B$ has finite kernel and cokernel, then $h(A) = h(B)$.

*Proof.* 1. We use Theorem 12.1 to calculate the quotient. We have the exact sequences

$$\begin{tikzcd} 0 \arrow[r] & {}_N A \arrow[r] & A \arrow[r, "N"] & NA \arrow[r] & 0 \end{tikzcd} \qquad \begin{tikzcd} 0 \arrow[r] & \ker D \arrow[r] \arrow[d, equal] & A \arrow[r] & DA \arrow[r] & 0. \\ & A^G & & & \end{tikzcd}$$

Hence
$$|NA||{}_N A| = |A| = |A^G||DA|,$$
giving
$$|H^1(G, A)| = |{}_N A/DA| = |A^G/NA| = |H^2(G, A)|.$$

2. Keeping the notation in the hexagon 11.8, we have
$$H^0(G, A) = |\ker f_1| \cdot \frac{|H^0(G, A)|}{|\ker f_1|} = |\mathrm{im} f_6||\mathrm{im} f_1|.$$
We can similarly calculate the other quantities to get the result.

3. Let $|G| = n$, and $[n]$ denote multiplication by $n$. We have
$$h(G, \mathbb{Z}) = \frac{|H_T^0(G, \mathbb{Z})|}{|H_T^{-1}(G, \mathbb{Z})|} = \frac{|\mathbb{Z}^G/N\mathbb{Z}|}{|{}_N\mathbb{Z}/I_G\mathbb{Z}|} = \frac{|\mathbb{Z}/n\mathbb{Z}|}{|\ker[n]|} = \frac{|G|}{1} = |G|.$$

4. The exact sequence $1 \to \ker f \to A \to B \to \operatorname{coker} f \to 1$ gives $h(G, \ker f)h(G, B) = h(G, A)h(G, \operatorname{coker} f)$ (split the exact sequence into 2 short exact sequences and use part 2). The result now follows from part 1. □

# §13 Tate's Theorem

tate-thm-section Our main goal in this section is to prove the following.

**Theorem 13.1** (Tate's Theorem)**:** tate-thm Let $G$ be a finite group and $M$ be a $G$-module. Suppose that for all subgroups $H \subseteq G$,

1. $H^1(H, M) = 0$ and
2. $H^2(H, M)$ is cyclic of order $|H|$.

Then given a generator $u \in H^2(G, M)$, there is an isomorphism

$$H_T^r(G, \mathbb{Z}) \xrightarrow{\bullet \cup u} H_T^{r+2}(G, M)$$

for all $r$.

This is the main application of group cohomology to class field theory, as this will be the inverse of the Artin map: for instance, in local class field theory we have

$$\begin{aligned} &H_T^{-2}(G(L/K), \mathbb{Z}) = G(L/K)^{\text{ab}} \\ &H_T^0(G(L/K), L^\times) = (L^\times)^{G(L/K)} / \operatorname{Nm}_{L/K}(L^\times) = K^\times / \operatorname{Nm}_{L/K}(L^\times). \end{aligned}$$

The conditions of Tate's Theorem may seem unmotivated, but keep in mind that they are basically the key conditions satisfied in the number-theoretic setting, when $G$ is taken to be a Galois group and $M$ is taken to be a field (or idele group).

Class field theory was initially proved without group cohomology, but group cohomology gives a much nicer way to organize and abstract the proof. This theorem is a key part of that abstraction: isolating the key number-theoretic conditions that result in the Artin isomorphism. In proving both local and global class field theory, we will spend significant time showing that the hypothesis of Tate's Theorem holds. (The key difference in local and global class field theory is that we put in different things for $M$.)

*Proof.* Serre [14], Section IX.8. □

# §14 Profinite groups

profinite-cohom In this section we study the cohomology groups when $G$ is a profinite group. In this case topology becomes important. We will apply the results when $G$ is an infinite Galois group.

We find that we have two ways of interpreting the resulting cohomology groups:

1. Imitate the previous construction but work in the category of topological $G$-modules instead. I.e. feed in "category of topological groups" into our cohomology functor.

2. Take the direct limit over finite quotients of $G$.

**Definition 14.1:** top-g-mod A **topological** $G$**-module** is a $G$-module that is a topological group, and such that the map

$$\begin{aligned} \varphi : G \times M &\to M \\ (g, m) &\mapsto gm \end{aligned}$$

is continuous.

We will always give $M$ the discrete topology, so this is equivalent to the following condition:

$$M = \bigcup_{H \text{ open subgroup of } G} M^H.$$

Indeed, because $M$ has the discrete topology, for the action to be continuous, $\pi_G(\varphi^{-1}(m))$ must be open, where $\pi_G : G \times M \to G$ is the projection. This is just the stabilizer of $m$, so the stabilizer of $m$ must contain an open subgroup of $G$. Hence, every $m \in M$ must be contained in some $M^H$.

We define $H^n(G, M)$ as before, but now in the category of topological $G$-modules, i.e. we replace every instance of $\mathrm{Hom}_G$ with $\mathrm{Hom}_G^{\mathrm{cont}}$, since in this category the morphisms are *continuous* $G$-homomorphisms. Note that the category of discrete $G$-modules has enough injectives.

**Theorem 14.2:** profinite-lim2 Let $G$ be a profinite group. We have

$$H^n(G, M) = \varinjlim H^n(G/S, M^S)$$

where the limit is over open normal subgroups $S$ and the maps are the inflation maps

$$\mathrm{Inf}^n : H^n(G/S, M^S) \to H^n(G/T, M^T), \quad S \supseteq T.$$

*Proof.* Milne [9], II.4.2. □

We have a similar result if we take the limit over $M$.

**Proposition 14.3:** pr:H-commutes-lim Let $G$ be a profinite group and suppose $M = \varinjlim H^r(G, M_i)$ is a discrete $G$-module, and each $M_i$ injects into $M$. Then

$$H^n(G, M) = \varinjlim H^n(G, M_i).$$

*Proof.* Milne [9], II.4.4. □

# §15 Nonabelian cohomology

nonabelian-cohom In this section we define cohomology $H^n(G, A)$ when $A$ is *non-abelian*. (It was okay for $G$ to be non-abelian because we saw it in the guise of $\mathbb{Z}G$, but we needed $A$ to be in an abelian category.) The cohomological construction fails and we instead imitate the results of Theorem 7.2. (The description of $H^1$ and $H^2$ in Theorem 7.2 are useful because derivations and factor sets are used to classify a lot of things.)

We will only be able to get a "piece" of the long exact sequence. Cohomology also lacks a lot of structure: we speak not of cohomology groups, because they are now only pointed sets. We write $A$ multiplicatively, as is the convention for nonabelian groups.

**Definition 15.1:** The category of **pointed sets** is the category whose objects are pairs $(A, a)$, where $A$ is a set and $a \in A$, and such that a morphism $(A, a) \to (B, b)$ is a function $A \to B$ taking $a$ to $b$.

The **kernel** of $f : (A, a) \to (B, b)$ is $f^{-1}(b)$. Thus we can define an exact sequence of pointed sets.

We now define the cohomology (pointed) sets. These will coincide with the definition in the abelian case by Theorem 7.2, except we only retain the structure of a pointed set.

**Definition 15.2:** df:nonabelian-cocycles Let $G$ be a group and $A$ a group with $G$-action.

1. Define
$$H^0(G, A) = A^G := \{a \in A : sa = a \text{ for all } s \in G\}.$$
The distinguished element is 1.

2. Define a **1-cocycle** to be a map $d : G \to A$ such that
$$d(xy) = d(x) \cdot xd(y)$$
and let $\mathrm{Der}(G, A)$ be the set of 1-cocycles. Two cocycles $d_1, d_2$ are **cohomologous** if there exists $a \in A$ so that[12]
$$d_2(x) = a^{-1} \cdot d_1(x) \cdot xa.$$
Note this is an equivalence relation; define $H^1(G, A)$ to be the pointed set of 1-cocycles modulo equivalence. The distinguished element is the unit cocycle $d(x) \equiv 1$.

For an exact sequence of non-abelian $G$-modules
$$1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$$
with $i(A) \trianglelefteq B$, define the **coboundary operator** $\delta : H^0(G, C) \to H^1(G, A)$ as follows: given $c \in G^G$, choose any $b \in p^{-1}(c)$ and set
$$\delta(c) = d \text{ where } d(s) = i^{-1}(b^{-1}s(b)).$$

[12]The analogue in the abelian case was $d_2(x) = -a + d_1(x) + xa$.

If furthermore $i(A)$ is in the center of $B$ (so $A$ is abelian), define $\Delta : H^1(G,C) \to H^2(G,A)$ as follows: for $d_c \in H^1(G,C)$, choose $d_b$ such that $p_* d_b = d_c$, and set

$$[\Delta(d)](x,y) = d_b(s) \cdot s(d_b(t)) \cdot d_b(st)^{-1}.$$

*Proof of well-definedness.* Note the coboundary operator is defined by imitating the construction in the snake lemma.

$$\begin{tikzcd} & & C^G \arrow[d] \\ A \arrow[r, dotted, "i"] \arrow[d, dotted, "d_1"] & B \arrow[r, "p"] \arrow[d, "d_1"] & C \\ \mathrm{Der}(G,A) \arrow[r, "i"] & \mathrm{Der}(G,B) & \end{tikzcd} \qquad \begin{tikzcd} & c \arrow[d] \\ b \arrow[r, "p"] \arrow[d, "d_1"] & c \\ (s \mapsto b^{-1}s(b)) & \end{tikzcd}$$

$$(s \mapsto i^{-1}(b^{-1}s(b))) \xrightarrow{i} (s \mapsto b^{-1}s(b))$$

We need to show that $s \mapsto b^{-1}s(b)$ is actually a cocycle; its image is in $A$ because $s(b) \equiv b^{-1} \pmod{i(A)}$ by exactness; show that the cohomology class is independent of the choice of $b$.

The second part is similar. Everything is easy to prove so we omit it. See Serre [14], Appendix to Chapter VII. □

**Theorem 15.3** (Exact sequence in nonabelian cohomology)**:** thm:nonabelian-les Let $1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$ be an exact sequence of non-abelian $G$-modules. Then the following is exact.

$$\begin{tikzcd} 1 \arrow[r] & H^0(G,A) \arrow[r, "i_0"] & H^0(G,B) \arrow[r, "p_0"] & H^0(G,C) \arrow[r, "\delta"] & H^1(G,A) \arrow[r, "i_1"] & H^1(G,B) \arrow[r, "p_1"] & H^1(G,C) \arrow[d, dotted, "\Delta"] \\ & & & & & & H^2(G,A) \end{tikzcd}$$

(with the last map present if $A$ is in the center of $B$).

# Chapter 12
# Introduction to Galois cohomology

galois-cohomology-ch We will apply group (co)homology as follows: Take a Galois extension $L/K$ and let $G := G(L/K)$. Take as a $G$-module a multiplicative or additive subgroup $S$ of $L$. The special case that $G$ is cyclic will come up often, since if $L/K$ is an unramified extension of local fields, then $G$ is cyclic. Furthermore, the norm map $N_G$ has a natural interpretation:

1. If $S \subseteq L^\times$ then for $a \in S$,
$$N_G(a) = \prod_{\sigma \in G} \sigma(a) = \mathrm{Nm}_{L/K}(a).$$
2. If $S \subseteq L^+$ then for $a \in S$,
$$N_G(a) = \sum_{\sigma \in G} \sigma(a) = \mathrm{Tr}_{L/K}(a).$$

In Section 2 we give an application to Kummer theory (characterizing certain abelian extensions $L$ of $K$ in terms of $L^{\times n} \cap K$). Kummer theory will allow us to prove the linear independence of $n$th roots.

Finally, we give two interpretations of Galois cohomology groups.

1. $H^1(G(L/K), \mathrm{Aut}(V))$ parameterizes algebraic structures defined over $K$ that become isomorphic in $L$ (Section 3). This is called *descent*.
2. $H^2(G(L/K), L^\times)$ parameterizes classes of $K$-algebras "split" over $L$ (Section 4), i.e. it is the *Brauer group*.

## §1 Basic results

galois-cohomology We prove two fundamental theorems on the cohomology of $L^\times$ and $L^+$.

**Theorem 1.1** (Hilbert's Theorem 90)**:** h90 (†) Let $L/K$ be a Galois extension with Galois group $G$. Then
$$H^1(G, L^\times) = \{1\}.$$
Moreover, if $G = \langle \sigma \rangle$ is cyclic and $u \in L^\times$, then the following are equivalent.

1. $\mathrm{Nm}_{L/K}(u) = 1$.

2. There exists $v \in L^\times$ such that $u = \sigma(v)v^{-1}$.

We will often abbreviate $H^1(G(L/K), L^\times)$ as $H^1(L/K)$.

*Proof.* First suppose $G$ is finite. Let $c : G \to L^\times$ be a 1-cocycle; we have $c_{\sigma\tau} = \sigma(c_\tau)c_\sigma$. Consider the function

$$b(e) := \sum_{\tau\in G} c_\tau \tau(e).$$

By linear independence of the characters $\tau \in G$, $b$ is not identically zero; hence there exists $e \in L^\times$ so that $b(e) \neq 0$. Operating by $\sigma$ on both sides and using the cocycle condition gives

$$eq : h90pf\,\sigma(b(e)) = \sum_{\tau\in G} \sigma(c_\tau)(\sigma\tau)(e) = \sum_{\tau\in G} c_{\sigma\tau}c_{\sigma^{-1}}(\sigma\tau)(e) = c_\sigma^{-1}b(e) \tag{12.1}$$

and $c_\sigma = b(e)\sigma(b(e))^{-1}$, so $c$ is a coboundary.

The infinite case follows from the finite case and Theorem 11.14.2.

For the second part, note that $H^1(G, L^\times) = \ker(N)/\mathrm{im}(D) = 0$ gives $\ker(N) = \mathrm{im}(D)$. Here $N$ is the norm map $\mathrm{Nm}_{L/K}$ and $D$ is the map $\sigma - 1$, i.e. the map $v \mapsto \frac{\sigma(v)}{v}$. □

Next we think of $L$ as an additive group.

**Theorem 1.2:** h+0 Let $L/K$ be a finite Galois extension. Then

$$H^r(G, L^+) = 0, \quad r > 0.$$

*Proof.* From the normal basis theorem **??.??**, there exists $\alpha \in L$ such that $\{\sigma\alpha : \sigma \in G\}$ is a basis for $L$ over $K$. We get that $K[G] \cong L$ as $G$-modules by the map

$$\sum_{\sigma\in G} a_\sigma \sigma \mapsto \sum_{\sigma\in G} a_\sigma \sigma\alpha.$$

Since $K[G] \cong \mathrm{Ind}_{\{1\}}^G(K)$,

$$H^r(G, L^+) \cong H^r(\{1\}, K) = 0$$

by Shapiro's Lemma 8.6. □

# §2 Kummer theory

kummer We use Galois cohomology to prove the following.

**Theorem 2.1** (Kummer theory)**:** kummer-theorem Suppose $K$ is a field containing a primitive $n$th root of 1. Then there is a bijection between

1. Finite abelian extensions of $K$ of exponent dividing $n$ (i.e. for any $\sigma$ in the Galois group $G(L/K)$, $\sigma^n = 1$).
2. Subgroups of $K^\times$ containing $K^{\times n}$ as a subgroup of finite index (i.e. subgroups of $K^\times/K^{\times n}$).

This correspondence is given by

$$\begin{aligned} L &\mapsto K^\times \cap L^{\times n} \\ K[B^{\frac{1}{n}}] &\leftarrow\!\shortmid B. \end{aligned}$$

Moreover,

$$degree - order[L:K] = [K^\times \cap L^{\times n} : K^\times] \tag{12.2}$$

(Note in the reverse map, which $n$th roots we take doesn't matter because $K$ contains $n$th roots of unity.)

In the course of proving this theorem, we will show the following useful proposition.

**Proposition 2.2:** pr:kummer-char Let $K$ be a field containing a primitive $n$th root of 1 and $L/K$ an abelian extension with Galois group $G$. Then there is a natural isomorphism

$$\begin{gathered} K^\times \cap L^{\times n}/K^{\times n} \cong H^1(G, \mu_n) = \operatorname{Hom}(G, \mu_n) \\ a \mapsto \left(\sigma \mapsto \frac{\sigma\left(a^{\frac{1}{n}}\right)}{a^{\frac{1}{n}}}\right). \end{gathered}$$

In particular, there is a natural isomorphism

$$K^\times/K^{\times n} \cong H^1(G(K^s/K), \mu_n) = \operatorname{Hom}(G(K^s/K), \mu_n).$$

*Proof.* Let $G = G(L/K)$, and denote the forward map by $B(L) = K^\times \cap L^{\times n}$. The key step is showing that (12.2) holds; we do this by interpreting $K^\times \cap L^{\times n}$ as a 0th cohomology module. The inclusions $L \supseteq K(B(L)^{\frac{1}{n}})$ and $B(K(B^{\frac{1}{n}})) \supseteq B$ are easily seen to hold (Step 2), so (12.2) will give that equality holds (Steps 3-4).

Step 1: By Theorem 11.4.6, the short exact sequence of $G$-modules

$$1 \to \mu_n \to L^\times \xrightarrow{x \mapsto x^n} L^{\times n} \to 1$$

induces the long exact sequence

$$1 \to H^0(G, \mu_n) \to H^0(G, L^\times) \to H^0(G, L^{\times n}) \to H^1(G, \mu_n) \to H^1(G, L^\times) \to \cdots.$$

We need not go further because Hilbert's Theorem 90 (Theorem 1.1) tells us

$$H^1(G(L/K), L^\times) = 1.$$

Next, note that $H^0(G,H)$ is simply the subgroup of $H$ fixed by $G$, and that the subfield of $L$ fixed by $G$ is $K$. As $\mu_n \subset K$, $G$ acts trivially on $\mu_n$ and $H^1(G,\mu_n) = \mathrm{Hom}(G,\mu_n)$ by Corollary 11.7.3. The sequence becomes

$$1 \to \mu_n \to K^\times \xrightarrow{x\mapsto x^n} K^\times \cap L^{\times n} \to \mathrm{Hom}(G,\mu_n) \to 1,$$

giving an isomorphism

$$K^\times \cap L^{\times n}/K^{\times n} \cong \mathrm{Hom}(G,\mu_n).$$

The map is $\partial^1(a) = \left(\sigma \mapsto \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}\right)$, as shown by tracing through the construction in Theorem 11.3.3. This proves Proposition 2.2.

$$\begin{tikzcd}
 & & K^\times \cap L^{\times n} \arrow[d] \\
\mu_n \arrow[r, dotted, "i"] \arrow[d, dotted, "d_1"] & L^\times \arrow[r, "x\mapsto x^n"] \arrow[d, "d_1"] & L^{\times n} \\
\mathrm{Der}(G,\mu_n) \arrow[r, "i"] & \mathrm{Der}(G,L^\times) &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & a \arrow[d] \\
 & a^{\frac{1}{n}} \arrow[r, "x\mapsto x^n"] \arrow[d, "d_1"] & a \\
\left(\sigma \mapsto \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}\right) \arrow[r, "i"] & \left(\sigma \mapsto \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}\right) &
\end{tikzcd}$$

We claim that $|\mathrm{Hom}(G,\mu_n)| = |G|$. Indeed, by the structure theorem for abelian groups, $G$ decomposes as $(\mathbb{Z}/n_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/n_m\mathbb{Z})$ where $n_1,\ldots,n_m \mid n$. To choose a homomorphism for $G$ means choosing images for the generators of $\mathbb{Z}/n_1\mathbb{Z},\ldots,\mathbb{Z}/n_m\mathbb{Z}$; there are $n_1,\ldots,n_m$ possibilities, respectively, for a total of $|G|$.

Then

$$[L:K] = |G(L/K)| = [K^\times \cap L^{\times n} : K^\times].$$

This shows (12.2).

<u>Step 2:</u> Next note the following two inclusions.

1. $K[B(L)^{\frac{1}{n}}] \subseteq L$: Anything in $(K^\times \cap L^{\times n})^{\frac{1}{n}}$ is in the form $(\beta^n)^{\frac{1}{n}}$ and hence in $L$.
2. $B(K[B^{\frac{1}{n}}]) \supseteq B$: Anything in $B$ is in the form $(b^{\frac{1}{n}})^n$ and hence in $K^\times \cap K(B^{\frac{1}{n}})^{\times n}$.

<u>Step 3:</u> We show that $K[B(L)^{\frac{1}{n}}] = L$. By the inclusions in step 2,

$$[L:K] \geq [K[B(L)^{\frac{1}{n}}]:K] \overset{(12.2)}{=} [B(K[B(L)^{\frac{1}{n}}]) : K^\times] \geq [B(L):K^\times].$$

But $[L:K] = [B(L):K^\times]$ by (12.2), so equality holds everywhere. The first equality gives the conclusion.

<u>Step 4:</u> We show that $B(K[B^{\frac{1}{n}}]) = B$. We apply step 1 with $L = K[B^{\frac{1}{n}}]$ to get the isomorphism

$$B(L) = K^\times \cap L^{\times n}/K^{\times n} \xrightarrow{\cong} \mathrm{Hom}(G,\mu_n)$$
$$a \mapsto \left(\sigma \mapsto \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}\right).$$

Now $B \subseteq B(L)$ gets mapped to a subgroup $H' \subseteq \mathrm{Hom}(G, \mu_n)$, which can be identified with $\mathrm{Hom}(G/H, \mu_n)$[1]. But as the $a^{\frac{1}{n}}$ generate $L$ over $K$ and the fixed field of $G$ is $K$, $\bigcap_{h \in H'} \ker h = 1$. Thus $H = \{1\}$. Hence $|B(L)| = |G| = |B|$, and $B = B(L)$. □

**Corollary 2.3** ($n$th roots are linearly independent)**:** Let $S$ be a set of nonzero integers so that $\frac{a}{b}$ is not a perfect $n$th power for any distinct $a, b \in S$. Then the elements

$$\sqrt[n]{s}, \quad s \in S$$

are linearly independent over $\mathbb{Q}$.

*Proof.* Step 1: It suffices to show that for distinct primes $p_1, \ldots, p_k$, we have

$$roots-right-degree[\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k}) : \mathbb{Q}] = n^k. \tag{12.3}$$

Then a basis for this extension over $\mathbb{Q}$ is formed by taking products of basis elements for the $\mathbb{Q}(\sqrt[n]{p_j})$:

$$basis-sqrt\left\{\sqrt[n]{p_1^{a_1} \cdots p_k^{a_k}} : 0 \le a_j < n\right\}. \tag{12.4}$$

However, the radicands are exactly the representatives of elements in $\mathbb{Q}^\times/\mathbb{Q}^{\times n}$. The elements of $S$ are all represented by distinct elements of (12.4) modulo $\mathbb{Q}^\times$, so the theorem will follow. (To deal with $s \in S$ negative, note if $s$ is negative then $\sqrt[n]{s}$ is a not in $\mathbb{R}$.)

We want to use Kummer theory to conclude (12.3). However, $\mathbb{Q}$ only has square roots of unity ($\pm 1$), so we have to consider all other roots separately. We may as well assume $2 \mid n$.

Step 2: We first show

$$roots-indpt-index1[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k. \tag{12.5}$$

Let $B$ be the subgroup of $\mathbb{Q}^\times$ generated by $p_1, \ldots, p_k$ and $\mathbb{Q}^{\times 2}$. By Theorem 2.1,

$$[\mathbb{Q}(B^{\frac{1}{2}}) : \mathbb{Q}] = [B : \mathbb{Q}^{\times 2}] = 2^k,$$

as needed.

[1] The subgroups of $G$ are in bijective correspondence with the subgroups of $\mathrm{Hom}(G, \mu_n)$ via the map

$$\begin{aligned} H &\xrightarrow{\Phi} \{h \in \mathrm{Hom}(G, \mu_n) : H \subseteq \ker h\} \cong \mathrm{Hom}(G/H, \mu_n) \\ \bigcap_{h \in H'} \ker h &\xleftarrow{\Psi} H' \end{aligned}$$

Indeed, clearly $\Psi(\Phi(H)) \supseteq H$, and we have equality since for every $g \in G \backslash H$ we can find $h \in \mathrm{Hom}(G, \mu_n)$ with kernel containing $H$, so that $h(g) \neq 1$. Since $\mathrm{Hom}(G, \mu_n) \cong G$, they have the same number of subgroups, and this is a bijection.

Step 3: We now adjoin $n$th roots of unity such that we can apply Kummer theory for $n$th roots. Let $N$ be a positive integers such that $n \mid N$ and $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) \subseteq \mathbb{Q}(\zeta_N)$ (every quadratic extension is contained in a cyclotomic extension; we can take $N = 4p_1 \cdots p_k n$).

However, if we look at $K := \mathbb{Q}(\zeta_N)$, what if elements that aren't $n$th powers in $\mathbb{Q}$ become $n$th powers? Fortunately, this doesn't happen for $n \neq 2$. We show that for even $n \neq 2$ and $m \in \mathbb{Q}$ not a perfect $\frac{n}{2}$th power,

$$root-not-in-cyclotomic \sqrt[n]{m} \notin \mathbb{Q}(\zeta_N). \tag{12.6}$$

By taking roots, we may assume that $m$ is not a perfect $d$th power for any $d \mid n$.

Note $L := \mathbb{Q}(\sqrt[n]{m}, \zeta_n)$ is a Galois extension of $\mathbb{Q}$ since it is the splitting field of $X^n - m$. Note $X^n - m$ is irreducible over $\mathbb{Q}$ because the constant term of any proper factor must be in the form $m^{\frac{j}{n}} \notin \mathbb{Q}$ where $0 < j < n$. Hence there exists $\tau \in G(L/\mathbb{Q})$ sending $\sqrt[n]{m}$ to $\zeta_n \sqrt[n]{m}$. Let $\sigma \in G(L/\mathbb{Q})$ denote complex conjugation. Then

$$\begin{aligned}\sigma\tau(\sqrt[n]{m}) &= \sigma(\zeta_n \sqrt[n]{m}) = \zeta_n^{-1} \sqrt[n]{m} \\ \tau\sigma(\sqrt[n]{m}) &= \tau(\sqrt[n]{m}) = \zeta_n \sqrt[n]{m}.\end{aligned}$$

Hence $G(L/\mathbb{Q})$ is not abelian. Since all cyclotomic extensions are abelian, $L$ cannot be contained in an abelian extension, giving (12.6).

Let $C$ be the subgroup of $\mathbb{Q}(\zeta_N)^\times$ generated by $\sqrt{p_1}, \ldots, \sqrt{p_k}$ and $\mathbb{Q}(\zeta_N)^{\times \frac{n}{2}}$. We showed above that $\sqrt[n]{m} \notin \mathbb{Q}(\zeta_N)^{\times \frac{n}{2}}$ for any $m$ not a perfect $\frac{n}{2}$th power so $[C : \mathbb{Q}(\zeta_N)^{\times \frac{n}{2}}] = \left(\frac{n}{2}\right)^k$. By Kummer Theory,

$$[\mathbb{Q}(\zeta_N, \sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k}) : \mathbb{Q}(\zeta_N)] = [\mathbb{Q}(C^{\frac{n}{2}}) : K] = [C : \mathbb{Q}(\zeta_N)^{\times \frac{n}{2}}] = \left(\frac{n}{2}\right)^k.$$

Since $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k}) \subseteq \mathbb{Q}(\zeta_N)$ we get

$$roots-indpt-index2[\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})] = \left(\frac{n}{2}\right)^k. \tag{12.7}$$

Combining (12.5) and (12.7) gives (12.3), as needed. □

## §3 Nonabelian Galois cohomology

sec:nonabelian-galois-cohom Because of the definition of $H^1$ in Section 11.15, we find that we can often interpret $H^1(G(L/K), A)$ as parameterizing certain algebraic structures, specifically a set of them defined over $K$ that become isomorphic in $L$. (This is known as *descent* because it answers the question, how many ways can an algebraic structure (or in general, a variety) "descend" from $L$ to $K$?) In general,

$$\begin{aligned}&H^1(G(L/K), \{\text{automorphisms preserving } V \text{ over } K\}) \\ &\qquad \cong \{K\text{-isomorphism classes that are } L\text{-congruent to } V\} eq:descent\end{aligned} \tag{12.8}$$

In this section, we will see several examples where $A$ is an algebraic group. We could also take $A$ to be an abelian variety (see Silverman [16], Theorem X.2.2, for instance).

In particular, we find in the next section that a special cohomology group classifies algebra structures over $K$: the Brauer group.

First, we need the following nonabelian generalization of Hilbert's Theorem 90 (1.1).

**Theorem 3.1** (Generalization of Hilbert's Theorem 90)**:** thm:gen-h90 For any finite Galois extension $L/K$, letting $G = G(L/K)$,

$$H^1(G, \mathrm{GL}_n(L)) = H^1(G, \mathrm{SL}_n(L)) = 1.$$

*Proof.* As in Theorem 1.1, given a 1-cocycle $c : G \to GL_n(L)$, consider the function

$$\begin{aligned} b : \mathrm{GL}_n(L) &\to \mathcal{M}_n(L) \\ b(A) &:= \sum_{\tau \in G} c_\tau \tau(A). \end{aligned}$$

Note that unlike in the proof of Theorem 1.1, we not only have to choose $A$ to be nonzero, but also invertible.

Also define $b$ on $L^n$ in the same way:

$$\begin{aligned} b : L^n &\to L^n \\ b(\mathbf{x}) &:= \sum_{\tau \in G} c_\tau \tau(\mathbf{x}). \end{aligned}$$

We show that $\{b(\mathbf{x}) : \mathbf{x} \in L^n\}$ generate $L^n$ as a vector space over $L$.[2] Suppose a linear functional $f : L^n \to L$ vanishes on all the $b(\mathbf{x})$. Then for every $\alpha \in L$,

$$0 = f(b(\alpha\mathbf{x})) = \sum_{\tau \in G} f(c_\tau \tau(\alpha)\tau(\mathbf{x})) = \sum_{\tau \in G} \tau(\alpha) f(c_\tau \tau(\mathbf{x})).$$

By linear independence of characters, we get that all the coefficients of the $\tau(\alpha)$ must be 0, i.e. $f(c_\tau \tau(\mathbf{x}))$ for all $c_\tau, \mathbf{x}$. But $c_\tau \in \mathrm{GL}_n(L)$ is invertible, so $f$ must vanish identically on $L^n$. We've shown that every linear functional vanishing on $\{b(\mathbf{x})\}$ vanishes on $L^n$; therefore $\mathrm{span}_L\{b(\mathbf{x})\} = L^n$.

Thus we can choose $\mathbf{x}_1, \ldots, \mathbf{x}_n$ such that $\mathbf{y}_j = b(\mathbf{x}_j)$ form a basis for $L^n$ over $L$. Let $A$ be the matrix sending the canonical basis $\mathbf{e}_j$ to the $\mathbf{x}_j$. Then (note $\tau$ acts trivially on the $e_j$)

$$b(A)\mathbf{e}_j = b(A\mathbf{e}_j) = \mathbf{y}_j$$

so $b(A)$ is invertible.

The the rest of the proof of Theorem 1.1 goes through: we have as in (12.1) that

$$c_\sigma = b(A)\sigma(b(A))^{-1},$$

[2] Note $b$ is not a $L$-linear transformation; it is a $K$-linear transformation.

i.e. $c$ is a coboundary. This shows $H^1(G, \mathrm{GL}_n(L)) = 1$.

For the second part, the exact sequence

$$1 \to \mathrm{SL}_n(L) \to GL_n(L) \xrightarrow{\det} L^\times \to 1$$

gives the long exact sequence 11.15.3

$$\begin{tikzcd} H^0(G, \mathrm{GL}_n(L)) \arrow[r, "\det"] \arrow[d, equal] & H^0(G, L^\times) \arrow[r] \arrow[d, equal] & H^1(G, \mathrm{SL}_n(L)) \arrow[r] & H^1(G, \mathrm{GL}_n(L)) \arrow[d, equal] \\ \mathrm{GL}_n(K) \arrow[r, two heads, "\det"] & K^\times & & 0. \end{tikzcd}$$

As the map on the left is surjective, we get $H^1(G, \mathrm{SL}_n(L)) = 1$. $\square$

We have now established (12.8) when $V$ is a vector space: all vector spaces that become isomorphic in $L$ have the same dimension to begin with so are isomorphic in $K$, so the right-hand side of (12.8) is $\{1\}$, and if $V = K^n$, $\mathrm{GL}_n(L)$ is the group of automorphisms preserving $V$ over $L$, and Theorem 3.1 shows the right-hand side of (12.8) is $\{1\}$. We now extend this to other algebraic structures.

To encode an algebraic structure, we consider vector spaces and tensors.

**Example 3.2:** ex:tensors
Let $V$ be a finite-dimensional vector space. The space $V^{\otimes p} \otimes V^{*\otimes q}$ encodes...

| $p$ | $q$ | Structure |
|---|---|---|
| 1 | 0 | vectors |
| 0 | 1 | linear functionals |
| 1 | 1 | linear operators |
| 0 | 2 | bilinear forms |
| 1 | 2 | algebra structures |

We focus on the case $p = 1$, $q = 2$. Given a tensor $\sum_i v_i \otimes f_i \otimes g_i \in V \otimes V^{*\otimes 2}$, define a (not necessarily commutative or associative) algebra structure on $V$ by

$$v \cdot w = \sum_i f_i(v) g_i(w) v_i.$$

Conversely, any algebra structure can be encoded in this way: Take a basis $\{v_i\}$ for $V$ and a dual basis $f_i$ for $V^*$, and encode the structure by $\sum_{i,j} (v_i \cdot v_j) \otimes f_i \otimes g_j$.

**Definition 3.3:** Let $V$ be a vector space over $K$ and $x \in V^{\otimes p} \otimes V^{*\otimes q}$ be a tensor of type $(p, q)$. Two pairs $(V, x)$ and $(V', x')$ are isomorphic if there is a $K$-linear isomorphism

$$f : V \to V'$$

such that $f(x) = x'$. Here, $f$ sends

$$eq:extend-tensor x_1 \otimes \cdots \otimes x_p \otimes f_1 \otimes \cdots \otimes f_q \mapsto f(x_1) \otimes \cdots f(x_p) \otimes (f_1 \circ f^{-1}) \otimes \cdots \otimes (f_q \circ f^{-1}). \tag{12.9}$$

Given $(V, x)$ defined over $K$, we can consider it over $L$ by extending scalars; denote the resulting pair by $(V_L = V \otimes_K L, x_L)$.

We say that $(V, x)$ and $(V', x')$ are $L$-isomorphic if $(V_L, x_L)$ and $(V'_L, x'_L)$ are isomorphic. Let $E_{V,x}(L/K)$ denote the $L$-isomorphism classes of pairs that are $K$-equivalent to $(V, x)$. If $L/K$ is Galois, let $s \in G(L/K)$ act on $v \otimes \alpha \in V \otimes_K L = V_L$ by $s(v \otimes_K \alpha) := v \otimes_K s(\alpha)$ and let $s$ act on $A_L$ by conjugation:

$$f^s := s \circ f \circ s^{-1}.$$

**Theorem 3.4** (Descent for tensors)**:** thm:descent-tensors Let $L/K$ be a Galois extension, $G = G(L/K)$, and let $A_L$ be the group of $L$-automorphisms of $(V_L, x_L)$. Define the map

$$\begin{aligned} \theta : E_{V,x}(L/K) &\to H^1(G, A_L) \\ (V', x') &\mapsto (d : \sigma \mapsto f^{-1} \circ f^\sigma = f^{-1} \circ \sigma \circ f \circ \sigma^{-1}) \end{aligned}$$

where $f : (V_L, x_L) \to (V'_L, x'_L)$ is any $L$-automorphism. Then $\theta$ is a bijection.

*Proof.* We show the following.

1. $\theta$ is well-defined. First, $\theta(V', x')$ is a cocycle as

   $$d(\sigma t) = f^{-1}\sigma t f t^{-1}\sigma^{-1} = (f^{-1}\sigma f \sigma^{-1})[\sigma(f^{-1} t f t^{-1})\sigma^{-1}] = d(\sigma) \circ d(t)^\sigma.$$

   (See Definition 11.15.2.) Next, we show $\theta(V', x')$ does not depend on the choice of $f$: Let $d_f(\sigma) = f^{-1}\sigma f \sigma^{-1}$ and $d_g(s) = g^{-1}\sigma g \sigma^{-1}$. Then

   $$d_g(\sigma) = g^{-1}\sigma g \sigma^{-1} = g^{-1} f (f^{-1}\sigma f \sigma^{-1})\sigma f^{-1} g \sigma^{-1} = (fg^{-1})^{-1} d_f(\sigma)(fg^{-1})^\sigma$$

   so $d_f$ and $d_g$ are cohomologous.

2. $\theta$ is injective. Suppose $\theta(V'_1, x'_1) = \theta(V'_2, x'_2)$. We can choose the isomorphisms $f_1$ and $f_2$ such that $f_1^{-1} f_1^\sigma = f_2^{-1} f_2^\sigma$ for all $\sigma \in G(L/K)$. Then $(f_2 f_1^{-1})^\sigma = f_2 f_1^{-1}$ for all $\sigma \in G(L/K)$, i.e. $f_2 f_1^{-1}$ is an isomorphism defined over $K$. Thus $(V'_1, x'_1)$ and $(V'_2, x'_2)$ are $K$-isomorphic.

3. $\theta$ is surjective. Let $c_\sigma$ be a 1-cocycle of $G$ with values in $A_L$. Since $A_L \subseteq \mathrm{GL}(V_L)$, by Theorem 3.1 there exists $f \in \mathrm{GL}(V_L)$ such that

   $$c_\sigma = f^{-1} \circ f^\sigma$$

   Let $f$ operate on $V^{\otimes p} \otimes V^{*\otimes q}$ as in (12.9) and let $x' = f(x)$. As $x \in V_K^{\otimes p} \otimes V_K^{*\otimes q}$ and $c_\sigma$ fixes $K$, we have

   $$\sigma(x') = f^\sigma(\sigma(x)) = f^\sigma(x) = f \circ c_\sigma(x) = f(x) = x'.$$

   Thus $x'$ is rational over $K$ (i.e. in $V_K^{\otimes p} \otimes V_K^{*\otimes q}$), and $(V, x')$ maps to $c_\sigma$.

□

Note that since we always take an isomorphism $V \to V'$, we can really consider all the vector spaces to be the "same," and just vary the tensors $x$. If we consider $V = V'$, then we abbreviate $f : (V_L, x_L) \to (V'_L, x'_L)$ by $f : x \to x'$.

**Example 3.5:** We can use Galois cohomology to classify quadratic forms over a field $K$. Let $\Phi$ be a quadratic form (which corresponds to a bilinear form and can be represented by a tensor of type $(0, 2)$), and $O_L(\Phi)$ be the orthogonal group of $\Phi$, i.e. linear transformations that preserve $\Phi$. Then $H^1(G(L/K), O_L(\Phi))$ classifies the quadratic forms over $K$ that are $L$-isomorphic to $\Phi$.

# §4 Brauer group

brauer The Brauer group characterizes algebras over a field $K$. We already know a simple way of making algebras: just consider the algebra of $n \times n$ matrices, $\mathcal{M}_n(K)$. Thus, we will essentially "mod out" by these when constructing the group.

As we will see, there is an isomorphism to a second cohomology group. Thus, we can apply results about algebras over $K$ to Galois cohomology, or conversely, apply Galois cohomology to get information on algebras over $K$.

First, we need some results from noncommutative algebra. We refer the reader to Cohn [4], Chapter 5, or Milne [9], Chapter IV.1–2, for the proofs.

## 4.1 Background from noncommutative algebra

**Definition 4.1:** An **algebra** over a field $K$ is a ring $A$ with $K$ in its center[3]. Its dimension is the dimension of $A$ as a $K$-vector space, denoted $[A : K]$. *In this chapter we assume all algebras to be finite-dimensional as $K$-vector spaces.*

An algebra over $K$ is

1. **simple** if it has no proper two-sided ideals.

2. **central** if its center in $K$.

An algebra is a **division algebra** if every nonzero element has an inverse.

**Example 4.2:** The algebra of $n \times n$ matrices $\mathcal{M}_n(K)$ is a central simple algebra over $K$.

**Definition 4.3:** Let $A$ be an algebra over $K$. We use "$A$-module" to mean any finitely generated left $A$-module $V$; the map $A \to \mathrm{End}(V)$ is called a **representation** of $A$. The module (or representation) is **faithful** if $av = 0$ for all $v \in V$ implies $a = 0$, i.e. $A \hookrightarrow \mathrm{End}(V)$ is injective. A module is **simple** if it doesn't contain a proper $A$-submodule, and

[3]The center of a ring $R$ is the set of elements commuting with all elements of $R$.

**indecomposable** if it is not the direct sum of two proper $A$-submodules. (Note that simple implies indecomposable, but not vice versa.) A module is **semisimple** if it is the direct sum of simple $A$-modules.[4]

We say $A$ is semisimple if it is semisimple as a module.

We need some basic results from noncommutative algebra.

**Definition 4.4:** Let $B \subseteq A$ be a subalgebra. Define the **centralizer** of $B$ to be the elements of $A$ commuting with $B$:

$$C(B) := \{a \in A : ab = ba \text{ for all } b \in B\}.$$

**Theorem 4.5** (Double centralizer theorem)**:** thm:double-centralizer Let $A$ be a $K$-algebra, and $V$ a faithful semisimple $A$-module. Consider $A$ as a subalgebra of $\text{End}_K(V)$. Then

$$C(C(A)) = A.$$

*Proof.* Milne [9], Theorem IV.1.3, or Etingof [7], Theorem 4.54. □

**Theorem 4.6** (Wedderburn's structure theorem)**:** thm:wedderburn An algebra $A$ is semisimple iff it is isomorphic to the direct sum of matrix algebras over division algebras.

If $A$ is an algebra over an algebraically closed field $K$ and $K$, then any semisimple algebra over $K$ is isomorphic to a direct sum of matrix algebras over $K$.

*Proof.* Milne [9], Theorem IV.1.15.

For the second part, we need to show the only division algebra over an algebraically closed field $K$ is $K$ itself. Suppose $D$ is a division algebra and $\alpha \in D$. As $[D : K]$ is finite-dimensional, $K(\alpha)$ is a finite extension of $K$. Hence $\alpha \in K$, giving $D = K$. □

**Theorem 4.7** (Noether-Skolem theorem)**:** thm:noether-skolem Let $f, g : A \to B$ be homomorphisms, where $A$ is a simple $K$-algebra and $B$ is a central simple $K$-algebra. Then there exists $b \in B$ such that

$$f(a) = b \cdot g(a) \cdot b^{-1}$$

for all $a \in A$, i.e. $f, g$ differ by an inner automorphism of $B$.

In particular, taking $A = B$ and $g = 1$, all automorphisms of a central simple $K$-algebra are inner (come from conjugation). In particular, this is true for $\mathcal{M}_n(K)$.

[4] Equivalently, the radical of $A$ is trivial. If it is semisimple the factors in the decomposition are unique up to isomorphism (Jordan-Hölder).

## 4.2 Central simple algebras and the Brauer group

We now define the Brauer group.

**Definition 4.8:** Let $A$ and $B$ be simple algebras over $K$. We say $A$ and $B$ are similar and write $A \sim B$ if

$$A \otimes_K \mathcal{M}_m(K) \cong B \otimes_K \mathcal{M}_n(K)$$

for some $m, n$.

The **Brauer group** $\mathrm{Br}_K$ is the set of similarity classes of central simple algebras over $K$, with multiplication defined by

$$[A][B] = [A \otimes_K B].$$

The Brauer group $\mathrm{Br}_{L/K}$ is the subgroup of classes of central simple algebras over $K$ that are **split** over $L$, i.e. such that $A \otimes_K L$ is a matrix algebra.

*Proof (sketch) that this is a group.* We need to check that...

1. The tensor product of two central simple algebras is central simple. By Wedderburn's Theorem 4.6 we can write the algebras as $A = M_m(D)$ and $B = M_{m'}(D')$, where $D, D'$ are division algebras. One can show $A \otimes_K D'$ is simple; hence it equals $M_n(D'')$ for some $D''$. Then $A \otimes_K B \cong M_{m'n}(D'')$ is simple. It is central because $C(A \otimes_K B) = C(A) \otimes_K C(B) = K$.

2. "$\sim$" is an equivalence relation. If $A \sim B$ and $B \sim C$, then $A \otimes_K \mathcal{M}_m(K) \cong B_K \otimes_K \mathcal{M}_n(K)$, $B \otimes_K \mathcal{M}_{n'}(K) \cong C \otimes_K \mathcal{M}_p(K)$ for some $m, n, n', p$. Then

   $$A \otimes_K \mathcal{M}_{mn'}(K) \cong A \otimes_K \mathcal{M}_m(K) \otimes_K \mathcal{M}_{n'}(K) \cong C \otimes_K \mathcal{M}_n(K) \otimes_K \mathcal{M}_p(K) \cong C \otimes_K M_{np}(K).$$

3. "$\sim$" is preserved under the operation $\otimes$. If $A_i \otimes_K \mathcal{M}_{m_i}(K) \cong B_i \otimes_K \mathcal{M}_{n_i}(K)$ for $i = 1, 2$, then $A_1 \otimes_K A_2 \otimes_K \mathcal{M}_{m_1 m_2}(K) \cong B_1 \otimes_K B_2 \otimes_K \mathcal{M}_{n_1 n_2}(K)$.

4. $A$ has an inverse. Letting $A^{\mathrm{opp}}$ be the opposite algebra, we find that

   $$A \otimes_K A^{\mathrm{opp}} \cong \mathcal{M}_n(K), \quad n = [A : K].$$

5. The operation is commutative and associative. This follows since tensor product is commutative and associative.

$\square$

By Wedderburn's Structure Theorem 4.6, each (central) simple algebra is $M_n(D) \cong M_n(K) \otimes_K D$ for some (central) division algebra $D$, so every similarity class is represented by a central division algebra. Thus to determine the Brauer group it suffices to classify central division algebras.

**Example 4.9:** We have

$$\mathrm{Br}_{\mathbb{R}} = \{\mathbb{R}, \mathbb{H}\}$$

where $\mathbb{H}$ denotes the quaternions: the algebra with basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k} = \mathbf{ij}$ and relations $\mathbf{i}^2 = 1$, $\mathbf{j}^2 = 1$, and $\mathbf{ij} = -\mathbf{ji}$.

Indeed, by Frobenius's Theorem, the only finite-dimensional (associative) division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$, and only $\mathbb{R}$ and $\mathbb{H}$ have center equal to $\mathbb{R}$.

**Proposition 4.10:** For any algebraically closed field $K$,

$$\mathrm{Br}_{\overline{K}} = 0.$$

*Proof.* By Wedderburn's Theorem 4.6, all central simple algebras over $K$ are $\mathcal{M}_n(K)$ for some $n$. □

## 4.3 Subfields and splitting of central simple algebras

An important way of studying a central simple algebra is to look at its subfields.

**Theorem 4.11** (Double centralizer theorem, generalization)**:** thm:dct-gen Let $A$ be a central simple $K$-algebra and $B$ be a simple $K$-subalgebra. Let $C = C(B)$. Then $C$ is simple, $C(C) = A$, and

$$[B : K][C : K] = [A : K].$$

*Proof.* See Milne [9], Theorem IV.3.1. □

**Corollary 4.12:** Let $A$ be central simple over $K$, and $L$ be a subfield with $K \subseteq L \subseteq A$. Then the following are equivalent.

1. $L = C(L)$.
2. $[A : K] = [L : K]^2$.
3. $L$ is the maximal commutative $K$-subalgebra of $A$.

*Proof.* Milne [9], Corollary IV.3.4. □

The following describes the fields over which a central simple algebra splits.

**Corollary 4.13:** cor:csa-split Let $A$ be central simple over $K$. A finite extension field $M$ splits $A$ iff there exists an algebra $B \sim A$ containing $M$ with $[B : K] = [L : K]^2$. In particular, any subfield $L$ of $A$ of degree $\sqrt{[A : K]}$ splits $A$.

If $D$ is a divison algebra of degree $n^2$ over $K$, and $L$ is a field of degree $n$ over $K$ (equivalently a maximal commutative subfield of $D$), then $L$ splits $D$, i.e. $D \cong \mathcal{M}_n(L)$.

*Proof.* Milne [9], IV.3.6, and 3.7. □

**Theorem 4.14:** thm:all-split Every central division algebra over $K$ is split over some finite Galois extension $L/K$. Therefore

$$\mathrm{Br}_K = \mathrm{Br}_{\overline{K}/K} = \bigcup_{L/K \text{ finite Galois}} \mathrm{Br}_{L/K}.$$

*Proof.* When $K$ is perfect, this follows directly from Corollary 4.13. The general case requires a separate argument; see Milne [9], IV.3.10. □

Similar to the commutative case, we can define a valuation on division algebras.

**Proposition 4.15:** pr:div-alg-val Let $D$ be a division algebra of rank $n^2$ over a local field $K$. Then $D$ admits a discrete valuation extending the valuation on $K$, such that for any $a \in (0,1)$, $\|x\|_D := a^{v(x)}$ defines a norm on $D$. The set of integral elements $\{x : v(x) \geq 0\}$ is a subring of $D$.

# §5 Brauer group and cohomology

## 5.1 The Brauer group is a second cohomology group

**Definition 5.1:** Let $\mathrm{Br}_{L/K,n}$ denote the subset of $\mathrm{Br}_{L/K}$ consisting of $[A]$ where $A \otimes_K L \cong \mathcal{M}_n(L)$. Note that $\mathrm{Br}_{L/K} = \bigcup_{n\in\mathbb{N}} \mathrm{Br}_{L/K,n}$.

**Theorem 5.2** (Cohomological interpretation of Brauer group)**:** thm:brauer-cohom There are canonical bijections

$$\theta_n : \mathrm{Br}_{L/K,n} \to H^1(G, \mathrm{PGL}_n(K))$$

and canonical isomorphisms

$$\delta : \mathrm{Br}_{L/K} \to H^2(L/K)$$
$$\delta : \mathrm{Br}_K \to H^2(K)$$

where $H^2(K) := H(\overline{K}/K) = \varinjlim_{L/K \text{ finite Galois}} H^2(L/K)$.

*Proof.* We can represent elements of $\mathrm{Br}_{L/K,n}$ as algebras of dimension $n^2$ over $K$, that are $L$-isomorphic to the algebra $\mathcal{M}_n(L)$. By Example 3.2, we can encode the algebra $\mathcal{M}_n(L)$ by a tensor of type $(1,2)$. By Theorem 3.4,

$$eq:brauer-descent\, \mathrm{Br}_{L/K,n} \cong H^1(G, \mathrm{Aut}(\mathcal{M}_n(L))). \tag{12.10}$$

By the Noether-Skolem Theorem 4.7, every automorphism of $\mathcal{M}_n(L)$ is conjugation by an element of $\mathrm{GL}_n(K)$. Since the matrices that act trivially by conjugation are just the scalar matrices, we have the short exact sequence

$$eq:noether-skolem\, 1 \to L^\times \to \mathrm{GL}_n(L) \to \mathrm{Aut}(\mathcal{M}_n(L)) \cong \mathrm{PGL}_n(L) \to 1. \tag{12.11}$$

Along with (12.10) this proves the first part.

The long exact sequence 11.15.3 of (12.11) gives

$$0 = H^1(G, \mathrm{GL}_n(L)) \to H^1(G, \mathrm{PGL}_n(L)) \xrightarrow{\Delta_n} H^2(G, L^\times),$$

where the LHS follows from Theorem 3.1. Let $\delta_n = \Delta_n \circ \theta_n$; then $\delta_n$ is an injective map.

We show the following.

1. The $\delta_n$ for different $n$ combine compatibly into an injective group homomorphism $\delta : \mathrm{Br}(L/K) \to H^2(L/K)$: We need to show

$$\delta_{nn'}(A \otimes A') = \delta_n(A)\delta_{n'}(A')$$

for any $A \in \mathrm{Br}_{L/K,n}$ and $A' \in \mathrm{Br}_{L/K,n'}$.

First, note that if $a, a'$ are tensors encoding the algebras $A, A'$ on $V \otimes V^{*\otimes 2}$ and $V' \otimes V'^{*\otimes 2}$, then $x \otimes x'$ encodes the algebra $A \otimes A'$ on $(V \otimes V') \otimes (V \otimes V')^{*\otimes 2}$. Let $x, x'$ encode $\mathcal{M}_n(K)$ and $\mathcal{M}_{n'}(K)$, so that $x \otimes x'$ encodes $\mathcal{M}_{nn'}(K)$. If $f : x \to a$ and $f' : x' \to a'$ are $L$-linear maps, then we have the $L$-linear map on $\mathcal{M}_{nn'}(L)$,

$$f \otimes f' : x \otimes x' \to a \otimes a'.$$

Now $\theta_n, \theta_{n'}$ map $A$ and $A'$ to $c_\sigma = f^{-1} \circ f^\sigma$ and $c'_\sigma = f'^{-1} \circ f'^\sigma$. Suppose $c_\sigma$ and $c'_\sigma$ are represented by conjugation by $S_\sigma$ and $S'_\sigma$, respectively. Now $\theta_{nn'}$ maps $A \otimes A'$ onto $d_\sigma = (f \otimes f')^{-1} \circ (f \otimes f')^\sigma$, which corresponds to conjugation by $S_\sigma \otimes S'_\sigma$. Then by the description of $\Delta$ in Theorem 11.15.2, we see that

$$\delta_{nn'}(A \otimes A') = \left\{a_{\sigma,\tau} = i_{nn'}^{-1}[(S_\sigma \otimes S'_\sigma)\sigma(S_\tau \otimes S'_\tau)(S_{\sigma\tau} \otimes S'_{\sigma\tau})^{-1}]\right\} = \delta_n(A)\delta_n(A')$$

where $i_{nn'}$ is the inclusion map $L^\times \to \mathrm{GL}_{nn'}(L)$. Under the inverse of $i_{nn'} = i_n \otimes i_{n'}$, tensor product becomes simply the product.

2. $\delta$ is surjective. It suffices to show $\Delta_n$ is surjective, where $n = [L : K]$.[5] Take an 2-cocycle $a_{\sigma,\tau} \in H^2(G, L^\times)$. We need to show that

$$a_{\sigma,\tau} = S_\sigma \sigma(S_\tau) S_{\sigma\tau}^{-1}$$

for some values of $S_\sigma \in \mathrm{GL}_n(L)$. We identify $L^n$ with the group algebra $L[G]$, and let $S_\sigma \in \mathrm{GL}(L[G])$ be the map sending $\tau$ to $a_{\sigma,\tau}\sigma\tau$ (it is invertible as $a_{\sigma,\tau} \in L^\times$). Then we calculate for every $u \in G \subset L[G]$,

$$[S_\sigma\sigma(S_\tau)]u = [a_{\sigma,\tau u}\sigma(a_{\tau,u})]\sigma\tau u$$
$$[a_{\sigma\tau} S_{\sigma\tau}]u = [a_{\sigma,\tau} a_{\sigma\tau,u}]\sigma\tau u.$$

The right-hand sides are equal since $a_{\sigma,\tau}$ is a cocycle. Hence

$$a_{\sigma,\tau} = S_\sigma \sigma(S_\tau) S_{\sigma\tau}^{-1}$$

is in the image of $\Delta_n$.

[5] Incidentally, this shows that every equivalence class of algebras is represented by one of dimension at most $[L : K]^2$. This is consistent with results of the previous section.

3. $\delta$ gives an isomorphism $\mathrm{Br}_K \cong H^2(K)$: This follows from Theorem 4.14, the following easy-to-check commutative diagram (which holds for any $K \subseteq L \subseteq M$),

$$\begin{tikzcd} H^2(L/K) \arrow[r, hook, "\mathrm{Inf}"] \arrow[d, "\delta"'] & H^2(M/K) \arrow[d, "\delta"'] \\ \mathrm{Br}_{L/K} \arrow[r, hook] & \mathrm{Br}_{M/K}, \end{tikzcd}$$

   and taking the direct limit of the maps $\mathrm{Br}_{L/K} \to H^2(L/K)$.

□

**Remark:** Milne [9] makes this correspondence more explicit. The relationship between the two approaches can be seen by choosing a basis for the tensor product $V \otimes V^{*\otimes 2}$; the coefficients are called the *structure constants* of the algebra. (We followed Serre; note that the isomorphism in Serre is the opposite of the isomorphism in Milne.)

## 5.2 Exact sequence of Brauer groups

The importance of the Brauer group in class field theory is given by the following proposition.

**Theorem 5.3:** brauer2 Let $M/L/K$ be Galois extensions. Then there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H^2(L/K) \arrow[r] \arrow[d, equal] & H^2(M/K) \arrow[r] \arrow[d, equal] & H^2(M/L) \arrow[d, equal] \\ & \mathrm{Br}_{L/K} & \mathrm{Br}_{M/K} & \mathrm{Br}_{M/L}\,. \end{tikzcd}$$

For any Galois extension $L/K$ there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H^2(L/K) \arrow[r] \arrow[d, equal] & H^2(K) \arrow[r] \arrow[d, equal] & H^2(L) \arrow[d, equal] \\ & \mathrm{Br}_{L/K} & \mathrm{Br}_{K} & \mathrm{Br}_{L}\,. \end{tikzcd}$$

*Proof.* Since $H^1(L/K) = 0$ by Hilbert's Theorem 90 (1.1), the inflation-restriction exact sequence 11.11.10 with $G = G(M/K)$ and $H = G(M/L)$ gives

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

The equality with the Brauer groups follows from Theorem 5.2.

Taking the direct limit over all finite Galois extensions $M/K$ gives the second result. □

## §6 Problems

2.1 (Artin-Schreier) Let $L/K$ be a Galois extension of degree $p$, with $K/\mathbb{F}_p$ a finite extension. Prove that $L = K(\alpha)$ for some $\alpha$ such that $\alpha^p - \alpha \in K$. (Hint: Consider a short exact sequence as in the proof of Kummer theory. However, use the map $x \mapsto x^p - x$ instead of $x \mapsto x^p$, and consider additive instead of multiplicative groups.)

# Chapter 13
# Local class field theory

lcft We now prove the main theorems of class field theory using cohomology. Throughout this chapter, $K$, $L$, etc. will denote nonarchimedean local fields, unless specified otherwise.[1] The main steps are the following.

1. Construct the invariant map $H^2(K^{\mathrm{ur}}/K) \to \mathbb{Q}/\mathbb{Z}$. (Proposition 2.1)
   (a) Show that $H^2(G(K^{\mathrm{ur}}/K), U_{K^{\mathrm{ur}}}) = 0$. (Theorem 1.1)
   (b) From the decomposition $K^{\mathrm{ur}\times} = U_{K^{\mathrm{ur}}} \times \mathbb{Z}$ and step 1, we get $H^2(G(K^{\mathrm{ur}}/K), K^{\mathrm{ur}\times}) \cong H^2(G(K^{\mathrm{ur}}/K), \mathbb{Z})$. (Note the projection $K^{\mathrm{ur}\times} \to \mathbb{Z}$ is the valuation map $v_{K^{\mathrm{ur}}}$.) Relate $H^2(G(K^{\mathrm{ur}}/K), \mathbb{Z})$ to $\mathbb{Q}/\mathbb{Z}$ using the long exact sequence in cohomology associated to $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

2. Now show that there is an isomorphism $\mathrm{Br}_K := H^2(\overline{K}/K) \cong H^2(K^{\mathrm{ur}}/K)$ (Theorem 3.1). Thus we can restrict attention to unramified extensions of $K$ and use step 1. Unramified extensions are easier to deal with! There are two approaches:
   (a) By Theorem 12.5.3 there is an exact sequence
   $$0 \to H^2(K^{\mathrm{ur}}/K) \to \mathrm{Br}_K \to \mathrm{Br}_{K^{\mathrm{ur}}}.$$
   Show that $\mathrm{Br}_{K^{\mathrm{ur}}} = 0$ by considering central simple algebras over local fields.
   (b) Study the cohomology of $U_L$ when $L/K$ is cyclic to conclude that the Herbrand quotient $h(U_L)$ is 1. From this get $h(L^\times) = [L : K]$. From this calculation and Hilbert's Theorem 90 (12.1.1), compute[2]
   $$|H^1(L/K)| = 1,$$
   $$|H^2(L/K)| = [L : K].$$
   Conclude that $H^2(L/K)$ is cyclic of order $[L : K]$ and hence included in $H^2(K^{\mathrm{ur}}/K)$, for any finite $L/K$.

[1] Local class field theory for $\mathbb{R}$ and $\mathbb{C}$ is trivial and left to the reader. (The only nontrivial field extension is $\mathbb{C}/\mathbb{R}$.)

[2] This is the input for *abstract class field theory* according to Neukirch [11].

3. Combining the first two steps, we get the invariant map $\mathrm{inv}_K : \mathrm{Br}_K \to \mathbb{Q}/\mathbb{Z}$. Show that this is compatible with restriction and hence that $(G(\overline{K}/K), \overline{K})$ is a *class formation.* Note $\mathrm{inv}_K$ restricts to $H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}$; supposing its image is generated by $u_{L/K}$, Tate's Theorem 11.13.1 gives an isomorphism

$$\begin{tikzcd} H_T^{-2}(G(L/K), \mathbb{Z}) \arrow[r, "\bullet\cup u_{L/K}", "\cong"'] \arrow[d, equal] & H_T^0(G, L^\times) \arrow[d, equal] \\ G(L/K)^{\mathrm{ab}} & K^\times / \mathrm{Nm}_{L/K}(L^\times) \end{tikzcd}$$

   that sends $\mathrm{Frob}_{L/K}$ to $[\pi]$ when $L/K$ is unramified. Taking a direct limit, we get a map $K^\times \to G(K^{\mathrm{ab}}/K)$. Note we only get a map from $G^{\mathrm{ab}}$ (norm limitation).

4. Study the Hilbert symbol to prove the existence theorem (See Sections 6–7).

Unfortunately it is quite difficult to trace through the maps to find out what the Artin map actually is—for this Lubin-Tate Theory is better.

# §1 Cohomology of the units

For an unramified extension, the cohomology of the units is trivial.

**Theorem 1.1** (Cohomology of units)**:** cohomology-units-trivial Suppose $L/K$ is a finite unramified extension of local fields with Galois group $G$. Let $U_L$ be the group of units of $L$. Then

$$H_T^r(G, U_L) = 1$$

for any $r$. Hence $H^n(G(K^{\mathrm{ur}}/K), U_{K^{\mathrm{ur}}}) = 0$ for $n > 0$.

*Proof.* We will show that

$$H_T^1(G, U_L) = H_T^0(G, U_L) = 1.$$

Then it follows from Proposition 11.12.1 that all the Tate groups are trivial. The second part follows from taking the direct limit.

We have

$$eq:L=ULxZ\, L^\times = U_L \times \pi^{\mathbb{Z}} \cong U_L \times \mathbb{Z} \tag{13.1}$$

where $\pi$ is a uniformizer for $L$. Since $L/K$ is unramified, we can choose $\pi \in K$. Then $G$ acts trivially on $\pi$, so acts trivially on $\mathbb{Z}$ in the decomposition above. Thus (13.1) gives a decomposition of $L^\times$ as a $G$-module (not just as a group). We have by Hilbert's Theorem 90 (Theorem 12.1.1) and the fact that cohomology respects products (Proposition 11.6.6) that

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

Hence $H^1(G, U_L) = 1$.

It remains to show $H_T^0(G, U_L) = 1$. To do this, let $\mathfrak{m}$ be the maximal ideal of $L$, $U_L^{(m)} := 1 + \mathfrak{m}^n$, and consider the filtration

$$U_K^{(0)} := U_K \supset U_K^{(1)} \supset U_K^{(2)} \supset \cdots .$$

Proposition 1.2 and 1.3 below show that each quotient has trivial cohomology:

$$H_T^0(G, U_L^{(i)}/U_L^{(i+1)}) = 1.$$

Then Lemma 1.4 gives that $H_T^0(G, U_L) = 1$, as needed. □

**Proposition 1.2:** units-filtration-2 Let $K$ be a complete field with discrete valuation, $\mathfrak{m}$ be the associated maximal ideal, and $U_K^{(m)} := 1 + \mathfrak{m}^m$. Then we have isomorphisms

$$\begin{aligned} U_K/U_K^{(1)} &\xrightarrow{\cong} k^\times \\ u &\mapsto u \pmod{\mathfrak{m}} \end{aligned} \qquad\qquad \begin{aligned} U_K^{(m)}/U_K^{(m+1)} &\xrightarrow{\cong} k^+ \\ 1 + a\pi^m &\mapsto a \pmod{\mathfrak{m}} \end{aligned}$$

that preserve Galois action.

*Proof.* This is Proposition 9.4.8. □

**Proposition 1.3:** cohom-finite-fields Let $l/k$ be an extension of finite fields and $G := G(l/k)$. Then

$$\begin{aligned} H_T^r(G, l^\times) &= \{1\} \\ H_T^r(G, l^+) &= \{0\} \end{aligned}$$

for all $r \in \mathbb{Z}$. Moreover, the maps $\mathrm{Nm}_{l/k} : l \to k$ and $\mathrm{Tr}_{l/k} : l \to k$ are surjective.

*Proof.* By Hilbert's Theorem 90 (12.1.1), $H^1(G, l^\times) = 0$. Since $G$ is cyclic and $l$ is finite, by Proposition 11.12.4, $h(l^\times) = 1$, giving $H^2(G, l^\times) = 0$. Again since $G$ is cyclic, by Theorem 11.12.1, all the Tate groups are 0.

From Theorem 12.1.2, $H_T^r(G, l^+) = 0$ for $r \geq 0$.

For the second statement, just note

$$\begin{aligned} \{1\} &= H_T^0(G, l^\times) = (l^\times)^G/N_G(l^\times) = k^\times/\mathrm{Nm}_{l/k}(l^\times) \\ \{0\} &= H_T^0(G, l^+) = l^G/N_G(l) = k/\mathrm{Tr}_{l/k}(l). \end{aligned}$$ □

**Lemma 1.4:** filtration0-h Let $G$ be a finite group and $M$ be a $G$-module. Let

$$M = M^0 \supseteq M^1 \supseteq \cdots$$

be a decreasing sequence of $G$-submodules and suppose $M = \varprojlim M/M^i$ (i.e. $M$ is complete with respect to this filtration). If $H^q(G, M^i/M^{i+1}) = 0$ for all $i$, then $H^q(G, M) = 0$.

*Proof.* Let $f$ be a $q$-cocycle of $M$. Since $H^q(G, M/M^1) = 0$, the long exact sequence of $0 \to M^1 \to M \to M/M^1$ gives $H^q(G, M^1) \twoheadrightarrow H^q(G, M)$ and we can write $f = g_0 + f_1$, where $g_0 = \delta h_0$ is a coboundary in $M$ and $f_1$ is a $q$-cocycle in $M^1$. Given $f_n \in H^q(G, M^n)$, we can write

$$f_n = \delta h_n + f_{n+1}$$

where $h_n$ is a $(q-1)$-cocycle of $M^n$ and $f_{n+1}$ is a $q$-cocycle of $M^{n+1}$. Then

$$f = \delta(h_1 + h_2 + \cdots),$$

the infinite series being defined in $H^{q-1}(G, M)$ since $h_n$ is a cochain with values in $M^n$, and $M$ is complete with respect to this filtration. □

This proves Theorem 1.1. We record the following corollary, for easy reference.

**Corollary 1.5:** thm:local-nm-surj Suppose $L/K$ is a finite extension of local fields. Then

$$U_K \subseteq \mathrm{Nm}_{L/K} U_L.$$

*Proof.* If $L/K$ is Galois, then this follows since by Theorem 1.1

$$U_K / \mathrm{Nm}_{L/K} U_L = H^0_T(G(L/K), U_L) = \{1\}$$

so the norm map $U_L \to U_K$ is surjective.

For general extensions $L/K$, consider the Galois closure and use transitivity of norms. □

# §2 The invariant map

## 2.1 Defining the invariant maps

**Proposition 2.1:** invariant-map For any finite unramified Galois extension of local fields $L/K$ there is a canonical isomorphism

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

Taking the direct limit gives an injective map

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

*Proof.* Consider the short exact sequence

$$1 \to U_L \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0.$$

Since $H^n_T(G, U_L) = 0$ for all $n$ by Theorem 1.1, taking the long exact sequence gives

$$\underbrace{\cancel{H^2(G, U_L)}}_{0} \to H^2(L/K) \xrightarrow{\cong} H^2(G, \mathbb{Z}) \to \underbrace{\cancel{H^3(G, U_L)}}_{0}.$$

We relate $H^2(G,\mathbb{Z})$ to a lower cohomology group by considering the short exact sequence

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

Note $H^n(G,\mathbb{Q})$ is torsion for any $n > 0$ by Corollary 11.11.6. Since $\mathbb{Q}$ is a divisible group, so is $H^n(G,\mathbb{Q})$, by looking at the description of $H^n$ in terms of cocycles (Section 11.7). Hence $H^n(G,\mathbb{Q}) = 0$ for any $n > 0$. Taking the long exact sequence of the above we get

$$\cancelto{0}{H^1(G,\mathbb{Q})} \to H^1(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\cong} H^2(G,\mathbb{Z}) \to \cancelto{0}{H^2(G,\mathbb{Q})}.$$

Thus we get a map

$$eq : inv - unram\ \mathrm{inv}_{L/K} : \quad H^2(L/K) \xrightarrow{\cong} H^2(G,\mathbb{Z}) \xleftarrow{\cong} H^1(G,\mathbb{Q}/\mathbb{Z}) \overset{11.7.3}{\cong} \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\cong} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}. \tag{13.2}$$

where the last is defined by taking the Frobenius element $\sigma$ of $G$ and mapping $f \mapsto f(\sigma)$. (Note $G$ is cyclic and $\sigma$ generates $G$; the Frobenius is a canonical choice.)

Now define $\mathrm{inv}_{K^{\mathrm{ur}}/K} = \varinjlim_{L/K \text{ finite Galois unramified}} \mathrm{inv}_{L/K}$, taking the direct limit under inflation. Since inflation is functorial, the first two maps in (13.2) commute with it. Identifying $H^1(G,\mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$, inflation sends a map $G(L/K) \to \mathbb{Q}/\mathbb{Z}$ to $G(M/K) \twoheadrightarrow G(L/K) \to \mathbb{Q}/\mathbb{Z}$. Moreover, $\mathrm{Frob}_{L/K}$ is the projection of $\mathrm{Frob}_{M/K}$ to $G(L/K)$. Hence $\mathrm{Inf}_{M/L}$ commutes with the inclusion map $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \hookrightarrow \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z}$, and the $\mathrm{inv}_{L/K}$ form a compatible system under inflation. $\square$

**Remark:** Let $K$ be any nonarchimedean complete field (not necessarily local) with residue field $k$. Then

$$H^n(L/K) = H^n(l/k) \times H^n(G(L/K),\mathbb{Q}/\mathbb{Z}).$$

Indeed, Proposition 1.2 and Theorem 12.1.2 still give

$$H_T^r(G, U_L^{(i)}/U_L^{(i+1)}) \cong H_T^r(G, l^+) = 0$$

for $i \geq 1$. This gives $H_T^r(G, U_L^{(1)}) = 0$ by Lemma 1.4. From the long exact sequence associated to

$$1 \to U_L^{(1)} \to U_L \to U_L/U_L^{(1)} \cong l^\times \to 1$$

we get

$$H^n(L/K) \cong H^n(G,U_L) \times H^n(G,\mathbb{Z}) = H^n(G,l^\times) \times H^n(G,\mathbb{Z}).$$

In the case of a local field, $l$ was finite so $H^n(G,l^\times) = 1$.

## 2.2 Compatibility of the invariant maps

We show that the invariant maps are compatible, in the following sense.

**Theorem 2.2:** thm:inv-compatible Let $L/K$ be a Galois extension of local fields, and $n = [L : K]$. Then

$$\operatorname{inv}_{K^{\mathrm{ur}}/L} \circ \operatorname{Res}_{K/L} = n \operatorname{inv}_{K^{\mathrm{ur}}/K}$$

*Proof.* To do this we have to unravel all those steps we took to define $\operatorname{inv}_{K^{\mathrm{ur}}/K} \dots$ We first prove this for two special cases.

1. $L/K$ is unramified. Let $G = G(K^{\mathrm{ur}}/K)$ and $S = G(K^{\mathrm{ur}}/L)$. We claim the following commutes.

$$\begin{tikzcd}
H^2(K^{\mathrm{ur}}/K) \arrow[r] \arrow[d, "\mathrm{Res}"] & H^2(G,\mathbb{Z}) \arrow[d, "\mathrm{Res}"] & H^1(G,\mathbb{Q}/\mathbb{Z}) \arrow[l] \arrow[r, "\gamma"] \arrow[d, "\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n"] \\
H^2(K^{\mathrm{ur}}/L) \arrow[r] & H^2(S,\mathbb{Z}) & H^1(S,\mathbb{Q}/\mathbb{Z}) \arrow[l] \arrow[r, "\gamma"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

   For the squares involving Res, this follows from naturality of Res. For the last square, identify $H^1(G, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$; Res becomes simply restriction of homomorphisms. Recall that $\gamma$ was defined taking the Frobenius $\operatorname{Frob}(K^{\mathrm{ur}}/K) \in G(K^{\mathrm{ur}}/K)$ and sending $f \in H^1(G, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$ to $f(\sigma)$, and we have

$$\operatorname{Frob}^n_{K^{\mathrm{ur}}/K} = \operatorname{Frob}_{K^{\mathrm{ur}}/L}$$

   by Proposition 10.1.4.

2. $L/K$ is totally ramified. Note that $G = G(K^{\mathrm{ur}}/K) = G(K^{\mathrm{ur}}L/L) = G(L^{\mathrm{ur}}/L)$ in this case, from the description of $K^{\mathrm{ur}}$ in Theorem 8.2.6. We show the following commutes:

$$\begin{tikzcd}
H^2(K^{\mathrm{ur}}/K) \arrow[r] \arrow[d, "\mathrm{Res}"] & H^2(G,\mathbb{Z}) \arrow[d, "n"] & H^1(G,\mathbb{Q}/\mathbb{Z}) \arrow[l] \arrow[r, "\gamma"] \arrow[d, "n"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n"] \\
H^2(K^{\mathrm{ur}}/L) \arrow[r] & H^2(G,\mathbb{Z}) & H^1(G,\mathbb{Q}/\mathbb{Z}) \arrow[l] \arrow[r, "\gamma"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

   The first square commutes by commutativity of

$$\begin{tikzcd}
K^{\mathrm{ur}\times} \arrow[r, "v_K"] \arrow[d, hook] & \mathbb{Z} \arrow[d, "n"] \\
L^{\mathrm{ur}\times} \arrow[r, "v_L"] & \mathbb{Z}.
\end{tikzcd}$$

   (and of course, naturality of cohomology). Here $v_K$ and $v_L$ are the valuation maps, i.e. the projections $K^\times \cong U_K \times \mathbb{Z} \to \mathbb{Z}$ and $L^\times \cong U_L \times \mathbb{Z} \to \mathbb{Z}$.

The general case follows by considering $L/L^{I_{L/K}}$ (totally ramified) and $L^{I_{L/K}}/K$ (unramified). (See Theorem 2.7.2.) □

# §3 $H^2(\overline{K}/K) \cong H^2(K^{\mathbf{ur}}/K)$

We prove the following.

**Theorem 3.1:** hkur The inclusion (inflation) map

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

is an isomorphism.

For short we write $H^2(K) := H^2(\overline{K}/K)$.

## 3.1 First proof (Brauer group)

*First proof.* By Proposition 12.5.3 there is an exact sequence

$$0 \to H^2(K^{\mathrm{ur}}/K) \to H^2(K) \to H^2(K^{\mathrm{ur}}) = \cancel{\mathrm{Br}_{K^{\mathrm{ur}}}.}\ 0$$

The last term is zero by Theorem 3.2 below. Thus we get $H^2(K^{\mathrm{ur}}/K) \cong H^2(K)$, as needed. $\square$

**Theorem 3.2:** brkur0 Let $K$ be a local field. Then $\mathrm{Br}_{K^{\mathrm{ur}}} = 0$.

We need two lemmas.

**Lemma 3.3:** lem:brkur0-1 Suppose $D$ is a central division algebra of rank $n^2 > 1$ over a field $K$, and the residue field $k$ is perfect. Then there exists a commutative subfield $L$ of $D$ properly containing $K$, unramified over $K$.

**Lemma 3.4:** lem:brkur0-2 Keep the same hypotheses as Lemma 3.3. There is a subfield of $D$ of degree $n$ unramified over $K$.

Note this is a maximal subfield by Corollary 4.13.

*Proof of Lemma 3.3.* Suppose by way of contradiction that every commutative subfield $L$ of $D$ properly containing $K$ is ramified. Then the extension of residue fields $l/k$ must be trivial (see Theorem 2.7.2). Let $a \in D$ be integral and $\pi \in D$ be a uniformizer for $D$. (See Proposition 12.4.15.) Since $l = k$, there exists $b \in K$ such that $b \equiv a \pmod{\pi}$, and we can write $a = b + \pi b_1$ for some $b_1 \in \mathcal{O}_D$, where $\mathcal{O}_D$ is the ring of integers in $D$. Iterating this with $b_1$, we find

$$a = b + \pi b_1 + \cdots + \pi^{n-1} b_{n-1} + \pi^n b_n$$

where $b_1, \ldots, b_{n-1} \in \mathcal{O}_K$ and $b_n \in \mathcal{O}_D$. Thus $a$ is in the closure of $K(\pi)$. But $K(\pi)$ is closed (it is a finite-dimensional vector space over $K$), so $a \in K(\pi)$, i.e. $D = K(\pi)$ and $D$ is commutative, a contradiction. $\square$

*Proof of Lemma 3.4.* Induct on $n$. The case $n = 1$ is clear. Let $n \geq 2$. By Lemma 3.3 there exists a proper unramified extension $K'/K$ inside $D$. Let $D' = C(K')$. Since $D' \subseteq D$, $D'$ must be a division algebra (a finite dimensional integral domain must contain inverses). Let its center be $K''$. The maximal commutative subfield of $D'$ then has dimension $\sqrt{[D' : K'']}$ over $K''$, or dimension $\sqrt{[D' : K'']}[K'' : K] = \sqrt{[D' : K][K'' : K]}$ over $K$. This is at most $n$, since the field is also contained in $D$. But $\sqrt{[D' : K][K' : K]} = n$ by the double centralizer theorem 12.4.11, so we must have $K'' = K$. Thus $D'$ is a division algebra with center $K'$. Its degree over $K'$ is less than $n^2$, so by the induction hypothesis, $D'$ has a maximal commutative subfield $L$ containing $K'$, of degree $\sqrt{[D' : K']}$, and unramified over $K'$, hence over $K$. We calculate

$$[L : K] = [L : K'][K' : K] = \sqrt{[D' : K']}[K' : K] = \sqrt{[D' : K][K' : K]} = \sqrt{[D : K]}$$

where we used Theorem 12.4.11 in the last step. This finishes the induction step. $\square$

*Proof of Theorem 3.2.* Suppose $D$ is a central division algebra over $K^{\mathrm{ur}}$ of rank $n^2$. Then lemma 2 furnishes a subfield of $K^{\mathrm{ur}}$ of degree $n$, unramified over $K^{\mathrm{ur}}$. Hence $n = 1$, and $D$ is trivial. Thus $\mathrm{Br}_{K^{\mathrm{ur}}} = 0$. This proves Theorem 3.2 and hence Theorem 3.1. $\square$

## 3.2 Second proof (Herbrand quotient calculation)

### 3.2.1 Herbrand quotient calculation

We first need the following lemma.

**Lemma 3.5:** subgroup-trivial-cohom Given a local field $L$, there exists an open subgroup $V$ of $U_L$ with trivial cohomology, i.e. $H^q(G, V) = 0$ for all $q$.

*Proof.* The idea is to compare a multiplicative $G$-module $V$ with an additive $G$-module (more accurately, compare the filtration of $V$), and use the same argument as in Theorem 1.1.2.[3]

By the normal basis theorem, $L^+$ has a normal basis $\{\sigma(\alpha) : \sigma \in G\}$, i.e. it is free over $K[G]$. Let $A = \sum_{\sigma\in G} \mathcal{O}_K\sigma(\alpha)$.[4] By multiplying $\alpha$ by a power of $\pi_K$ we may assume that $\alpha \in \mathcal{O}_L$. Suppose that

$$\pi_K^n \mathcal{O}_L \subseteq A \subseteq \mathcal{O}_L.$$

Let $M = \pi_K^{n+1}A$, $V = 1 + M$ and $V^{(i)} = 1 + \pi_K^i M$. Note that

$$M \cdot M \subseteq \pi_K^{2n+2} A \cdot A \subseteq \pi_K \pi_K^{n+1}\pi_K^n \mathcal{O}_L \subseteq \pi_K\pi_K^{n+1}A \subseteq \pi_K M.$$

[3] If $\mathrm{char}(L) = 0$ there is a faster proof: Note that $e^x$ is a topological isomorphism from a neighborhood of 0 in the additive group $L$ to a neighborhood of 1 in the multiplicative group $\mathcal{O}_L$. Moreover, it preserves the action of $G$ because the fact that $G$ acts continuously on $L$ gives

$$e^{\sigma x} = \sum_{n=0}^{\infty} \frac{(\sigma x)^n}{n!} = \sum_{n=0}^{\infty} \frac{\sigma(x^n)}{n!} = \sigma e^x.$$

Now Theorem 1.1.2 applies directly.

[4] Warning: $A$ is a $\mathcal{O}_K[G]$-module; we don't know it is an $\mathcal{O}_L$-module.

This shows that

1. $V$ is a subgroup: Indeed, $(1+M)(1+M) \subseteq 1+M+M\cdot M \subseteq 1+M$ by the above.

2. $V^i/V^{i+1} \cong A/\pi_K A$ as $G$-modules. Indeed, if $m_1, m_2 \in M$, then for some $m_3 \in M$, we have

$$(1+\pi_K^i m_1)(1+\pi_K^i m_2) = 1+\pi_K^i(m_1+m_2)+\pi_K^{2i}\pi_K m_3 \equiv 1+\pi_K^i(m_1+m_2) \pmod{\pi_K^{i+1}M}.$$

Hence

$$H^q(G, V^{(i)}/V^{(i+1)}) = H^q(G, M/\pi_K M) = 0$$

for each $q$, since $M/\pi_K M$ is an induced module over $G$ (and has trivial cohomology by Shapiro's Lemma 11.8.1). (By construction $M/\pi_K M = \mathrm{Ind}^G[(\pi_K^{n+1}\alpha\mathcal{O}_K)/(\pi_K^{n+2}\alpha\mathcal{O}_K)]$.) Lemma 1.4 applied to $V$ finishes the proof. □

**Proposition 3.6:** herbrand-units-l Suppose $L/K$ is cyclic of degree $n$. Then

$$h(U_L) = 1.$$
$$h(L^\times) = n.$$

*Proof.* Choose $V$ as in Lemma 3.5. Since $V$ is open, $U_L/V$ is finite. By Proposition 11.12.4(1), $h(U_L/V) = 1$. Hence

$$h(U_L) = h(V)h(U_L/V) = 1.$$

By Proposition 11.12.4(3), $h(\mathbb{Z}) = |G| = n$. Since $L^\times = U_L \times \pi_L^{\mathbb{Z}}$ we get

$$h(L^\times) = h(U_L)h(\mathbb{Z}) = n.$$

□

**Theorem 3.7** (Class field axiom for local class field theory)**:** thm:cfa-lcft Let $L/K$ be a cyclic extension of degree $n$. Then

$$|H^1(L/K)| = 1$$
$$|H^2(L/K)| = n.$$

*Proof.* The first follows directly from Hilbert's Theorem 90 (1.1). For the second, we have $|H^2(L/K)| = h(L^\times)|H^1(L/K)| = n$ using Proposition 3.6. □

We want to show that $|H^2(L/K)| = n$ for all Galois extensions $L/K$, and in fact $H^2(L/K)$ is cyclic of order $n$. We proceed in 2 steps.

### 3.2.2 First inequality

We show that for all Galois extensions $L/K$, $|H^2(L/K)| \geq [L : K]$. In fact, we show the following.

**Lemma 3.8:** lem:local-1eq Let $L/K$ be a Galois extension of local fields of degree $n$. Then $H^2(L/K)$ contains a subgroup canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

*Proof.* We prove this using Theorem 2.2, which relates the invariant maps on $K^{\mathrm{ur}}/K$ and $L^{\mathrm{ur}}/L$. By Theorem 12.5.3, we have the exact sequence $0 \to H^2(L/K) \to H^2(K) \to H^2(L)$. Inflation and restriction commute by functoriality of change of group, so we have the commutative diagram with exact columns

$$\text{eq : local} - 1eq \qquad \begin{tikzcd} 0 \arrow[d] & 0 \arrow[d] \\ H^2(L/K) \arrow[d] & \ker(\mathrm{Res}) \arrow[l, dotted] \arrow[d] \\ H^2(K) \arrow[d, "\mathrm{Res}"] & H^2(K^{\mathrm{ur}}/K) \arrow[l, hook', "\mathrm{Inf}"'] \arrow[d, "\mathrm{Res}"] \\ H^2(L) & H^2(K^{\mathrm{ur}}/L). \arrow[l, hook', "\mathrm{Inf}"'] \end{tikzcd} \tag{13.3}$$

By Theorem 2.2, the map $H^2(K^{\mathrm{ur}}/K) \to H^2(L^{\mathrm{ur}}/L)$ corresponds to the multiplication-by-$[L : K]$ map after identifying both sides with a subgroup of $\mathbb{Q}/\mathbb{Z}$ through the respective invariant maps. Hence $\ker(\mathrm{Res}) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. The top map exists and is an injection because the other two are (4-lemma). Hence $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(L/K)$, as needed. □

### 3.2.3 Second inequality

Next we show $|H^2(L/K)| \leq [L : K]$, so $|H^2(L/K)| = [L : K]$.

**Lemma 3.9:** lem:local-2ineq Let $L/K$ be a Galois extension of local fields of degree $n$. Then $H^2(L/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

*Proof.* We already know that $|H^2(L/K)| = [L : K]$ for $L/K$ cyclic (Theorem 3.7). We prove that $|H^2(L/K)| = [L : K]$ by induction on the degree.

By Corollary 9.4.12, $G(L/K)$ is solvable. Thus, if $G(L/K)$ is not cyclic, it has a normal subgroup $G(L/K')$. By Theorem 12.5.3 we have an exact sequence

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

so

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

By Lemma 3.8, equality holds. □

#### 3.2.4 Finishing the proof

*Second proof of Theorem 3.1.* Take any element $a \in H^2(\overline{K}/K)$; it is in $H^2(L/K)$ for some finite Galois $L/K$. The top injection in (13.3) is an isomorphism by Lemma 3.9, and we get $a \in H^2(K^{\mathrm{ur}}/K)$. □

# §4 Class formations

sec:class-formations The preceding sections show that

$$(G(\overline{K}/K), \{G(L/K) : L/K \text{ finite Galois}\}, \overline{K})$$

is a *class formation*. That is, it satisfies the basic axioms that allow us to obtain the conclusions of class field theory. With the abstraction of class formations, when we prove global class field theory, we only have to verify the axioms and we will get the desired conclusions in the same way as in local class field theory.

## 4.1 Class formations in the abstract

**Definition 4.1:** An **abstract Galois group** is a group $G$ with a family of subgroups of finite index $\{G_L\}_{L\in X}$ such that

1. (Closure under intersection) If $L_1, L_2 \in X$, then there exists $M$ such that
$$G_{L_1} \cap G_{L_2} = G_M.$$
2. (Closure under superset) If $G_L \subseteq G' \subseteq G$ are subgroups, then $G' = G_{K'}$ for some $K'$.
3. (Closure under conjugation) For every $s \in G$ and $L \in X$ there exists $L'$ so that
$$sG_Ls^{-1} = G_{L'}.$$

This definition is motivated by the fact that these are the key properties of Galois groups.

**Proposition 4.2:** A topological Galois group $G(\Omega/K_0)$ with all its closed subgroups, is an abstract Galois group.

*Proof.* By the fundamental theorem of infinite Galois theory **??**.**??**, the closed subgroups of $G(\Omega/K_0)$ are exactly those in the form $G(\Omega/K)$ with $K_0 \subseteq K \subseteq \Omega$. The above properties correspond to the following facts from Galois theory.

1. $G(\Omega/K) \cap G(\Omega/L) = G(\Omega/KL)$.
2. The subgroups of $G(\Omega/K_0)$ containing $G(\Omega/L)$ correspond to intermediate extensions between $K_0$ and $L$.

3. $sG(\Omega/K)s^{-1} = G(\Omega/sK)$. □

We transfer some terminology about Galois groups to the abstract case.

**Definition 4.3:** Let $(G, \{G_L\}_{L\in X})$ be an abstract Galois group. The elements of $X$ are called fields. The field $K_0$ with $G_{K_0} = G$ is called the basefield. For $G_M \subseteq G_L$, define $[M : L]$ to be $[G_L : G_M]$; we say $M/L$ is a Galois extension if $G_M \trianglelefteq G_L$, and write

$$G(M/L) = G_L/G_M$$

(called the "Galois group" of $M/L$). We say $M/L$ is abelian, etc. if $G(M/L)$ is abelian, etc.

The field $M$ such that $G_{L_1} \cap G_{L_2} = G_M$ is called the composite of $L_1$ and $L_2$, and denoted by $L_1L_2$; the field $L'$ such that $sG_Ls^{-1} = G_{L'}$ is denoted by $sL$.

Note every extension $M/L$ is contained in a Galois extension: Since $[G_L : G_M]$ is finite $G_M$ has finitely many conjugates $sG_Ms^{-1}$ in $G_L$; by the axioms $G_{M'} = \bigcap_s sG_Ls^{-1}$ for some $M'$, called the Galois closure of $M/L$.

**Definition 4.4:** A **formation** is a triple $(G, \{G_K\}_{K\in X}, A)$ where $(G, \{G_K\}_{K\in X})$ is an abstract Galois group and $A$ is a discrete topological $G$-module (see Definition 11.14.1). Let $A_K := A^{G_K}$.

Define the norm $\mathrm{Nm}_{L/K} : A_L \to A_K$ by letting $\mathrm{Nm}_{L/K}(a) = \prod_{\sigma\in G(L'/K)/G(L'/K)} \sigma(a)$ for any $L'$ Galois over $K$.

For $L/K$ Galois, we define $H^n(L/K) := H^n(G(L/K), A_L)$. We can define inflation, restriction, and corestriction maps in the natural way, with $\mathrm{Res}_{K/L} = \mathrm{Res}_{G_K/G_L}$, and so forth.

**Definition 4.5:** def:class-formation A **class formation** is a formation $(G, \{G_K\}_{K\in X}, A)$ with a homomorphism $\mathrm{inv}_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$ for each Galois extension $L/K$, such that the following hold.

1. $H^1(L/K) = 0$ for every cyclic extension of prime degree.
2. $\mathrm{inv}_{L/K}$ is an isomorphism from $H^2(L/K)$ to $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.
3. (Compatibility under inflation) For any finite extension $M/L$,

$$\mathrm{inv}_{M/K} \circ \mathrm{Inf}_{M/L} = \mathrm{inv}_{L/K}.$$

   Hence we can define $\mathrm{inv}_K : \varinjlim_L H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$. (This axiom implies that inflations are injective on $H^2$, so we can think of $H(K) := \varinjlim_L H^2(L/K)$ as $\bigcup_L H^2(L/K)$.)

4. (Compatibility with restriction) For any finite Galois extension $L/K$,

$$\mathrm{inv}_L \circ \mathrm{Res}_{K/L} = [L : K]\,\mathrm{inv}_K.$$

Define the **fundamental unit** of $L/K$ to be

$$u_{L/K} = \mathrm{inv}_K^{-1}\left(\frac{1}{[L:K]}\right).$$

**Proposition 4.6:** Assume a formation satisfies axiom 1. Then for every Galois extension $L/K$,

$$H^1(L/K) = 0.$$

*Proof.* First we show this when $[L:K]$ is a prime power $p^n$. Induct on the degree. The base case is given. Every $p$-group has a subgroup of index $p$, so there is $K \subset K' \subset L$ such that $G(K'/K)$ has order $p$. By the inflation-restriction exact sequence 11.11.10, we get

$$0 \to \cancelto{0}{H^1(K'/K)} \xrightarrow{\mathrm{Inf}} H^1(K/L) \xrightarrow{\mathrm{Res}} \cancelto{0}{H^1(L/K')};$$

the first and last terms are 0 by axiom 1 and by the induction hypothesis. So $H^1(K/L) = 0$.

For general $L/K$, this shows $H^1(G(L/K)_p, A_L) = 0$, so the result follows from Corollary 11.11.8. □

**Proposition 4.7:** Assume a formation satisfies axiom 2. Transferring the action of Res, Cor, and Inf to the subgroups of $\mathbb{Q}/\mathbb{Z}$, we get the following diagram:

$$\begin{tikzcd}
M \arrow[d, dash, "{[M:L]}"'] & & & & & \\
L \arrow[d, dash, "{[L:K]}"'] & H^2(M/L) \arrow[r, "\mathrm{inv}_L"] \arrow[d, bend right, "\mathrm{Cor}_{L/K}"'] & \frac{1}{[M:L]}\mathbb{Z}/\mathbb{Z} \arrow[d, bend right, "i"'] & L \arrow[d, dash] & & \\
K & H^2(M/K) \arrow[r, "\mathrm{inv}_K"] \arrow[u, bend right, "\mathrm{Res}_{K/L}"'] & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \arrow[u, bend right, "{[L:K]}"'] & K & H^2(L/K) \arrow[r, "\mathrm{inv}_K"] \arrow[llll, hook, bend left, "\mathrm{Inf}_{M/L}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[lll, hook, bend left, "i"]
\end{tikzcd}$$

(Note $\mathrm{Cor}_{L/K} \circ \mathrm{Res}_{K/L} = [L:K]$.) Moreover (passing to the limit), the following hold.

1. For every extension $L/K$,

$$\mathrm{Res}_{K/L} : H^2(K) \twoheadrightarrow H^2(L)$$

is surjective.

2. For every extension $L/K$,

$$\mathrm{Cor}_{L/K} : H^2(L) \hookrightarrow H^2(K)$$

is injective, and

$$\mathrm{inv}_K \circ \mathrm{Cor}_{L/K} = \mathrm{inv}_L .$$

3. For every $s \in G$, letting $s^* : H^2(K) \to H^2(sK)$,

$$\mathrm{inv}_{sK} \circ s^* = \mathrm{inv}_K .$$

*Proof.* The surjectivity of $\mathrm{Res}_{K/L}$ in the diagram comes directly from the injectivity of $\mathrm{inv}_K$ and $\mathrm{inv}_L \circ \mathrm{Res}_{K/L} = [L : K]\,\mathrm{inv}_K$.

For the action of $\mathrm{Cor}_{L/K}$, note

$$\mathrm{inv}_K \circ \mathrm{Cor}_{L/K} \circ \mathrm{Res}_{K/L} = \mathrm{inv}_K \circ [L : K] = \mathrm{inv}_L \circ \mathrm{Res}_{K/L}$$

where the first follows from Theorem 11.11.5 and the second from the axiom. Surjectivity of $\mathrm{Res}_{K/L}$ gives $\mathrm{inv}_K \circ \mathrm{Cor}_{L/K} = \mathrm{inv}_L$, as needed.

Items 1 and 2 now follow from taking the direct limit.

For 3, let the basefield be $K_0$; note the map $s^* : H^2(K_0) \to H^2(sK_0) = H^2(K_0)$ is the identity by Proposition 11.11.3, so $\mathrm{inv}_{sK_0} \circ s^* = \mathrm{inv}_{K_0}$. For arbitrary $x \in H^2(K)$, by surjectivity of $\mathrm{Res}_{K/L}$ we can write $x = \mathrm{Res}_{K/L}(x_0)$. Since Res and $s^*$ commute (transport of structure),

$$\mathrm{inv}_{sK}(s^* x) = \mathrm{inv}_{sK}(s^* \mathrm{Res}_{K_0/K} x_0) = \mathrm{inv}_{sK} \mathrm{Res}_{sK/sK_0}(s^* x_0) = [sK : sK_0]\,\mathrm{inv}_{sK_0}(x_0) = \mathrm{inv}_K(x).$$

$\square$

The reciprocity law follows from the properties of class formations.

**Theorem 4.8** (Abstract reciprocity law)**:** thm:abstract-reciprocity Let $(G, \{G_K\}_{K \in X}, \{A_K\}, \mathrm{inv}_{L/K})$ be a class formation. Then there is a isomorphism

$$\begin{array}{ccc} H_T^{-2}(G(L/K), \mathbb{Z}) & \xrightarrow[\cong]{u_{L/K} \cup \bullet} & H_T^0(G, A_L) \\ \| & & \| \\ G(L/K)^{\mathrm{ab}} & & A_K / \mathrm{Nm}_{L/K}(A_L) \end{array}$$

Here $\mathrm{Nm}_{L/K}$ means $N_{G_K/G_L}$. Denote the reverse map by $\phi_{L/K}$.

*Proof.* The identifications are from Theorem 11.8.3 and Definition 11.9.2. Axioms 1 and 2 for class formation give that the two conditions of Tate's Theorem 11.13.1 are satisfied. $\square$

This map is hard to calculate directly because cup products on negative Tate cohomology are hard to deal with. The following helps us by transferring the cup products to nonnegative Tate groups.

**Theorem 4.9:** thm:calculate-local-artin Keep the above hypothesis. Then for any $\chi \in \mathrm{Hom}^{\mathrm{cont}}(G(L/K), \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$ and $a \in A_K$,

$$\chi(\phi_{L/K}(a)) = \mathrm{inv}_K(\overline{a} \cup \delta\chi).$$

Here $\overline{a}$ denotes the image of $a$ in $H_T^0(G(L/K), A_L) = A_L / \mathrm{Nm}_{L/K} A_L$, and $\delta$ is the diagonal morphism corresponding to the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

Note this characterizes the reciprocity map since knowing the image of an element of an abelian group under all homomorphisms to $\mathbb{Q}/\mathbb{Z}$ is equivalent to knowing the element itself.[5]

*Proof.* Suppose $\chi(\phi_{L/K}(a)) = \frac{r}{n}$.

By the definition of the Artin map as the inverse of $u_{L/K} \cup \bullet$, we have

$$\overline{a} = u_{L/K} \cup \phi_{L/K}(a).$$

We now calculate the following (for easy reference, we note which cohomology groups the elements are in).

$$\begin{aligned}
\underbrace{\overline{a}}_{0} \cup \underbrace{\delta\chi}_{2} &= [\underbrace{u_{L/K}}_{2} \cup \underbrace{\phi_{L/K}(a)}_{-2}] \cup \underbrace{\delta\chi}_{2} \\
&= \underbrace{u_{L/K}}_{2} \cup [\underbrace{\phi_{L/K}(a)}_{-2} \cup \underbrace{\delta\chi}_{2}] && \text{associativity} \\
&= \underbrace{u_{L/K}}_{2} \cup [\delta(\underbrace{\phi_{L/K}(a)}_{-2} \cup \underbrace{\chi}_{1})] && \text{Theorem 11.10.1(4)} \\
&= \underbrace{u_{L/K}}_{2} \cup \underbrace{\delta(\chi(\phi_{L/K}(a)))}_{0} && \text{Theorem 11.10.3(3)} \\
&= \underbrace{u_{L/K}}_{2} \cup \underbrace{\delta\left(\frac{r}{n}\right)}_{0} \\
eq : calc - artin1 &= \underbrace{u_{L/K}}_{2} \cup \underbrace{r}_{0} \qquad (13.4) \\
&= r u_{L/K} && \text{Theorem 11.10.3(1)} \\
\operatorname{inv}_K(\overline{a} \cup \delta\chi) &= \frac{r}{n} = \chi(\phi_{L/K}(a)).
\end{aligned}$$

In (13.4), we use the map in the snake lemma to calculate $\delta\left(\frac{r}{n}\right)$: it pulls back to $\frac{r}{n} \in \mathbb{Q} \cong H_T^{-1}(G, \mathbb{Q})$; the norm maps it to $r = n \cdot \frac{r}{n} \in \mathbb{Q} \cong H_T^0(G, \mathbb{Q}) \supseteq H_T^0(G, \mathbb{Z})$. In the second-to-last line, we note that $\bullet \cup r$ is simply multiplication by $r$ in dimension 0, so Theorem 11.10.3(1) tells us it is multiplication by $r$ in dimension 2 as well. □

We need several naturality properties of the reciprocity map.

**Theorem 4.10:** thm:reciprocity-natural Let $M/L/K$ be Galois extensions. The following

[5] It may seem odd to calculate $\chi \circ \phi_{L/K}$ instead of $\phi_{L/K}$ directly but keep in mind that for general $L/K$, $\mathrm{Frob}_{L/K}(\mathfrak{p})$ is only defined to be a *conjugacy class*, and it is natural to look at the action of characters on conjugacy classes because characters are class functions.

are commutative.

$$\begin{tikzcd} A_L \arrow[r, "\mathrm{Cor}^0=\mathrm{Nm}_{L/K}"] \arrow[d, "\phi_{M/L}"'] & A_K \arrow[d, "\phi_{M/K}"'] \\ G(M/L)^{\mathrm{ab}} \arrow[r, "\mathrm{Cor}^{-2}", "\text{natural}"'] & G(M/K)^{\mathrm{ab}} \end{tikzcd} \qquad \begin{tikzcd} A_K \arrow[r, hook, "\mathrm{Res}^0=i"] \arrow[d, "\phi_{M/K}"'] & A_L \arrow[d, "\phi_{M/L}"] \\ G(M/K)^{\mathrm{ab}} \arrow[r, "\mathrm{Res}^{-2}=V"] & G(M/L)^{\mathrm{ab}} \end{tikzcd}$$

$$\begin{tikzcd} A_K \arrow[r, "s^*"] \arrow[d, "\phi_{L/K}"] & A_{sK} \arrow[d, "\phi_{sL/sK}"] \\ G(L/K)^{\mathrm{ab}} \arrow[r, "s^*"] & G(sL/sK) \end{tikzcd} \qquad \begin{tikzcd} A_K \arrow[d, "\phi_{M/K}"] \arrow[dr, "\phi_{L/K}"] & \\ G(M/K)^{\mathrm{ab}} \arrow[r] & G(L/K)^{\mathrm{ab}}. \end{tikzcd}$$

*Proof.* First note that the maps in the first diagram are corestrictions and the maps in the second diagram (on the right) are restrictions by Proposition 11.4.

From axiom 4 of Proposition 4.5, we have

$$\mathrm{Res}_{K/L}(u_{M/K}) = u_{M/L}.$$

We will use Proposition 11.11.9, about the commutativity of cup products with restriction and corestriction. The first diagram follows from

$$\mathrm{Cor}^0_{L/K}(x \cup u_{M/L}) = \mathrm{Cor}^0_{L/K}(x \cup \mathrm{Res}_{K/L}(u_{M/K})) = \mathrm{Cor}^2_{L/K}(x) \cup u_{M/K}, \quad x \in G(M/L)^{\mathrm{ab}}.$$

The second diagram follows from

$$\mathrm{Res}^0_{K/L}(x \cup u_{M/K}) = \mathrm{Res}^{-2}_{K/L}(x) \cup u_{M/L}.$$

The third diagram follows from the fact that the map $s^* : AL \to A_{sK}$ takes $u_{L/K}$ to $u_{sL/sK}$.

For the last diagram, let $\chi$ be a character on $G(L/K)$, which gives a character $\chi_{M/K}$ on $G(M/K)$ using the projection $G(M/K) \to G(L/K)$. By Theorem 4.9 we have, for any character $\chi$,

$$\chi_{M/K}(\phi_{M/K}(a)) = \mathrm{inv}_K(\overline{a}_{M/K} \cup \delta\chi_{M/K}) = \mathrm{inv}_K(\overline{a}_{L/K} \cup \delta\chi) = \chi(\phi_{L/K}(a))$$

where $\overline{a}_{M/K}, \overline{a}_{L/K}$ are the images in $H^0_T(M/K)$ and $H^0_T(L/K)$, respectively. □

The fourth diagram means that the maps $\phi_{L/K}$ are compatible, so we can define

$$\phi_K = \varprojlim_L \phi_{L/K} : A \to G^{\mathrm{ab}}.$$

(Note $A = \bigcup A^H$.)

**Theorem 4.11** (Norm limitation)**:** norm-limitation Let $(G, \{G_K\}, \{A_K\}, \mathrm{inv}_{L/K})$ be a class formation. Let $L/K$ be an extension and $E/K$ be the largest abelian subextension. Then

$$\mathrm{Nm}_{L/K} A_L = \mathrm{Nm}_{E/K} A_E.$$

*Proof.* Let $L^{\mathrm{gal}}$ be the Galois closure of $L$. Transitivity of norms (just look at the definition of norm...) gives us $\subseteq$. Conversely, suppose $a \in \mathrm{Nm}_{E/K} A_E$. Let $G = G(L^{\mathrm{gal}}/K)$ and $H = G(L'/L)$. Since $E$ is the largest abelian subextension of $L^{\mathrm{gal}}$ abelian over $K$ and contained in $L$, the subgroup of $G$ fixing it is $G'H$. We have the commutative diagram

$$\begin{tikzcd}
A_L \arrow[r, "\phi_{L^{\mathrm{gal}}/L}"] \arrow[d, "\mathrm{Nm}_{L/K}"] & H/H' \arrow[d, "i"] \\
A_K \arrow[r, "\phi_{L^{\mathrm{gal}}/K}"] \arrow[dr, "\phi_{E/K}"'] & G/G' \arrow[d, two heads] \\
 & G/G'H
\end{tikzcd}$$

where $i$ is induced by inclusion. Because $a \in \mathrm{Nm}_{E/K} A_E$, $\phi_{E/K}(a) = 1$ in $G/G'H$. Thus $\phi_{L^{\mathrm{gal}}/K}(a) \in G'H/G'$, and $\phi_{L^{\mathrm{gal}}/K}(a)$ is in the image of $i$ and hence $i \circ \varphi_{L'/L}$, and there exists $b \in A_L$ such that $\phi_{L^{\mathrm{gal}}/K}(a) = i(\phi_{L^{\mathrm{gal}}/L}(b))$. Then

$$\phi_{L^{\mathrm{gal}}/K}(a) = i(\phi_{L^{\mathrm{gal}}/L}(b)) = \phi_{L^{\mathrm{gal}}/K}(\mathrm{Nm}_{L/K}(b)).$$

This means $\frac{a}{\mathrm{Nm}_{L/K}(b)} \in \ker(\phi_{L^{\mathrm{gal}}/K}) = \mathrm{Nm}_{L^{\mathrm{gal}}/K}(A_{L'})$; say it equals $\mathrm{Nm}_{L^{\mathrm{gal}}/K}(c)$. Then

$$a = \mathrm{Nm}_{L/K}(b\, \mathrm{Nm}_{L^{\mathrm{gal}}/L}(c)) \in \mathrm{Nm}_{L/K}(A_L),$$

as needed. □

**Definition 4.12:** A subgroup $S$ of $A_K$ is a **norm group** if there exists an extension $L/K$ such that $S = \mathrm{Nm}_{L/K}(A_L)$.

**Theorem 4.13** (Bijective correspondence)**:** thm:abstract-bijection Let $(G, \{G_K\}, \{A_K\}, \mathrm{inv}_{L/K})$ be a class formation. Then there is a bijective correspondence between finite abelian extensions of $K$ and the set of norm groups of $A_K$, given by

$$L \mapsto \mathrm{Nm}_{L/K}(A_L).$$

Furthermore, this is an inclusion-reserving bijection that takes intersections to products and products to intersections:

$$\begin{aligned} L \subseteq M &\iff \mathrm{Nm}_{L/K}(A_L) \supseteq \mathrm{Nm}_{M/K}(A_M) \\ \mathrm{Nm}_{L\cdot L'/K}(A_{L\cdot L'}) &= \mathrm{Nm}_{L/K}(A_L) \cap \mathrm{Nm}_{L'/K}(A_{L'}) \\ \mathrm{Nm}_{L\cap L'/K}(A_{L\cap L'}) &= \mathrm{Nm}_{L/K}(A_L) \cdot \mathrm{Nm}_{L'/K}(A_{L'}). \end{aligned}$$

Finally, every subgroup of $A_K$ containing a norm group is a norm group.

*Proof.* Abbreviate $\mathrm{Nm}_{L/K}(A_L)$ by $N_L$.

First we show $N_{LL'} = N_L \cap N_{L'}$. By reciprocity,

$$N_L \cap N_{L'} = \ker(\phi_{L/K}) \cap \ker(\phi_{L'/K}) \overset{(*)}{=} \ker(\phi_{LL'/K}) = N_{LL'}$$

where $(*)$ comes from compatibility of the $\phi$ and the fact that the map $G(LL'/K) \to G(L/K) \times G(L'/K)$ is injective.

If $L \subseteq M$, then $N_L \supseteq N_M$ from transitivity of norms. Conversely, if $N_L \supseteq N_M$, then by the above $N_L = N_L N_M = N_{LM}$. Thus $[A_K : N_L] = [A_K : N_{LM}]$, and reciprocity gives $[L : K] = [LM : K]$, i.e. $LM = L$, i.e. $L \subseteq M$. Thus, $L \mapsto N_L$ is an inclusion-reversing bijection.

Next we show that every subgroup containing a norm group is a norm group. Suppose $N_L \subseteq N$; we show $N$ is a norm group. We have that $\phi_{L/K}$ maps $N$ isomorphically onto $G(L/K')$, where $K' = L^{\phi_{L/K}(N)}$, the fixed field of $\phi_{L/K}(N)$. Consider the following commutative diagram from Theorem 4.10:

$$\begin{tikzcd}
A_K \arrow[r, two heads, "\phi_{L/K}"] \arrow[dr, two heads, "\phi_{K'/K}"'] & G(L/K) \arrow[d] \\
& G(K'/K).
\end{tikzcd}$$

From this we find

$$N = \ker(\phi_{K'/K}) = N_{K'}$$

as needed.

Finally, we show $N_{L\cap L'} = N_L \cdot N_{L'}$. Note $L \cap L'$ is the largest extension contained in both $L$ and $L'$, while $N_L \cdot N_{L'}$ is the smallest group containing both $N_L$ and $N_{L'}$, and it is a norm group by the above. Since $L \mapsto N_L$ is an inclusion-reversing bijection, we must have $N_{L\cap L'} = N_L \cdot N_{L'}$. ☐

## 4.2 Class formations for local class field theory

As promised, we apply the results of the last section to $(G(\overline{K}/K), \overline{K})$ where $K$ is a local field. (In the global case we will set $A$ to be the ideles instead.)

**Theorem 4.14:** thm:lcft-class-form Let $L$ be a local field. Then

$$(G(\overline{K}/K), \{G(L/K) : L/K \text{ finite Galois}\}, \overline{K})$$

is a class formation.

*Proof.* We verify the axioms of class formations.

1. $H^1(L/K) = 0$ for every cyclic extension of prime degree, by Hilbert's Theorem 90 (1.1).

2. Take the composition of the isomorphism $H^2(K) \cong H^2(K^{\text{ur}}/K)$ of Theorem 3.1 with the invariant map $H^2(K^{\text{ur}}/K) \to \mathbb{Q}/\mathbb{Z}$ to get
$$\operatorname{inv}_K : H^2(K) \to \mathbb{Q}/\mathbb{Z}.$$
The maps $\operatorname{inv}_{L/K} : H^2(L/K) \hookrightarrow H^2(K) \to \mathbb{Q}/\mathbb{Z}$ are isomorphisms onto their image, which much be $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

   Now we verify that
$$\operatorname{inv}_L \circ \operatorname{Res}_{K/L} = n \operatorname{inv}_K, \quad n = [L : K].$$
This follows from the following commutative diagram. From Theorem 2.2, the right square commutes; from the fact that inflation commutes with restriction (by functoriality), the left square commutes.
$$\begin{tikzcd}
H^2(K) \arrow[d, "\operatorname{Res}_{K/L}"] & H^2(K^{\text{ur}}/K) \arrow[l, "\text{Inf}"', "\cong"] \arrow[r, "\operatorname{inv}_{K^{\text{ur}}/K}"] \arrow[d, "\operatorname{Res}_{K/L}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n"] \\
H^2(L) & H^2(L^{\text{ur}}/L) \arrow[l, "\text{Inf}"', "\cong"] \arrow[r, "\operatorname{inv}_{L^{\text{ur}}/L}"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$
(Note that the target of the restriction in the middle is $H^2(K^{\text{ur}}/L)$, which is a subgroup of $H^2(L^{\text{ur}}/L)$.) $\square$

Applying results about class field theory, we get the main results of local class field theory, restated below.

**Theorem** (Local reciprocity law, Theorem 10.2.1)**:** For any nonarchimedean local field $K$, there exists a unique homomorphism
$$\phi_K : K^\times \to G(K^{\text{ab}}/K),$$
called the **local Artin (reciprocity) map** with the following properties.

1. (Relationship with Frobenius map) For any prime element $\pi$ of $K$ and any finite unramified extension $L$ of $K$, $\phi_K(\pi)$ acts on $L$ as $\operatorname{Frob}_{L/K}(\pi)$.

2. (Isomorphism) Let $p_L$ be the projection $G(K^{\text{ab}}/K) \to G(L/K)$. For any finite abelian extension $L/K$, $\phi_K$ induces an isomorphism $\phi_{L/K} : K^\times/\operatorname{Nm}_{L/K}(L^\times) \to G(L/K)$ making the following commute:
$$\begin{tikzcd}
K^\times \arrow[r, "\phi_K"] \arrow[d] & G(K^{\text{ab}}/K) \arrow[d, "p_L"] \\
K^\times/\operatorname{Nm}_{L/K}(L^\times) \arrow[r, "\phi_{L/K}", "\cong"'] & G(L/K).
\end{tikzcd}$$

3. (Compatibility with norm map) For any $K \subseteq K'$, the following diagram commutes.

$$\begin{tikzcd}
K'^{\times} \arrow[r, "\phi_{K'}"] \arrow[d, "\mathrm{Nm}_{K'/K}"] & G(K'^{\mathrm{ab}}/K') \arrow[d, "\bullet|_{K^{\mathrm{ab}}}"] \\
K^{\times} \arrow[r, "\phi_K"] & G(K^{\mathrm{ab}}/K)
\end{tikzcd}$$

*Proof.* By Theorem 4.14, $(G(\overline{K}/K), \{G(L/K) : L/K \text{ finite Galois}\}, \overline{K})$ is a class formation. By the Abstract Reciprocity Law applied to $A_K = K$, we thus have an isomorphism $K^\times / \mathrm{Nm}_{L/K} L^\times \xrightarrow{\cong} G(L/K)^{\mathrm{ab}}$. These maps are compatible by the first and fourth diagrams in Theorem 4.10.

Next we show that $\phi_K(\pi)$ acts on $L$ as $\mathrm{Frob}_{L/K}$. For the first, we use Theorem 4.9, which says

$$\chi(\phi_{L/K}(\pi)) = \mathrm{inv}_K(\overline{\pi} \cup \delta\chi).$$

We calculate the invariant map on $\overline{\pi} \cup \delta\chi$, recalling that the map $H^1(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ is evaluation at the Frobenius:

$$\begin{tikzcd}
H^2(L/K) \arrow[r] & H^2(G,\mathbb{Z}) & H^1(G,\mathbb{Q}/\mathbb{Z}) \arrow[l, "\delta"'] \arrow[r] & \mathbb{Q}/\mathbb{Z} \\
\overline{\pi} \cup \delta\chi \arrow[r] & v(\pi) \cup \delta\chi = 1 \cup \delta\chi & 1 \cup \chi \arrow[l] \arrow[r] & \chi(\mathrm{Frob}_{L/K}).
\end{tikzcd}$$

Thus $\chi(\phi_{L/K}(\pi)) = \chi(\mathrm{Frob}_{L/K})$ for all characters $\chi$ on $G(L/K)$, and $\phi_{L/K}(\pi) = \mathrm{Frob}_{L/K}$.

We will prove uniqueness in Section 8.1 $\square$

*Proof of norm limitation, Theorem 2.6.* This follows directly from Theorem 4.14 and Theorem 4.11. $\square$

# §5 Examples

Before we move on to the existence theorem, we seek to understand the reciprocity map a bit better.

## 5.1 Unramified case

The reciprocity map is easiest to understand for unramified extensions.

**Example 5.1:** ex:unramified-rec Suppose $L/K$ is an unramified extension of local fields of degree $n$ (possibly infinite). Then the reciprocity map is

$$\begin{aligned}
\phi_{L/K} : K^\times / \mathrm{Nm}_{L/K}(L^\times) \cong K^\times / \pi^{n\mathbb{Z}} U_K &\to G(L/K) \\
a &\mapsto \mathrm{Frob}_{L/K}^{v(a)}.
\end{aligned}$$

*Proof.* There are many ways to see this. We know that any uniformizer maps to $\mathrm{Frob}_{L/K}$. But the uniformizers generate $K^\times$, so $\phi_{L/K}$ must be the map $a \mapsto \mathrm{Frob}_{L/K}^{v(a)}$. As $\mathrm{Frob}_{L/K}$ has order $n$, the kernel is $\pi^{n\mathbb{Z}}U_K$.

Alternatively, in the proof of Theorem 10.2.1 above, run the argument with arbitrary $a$ instead of $\pi$. □

## 5.2 Ramified case

To understand the reciprocity map on ramified extensions, we have the following.

**Proposition 5.2:** pr:unit-to-inertia For any Galois extension of local fields $L/K$,

$$\phi_{L/K}(U_K) \subseteq I(L/K),$$

where $I(L/K)$ is the inertia group.

*Proof.* By Theorem 2.7.2, $L^{I(L/K)}/K$ is the maximal unramified subextension of $L/K$, so $U_K \subseteq \ker(\phi_{L^{I(L/K)}/K})$ from Example 5.1. This means that $\phi_{L/K}(U_K)$ projects trivially on $G(L^{I(L/K)}/K)$, i.e. $\phi_{L/K}(U_K) \subseteq I(L/K)$. □

In fact, the reciprocity map relates filtration on the unit group $U_K$ with the filtration on ramification groups (cf. Section 9.4.2), so Proposition 5.2 is just the beginning of the story.

**Theorem 5.3:** The reciprocity map transforms the filtration

$$K^\times/\,\mathrm{Nm}_{L/K}(L^\times) \supseteq U_K/\,\mathrm{Nm}_{L/K}(U_L) \supseteq U_K^{(1)}/\,\mathrm{Nm}_{L/K}(U_L^{\psi(1)}) \supseteq \cdots$$

into the filtration

$$G(L/K) \supseteq G^0 = I(L/K) \supseteq G(L/K)^1 \supseteq \cdots.$$

*Proof.* This uses more about local fields and local symbols than we'll prove. See Serre [14], Chapter XV or Neukirch [11], V.§6. □

**Example 5.4:** For the totally ramified extension $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$, the reciprocity map sends

$$p^{\mathbb{Z}}(1+(p^r)) \mapsto G(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p(\zeta_{p^r})).$$

The RHS is the $r$th upper ramification group $G^r$.

Explicit computation of the reciprocity map in the ramified case is difficult without Lubin-Tate Theory.

# §6 Hilbert symbols

sec:hilbert-symbol To prove the existence theorem, we need to show that every closed subgroup of $G$ occurs as a norm group, i.e. as the kernel of some Artin map $\phi_{L/K}$. To do this, we explicitly construct field extensions $L/K$ that give these norm groups. We will construct Kummer extensions, extensions that come from adjoining an $n$th root. We focus on these extensions for several reasons.

1. Recall that we don't have a way to directly calculate the action of $\phi_{L/K}$. Instead, we calculate indirectly by Theorem 4.9: If we know $\chi(\phi_{L/K}(a))$ for all characters on $G(L/K)$, then we have determined $\phi_{L/K}(a)$.

   An easy source of characters comes from Kummer Theory 12.2.2, since the group of characters is isomorphic to a cyclic group.[6]

2. We want to show that certain subgroups of norm groups are also norm groups. After verifying several topological properties of $\phi_K$, we can reduce this to a statement about $p$th powers/roots of norm groups. In the abstract existence theorem 7.2, properties 1 and 3 are easy to check; they are basically the reductions that allow property 2 to be sufficient.

Recally from Proposition 12.2.2 that $K^\times/K^{\times n} \cong \mathrm{Hom}(G(K^s/K), \mu_n)$. Thus the characters we get are in bijection with elements of $K^\times/K^{\times n}$. We can also consider $a \in K^\times$ as inside $K^\times/K^{\times n}$, and this gives us a sort of "duality": the Kummer pairing. We will see eventually that this is the source of reciprocity laws (Section 15.1), so these symbols are good for more than just proving the existence theorem.

We assume throughout that $K$ contains a $n$th root of unity, and $\mathrm{char}(K) \nmid n$.

**Definition 6.1:** Let $G = G(K^s/K)$. Define the local symbol

$$( \, , \, )_n : H^1(G, \mathbb{Q}/\mathbb{Z}) \times \underbrace{H^0(G, K^{s\times})}_{K^\times} \to H^2(G, K^{s\times}) = \mathrm{Br}_K$$
$$(\chi, b) = \bar{b} \cup \delta\chi$$

Here $\delta$ is with respect to the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Z}/\mathbb{Q} \to 0$ and $\bar{b}$ is the image of $K^{s\times}$ in $H^0_T(G, K^{s\times})$.

We will drop the subscript $n$ when the context is clear.

Since cup product is bilinear and $\delta$ is linear, $( \, , \, )$ is bilinear. If $K$ is local, by Theorem 4.9, we have for any Galois $L/K$ and any character $\chi$ on $G(L/K)$,

$$eq:invk-calc\,\mathrm{inv}_K(\chi, \phi_{L/K}(a)) = \mathrm{inv}_K(a \cup \delta\chi) = \chi(\phi_{L/K}(a)). \quad (13.5)$$

As promised, we now transfer this action to $K^\times/K^{\times n}$.

[6] Artin-Schreier theory, from exercise 12.2.1, is another source of characters.

**Definition 6.2:** Suppose $K$ is a local field, and let $G = G(K^s/K)$. For $a \in K^\times$, define the character as in Proposition 12.2.2 by

$$\chi_a(\sigma) = \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}, \quad \chi_a \in H^1\left(G, \frac{1}{n}\mathbb{Z}/\mathbb{Z}\right) \cong H^1(G, \mu_n),$$

where $G = G(L/K)$ and $L = K(a^{\frac{1}{n}})$. Here we choose a root of unity $\zeta$ to make a correspondence $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mu_n$.

Define the **Hilbert symbol** by

$$\begin{aligned} K^\times \times K^\times &\to \mathrm{Br}_K[n] \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mu_n \\ (a, b) &:= (\chi_a, b) = b \cup \delta\chi_a. \end{aligned}$$

If $K$ is a global field, let $(a, b)_v$ denote the Hilbert symbol where $a, b$ are considered as elements of $K_v$.

Note that the image is in $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, not just in $\mathbb{Q}/\mathbb{Z}$, because $n\chi_a = 0$.

We'll abuse notation and not make a clear distinction between $\mathrm{Br}_K[n] \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mu_n$, where $\mathrm{Br}_K[n]$ denotes the $n$-torsion subgroup of $\mathrm{Br}_K$. The first isomorphism is given by $\mathrm{inv}_K$ and the second by $\frac{1}{n} \leftrightarrow \zeta$. We transfer the $\chi_a$ from being defined on $\mu_n$ to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, then transfer back from $\mathrm{Br}_K[n] \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ to $\mu_n$ at the end, so we may as well use the formula (13.5) for the $\chi_a$ treated in $H^1(G, \mu_n)$.

The following relates the Hilbert symbol to the Artin map.

**Proposition 6.3:** pr:hilbert-explicit We have

$$(a, b) = \frac{[\phi_{L/K}(b)](\sqrt[n]{a})}{\sqrt[n]{a}}$$

where $L = K(\sqrt[n]{a})$.

*Proof.* Formula (13.5) gives (remember we're identifying $\mathrm{Br}_K \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mu_n$; by abuse of notation we drop the "$\mathrm{inv}_K$" because it is an isomorphism)

$$(a, b) = (\chi_a, \phi_{L/K}(b)) = \chi_a(\phi_{L/K}(b)) = \frac{[\phi_{L/K}(b)](\sqrt[n]{a})}{\sqrt[n]{a}}$$

where $L$ is any field Galois over $K$, containing $\sqrt[n]{a}$. $\square$

**Theorem 6.4:** thm:hilbert-bilinear The Hilbert symbol descends to a nondegenerate skew-symmetric bilinear map

$$K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$$

satisfying the following.

1. $(a, b) = 1$ iff $b \in \mathrm{Nm}_{K(a^{\frac{1}{n}})/K}(K(a^{\frac{1}{n}})^\times)$.

2. If $a \in K^\times$, $x \in K^\times$, and $x^n - a \neq 0$, then

$$(a, x^n - a) = 1.$$

In particular, $(a, -a) = 1 = (a, 1-a)$.

*Proof.* Everything that went into defining $(,)$ was linear in either variable (cup products, evaluation homomorphisms, snake lemma morphism), so $(,)$ gives a bilinear map $K^\times \times K^\times \to \mu_n$.

Suppose $\chi$ is an element of order $n$. Then its kernel $\ker(\chi)$ has index $n$ in $G(K^s/K)$. Under the Artin map this corresponds to a extension $L_\chi$ of degree $n$, such that $\ker(\chi) = \phi_K(\mathrm{Nm}_{L_\chi/K}(L_\chi^\times))$. Then

$$(\chi, b) = \chi(\phi_K(b)) = 0 \iff \phi_K(b) \in \ker(\chi)$$

iff $b \in \mathrm{Nm}_{L_\chi/K}(L_\chi^\times)$.

We apply this to $\chi = \chi_a$. Note that $\chi$ has order $[K(a^{\frac{1}{n}}) : K]$ and $\chi_a(G(K^s/K(a^{\frac{1}{n}}))) = 0$. Hence $\phi_K(\mathrm{Nm}_{K(a^{\frac{1}{n}})/K}(K(a^{\frac{1}{n}})^\times) \subseteq \ker \chi_a$. By comparing indices in $G(K^s/K)$, equality holds, giving the first item.

For the second item, note that

$$x^n - a = \prod_{j=0}^{n-1}(x - \zeta_n^j a^{\frac{1}{n}})$$

(for any choice of $n$th root). The factors in the product can be grouped into conjugates over $K$, so $x^n - a$ is a norm from $K(a^{\frac{1}{n}})/K$. Then $(a, x^n - a) = 1$ from the first item. Setting $x = 0, 1$ gives $(a, -a) = 1$ and $(a, 1-a) = 1$.

To show skew-symmetry, note from item 2 and bilinearity that

$$1 = (ab, -ab) = (a, -a)(a, b)(b, a)(b, -b) = (a, b)(b, a).$$

To show nondegeneracy, suppose $b \in K^\times$ such that $(a, b) = 1$ for all $a \in K^\times$; we show $b \in K^{\times n}$. The condition $(a, b) = 1$ translates into $\chi_a(\phi_K(b)) = 1$ for all $a$. Now the image of $\phi_K$ is dense in $G(L/K)^{\mathrm{ab}}$ (because it is surjective for every finite extension $L/K$, and $G(L/K)$ has the profinite topology). Hence $\chi_a = 0$. This means $a^{\frac{1}{n}} \in K$, i.e. $a \in K^{\times n}$. $\square$

**Corollary 6.5:** cor:hilbert-local Suppose $K$ is a local field, $K(a^{\frac{1}{n}})/K$ is unramified, and $b$ is a unit in $K$. Then $(a, b) = 1$.

If $K$ is a global field, then $(a, b)_v = 1$ in $K_v$ unless either $a$ or $b$ is not a unit in $K_v$, or $K(a^{\frac{1}{n}})/K$ is ramified (which happen at finitely many places).

*Proof.* Since $K(a^{\frac{1}{n}})/K$ is unramified, $U_K \subset \mathrm{Nm}_{K(a^{\frac{1}{n}})/K}(K(a^{\frac{1}{n}})^\times)$. The result now follows from Theorem 6.4.

The second part says that $(a, b)_v = 1$ if $a, b$ are units in $K_v$ and $K(a^{\frac{1}{n}})/K$ is unramified, which is clear from part 1. $\square$

**Remark:** In fact, $(a,b) = i(\chi_a \cup \chi_b)$ where $i : H^2(G, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{Br}_K$. (See Serre, p. 207.) This explains the symmetry better but takes more work to prove.

# §7 Existence theorem

sec:local-existence We show that the existence theorem follows from several further (topological) axioms on formations. We then prove that in local class field theory, these axioms are satisfied.

## 7.1 Existence theorem in the abstract

First, a definition.

**Definition 7.1:** Let $(G, \{G_K\}_{K \in X}, A)$ be a class formation. The **universal norm group** $D_K$ of $K$ is the intersection of all norm groups of $A_K$:

$$D_K = \bigcap_{L/K} \mathrm{Nm}_{L/K}(A_L).$$

**Theorem 7.2** (Abstract existence)**:** thm:abstract-existence Suppose that $(G, \{G_K\}_{K \in X}, A)$ is a formation satisfying the following conditions.

1. For every extension $L/K$, the norm homomorphism has closed image and compact kernel.

2. Let $[p]$ denote the map $x \mapsto px$ on $A$. For every prime $p$, there exists a field $K_p$ such that for $K$ containing $K_p$, $\ker([p]|_{A_K})$ is compact and $\mathrm{im}([p]|_{A_K})$ contains $D_K$.

3. There exists a compact subgroup $U_K$ of $A_K$ such that every closed subgroup of finite index in $A_K$ containing $U_K$ is a norm group.

Then a subgroup of $A_K$ is a norm group iff it is closed of finite index.

If the conclusion holds, $nA_K \subseteq D_K$ for every $K$, because $nA_K$ is closed of finite index and hence a norm group. Conversely, $D_K \subseteq \bigcap_{n \ge 1} nA_K$ because every norm group $N$ has finite index so $n$ kills $A_K/N$ for some $n$. Furthermore, $D_K$ must be divisible: else we could find a norm group $N \supseteq D_K$, and $n$ such that $nN \not\supseteq D_K$, even though $nN$ is still of finite index. (Note we write $A_K$ additively here, but in class field theory, $A_K = K$ and $nA_K$ actually means $A_K^n$.) The most important condition is item 2, because it will give us these two conditions. This gives us a large set of norm groups, and items 1 and 3 (which are more topological in nature) will give us the rest of the desired norm groups.

*Proof.* Step 1: Suppose axiom 1 holds. We show that for every extension $L/K$, $\mathrm{Nm}_{L/K}(D_L) = D_K$.

By transitivity of norms, $\mathrm{Nm}_{L/K}(D_L) \subseteq D_K$.

Conversely, suppose $a \in D_K$. Since $a \in D_K$, for any extension $M/L$, $A_M$ contains an element $b$ such that $\mathrm{Nm}_{M/K}(b) = \mathrm{Nm}_{L/K}\mathrm{Nm}_{M/L}(b) = a$. Thus

$$S_M := \mathrm{Nm}_{L/K}^{-1}(a) \cap \mathrm{Nm}_{M/L}(A_M)$$

is nonempty. Since Nm has compact kernel, the first group is compact; since Nm has closed image, the second group is closed; thus $S_M$ is compact. Since the $S_M$ for all $M/L$ form a directed system of compact subsets, $S = \bigcap_M S_M$ is nonempty. Any element of $S$ is an element of $\mathrm{Nm}_{L/K}^{-1}(a) \cap D_L$. This shows $a \in \mathrm{Nm}_{L/K}(D_L)$.

Step 2: Suppose axioms 1 and 2 hold. We show $D_K$ is divisible and

$$D_K = \bigcap_{n \geq 1} nA_K.$$

First we show that for every prime $p$, $pD_K = D_K$. Let $L$ be a field containing $K_p$, $a \in D_K$, and set

$$S_L = [p]^{-1}(a) \cap \mathrm{Nm}_{L/K} A_L.$$

Since $[p]^{-1}(a)$ is compact (as $\ker([p]|_{A_K})$ is compact by axiom 2) and $\mathrm{Nm}_{L/K} A_L$ is closed, $S_L$ is compact. Now this set this nonempty: since $a \in D_K = \mathrm{Nm}_{L/K} D_L$ by step 1, we can write $a = \mathrm{Nm}_{L/K}\, x$, $x \in D_L$. By axiom 2, $x = py$ with $y \in A_K$, so $b := \mathrm{Nm}_{L/K}\, y \in S_L$. Then $\bigcap_{L \supseteq K_p} S_L$ is nonempty as in step 1. Hence $a \in pD_K$.

This shows $pD_K = D_K$, and we get $D_K = \bigcap_{n\geq 1} nD_K \subseteq \bigcap_{n \geq 1} nA_K$.

For the other direction, note that $na$ is the norm of any extension of degree $n$, so $\bigcap_{n \geq 1} nA_K \subseteq D_K$.

Step 3: Assume all the axioms. We prove the theorem.

First, note that any norm group is closed by axiom 1, and has finite index by the reciprocity law 4.8. Indeed, by transitivity of norm, it suffices to consider Galois extensions, and the reciprocity law says $\mathrm{Nm}_{L/K}(A_L)$ has index equal to $G(L/K)^{\mathrm{ab}}$.

Conversely, suppose $S$ is a closed subgroup of finite index $n$. We will find a norm subgroup contained in $S$ and then apply Theorem 4.13. Since $A_K/S$ has order $n$, we get $D_K \subseteq nA_K \subseteq S$, so

$$\bigcap_{N \text{ norm group}} (N \cap U_K) = D_K \cap U_K \subseteq S.$$

Since $N \cap U_K$ are compact ($N$ is closed and $U_K$ is compact) and $S$ is open (closed subgroups of finite index are also open), there exists $N$ such that

$$N \cap U_K \subseteq S.$$

Note $U_K + (N \cap S)$ is closed of finite index in $A_K$ because $N, S$ are closed of finite index; we show we can replace $U_K$ with $U_K + (N \cap S)$ above:

$$N \cap (U_K + (N \cap S)) \subseteq S.$$

Suppose $a \in U_K$ and $a' \in N \cap S$ such that $a + a' \in N$. Then $a \in N$, but $N \cap U_K \subseteq S$ so $a \in S$ as well. Thus $a + a' \in S$, as needed.

Now $N \cap (U_K + (N \cap S))$ is is closed of finite index containing $U_K$, so is a norm group by axiom 3. By Theorem 4.13, we get $S$ is also a norm group. □

## 7.2 Existence theorem for local class field theory

*Proof of Theorem 10.2.3.* We verify that the class formation for LCFT satisfies the three axioms of Theorem 13.7.2.

1. To see that the norm map is closed, note that

$$\mathrm{Nm}_{L/K}(L^\times) \cap U_K = \mathrm{Nm}_{L/K}(U_L)$$

   because an element is a unit iff its norm is a unit. As $U_L$ is compact and $\mathrm{Nm}_{L/K}$ is continuous (Proposition 8.1.6), $\mathrm{Nm}_{L/K}(U_L)$ is compact and hence closed. Now $\mathrm{Nm}_{L/K}(L^\times)$ is a union of translates of $U_L$, therefore closed as well.

   The kernel of $\mathrm{Nm}_{L/K}$ is a closed subset of $U_L$, hence compact.

2. Take $K_p$ containing all $p$th roots of unity. The kernel of the $p$th power map is the $p$th roots of unity, which is a compact set. Suppose $K \supseteq K_p$, and let $b \in D_K$ be a universal norm. Then $(a, b) = 1$ for all $a$ by Theorem 6.4. Since the $p$th power Hilbert symbol is nondegenerate on $K^\times / K^{\times p}$, $a \in K^{\times p}$. Thus $D_K \subseteq K^{\times p}$.

3. Take $U_K$ to be the group of units of $K^\times$. The closed subgroups of finite index containing $U_K$ are just $\pi^{n\mathbb{Z}} U_K$ for $n \neq 0$; these are the norm groups of unramified extensions of degree $n$ by Proposition 5.1. (Note these extensions exist—just adjoin appropriate roots of unity.) □

*Proof of Theorem 10.2.5.* This follows from Theorem 4.13, Theorem 4.14 (class formation for LCFT), and the existence theorem just proved. □

Note the existence theorem gives the following.

**Corollary 7.3:** cor:univ-norm-1 The universal norm group $D_K$ is $\{1\}$.

*Proof.* All open subgroups of finite index are norm groups by the Existence Theorem 10.2.3. The intersection of all open subgroups of finite index is $\{1\}$, as $\bigcap_{m,n}(1+(\pi^m))\pi^{n\mathbb{Z}} = \{1\}$. □

# §8 Topology of the local reciprocity map

We now prove that $\phi_K$ gives a topological isomorphism $K^\times \to W(L/K)$.

*Proof of Theorem 10.2.4.* By Proposition 5.2, $\phi_{L/K}(U_K) \subseteq I(L/K)$, so we have the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & U_K \arrow[r] \arrow[d, "\phi_{L/K}"] & K^\times \arrow[r, "v"] \arrow[d, "\phi_{L/K}"] & \mathbb{Z} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I(L/K) \arrow[r] & G(L/K) \arrow[r] & G(l/k) \arrow[r] & 1.
\end{tikzcd}$$

where the rightmost vertical map sends 1 to the $p$th power Frobenius ($p = |k|$). The vertical maps factor as

$$\begin{tikzcd}
1 \arrow[r] & U_K/\operatorname{Nm}_{L/K}(U_L) \arrow[r] \arrow[d, "\phi_{L/K}", "\cong"'] & K^\times/\operatorname{Nm}_{L/K}(L^\times) \arrow[r, "v"] \arrow[d, "\phi_{L/K}", "\cong"'] & \mathbb{Z}/f\mathbb{Z} \arrow[r] \arrow[d, "\cong"'] & 1 \\
1 \arrow[r] & I(L/K) \arrow[r] & G(L/K) \arrow[r] & G(l/k) \arrow[r] & 1.
\end{tikzcd} \quad eq : decomp - K/nmL \tag{13.6}$$

where $f = [l : k]$. Recall $\phi_K = \varprojlim_L \phi_{L/K}$. The intersection of all norm groups is $\{1\}$ by Corollary 7.3, so $\phi_K$ is injective on $K^\times$.

In forming $\phi_K = \varprojlim_L \phi_{L/K}$, we are really considering the embedding

$$K^\times \hookrightarrow \widehat{K^\times} := \varprojlim_L K^\times/\operatorname{Nm}_{L/K}(L^\times) \xrightarrow{\cong} G(K^{\mathrm{ab}}/K).$$

Decomposing $K^\times/\operatorname{Nm}_{L/K}(L^\times)$ as in (13.6), we have that

1. $\varprojlim_L U_K/\operatorname{Nm}_{L/K}(U_L) \cong U_K$ since $U_K$ is compact, hence complete, so $U_K \cong I(K^{\mathrm{ab}}/K)$.

2. $\varprojlim_L \mathbb{Z}/f\mathbb{Z} = \widehat{\mathbb{Z}}$.

Thus $K^\times \hookrightarrow \widehat{K^\times}$ is the embedding $U_K \times \pi^{\mathbb{Z}} \hookrightarrow U_K \times \pi^{\widehat{\mathbb{Z}}}$.

Recalling that $W(L/K)$ is the inverse image of $\operatorname{Frob}^{\mathbb{Z}} \subseteq G(\overline{k}/k)$, we get $\phi_{L/K} : K^\times \to W(L/K)$ is a topological isomorphism. In summary, we have the diagram

$$\begin{tikzcd}
1 \arrow[r] & U_K \arrow[r] \arrow[d, "\phi_K", "\cong"'] & K^\times \arrow[r] \arrow[d, "\phi_K", "\cong"'] & \pi^{\mathbb{Z}} \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & I(K^{\mathrm{ab}}/K) \arrow[r] \arrow[dr] & W(K^{\mathrm{ab}}/K) \arrow[r] \arrow[d, hook] & \operatorname{Frob}^{\mathbb{Z}} \arrow[r] \arrow[d, hook] & 1 \\
 & & G(K^{\mathrm{ab}}/K) \arrow[r] & \operatorname{Frob}^{\widehat{\mathbb{Z}}} = G(\overline{k}/k) \arrow[r] & 1
\end{tikzcd}$$

∎

## 8.1 Uniqueness of the reciprocity map

sec:lcft-uniqueness Finally, we prove uniqueness. This finishes all the proofs of local class field theory.

We first restate Lemma 10.6.6.

**Lemma:** Suppose that $K$ is a nonarchimedean local field, $K^{\mathrm{ur}}$ is the maximal abelian unramified extension of $K$, and $L$ is an abelian extension containing $K^{\mathrm{ur}}$. Let $f : K^\times \to G(L/K)$ be a homomorphism satisfying (1) and either (2) or (2)$'$:

1. The composition $K^\times \xrightarrow{f} G(L/K) \to G(K^{\mathrm{ur}}/K)$ takes $\alpha$ to $\mathrm{Frob}_{K^{\mathrm{ur}}/K}(\pi)^{v(\alpha)}$.
2. For any uniformizer $\pi \in K$, $f(\pi)|_{K_\pi} = 1$, where
$$K_\pi := L^{\phi_K(\pi)}.$$

2'. For any finite subextension $K'/K$ of $K_\pi$, we have
$$f(\mathrm{Nm}_{K'/K}(K'^\times))|_{K'} = \{1\}.$$

Then $f$ equals the reciprocity map $\phi_K$.

*Proof of Lemma 10.6.6.* It suffices to prove this for $L = K^{\mathrm{ab}}$. We have the split exact sequence
$$eq:lcft-uniq \quad 1 \to U_K^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 1, \tag{13.7}$$
where the splitting is determined by the map $\mathbb{Z} \to K^\times$ sending $1 \mapsto \pi$, and the map $K^\times \to U_K$ sending $a \mapsto \frac{a}{\pi^{v(a)}}$. Under the Artin map, (13.7) gets sent to the split exact sequence of topological groups
$$1 \to I(K^{\mathrm{ab}}/K) = G(K/K^{\mathrm{ur}}) \to W(K^{\mathrm{ab}}/K) \to W(K^{\mathrm{ur}}/K) \cong \mathbb{Z} \to 1$$
by Theorem 10.2.4. This gives the exact sequence
$$1 \to G(K^{\mathrm{ab}}/K^{\mathrm{ur}}) \to G(K^{\mathrm{ab}}/K) \to G(K^{\mathrm{ur}}/K) \to 1,$$
where the splitting is by the map $\mathbb{Z} \cong G(K^{\mathrm{ur}}/K) \to G(K^{\mathrm{ab}}/K)$ sending $1 \mapsto \phi_K(\pi)$. This identifies $G(K^{\mathrm{ab}}/K^{\mathrm{ur}})$ with the quotient group $G(K_\pi/K)$ where
$$K_\pi = L^{\overline{\langle \phi_K(\pi) \rangle}} = L^{\phi_K(\pi)}.$$

If (2)$'$ holds, then for any uniformizer $\pi$, we have that $\pi \in \mathrm{Nm}_{K'/K}(K'^\times)$ for every finite subextension $K'$ of $K_\pi$. Then (2)$'$ gives that $f(\pi)|_{K_\pi} = 1$. Then (2) holds.

We now show if (1) and (2) hold, then $f = \phi$. Indeed, (1) and (2) imply that $\phi(\pi)|_{K^{\mathrm{ur}}K_\pi} = f(\pi)|_{K^{\mathrm{ur}}K_\pi}$ for any uniformizer $\pi$. But $K^{\mathrm{ur}}K_\pi = K^{\mathrm{ab}}$ and the set of uniformizers generate $K^\times$ (any unit is the quotient of two uniformizers). Hence $\phi = f$. $\square$

*Proof of uniqueness in Theorem 10.2.1.* Suppose $\phi'$ is another map satisfying the conditions of Theorem 10.2.1. It suffices to show $\phi'$ satisfies the conditions of Lemma 10.6.6 with $L = K^{\mathrm{ab}}$. By assumption it satisfies (1). For condition (2)$'$, we have $\phi_K(\pi)|_{K_\pi} = 1$ by definition of $K_\pi$. Hence $\pi$ is a norm from every finite subextension of $K_\pi$. By condition 2 of Theorem 10.2.1, this shows $\phi'_{K'/K}(\mathrm{Nm}_{K'/K}(K'^\times)) = \{1\}$ for every subextension $K'/K$ of $L$, as needed. Hence $\phi' = \phi$. □

# Problems

1. Using $\phi_K$, construct a natural bijection between the following two sets.

   - continuous characters $W(\overline{K}/K) \to \mathbb{C}^\times$ (i.e. continuous representations $W(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$).
   - continuous character $K^\times \to \mathbb{C}$ (i.e. continuous homomorphisms $GL_1(K) \to GL(\mathbb{C})$).

   This is the "local Langlands correspondence for $GL_1$ over $K$." Local class field theory generalizes more naturally in this form.

# Chapter 14
# Global class field theory

gcft To prove the global reciprocity law we need to do two things, namely construct a map

$$\phi_K : \mathbb{I}_K/K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L \xrightarrow{\cong} G(L/K),$$

and show that it is an isomorphism. To show it is an isomorphism, we need to show that the two sides have the same cardinality:[1]

$$|\mathbb{I}_K/K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L| = [L:K].$$

The first inequality "$\geq$" will be shown using cohomology, with lots of Herbrand quotient calculations. The second inequality "$\leq$" is most easily shown with $L$-functions, but can also be shown with a more complicated cohomological argument.

To construct a map, there are two approaches. We can define $\phi_K$ to be the map whose components are the local Artin map, and use the properties of the local Artin map given by local class field theory. Alternatively, we can construct it directly in the global case, without using local theory, and get local class field theory as a corollary. We will take the first approach. For an account of the second, see Lang [8].

## §1 Basic definitions

First, some basic definitions.

**Definition 1.1:** Define the action of $G(L/K)$ on $\mathbb{I}_L$ by permuting the places: For an idele $\mathbf{a} = (a_v)_{v\in V_L}$, define $\sigma\mathbf{a}$ by

$$(\sigma\mathbf{a})_{\sigma(v)} = \sigma(a_v).$$

**Definition 1.2:** Define the inclusion map $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ by

$$(a_v)_{v\in V_K} \mapsto \left((a_v)_{w|v}\right)_{v\in V_K},$$

[1]More precisely, we use this to show the invariant map is an isomorphism, then get the Artin map from the machinery of class formations.

i.e. it is induced by componentwise inclusions $K_v \hookrightarrow L^w$. Let the inclusion map $\mathbf{C}_K \hookrightarrow \mathbf{C}_L$ be induced by the above inclusion.

For an infinite extension $M/K$, define

$$\mathbb{I}_M = \varinjlim_{K \subseteq L \subseteq M} \mathbb{I}_L, \qquad \mathbf{C}_M = \varinjlim_{K \subseteq L \subseteq M} \mathbf{C}_L$$

where the limit is taken over finite Galois extensions $L/K$.

For short, let $H^n(L/K, A)$ denote $H^n(G(L/K), A)$ and $H^2(K, A) := H^n(\overline{K}/K, A)$. As in the local case, $H^n(L/K)$ denotes $H^n(G(L/K), K^\times)$.

**Proposition 1.3:** pr:ilg-is-ik Let $L/K$ be a Galois extension and $G = G(L/K)$. The inclusion map $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ sends $\mathbb{I}_K \xrightarrow{\cong} \mathbb{I}_L^G$ and the inclusion map $\mathbf{C}_K \hookrightarrow \mathbf{C}_L$ sends $\mathbf{C}_K \xrightarrow{\cong} \mathbf{C}_L^G$.

*Proof.* The first part holds because $G$ acts transitively on all the places in $L$ dividing a single $v \in V_K$, so any element of $\mathbb{I}_L^G$ has to be constant on all $w \mid v$, i.e. in the image of $\mathbb{I}_K$.

For the second part[2], take the long exact sequence in cohomology associated to

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

to get

$$\begin{tikzcd}
1 \arrow[r] & H^0(G, L^\times) \arrow[r] \arrow[d, equal] & H^0(G, \mathbb{I}_L) \arrow[r] \arrow[d, equal] & H^0(G, \mathbf{C}_L) \arrow[r] \arrow[d, equal] & H^1(G, L^\times) \arrow[d, equal] \\
& K^\times & \mathbb{I}_L^G = \mathbb{I}_K & \mathbf{C}_L^G & 1
\end{tikzcd}$$

where the equality on the right is Hilbert's Theorem 90 (Theorem 12.1.1) and the map $\mathbb{I}_K \to \mathbf{C}_L^G$ is induced by inclusion. Thus $\mathbf{C}_L^G = \mathbb{I}_K / K^\times = \mathbf{C}_K$. □

# §2 The first inequality

In this section we will prove the following.

**Theorem 2.1** (First inequality of global class field theory)**:** first-inequality If $L/K$ is cyclic, then

$$|\mathbb{I}_K / K^\times \operatorname{Nm}_{L/K} \mathbb{I}_L| \geq [L : K].$$

To prove the inequality, we first express the left-hand side in terms of cohomology. Letting $G = G(L/K)$, we know that

$$H_T^0(G, \mathbf{C}_L) = \mathbf{C}_K / \operatorname{Nm}_{L/K} \mathbf{C}_L = \mathbb{I}_K / K^\times \operatorname{Nm}_{L/K} \mathbb{I}_L.$$

[2] which isn't obvious, because we're taking quotients here

Then noting that the Herbrand quotient (with respect to $G$) of $\mathbf{C}_L$ is $h(\mathbf{C}_L) = \frac{|H_T^0(G,\mathbf{C}_L)|}{|H_T^{-1}(G,\mathbf{C}_L)|}$, we have that

$$eq: 1st-ineq-herbrand |\mathbb{I}_K/K^\times \operatorname{Nm}_{L/K}\mathbb{I}_L| = |H_T^0(G,\mathbf{C}_L)| \ge h(\mathbf{C}_L). \tag{14.1}$$

To calculate $h(\mathbf{C}_L)$ our plan is as follows.

1. First express $\mathbf{C}_L$ in terms of something involving a finite set of places; we find $T$ so that
$$\mathbb{I}_L = L^\times \mathbb{I}_L^T.$$
(Proposition 2.2). Then calculation shows that $h(\mathbf{C}_L) = \frac{h(\mathbb{I}_L^T)}{h(U_L^T)}$, where $U_L^T$ denotes the $T$-units in $L$.

2. Compute $h(\mathbb{I}_L^S) = \prod_{v\in S} n_v$. Note $\mathbb{I}_L^S$ is a direct product, not a restricted direct product, so we can just take the product of the Herbrand quotient of the factors. Breaking up the places into $G(L/K)$-orbits, we can calculate $h(\mathbb{I}_L^S)$ using the corollary to Shapiro's Lemma 11.8.6.

3. Compute $h(U_L^S) = \frac{1}{n}\prod_{v\in S} n_v$ by relating it to a lattice of codimension 1 in $\mathbb{R}^s$ by the log map, where $s = |S|$. (See ANT, Chapter 5.) We use the fact that the Herbrand quotient of a full lattice depends only on the vector space it resides in (Theorem 2.5) to change to a more convenient lattice whose basis consists of vectors representing the $s$ places in $U_L^S$, i.e. the lattice $\Lambda = \prod_{w\in S}\mathbb{Z}e_w$.

   The set $S$ breaks up into $G(L/K)$-orbits, so the lattice breaks up into induced $S$-modules, and we can calculate $h(U_L^S)$ using again using Shapiro's Lemma 11.8.6.

4. Putting all the steps together gives
$$h(\mathbf{C}_L) = n,$$
as needed.

## 2.1 Reduce to finite number of places

**Proposition 2.2:** illis Let $L$ be a number field. There exists a finite set of places $T$ of $L$ such that
$$\mathbb{I}_L = L^\times \mathbb{I}_L^T.$$

*Proof.* This basically follows from the finiteness of the class group.

For the first part, consider the map $p : \mathbb{I}_L \to C_L$, defined by sending
$$(a_v)_{v\in V_L} \mapsto \prod_{v=v_\mathfrak{p}\in V_L^0} \mathfrak{p}^{v(a_\mathfrak{p})}.$$

(Map $a$ to the prime ideal whose valuation at each prime equals the valuations of the corresponding coordinates of $a$.) The kernel—the set sent to the principal ideals—is $L^\times \mathbb{I}_L^{V^\infty}$, where $V^\infty$ is the set of infinite places. Thus we have an isomorphism $\mathbb{I}_L/L^\times \mathbb{I}_L^{V^\infty} \to C_L$[3]. The latter is finite; take the inverse image of a set of generators $A$. We can choose finite $T$ containing $V^\infty$ so that the coordinates of elements of $A$ are units outside of $T$. Then $\mathbb{I}_L^T$ generates $\mathbb{I}_L/L^\times$, as needed. □

## 2.2 Cohomology of $\mathbb{I}_L^S$ and $\mathbb{I}_L$

**Proposition 2.3:** hilt Let $L/K$ be a Galois extension of number fields. Let $S$ be a set of places in $K$ and let $\mathbb{I}_L^S := \mathbb{I}_L^T$ where $T = \{w \in V_L : w \mid v \text{ for some } v \in S\}$. Then for any $i > 0$ we have

$$H^i(G, \mathbb{I}_L^S) = \prod_{v \in S} H^i(G(L^v/K_v), L^{v\times}) \times \prod_{v \notin S} H^i(G(L^v/K_v), U^v).$$

This is also true for Tate groups if $G$ is finite.

In particular, if $L/K$ is cyclic, and $S$ contains all ramified places, then

$$H^1(G, \mathbb{I}_L^S) = 1$$
$$H^2(G, \mathbb{I}_L^S) = \prod_{v \in S} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$$
$$h(\mathbb{I}_L^S) = \prod_{v \in S} n_v$$

where $n_v$ is the local degree $[L_w : K_v]$, for any $w \mid v$.

*Proof.* We have

$$\mathbb{I}_L^S = \prod_{w \in T} L_w^\times \times \prod_{w \notin T} U_w$$

where $U_w := U_{K_w}$. We calculate the cohomology groups of each factor.

$$\begin{aligned}
H^i\left(G, \prod_{w \in T} L_w^\times\right) &= H^i\left(G, \prod_{v \in S}\prod_{w \mid v} L_w^\times\right) \\
&= \prod_{v \in S} H^i\left(G, \prod_{w \mid v} L_w^\times\right) && \text{cohomology respects products, Proposition 11.6.6} \\
&= \prod_{v \in S} H^i(G^v, L^{v\times}) && \text{by Corollary 11.8.7 to Shapiro's Lemma} \\
eq: hilt1 &= \prod_{v \in S} H^i(G(L^v/K_v), L^{v\times}) && (14.2) \\
eq: hilt2 &= \begin{cases} 1, & i = 1, \\ \prod_{v \in S} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}, & i = 2. \end{cases} && (14.3)
\end{aligned}$$

[3]cf. Example 5.10; there $\mathbb{I}_L^{V^\infty}$ is written as $\mathbb{U}_L$.

For $i = 1$, the last result follows from Hilbert's Theorem 90, and for $i = 2$, it follows from the fact that $\mathrm{inv}_{K_v} : H^2(G(L^v/K_v), L^{v\times}) \xrightarrow{\cong} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$ is an isomorphism (a consequence of the class formation for LCFT, Theorem 13.4.14, or actually just Theorem 13.3.1 and Proposition 13.2.1).

For the units, we have,

$$eq:hilt3 H^i\left(G, \prod_{w\notin T} U_w\right) = \prod_{v\notin S} H^i(G(L^v/K_v), U_w) \qquad \text{Proposition 11.6.6} \tag{14.4}$$

$$eq:hilt4 = 1 \qquad \text{if } T \text{ unramified, by Theorem 13.1.1.} \tag{14.5}$$

For the general case, take the product of (14.2) and (14.4). For the special case, take the product of (14.3) and (14.5). The Herbrand quotient calculation follows directly. $\square$

If we consider the full group $\mathbb{I}_L$, we get the following result. (We won't need this until Section 5.)

**Proposition 2.4:** pr:hi-as-prod For any Galois extension $L/K$ with Galois group $G$ and any $n \geq 0$, we have

$$H^n(G, \mathbb{I}_L) \cong \bigoplus_{v\in V_K} H^n(L^v/K_v).$$

This is also true for Tate groups when $G$ is finite.

In particular, we have

1. $H^1(G, \mathbb{I}_L) = 0$.
2. $H^2(G, \mathbb{I}_L) = \bigoplus_{v\in V_K} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$.

*Proof.* We have

$$\mathbb{I}_L = \varinjlim_{S \text{ finite}} \mathbb{I}_L^S.$$

Hence using Proposition 11.14.3,

$$\begin{aligned} H^n(G, \mathbb{I}_L) &= H^n(G, \varinjlim_S \mathbb{I}_L^S) \\ &= \varinjlim H^n(G, \mathbb{I}_L^S) \\ &= \begin{cases} \varinjlim_S \prod_{v\in S} H^n(G^v, L^{v\times}) \times \prod_{v\notin S} H^n(G^v, U^v) = \bigoplus_{v\in V_K} H^n(G^v, L^{v\times}), & \text{general case} \\ 1, & n = 1 \\ \bigoplus_{v\in V_K} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}, & n = 2 \end{cases} \end{aligned}$$

where the last statement follows from Proposition 2.3.

$\square$

## 2.3 Cohomology of lattices and $U_L^T$

**Proposition 2.5:** cohom-lattice Suppose $G$ is finite cyclic, $V$ is a finite real vector space and $\mathbb{R}[G]$-module, and $M, N$ are two lattices in $V$, stable under the action of $G$. Then

$$h(M) = h(N).$$

(If one is defined, so is the other.)

*Proof.* We proceed in 2 steps.

Step 1: We show that $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong N \otimes_{\mathbb{Z}} \mathbb{Q}$ as $G$-modules. We know $M \otimes_{\mathbb{Z}} \mathbb{R} = V = N \otimes_{\mathbb{Z}} \mathbb{R}$. Suppose $V = \mathbb{R}^n$. Choose bases $\{\beta_i\}$ for $M$ and $\{\gamma_i\}$ for $N$. Let $B(\sigma)$ and $C(\sigma)$ be matrices representing the action of a generator $\sigma \in G$ on these bases.[4] A linear map $M \otimes_{\mathbb{Z}} \mathbb{R} \to N \otimes_{\mathbb{Z}} \mathbb{R}$ represented by a matrix $A$ with respect to $\{\beta_i\}$ and $\{\gamma_i\}$ is a isomorphism of $G$-modules if

$$A \cdot B(\sigma) = C(\sigma) \cdot A.$$

These determine a system of homogeneous linear equations in the entries of $A$, with coefficients in $\mathbb{Z}$, since $B(\sigma)$ and $C(\sigma)$ have entries in $\mathbb{Z}$.

Letting the solution space be $W \subseteq \mathcal{M}_{n\times n}(\mathbb{R})$, we have

$$\dim_{\mathbb{R}} W = \dim_{\mathbb{Q}}(W \cap \mathcal{M}_{n\times n}(\mathbb{Q})),$$

because Gaussian elimination never needs to leave the world of $\mathbb{Q}$. Hence we can find a basis for $W$ contained in $\mathcal{M}_{n\times n}(\mathbb{Z})$, say $\{A_1, \ldots, A_k\}$. By the existence of an isomorphism between $M \otimes_{\mathbb{Z}} \mathbb{R}$ and $N \otimes_{\mathbb{Z}} \mathbb{R}$, there exist $a_1, \ldots, a_k \in \mathbb{R}$ such that $a_1 A_1 + \cdots + a_k A_k$ is nonsingular, i.e.

$$\det(a_1 A_1 + \cdots + a_k A_k) \neq 0.$$

The left hand side is hence a nonzero polynomial in the $a_k$; since it has coefficients in the infinite field $\mathbb{Q}$ it has a solution over $\mathbb{Q}$. Taking $A$ to be the corresponding linear combination, we get the desired $G$-isomorphism $M \otimes_{\mathbb{Z}} \mathbb{Q} \to N \otimes_{\mathbb{Z}} \mathbb{Q}$.

Step 2: We have an isomorphism $f : M \otimes_{\mathbb{Z}} \mathbb{Q} \to N \otimes_{\mathbb{Z}} \mathbb{Q}$; by scaling $f$ (since $M, N$ are finite-dimensional lattices) we may assume $f$ restricts to $f : M \to N$. Now $N/f(M)$ is finite; hence by Proposition 11.12.4(1) and (2),

$$h(N) = h(M)h(N/f(M)) = h(M).$$

□

**Proposition 2.6:** hult Let $L/K$ be a finite cyclic extension of number fields of degree $n$. Let $S$ be a set of places in $K$ containing the infinite places and $T = \{w \in V_L : w \mid v \text{ for some } v \in S\}$. We have

$$h(U_L^T) = \frac{1}{n} \prod_{w \in T} n_w$$

[4] $G$ cyclic is not important here; we could work with all elements of $G$.

where $U_L^T$ denotes the $T$-units in $L$ and $n_w$ is the local degree $[L_w : K_v]$, where $w \mid v$.

*Proof.* Consider the map $L : U_L^T \to \mathbb{R}^T$ defined by letting

$$L(a) = (\ln |a|_w)_{w \in T}$$

where $|\cdot|_w$ is the normalized valuation. Then $L(a)$ is a lattice of dimension $|T| - 1$ by Dirichlet's $S$-unit theorem 5.3.2; it is in the hyperplane where the sum of coordinates is 0 (take the log of the product formula 7.6.2). The kernel of $L$ consists the roots of unity in $L$, $\mu \cap L$, which is a finite group. By Proposition 11.12.4(1)–(2) applied to $1 \to \mu \cap L \to U_L^T \to L(U_L^T) \to 0$,

$$1 - ineq - 1 h(U_L^T) = h(\mu \cap L) h(L(U_L^T)) = h(L(U_L^T)) \tag{14.6}$$

Let $G(L/K)$ act on $\mathbb{R}^T$ by permuting the coordinates corresponding to the places. Note that $L$ is a $G$-module homomorphism with respect to this action. Let $\mathbf{x}$ be the vector $(1, 1, \ldots, 1)$; note it is fixed by $G(L/K)$. Note that

$$\Lambda := L(U_L^T) \oplus (1, 1, \ldots, 1)\mathbb{Z}$$

is a full lattice in $\mathbb{R}^T$. By Proposition 11.12.4(2)–(3), we have

$$1 - ineq - 2 h(\Lambda) = h(L(U_L^T)) h(\mathbb{Z}) = n \cdot h(L(U_L^T)). \tag{14.7}$$

Consider the lattice $\Lambda' = \mathbb{Z}^T$ in $\mathbb{R}^T$, where $e_v$ is the vector with 1 in the $v$ position and 0's elsewhere. By Proposition 2.5, $h(\Lambda) = h(\Lambda')$. Since $G$ permutes the places above $v \in S$ transitively, we have

$$\begin{aligned}
h(\Lambda) = h(\Lambda') &= h\left(\bigoplus_{w \in T} e_w \mathbb{Z}\right) \\
&= h\left(\bigoplus_{v \in S} \bigoplus_{w \mid v} e_w \mathbb{Z}\right) \\
&= \prod_{v \in S} h\left(\bigoplus_{w \mid v} e_w \mathbb{Z}\right) && \text{cohomology respects products, Proposition 11.6.6} \\
&= \prod_{v \in S} h(G^v, \mathbb{Z}) && \text{by Corollary 11.8.7 to Shapiro's Lemma} \\
&= \prod_{v \in S} |G^v| && \text{Proposition 11.12.4(3)} \\
&= \prod_{v \in S} n_v.
\end{aligned}$$

Together with (14.6) and (14.7), we get

$$h(U_L^T) = \frac{1}{n} h(\Lambda') = \frac{1}{n} \prod_{v \in S} n_v. \qquad \square$$

## 2.4 Herbrand quotient of $\mathbf{C}_L$

**Lemma 2.7:** hcl If $L/K$ is a cyclic extension of number fields of degree $n$,

$$h(\mathbf{C}_L) = n.$$

*Proof.* Choose a set of places $T$ for $L$ containing the ramified places and satisfying the conditions of Proposition 2.2. Enlarge $T$ so it is stable under $G(L/K)$. Using Propositions 2.3 and 2.6, we have that

$$h(\mathbf{C}_L) = h(L^\times \mathbb{I}_L^T / L^\times) = h(\mathbb{I}_L^T / \mathbb{I}_L^T \cap L^\times) = \frac{h(\mathbb{I}_L^T)}{h(U_L^T)} = \frac{\prod_{v\in S} n_v}{\frac{1}{n}\prod_{v\in S} n_v} = n$$

□

*Proof of Theorem 2.1.* We have

$$|\mathbb{I}_K / K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L)| = |H_T^0(G, \mathbf{C}_L)| = h(\mathbf{C}_L)|H_T^{-1}(G, \mathbf{C}_L)| \geq n$$

by Lemma 2.7. □

## 2.5 The Frobenius map is surjective

sec:frob-surj Using the first inequality, we can already prove surjectivity of the Artin map, defined on ideals.

**Proposition 2.8:** pr:frob-surj Let $L/K$ be a finite abelian extension, and $S$ be a finite set of primes. Define the map

$$\psi_{L/K} : I^S \to G(L/K)$$

by setting $\psi_{L/K}(\mathfrak{p}) = \operatorname{Frob}_{L/K}(\mathfrak{p})$ for primes $\mathfrak{p} \notin S$ and extending to a group homomorphism. Then $\psi_{L/K}$ is surjective.

*Proof.* Let $H = \operatorname{im}(\psi_{L/K})$. By compatibility of the Frobenisus map, $\operatorname{Frob}_{K^H/K}(\mathfrak{p})$ is the image of $\operatorname{Frob}_{L/K}(\mathfrak{p})$ under the projection $G(L/K) \to G(K^H/K)$. Hence the map $\psi_{K^H/K} : I^S \to G(K^H/K)$ is trivial, giving $(K^H)^v = K_v$ for every $v \notin S$, and

$$\mathbb{I}_K^S \subseteq \operatorname{Nm}_{K^H/K} \mathbb{I}_{K^H}.$$

However, $K^\times \mathbb{I}_K^S$ is dense in $\mathbb{I}_K$ by the weak approximation theorem 7.3.4, so $K^\times \mathbb{I}_K^S = K^\times \operatorname{Nm}_{K^H/K} \mathbb{I}_{K^H} = \mathbb{I}_K$. But by the First Inequality 2.1,

$$[K^H : K] \leq [\mathbb{I}_K : K^\times \operatorname{Nm}_{K^H/K} \mathbb{I}_{K^H}] = 1.$$

Hence $K^H = K$, i.e. $H = G$. □

# §3 The second inequality

We give two proofs of the second inequality, an analytic proof and an algebraic proof. The first has the advantage of being short and sweet, while the second has the advantage of staying completely within the algebraic realm, i.e. not requiring knowledge of $L$-functions.

**Theorem 3.1** (Second inequality for global class field theory)**:** thm:2ineq For any extension $L/K$ of degree $n$, and $G = G(L/K)$, we have

1. $|H_T^0(G, \mathbf{C}_L)|$ and $|H^2(G, \mathbf{C}_L)|$ divide $n$.
2. (HT90 for ideles) $|H^1(G, \mathbf{C}_L)| = 1$.

In particular,

$$|\mathbb{I}_K/K^\times \operatorname{Nm}_{L/K} \mathbb{I}_L| \le [L : K].$$

## 3.1 Analytic approach

We first show the inequality $|\mathbb{I}_K/K^\times \operatorname{Nm}_{L/K} \mathbb{I}_L| \le [L : K]$.

*Proof of inequality.* Let $\mathfrak{c}$ be admissible for $L/K$, i.e. such that $\mathbf{U}_K(1, \mathfrak{c}) \subseteq \operatorname{Nm}_{L/K}(\mathbb{I}_L)$. By Proposition 10.5.9 we know that $\mathbb{I}_K/K^\times \operatorname{Nm}_{L/K} \mathbb{I}_L \cong I_L^{\mathfrak{c}}/P_K(1, \mathfrak{c}) \operatorname{Nm}_{L/K}(I_L^{\mathfrak{c}})$. We show that

$$[I_K^{\mathfrak{c}} : P_K(1, \mathfrak{c}) \operatorname{Nm}_{L/K}(I_L^{\mathfrak{c}})] \le [L : K].$$

Let $H = P_K(1, \mathfrak{c}) \operatorname{Nm}_{L/K} I_L^{\mathfrak{c}}$ and let $\chi$ be a nontrivial character of $I_K^{\mathfrak{c}}/H$, viewed as a character of $I_K^{\mathfrak{c}}/P_K(1, \mathfrak{c})$.

Define the Hecke $L$-series $L_{\mathfrak{c}}(s, \chi)$ by

$$L_{\mathfrak{c}}(s, \chi) := \prod_{\mathfrak{p} \nmid \mathfrak{c}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s}} = \sum_{\mathfrak{a} \perp \mathfrak{c}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}\mathfrak{a}^s},$$

where equality follows from expanding the product. Define

$$m(\chi) := \operatorname{ord}_{s=1} L_{\mathfrak{c}}(s, \chi).$$

Since $L_{\mathfrak{c}}(s, \chi) = (s-1)^{m(\chi)} g(s, \chi)$ for some $g(s, \chi)$ nonzero at $s = 1$, taking logs gives

$$\ln L_{\mathfrak{c}}(s, \chi) \sim m(\chi) \ln(s-1) = -m(\chi) \ln \frac{1}{s-1}.$$

Taking the sum over all characters of $I_K^{S(\mathfrak{m})}$ gives

$$eq:2-ineq-anal \ln \zeta_K(s) + \sum_{\chi \ne 1} \ln L_{\mathfrak{m}}(s, \chi) \sim \left[1 - \sum_{\chi \ne 1} m(\chi)\right] \ln \frac{1}{s-1} \tag{14.8}$$

where we use the fact that $\zeta_K(s) := L(s,1)$ has a pole at $s=1$.

On the other hand, by the Taylor series expansion for ln,

$$\ln L_{\mathfrak{c}}(s,\chi) = -\sum_{\mathfrak{p}\nmid\mathfrak{c}} \ln\left(1-\frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s}\right) = \sum_{n=1}^{\infty}\sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi(\mathfrak{p})^n}{n\mathfrak{N}\mathfrak{p}^{ns}} \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{\mathfrak{N}\mathfrak{p}^s} = \sum_{\mathfrak{K}\in I^{\mathfrak{c}}/H} \chi(\mathfrak{K}) \sum_{\mathfrak{p}\in\mathfrak{K},\,\mathfrak{p}\nmid\mathfrak{c}} \frac{1}{\mathfrak{N}\mathfrak{p}^s}$$

where in the last step we grouped together the primes based on what they are modulo $H$. This is greater than the sum if we only include primes with $f(\mathfrak{P}/\mathfrak{p})=1$ ($\mathfrak{P}$ in $L$). Again we are off by at most a constant if we only include primes splitting completely in $L$, because the ramified primes are at most a finite subset. We can then "unrestrict" to all the primes of $L$, and be off by at most a constant in a neighborhood of 1, because the other terms are in the form $\frac{1}{p^{fs}}$ for $f>1$.

Let $h=[I^{S(\mathfrak{m})}:H]$. We get, for $s\to 1^+$,

$$\begin{aligned}
\ln\zeta_K(s) + \sum_{\chi\neq 1}\ln L_{\mathfrak{m}}(s,\chi) &\sim \sum_{\chi}\sum_{\mathfrak{K}\in I^{\mathfrak{c}}/H}\chi(\mathfrak{K})\sum_{\mathfrak{p}\in\mathfrak{K},\,\mathfrak{p}\nmid\mathfrak{m}}\frac{1}{\mathfrak{N}\mathfrak{p}^s} \\
&\gtrsim O(1) + h\sum_{\mathfrak{p}\in\mathrm{Spl}(L/K)}\frac{1}{\mathfrak{N}\mathfrak{p}^s} && \sum_{\chi}\chi(\mathfrak{K}) = \begin{cases} 0, & \mathfrak{K}\neq H \\ h, & \mathfrak{K}=H.\end{cases} \\
&\sim O(1) + \frac{h}{N}\sum_{f(\mathfrak{P})=1}\frac{1}{\mathfrak{N}\mathfrak{P}^s} && N \text{ primes above each } \mathfrak{p} \\
&\sim O(1) + \frac{h}{N}\ln\zeta_L(s) \\
&\sim O(1) + \frac{h}{N}\ln\frac{1}{s-1}.
\end{aligned}$$

Combining this with (14.8) gives $m(\chi)=0$ (since $\frac{h}{N}>0$) for all $\chi\neq 1$, and $h\le N$, as needed. $\square$

## 3.2 Algebraic approach

sec:2ineq-alg-proof The steps are as follows.

1. Carry out some preliminary local computations.

2. Consider the case where $L/K$ is an extension such that $G(L/K)\cong(\mathbb{Z}/n\mathbb{Z})^r$, and $K$ contains the $n$th roots of unity. Note this is a Kummer extension, so we can characterize it in terms of $L^{\times n}\cap K$. This will make computations easy for us.

   We construct an explicit set $E$ with

   $$E\subseteq \mathrm{Nm}_{L/K}\mathbb{I}_L\subseteq \mathbb{I}_K.$$

   We have $[\mathbb{I}_K : K^\times \mathrm{Nm}_{L/K}\mathbb{I}_L] \mid [I_K : K^\times E]$, so it suffices to show the latter equals $n^r$.

3. Show this.

4. This implies the cyclic prime case, and that the cyclic prime case implies the general case.

This section is incomplete; see Cassels-Frohlich [3], pg. 180-185.

#### 3.2.1 Local computations

**Proposition 3.2:** pr:local-power-index Let $K$ be a local field with $|\mu_n \cap K| = m$, i.e. $K$ contains $m$ $n$th roots of unity. Then

$$[K^\times : K^{\times n}] = \frac{nm}{|n|_v}$$

and

$$[U_K : U_K^n] = \frac{m}{|n|_v}.$$

*Proof.* There are two methods: appeal to the structure of $K^\times$ or calculate a Herbrand quotient. □

#### 3.2.2 Constructing $E$

Since $L$ is a Kummer extension we can write it in the form $K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$. Let $S$ be a set of primes satisfying the following conditions.

1. $S$ contains all infinite places.

2. $S$ contains all divisors of $n$.

3. $\mathbb{I}_K = K^\times \mathbb{I}_K^S$. (This is possible by Proposition 2.2.)

4. $S$ contains all prime factors in the numerator and denominator of all $a_i$, i.e. the $a_i$ are all $S$-units.

   Define

$$E = \prod_{v \in S} K_V^{\times n} \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v.$$

**Lemma 3.3:** $E \subseteq \mathrm{Nm}_{L/K} \mathbb{I}_L$.

We want to calculate $[\mathbb{I}_K : K^\times E]$ but $K^\times E$ is hard to deal with. $E$ however, is not, because to calculate the index of $E$ we can appeal to Proposition 3.2. Thus we use the following group theoretic fact.

**Proposition 3.4:** Let $B \subseteq A$ and $C$ be subgroups of a group $G$. Then

$$[CA : CB][C \cap A : C \cap B] = [A : B].$$

Then

$$[\mathbb{I}_K : K^\times E] = [K^\times \mathbb{I}_K^{S\cup T} : K^\times E] = \frac{[\mathbb{I}_K^{S\cup T} : E]}{[K^\times \cap \mathbb{I}_K^{S\cup T} : K^\times \cap E]}.$$

See Cassels-Frohlich.

## 3.3 Finishing the proof

Now we prove Theorem 3.1.

*Proof of Theorem 3.1.* Step 1: We show the theorem when $[L : K]$ is prime. In this case, both the first and second inequality hold, so

$$|H_T^2(G, \mathbf{C}_L)| = [\mathbb{I}_K : K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L)] = [L : K].$$

Since $h(\mathbf{C}_L) = n$ by Lemma 2.7, we get $|H_T^1(G, \mathbf{C}_L)| = 1$. Finally, note $H_T^2(G, \mathbf{C}_L) = H_T^0(G, \mathbf{C}_L)$ because $G(L/K)$ is cyclic.

Step 2: We show the theorem when $[L : K]$ is a prime power, by induction on the exponent. Suppose $|G| = p^n$. Every $p$-group has a normal subgroup of index $p$. Let $H \triangleleft G$ be such a group; it corresponds to $H = G(L/K')$ for some extension $K'/K$ of degree $p$. The inflation-restriction exact sequence 11.11.10 gives

$$0 \to \underbrace{H^1(G/H, \mathbf{C}_{K'})}_{=0 \text{ by prime case}} \xrightarrow{\text{Inf}} H^1(G, \mathbf{C}_L) \xrightarrow{\text{Res}} \underbrace{H^1(H, \mathbf{C}_L)}_{=0 \text{ by induction hypothesis}}.$$

Thus $H^1(G, \mathbf{C}_L) = 0$. This shows part 2. Using $H^1(G, \mathbf{C}_L) = 0$, the inflation-restriction exact sequence gives

$$0 \to \underbrace{H^2(G/H, \mathbf{C}_{K'})}_{\text{order } p} \xrightarrow{\text{Inf}} H^2(G, \mathbf{C}_L) \xrightarrow{\text{Res}} \underbrace{H^2(H, \mathbf{C}_L)}_{\text{order } |p^{n-1}}$$

by the case for cyclic extensions and the induction hypothesis. This shows $|H^2(G, \mathbf{C}_L)| \mid p^n$. Finally,

$$|H_T^0(G, \mathbf{C}_L)| = [\mathbf{C}_K : \operatorname{Nm}_{L/K} \mathbf{C}_L] = [\mathbf{C}_K : \operatorname{Nm}_{K'/K}(\mathbf{C}_{K'})][\operatorname{Nm}_{K'/K}(\mathbf{C}_{K'}) : \operatorname{Nm}_{L/K}(\mathbf{C}_L)].$$

Now $[\mathbf{C}_K : \operatorname{Nm}_{K'/K}(\mathbf{C}_{K'})] = p$ by the cyclic case, and the surjection $\operatorname{Nm}_{K'/K} : \mathbf{C}_{K'}/\operatorname{Nm}_{L/K'}(\mathbf{C}_L) \twoheadrightarrow \operatorname{Nm}_{K'/K}(\mathbf{C}_{K'})/\operatorname{Nm}_{L/K}(\mathbf{C}_L)$ and the induction hypothesis gives that the second factor divides $p^{n-1}$. This finishes the induction step.

Step 3: We show the theorem holds in general, using Corollary 11.11.7: the map

$$\operatorname{Res}^n : H^n(G, M) \to H^n(G_p, M)$$

is injective on the $p$-primary component. Using step 2, for $n = 1$, this gives us that $p \nmid H_T^1(G, \mathbf{C}_L)$ for any $p$, i.e. $H_T^1(G, \mathbf{C}_L) = 0$. For $n = 0, 2$, this gives that $v_p(|H^n(G, M)|) \le v_p(|H^n(G_p, M)|) \le v_p(G)$, giving part 1. $\square$

### 3.4 Local-to-global principle for algebras

The fact that $H^1(G, \mathbf{C}_L) = 0$ also gives the following corollary.

**Theorem 3.5** (Brauer-Hasse-Noether Theorem)**:** thm:b-h-n Let $L/K$ be any Galois extension with Galois group $G$. Then the map

$$H^2(G, L^\times) \to \bigoplus_{v \in V_K} H^2(G^v, L^{v\times})$$

is injective. A central simple algebra over a number field $K$ is split over $K$ iff it is split locally everywhere.

*Proof.* Taking cohomology of $0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$ gives

$$\begin{tikzcd} eq:b-h-n\; H^1(G, \mathbf{C}_L) \arrow[r] \arrow[d, equal] & H^2(G, L^\times) \arrow[r] \arrow[d, equal] & H^2(G, \mathbb{I}_L) \arrow[r] \arrow[d, equal] & \cdots \\ 0 \arrow[r] & \mathrm{Br}_K \arrow[r, hook] & \bigoplus_{v \in V_K} \mathrm{Br}_{K_v} & \end{tikzcd} \tag{14.9}$$

Here $H^1(G, \mathbf{C}_L) = 0$ directly from HT90 for ideles (Theorem 3.1), and equality on the right comes from

$$H^2(G, \mathbb{I}_L) = \bigoplus_{v \in V_K} H^2(L^v/K_v)$$

(Proposition 2.4). Brauer group is $H^2$ by Theorem 5.2. Injectivity of the bottom map gives the result.

(We do need to check that in the above diagram, the map $\mathrm{Br}_K \to \bigoplus_{v \in V_K} \mathrm{Br}_{K_v}$ is exactly the map sending an algebra to its reduction over every local field. This is a matter of tracing the long windy road between Br and $H^2$ and left to the reader.) $\square$

## §4 Proof of the reciprocity law

To construct the Artin map in the local case, we constructed the invariant map $\mathrm{inv}_K : H^2(K^{\mathrm{ur}}/K) \to \mathbb{Q}/\mathbb{Z}$. Then we used the fact that $H^2(K^{\mathrm{ur}}) = 0$, i.e. every $a \in H^2(K)$ splits in an unramified extension, to conclude that $H^2(K) \cong H^2(K^{\mathrm{ur}}/K)$.

In the global case we will construct the invariant map $\mathrm{inv}_K : H^2(K_c/K, \mathbb{I}_{K_c}) \to \mathbb{Q}/\mathbb{Z}$, for a certain infinite cyclotomic extension $K_c$. Then we show $H^2(K_c, \mathbb{I}_{\overline{K}}) = 0$, i.e. every $a \in H^2(K, \mathbb{I}_{\overline{K}})$ splits in this cyclotomic extension, to conclude $H^2(K, \mathbb{I}_{\overline{K}}) \cong H^2(K_c/K, \mathbb{I}_{\overline{K}_c})$.

We construct the global Artin map by taking the product of the local Artin maps:

$$\begin{aligned} \phi_{L/K} &: \mathbb{I}_K \to G(L/K) \\ \phi_{L/K}(\mathbf{a}) &= \prod_{v \in V_K} \phi_v(a_v).\, eq:artin-as-product \end{aligned} \tag{14.10}$$

(Only a finite number of the factors—those where $L^v/K_v$ is ramified or $a_v \notin U_v$—are not equal to the identity.)

We need to show that $K^\times \subseteq \ker \phi_{L/K}$, so that it factors through $\mathbb{I}_K/K^\times \cdot \mathrm{Nm}_{L/K}\,\mathbb{I}_L$. Consider the following two properties.

(A) Define the map $\phi_{L/K}$ as in (14.10). The map $\phi_{L/K}$ takes the value 1 on the principal ideles $K^\times \subseteq \mathbb{I}_K$.

(B) For all $\alpha \in H^2(G(L/K), L^\times) = \mathrm{Br}_{L/K}$,

$$\mathrm{inv}(\alpha) := \sum_{v\in V_K} \mathrm{inv}_v(i(\alpha)) = 0.$$

Note in (B), $\mathrm{inv}_v$ is defined as follows.

**Definition 4.1:** df:global-inv Define $\mathrm{inv}_v$ as the following composition:

$$\mathrm{inv}_v : H^2(G,\mathbb{I}_L) \xrightarrow{\mathrm{Res}_{G/G_v}} H^2(G_v,\mathbb{I}_L) \xrightarrow{H^2(G_v,p_v)} H^2(G_v,(L^v)^\times) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z}$$

where $p_v : \mathbb{I}_L \to (L^v)^\times$ is the projection map. (This looks complicated, but it is just what you think it is.)

We prove (A) for all finite abelian extensions of number fields and (B) for all finite Galois extensions of number fields.

We first show that (A) holds for a special class of extensions, and then use an "unscrewing" argument to show (A) and (B) hold for more general extensions. The plan of attack is as follows.

1. Show (A) holds for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.

2. Show (A) holds for all cyclotomic extensions.

3. Show that (B) holds for $\alpha$ split by a cyclotomic extension.

4. Every $\alpha$ is split by a cyclic cyclotomic extension, so (B) holds for all $\alpha \in H^2(K,\overline{K}^\times)$.?

5. Show that (A) holds for all abelian extensions.

Note that (A) is a statement about $H_T^{-2} \to H_T^0$ while (B) is a statement about $H^2$. We "transfer" the problem from (A) to (B) so that we can apply our characterization of $\phi_v$ in terms of the local invariant map (Theorem 13.4.9). First, we need an analogue of Theorem 13.4.9 in the global case.

**Lemma 4.2:** lem:sum-inv Let $G = G(L/K)$. For all $v \in V_K$ and all $\chi \in H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$, we have $\mathrm{inv}_v(\overline{\mathbf{a}} \cup \delta\chi) = \chi_v(\phi_v(a_v))$. ($\chi_v$ is the restriction of $\chi$ to $G_v$ and $\overline{\mathbf{a}}$ is the image of $\mathbf{a}$ in $H_T^0(G(L/K),\mathbb{I}_L)$. Hence

$$\mathrm{inv}(\overline{\mathbf{a}} \cup \delta\chi) = \sum_v \mathrm{inv}_v(\overline{\mathbf{a}} \cup \delta\chi) = \chi(\phi(a)).$$

*Proof.* Since restriction commutes with cup products (Proposition 11.11.9) and with $\delta$, we have

$$\begin{aligned}\mathrm{inv}_v(\overline{\mathbf{a}} \cup \delta\chi) &= \mathrm{inv}(p_v \operatorname{Res}_{G/G_v}(\overline{\mathbf{a}} \cup \delta\chi)) \\ &= \mathrm{inv}(p_v(\overline{\mathbf{a}}) \cup \delta\chi_v) \qquad\qquad \operatorname{Res}_{G/G_v}(\chi) = \chi_v \\ &= \mathrm{inv}(\overline{a_v} \cup \delta\chi_v) = \chi_v(\phi_v(a_v)).\end{aligned}$$

We invoked Theorem 13.4.9 in the last step.

Taking the product gives the second statement:

$$\chi(\phi(\mathbf{a})) = \chi\left(\prod_v \phi_v(a_v)\right) = \sum_v \chi_v(\phi_v(\mathbf{a})) = \sum_v \mathrm{inv}_v(\overline{\mathbf{a}} \cup \delta\chi).$$

□

## 4.1 (A) holds for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$

**Proposition 4.3:** For any $m \in \mathbb{N}$,

$$\phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathbb{Q}^\times) = 1.$$

First reduce to the case where $m = p$ is prime. We give two approaches.

*Proof 1.* By Example 10.4.2, we know the ideal version of global class field theory holds for all cyclotomic extensions of $\mathbb{Q}$. Note the maximal unramified extension of $\mathbb{Q}_p$ is included in $\mathbb{Q}_p(\zeta_\infty)$ for all $p$ (Theorem 8.2.6). Hence by Theorem 10.6.5(2), there is a map $\phi'$ satisfying the conditions of the idele version of GCFT, except that $\phi'_{\mathbb{R}}$ may not equal $\phi_{\mathbb{R}}$. Letting $\phi'_v$ be the restriction of $\phi'$ to $K_v$, we have (on $G(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$)

$$eq: idele-cft-cyclotomic\phi'(\mathbf{a}) = \phi'_{\mathbb{R}}(a_{\mathbb{R}}) \prod_{v \in V_{\mathbb{Q}}^0} \phi'_v(a_v) \stackrel{?}{=} \prod_{v \in V_{\mathbb{Q}}} \phi_v(a_v) = \phi'(\mathbf{a}) \qquad (14.11)$$

where the middle inequality is pending a proof that $\phi'_{\mathbb{R}} = \phi_{\mathbb{R}}$. We check this is true.

Since $\phi'_{\mathbb{R}}$ is a map $\mathbb{R}/\mathbb{R}_{>0} \to G(\mathbb{C}/\mathbb{R})$, it suffices to show complex conjugation is in the image of $\phi'$. We have $G(\mathbb{C}/\mathbb{R}) \cong G(\mathbb{R}(i)/\mathbb{R})$, so consider $\phi'$ on $G(\mathbb{Q}(i)/\mathbb{Q})$. As $\phi'(\mathbb{Q}^\times) = 1$, we have by (14.11) and the fact that $\mathbb{Q}(i)/\mathbb{Q}$ is only ramified at 2 that on $G(\mathbb{Q}(i)/\mathbb{Q})$,

$$1 = \phi'(-7) = \phi'_2(-7)\phi'_7(-7)\phi'_{\mathbb{R}}(-7)$$

Now $-7 \equiv 1 \pmod 8$ so $-7 \in \mathrm{Nm}_{\mathbb{Q}_2(i)/\mathbb{Q}_2}(\mathbb{Q}_2(i)^\times)$, and $\phi'_2(-7) = 1$. We have $v_7(-7) = 1$, so $\phi'(-7)$ equals the Frobenius element, complex conjugation. Hence $\phi'_{\mathbb{R}}(-7)$ is also complex conjugation.

Thus (14.11) holds, and we have $\phi_{\mathbb{Q}(\zeta_\infty)/\mathbb{Q}}(\mathbb{Q}^\times) = \phi'_{\mathbb{Q}(\zeta_\infty)/\mathbb{Q}}(\mathbb{Q}^\times) = 1$, as needed. □

*Proof 2.* Use explicit computations of local symbols, obtained from Lubin-Tate theory. See Cassels-Frohlich [3], p. 191. □

## 4.2 (B) holds for all cyclomic extensions

We prove the following more general proposition.

**Proposition 4.4** (Devissage)**:** [5]pr:gl-rec-devissage If (A) is true for $L/K$, then (A) holds for

1. any subextension $M/K$ and
2. any extension $LK'/K'$.

For an extension $K'(\zeta_n)/K'$, apply the proposition with $L = \mathbb{Q}(\zeta_n)$ and $K = \mathbb{Q}$ to obtain the following.

**Corollary 4.5:** (A) holds for all cyclotomic extensions.

*Proof of Proposition 4.4.*

1. For any place $v$, $\phi_{M^v/K_v}$ is the composition of $\phi_{L^v/K_v}$ and the projection $G(L^v/K_v) \to G(M^v/K_v)$. Since the global map is the product of the local maps, $\phi_{M/K}$ is the composition of $\phi_{L/K}$ and $G(L/K) \to G(M/K)$. Hence $\phi_{M/K}(K^\times) = 1$.
2. Let $L' = L \cdot K'$. We have a natural inclusion $G(L'/K') \hookrightarrow G(L/K)$. The local Artin map is compatible with basefield extension with respect to the norm map. Since the norm on ideles is computed componentwise, it follows the map $\phi = \prod_{v \in V_K} \phi_v$ is also compatible with field extensions.

$$\begin{tikzcd} \mathbb{I}_{K'} \arrow[r, "\phi_{L'/K'}"] \arrow[d, "\mathrm{Nm}_{K'/K}"] & G(L'/K') \arrow[d, "i"] \\ \mathbb{I}_K \arrow[r, "\phi_{L/K}"] & G(L/K). \end{tikzcd}$$

   Suppose $a \in K'^\times$. By commutativity and (A) for the extension $L/K$, we have

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

   Since $i$ is injective, this implies $\phi_{K'/K'}(a) = 1$. ∎

## 4.3 (A) for cyclotomic implies (B) for $\alpha$ split by cyclic cyclotomic

This follows from the more general proposition:

**Proposition 4.6:** If $L/K$ is cyclic, then (A) implies (B).

[5]Devissage means "unscrewing" in French.

*Proof.* Since $L/K$ is cyclic, we can take $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$ to be a generating character. We have the following commutative diagram.

$$\begin{tikzcd} K^\times \arrow[r, hook] \arrow[d, "\bullet\cup\delta\chi"] & \mathbb{I}_K \arrow[r, "\phi_{L/K}"] \arrow[d, "\bullet\cup\delta\chi"] & G(L/K) \arrow[d, "\chi"] \\ H^2(G, L^\times) \arrow[r] & H^2(G, \mathbb{I}_L) \arrow[r, "\mathrm{inv}"] & \mathbb{Q}/\mathbb{Z}. \end{tikzcd}$$

The left-hand square commutes by functoriality of cup products; the right-hand square commutes by Lemma 4.2. Recall $\bullet\cup\delta\chi$ is an isomorphism for $G$ cyclic, by Proposition 11.12.1. Hence if $a \in H^2(G, L^\times)$, then it is equal to $b \cup \delta\chi$ for some $b \in K^\times$, and

$$\mathrm{inv}(a) = \mathrm{inv}(b \cup \delta\chi) = \chi(\phi_{L/K}(b)) = 0.$$

In the last step we use (A) to give $\phi_{L/K}(b) = 0$. $\square$

## 4.4 (B) for cyclic cyclotomic implies (B) in general

It suffices to prove the following.

**Theorem 4.7:** thm:split-in-cyc-cyc For any $\beta \in H^2(K)$ there exists a cyclic cyclotomic extension $L/K$ such that $\beta$ maps to 0 in $H^2(L)$.

There exists a cyclotomic extension $K_c \subseteq K(\zeta_\infty)$ with $G(K_c/K) \cong \widehat{\mathbb{Z}}$ such that the inclusion map

$$H^2(K_c/K) \to H^2(K)$$

is an isomorphism.

We first give a criterion for $\beta$ to map to 0 in $H^2(L)$, then find a cyclotomic $L/K$ where this criterion holds.

**Lemma 4.8:** lem:criterion-split Let $\alpha \in H^2(K)$. Then $\mathrm{Res}_{K/L}(\alpha) = 0$ in $H^2(L)$ if and only if $[L^v : K_v]\,\mathrm{inv}_v(\alpha) = 0$ for every $v \in V_K$.

*Proof.* By the Brauer-Hasse-Noether Theorem 3.5, $\mathrm{Res}_{K/L}(\alpha) = 0$ in $H^2(L/K, L^\times)$ iff $\mathrm{Res}_{K/L}(\alpha) = 0$ in $H^2(L^v/K_v, L^{v\times}) = 0$ for all $v$. Since $\mathrm{inv}_{K_v}$ is an isomorphism, this is true iff $\mathrm{inv}_{K_v}\mathrm{Res}_{K_v/L^v}(\alpha) = 0$ for all $v$. But we know

$$\mathrm{inv}_{K_v}\mathrm{Res}_{K_v/L^v}(\alpha) = [L^v : K_v]\,\mathrm{inv}_v(\alpha),$$

from the class formation for LCFT (Theorem 13.4.14). $\square$

**Lemma 4.9:** lem:cyc-cyc-ext Suppose $K/\mathbb{Q}$ is a finite extension and $S$ be a finite set of places of $K$. There exists a cyclic cyclotomic extension $L/K$ such that

$$m \mid [L^v : K_v] \text{ for every finite } v \in S$$
$$2 \mid [L^v : K_v] \text{ for every real } v \in S.$$

(The second condition is just equivalent to $L$ being complex.)

*Proof.* First consider the case $K = \mathbb{Q}$. Note that for an odd prime $q$,

$$G(\mathbb{Q}(\zeta_{q^r})/\mathbb{Q}) \cong (\mathbb{Z}/q^r)^\times \cong \mathbb{Z}/(q-1)q^{r-1} \cong \mathbb{Z}/(q-1) \times \mathbb{Z}/q^{r-1}.$$

Let $L(q^r)$ be the subextension of $\mathbb{Q}(\zeta_{q^r})$ with Galois group $\mathbb{Z}/q^{r-1}$. Becuase $\mathbb{Q}_p$ only has a finite number of roots of unity, $v_q([L(q^r) : \mathbb{Q}_p]) \to \infty$ as $r \to \infty$.

Similarly for $q = 2$,

$$G(\mathbb{Q}(\zeta_{2^r})/\mathbb{Q}) \cong (\mathbb{Z}/2^r)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{r-2}.$$

The subextension $\mathbb{Q}(\zeta_{2^r} - \zeta_{2^r}^{-1})$ corresponds to the automorphisms $\zeta \mapsto \zeta^s$ with $s \equiv 1 \pmod 4$, which form a group isomorphic to $\mathbb{Z}/2^{r-2}$. Let $L(2^r) = \mathbb{Q}(\zeta_{2^r} - \zeta_{2^r}^{-1})$ (note this is complex), then similarly $\lim_{r\to\infty} v_2([L(2^r) : \mathbb{Q}]) = \infty$. Now take

$$L := \prod_{q_i | 2m} L(q_i^{r_i})$$

for $r_i$ large enough. As it is a compositum of cyclic cyclotomic extensions of relatively prime degrees, $L$ is cyclic cyclotomic.

Now suppose we are given general $K$. First construct $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ satisfying the conditions for $\mathbb{Q}$ with $m[K : \mathbb{Q}]$. Then take $L = K(\zeta_n)$. We have $[K^v(\zeta_n) : K^v] \mid m$ for finite primes $v$ of $\mathbb{Q}$ since $[K^v : \mathbb{Q}_v] \mid [K : \mathbb{Q}]$.

We can take $K_c = \bigcup_{S,r_i} K \cdot \prod_{q_i \in S} L(q_i^{r_i})$. □

*Proof of Theorem 4.7.* We know $\mathrm{inv}_v(\alpha) = 0$ except for a finite number of primes, say primes in $S$. Why? Suppose $m \,\mathrm{inv}_v(\alpha) = 0$. Use Lemma 4.9 to get $L = K(\zeta_N)$ such that works for $m$ and $S$. Then by Lemma 4.8, $\mathrm{Res}_{K/L}(\alpha) = 0$ in $H^2(K(\zeta_N))$. □

## 4.5 (B) implies (A) for all abelian extensions

This will follow from the following proposition.

**Proposition 4.10:** If $L/K$ is abelian, then (B) for $L/K$ implies (A) for $L/K$.

*Proof.* Let $a \in K^\times$. By Lemma 4.2, for any character $\chi$,

$$\chi(\phi_{L/K}(a)) = \mathrm{inv}(\underbrace{\overline{a} \cup \delta\chi}_{\in H^2(L/K, L^\times)}) = 0.$$

Hence $\phi_{L/K}(a) = 0$. □

We have now proved the following.

**Theorem 4.11:** thm:AB The following hold.

(A) For an abelian extension $L/K$, define the map $\phi_{L/K}$ as in (14.10). The map $\phi_{L/K}$ takes the value 1 on the principal ideles $K^\times \subseteq \mathbb{I}_K$.

(B) For any $\alpha \in H^2(\overline{K}/K)$,

$$\mathrm{inv}(\alpha) := \sum_{v \in V_K} \mathrm{inv}_v(\alpha) = 0.$$

# §5 The ideles are a class formation

sec:ideles-cf We now complete the proof of global class field theory by showing that the ideles are a *class formation* and invoking the theorems in Section 13.4. In the local case, the $G$-modules in the class formations are the fields themselves, but in the global case, the $G$-modules are the ideles.

**Theorem 5.1:** thm:global-class-form Let $K$ be a global field. Then

$$(G(\overline{K}/K), \{G(L/K) : L/K \text{ finite Galois}\}, \mathbf{C}_{\overline{K}})$$

is a class formation.

Note that $\mathbf{C}_{\overline{K}}^{G(\overline{K}/L)} = \mathbf{C}_L$ for each $L$ by Proposition 1.3.

*Proof.* We check the axioms in Definition 4.5.

Step 1: First, $H^1(G(L/K), \mathbf{C}_L) = 0$ for every cyclic extension of prime degree (in fact every finite extension), by Theorem 3.1.

Second, we need maps $\mathrm{inv}_{L/K} : H^2(L/K, \mathbf{C}_K) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}$. Right now we just have a map

$$\mathrm{inv}_{L/K} : H^2(G(L/K), \mathbb{I}_L) \to \mathbb{Q}/\mathbb{Z}.$$

We need to show $\mathrm{inv}_{L/K}$ "factors through" $H^2(G(L/K), \mathbf{C}_L)$. We also need to show compatibility with inflation and restriction, and that

$$\mathrm{inv}_{L/K} : H^2(G(L/K), \mathbf{C}_L) \xrightarrow{\cong} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

for all $L/K$. It is hard to show this directly, except in the cyclic case, when we know the first inequality holds. As we will see, though, showing the cyclic case is enough, because by Theorem 4.7, every element of $H^2(G(\overline{K}/K), \mathbf{C}_{\overline{K}})$ is contained in $H^2(G(L/K), \mathbf{C}_L)$ for some cyclic (in fact, also cyclotomic) $L/K$.

Step 2: Consider the following commutative diagram, whose columns are inflation-restriction sequences.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r, "i_1"] \arrow[d, "\mathrm{Inf}"] & H^2(L/K, \mathbb{I}_L) \arrow[r, "p_1"] \arrow[d, "\mathrm{Inf}"] \arrow[drr, "\mathrm{inv}"'] & H^2(L/K, \mathbf{C}_L) \arrow[d, "\mathrm{Inf}"] & \\
0 \arrow[r] & H^2(M/K, M^\times) \arrow[r, "i_2"] \arrow[d, "\mathrm{Res}"] & H^2(M/K, \mathbb{I}_M) \arrow[r, "p_2"] \arrow[d, "\mathrm{Res}"] \arrow[drr, "\mathrm{inv}"'] & H^2(M/K, \mathbf{C}_M) \arrow[d, "\mathrm{Res}"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\
0 \arrow[r] & H^2(M/L, M^\times) \arrow[r, "i_3"] & H^2(M/K, \mathbb{I}_M) \arrow[r, "p_3"] \arrow[drr, "\mathrm{inv}"'] & H^2(M/L, \mathbf{C}_M) & \mathbb{Q}/\mathbb{Z} \\
 & & & & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

The columns are exact by the inflation-restriction exact sequence (Proposition 11.11.10) and the following:

1. $H^1(M/L, M^\times) = 0$ by Hilbert's Theorem 90 (Theorem 12.1.1).

2. $H^1(M/L, \mathbb{I}_M) = 0$ by Proposition 2.4.

3. $H^1(M/L, \mathbf{C}_M) = 0$ by Theorem 3.1.

The rows are exact because they come from the long exact sequences of $0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$ and $0 \to M^\times \to \mathbb{I}_M \to \mathbf{C}_M \to 0$, and the fact that $H^1$ of $\mathbf{C}_L, \mathbf{C}_M$ is trivial (again by Theorem 3.1).

Step 3: Next we show the maps inv are compatible with inflation. Indeed, since we have a class formation for local class field theory (Theorem 13.4.14), for every $w \mid v$ we have the diagram

$$\begin{tikzcd}
H^2(L_w/K_v) \arrow[r, "\mathrm{inv}_{K_v}"] \arrow[d, "\mathrm{Inf}_{\overline{L_w}/L_w}"] & \frac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z} \arrow[d, "i"] \\
H^2(K_v) \arrow[r, "\mathrm{inv}_{K_v}"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Now $H^2(G(L/K), \mathbb{I}_K) \cong \bigoplus_{v \in V_K} H^2(G^v, (L^v)^\times)$ by Proposition 2.4 and $\mathrm{inv} = \sum_{v \in V_K} \mathrm{inv}_v$, so inv is compatible with inflation.

Step 4: Thus, we can take the direct limit over $M$, noting direct limits preserve exactness, to get (we will explain the dashed and dotted lines)

$eq : 3x3 - icf$

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r, "i_1"] \arrow[d, "\mathrm{Inf}"] & H^2(L/K, \mathbb{I}_L) \arrow[r, "p_1"] \arrow[d, "\mathrm{Inf}"] \arrow[drr, "\mathrm{inv}_1"'] & H^2(L/K, \mathbf{C}_L) \arrow[d, "\mathrm{Inf}"] \arrow[dr, dashed, "\mathrm{inv}_1'"] & \\
0 \arrow[r] & H^2(K, \overline{K}^\times) \arrow[r, "i_2"] \arrow[d, "\mathrm{Res}"] & H^2(K, \mathbb{I}_{\overline{K}}) \arrow[r, "p_2"] \arrow[d, "\mathrm{Res}"] \arrow[drr, "\mathrm{inv}_2"'] & H^2(K, \mathbf{C}_{\overline{K}}) \arrow[d, "\mathrm{Res}"] \arrow[dr, dashed, "\mathrm{inv}_2'"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[d, dotted] \\
0 \arrow[r] & H^2(L, \overline{L}^\times) \arrow[r, "i_3"] & H^2(L, \mathbb{I}_{\overline{K}}) \arrow[r, "p_3"] \arrow[drr, "\mathrm{inv}_3"'] & H^2(L, \mathbf{C}_{\overline{K}}) \arrow[dr, dashed, "\mathrm{inv}_3'"] & \mathbb{Q}/\mathbb{Z} \arrow[d, dotted, "n"] \\
 & & & & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd} \tag{14.12}$$

Step 5: Now we show the maps $\mathrm{inv}_j$ are compatible under restriction. Again, since we have a class formation for local class field theory (Theorem 13.4.14), we have the diagram

$$\begin{tikzcd}
H^2(K_v) \arrow[r, "\mathrm{inv}_{K_v}"] \arrow[d, "\mathrm{Res}_{K_v/L_w}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L_w:K_v]}"] \\
H^2(L_w) \arrow[r, "\mathrm{inv}_{L_w}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Using $H^2(G(L/K), \mathbb{I}_K) \cong \bigoplus_{v \in V_K} H^2(G^v, (L^v)^\times)$, we can write an element of $H^2(K, \mathbb{I}_K)$ as $\mathbf{x} = (x_v)_{v \in V_K}$, where $x_v \in H^2(G_v, (K_v)^\times)$. On degree 0, $\mathrm{Res}_{K/L}$ is the diagonal imbedding $\mathbb{I}_K \xrightarrow{\cong} \mathbb{I}_L^G \hookrightarrow \mathbb{I}_L$ of Proposition 1.3, so on degree 2,

$$\mathrm{Res}_{K/L}\,\mathbf{x} = \Big( \big(\mathrm{Res}_{K_v/L_w} x_v\big)_{w|v} \Big)_{v \in V_K} \in \bigoplus_{v \in V_K} \bigoplus_{w|v} H^2(G_w, \overline{K_v}^\times).$$

The invariant map then sends this to

$$\sum_{v \in V_K} \sum_{w|v} \mathrm{inv}_{L_w}(\mathrm{Res}_{K_v/L_w} x_v) = \sum_{v \in V_K} \sum_{w|v} n_{w/v} \,\mathrm{inv}_{K_v} x_v = n \sum_{v \in V_K} \mathrm{inv}_{K_v} x_v = n \,\mathrm{inv}_K \mathbf{x},$$

using the fact that $[L : K] = \sum_{w|v} n_{w/v}$, where $n_{w/v}$ is the local degree.

Step 6: By Theorem 4.11, the bent maps are complexes, i.e. $\mathrm{im}(i_j) \subseteq \ker(\mathrm{inv}_j)$ for all three rows.

Thus the maps $\mathrm{inv}_j$ factor through the images $\mathrm{im}(p_j)$, for $j = 1, 2, 3$ to give the maps $\mathrm{inv}_j'$. Be careful: we have only so far defined $\mathrm{inv}_1' : \mathrm{im}(p_1) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, and not $\mathrm{inv}_1' : H^2(L/K, \mathbf{C}_L) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. We want to show that for certain extensions $L/K$, the $p_j$ are in fact surjective, so the map $\mathrm{inv}_j'$ is an isomorphism $H^2(L/K, \mathbf{C}_L) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

To do this we orders of $\mathrm{im}(\mathrm{inv}_1)$ and $|H^2(L/K, \mathbf{C}_L)|$. Again, we use $H^2(L/K, \mathbb{I}_L) \cong \bigoplus_{v \in V_K} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$ (Proposition 2.4). Making this identification using the invariant maps $\mathrm{inv}_v$, the invariant map takes $(a_v)_v \in \bigoplus_{v \in V_K} \frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$ to $\sum_{v \in V_K} a_v$. Thus $\mathrm{im}(\mathrm{inv}_1) = \frac{1}{\mathrm{lcm}_v(n_v)}\mathbb{Z}/\mathbb{Z}$ and

$$|\mathrm{im}(\mathrm{inv}_1)| = \mathrm{lcm}_v(n_v).$$

We have that

$$eq:lcmnv\, \mathrm{lcm}_v(n_v) = |\mathrm{im}(\mathrm{inv}_1)| = |\mathrm{im}(\mathrm{inv}_1')| \le |\mathrm{im}(p_1)| \le |H^2(L/K, \mathbf{C}_L)| \le n, \tag{14.13}$$

where the last step is the second inequality. We don't get any information out of this unless $\mathrm{lcm}_v(n_v) = n$. For certain extensions $L/K$, we do know it is true, though.

Step 7: We show that if $L/K$ is cyclic, then $\mathrm{lcm}_v(n_v) = n$. Let $S$ be the set of ramified primes and infinite places of $K$. By Proposition 2.8, $G(L/K)$ is generated by the elements $\mathrm{Frob}_{L/K}(\mathfrak{p})$ for $\mathfrak{p} \notin S$. Now $\langle \mathrm{Frob}_{L/K}(\mathfrak{p}) \rangle$ is sent to a subgroup of index $n_v$ in $G(L/K)$. Since $G(L/K)$ to be generated by these elements, we must have $\mathrm{lcm}_v(n_v) = n$.

Then equality holds everywhere in (14.13), we have the exact sequence

$$0 \to H^2(L/K, L^\times) \to H^2(L/K, \mathbb{I}_L) \to H^2(L/K, \mathbf{C}_L) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \to 0,$$

where the map $H^2(L/K, \mathbb{I}_L) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is the invariant map.

Step 8: Taking the direct limit over all $L \subseteq K_c$ (as defined in Theorem 4.7) we get

$$\begin{array}{ccccccc}
0 \longrightarrow & H^2(K, K_c^\times) & \longrightarrow & H^2(K_c/K, \mathbb{I}_{K_c}) & \longrightarrow & H^2(K_c/K, \mathbf{C}_{K_c}) \cong \mathbb{Q}/\mathbb{Z} & \longrightarrow 0 \\
& \downarrow \mathrm{Inf} & & \downarrow \mathrm{Inf} & & \downarrow \mathrm{Inf} & \\
0 \longrightarrow & H^2(K) & \longrightarrow & H^2(K, \mathbb{I}_{\overline{K}}) & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} &
\end{array}$$

where the top row is exact. By Theorem 4.7, the left vertical map is an isomorphism. The middle map is also an isomorphism because Theorem 2.4 gives that it is the map

$$\bigoplus_{v \in V_K} H^2(K_c^v/K_v) \to \bigoplus_{v \in V_K} H^2(K_v).$$

This is surjective because $H^2(K_c^v/K_v) \cong \mathbb{Q}/\mathbb{Z}$ via the invariant map, $K_c^v$ being the directed union of $L_w$ with $[L_w : K_v]$ arbitrarily divisible. Hence it is an isomorphism. Finally, the right vertical map is clearly an isomorphism. Thus the bottom row is short exact and $\mathrm{inv}_K$ gives an isomorphism $H^2(K, \mathbf{C}_{\overline{K}}) \to \mathbb{Q}/\mathbb{Z}$, i.e. the map $\mathrm{inv}_2'$ in (14.12). Restricting to $H^2(L'/K, \mathbf{C}_{L'})$, it is an isomorphism to $\frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z}$ for any $L'$, as needed. $\square$

We are now ready to reap the rewards of our hard work.

**Theorem** (Global reciprocity, Theorem 10.6.1)**:** Given a finite abelian extension $L/K$, there is a unique continuous homomorphism $\phi_{L/K}$ that is compatible with the local Artin maps, i.e. the following diagram commutes:

$$\begin{tikzcd} \mathbb{I}_K \arrow[r, "\phi_{L/K}"] & G(L/K) \\ K_v^\times \arrow[u, hook, "i_v"] \arrow[r, two heads, "\phi_v"] & G(L^v/K_v). \arrow[u, hook] \end{tikzcd}$$

Moreover, $\phi_{L/K}$ satisfies the following properties.

1. (Isomorphism) For every finite abelian extension $L/K$, $\phi_K$ defines an isomorphism

$$\phi_{L/K} : \mathbf{C}_K/\operatorname{Nm}_{L/K}(\mathbf{C}_L) = \mathbb{I}_K/(K^\times \cdot \operatorname{Nm}_{L/K}(\mathbb{I}_L)) \xrightarrow{\cong} G(L/K).$$

2. (Compatibility over all extensions) For $L \subseteq M$, $L, M$ both finite abelian extensions of $K$, the following commutes:

$$\begin{tikzcd} & G(M/K) \arrow[d, "p_L"] \\ \mathbb{I}_K \arrow[ur, "\phi_{M/K}"] \arrow[r, "\phi_{L/K}"] & G(L/K) \end{tikzcd}$$

   Thus we can define $\phi_K := \varprojlim_{L/K \text{ abelian}} \phi_{L/K}$ as a map $\mathbb{I}_K \to G(K^{\mathrm{ab}}/K)$.

3. (Compatibility with norm map) $\phi_K$ is a continuous homomorphism $\mathbb{I}_K \to G(K^{\mathrm{ab}}/K)$, and the following commutes.

$$\begin{tikzcd} \mathbb{I}_L \arrow[r, "\phi_L"] \arrow[d, "\operatorname{Nm}_{L/K}"] & G(L^{\mathrm{ab}}/L) \arrow[d, "\bullet|_{K^{\mathrm{ab}}}"] \\ \mathbb{I}_K \arrow[r, "\phi_K"] & G(K^{\mathrm{ab}}/K) \end{tikzcd}$$

*Proof.* By Theorem 5.1 and the abstract reciprocity law (Theorem 13.4.8) we get isomorphisms $\phi'_{L/K} : \mathbf{C}_K/\operatorname{Nm}_{L/K}\mathbf{C}_L \to G(L/K)$ satisfying the required compatibility properties. We only have to check that $\phi'_{L/K} = \phi_{L/K}$ (recall we defined $\phi_{L/K}$ as the product of local maps). From Theorem 13.4.9, for every character $\chi$, $\chi(\phi'_{L/K}(\mathbf{a})) = \operatorname{inv}_K(\overline{\mathbf{a}} \cup \delta\chi)$. But this is also true for $\phi_{L/K}$ by Proposition 4.2. Hence $\phi_{L/K} = \phi'_{L/K}$, as needed.

Uniqueness is clear from the condition that $\phi$ restricts to the local Artin maps. $\square$

# §6 Existence theorem

We now prove the existence theorem for global class field theory.

*Proof of Theorem 10.6.2 and Theorem 10.6.3.* This involves explicitly constructing norm groups and calculating norm indices, which overlaps with Section 3.2. The proof is omitted for now. See Cassels-Frohlich [3], pg. 201-202.

Theorem 10.6.3 now follows from the Existence Theorem and Theorem 4.13. □

Finally, we prove that $\phi_K$ gives a topological isomorphism $\mathbb{I}_K/\overline{K^\times(K_\infty^\times)^0} \to G(K^{\text{ab}}/K)$. This finishes the proof of all theorems of global class field theory.

*Proof of Theorem 10.6.4.* First we prove that $\phi_K$ is surjective. We know that $\phi_{H_K/K} : \mathbb{I}_K \to G(H_K/K)$ is surjective, where $H_K$ is the Hilbert class field (See Definition 15.5), since this is a finite extensions. Thus it suffices to show $\phi_{H_K/K} : \mathbb{I}_K \to G(K^{\text{ab}}/H_K)$ is surjective.

We know that for each place $v$ of $K$, $\phi_K : K_v \twoheadrightarrow W(K_v^{\text{ab}}/K_v)$ is surjective (Theorem 10.2.4). Restricting to $U_v$, we get that $\phi_K|_{U_v} : U_v \twoheadrightarrow I(K_v^{\text{ab}}/K_v) \cong I_v(K^{\text{ab}}/K)$ is surjective. Since $K^\times \left(\prod_{v\in V_K} U_v\right)/K^\times \subseteq \mathbb{I}_K$, it suffices to show $\prod_{v\in V_K} I_v(K^{\text{ab}}/K) = G(K^{\text{ab}}/K)$. Let $K_v^{\text{ab,ur}}$ denote the maximal abelian extension of $K$ unramified at $v$. We have by Theorem 2.7.2 that

$$\prod_{v\in V_K} I_v(K^{\text{ab}}/K) = \prod_{v\in V_K} G(K^{\text{ab}}/K_v^{\text{ab,ur}}) = G\left(K^{\text{ab}}/\bigcap_{v\in V_K} K_v^{\text{ab,ur}}\right) = G(K/H_K)$$

since $H_K$ is the maximal abelian extension unramified at all places. This shows surjectivity.

To show the kernel is $\overline{K^\times(K_\infty^\times)^0}$, note that this is exactly the intersection of all open subsets of finite index in $\mathbb{I}_K$. Add details. □

# Chapter 15
# Applications

ch:cft-app In this chapter we give several important applications of class field theory to number theory, rewarding the reader for reading the difficult proofs in the last few chapters (or conversely, motivating the reader to read the proofs).

Why is class field theory useful? It relates a field $K$ to its Galois group $G(K^{\text{ab}}/K)$, so transfers information about the extensions of a field into information *contained in the field itself*, or conversely, relates the behavior of elements in the field $K$, to their behavior in various extension fields. Moreover, because the global Artin map is constructed from the local Artin maps, questions in number theory involving global fields like $\mathbb{Q}$ can be understood by patching together information from its completions (local fields). In the chapter, we will use the full power of class field theory to give solutions to the following problems.

Throughout, we will assume that $K$ is a number field.

1. **Reciprocity laws**: We show, roughly, that whether a prime $p$ is a perfect $n$th power modulo $q$, depends only on $q$ mod $p$ (actually, some multiple of $p$). Reciprocity hence shows that the Legendre symbol $\left(\frac{*}{\bullet}\right)$, is like a group homomorphism in *both* the top and bottom. The Artin isomorphism will give us the homomorphism in the bottom.

2. **Local-to-global principle**: We show the **Hasse-Minkowski theorem**: a quadratic form has a solution in $K$ iff it has a solution in every completion of $K$.

3. **Density of primes**: We prove the **Chebotarev density theorem** on the distribution of prime ideals in a number field.

4. **Splitting of primes**: We show how a prime $\mathfrak{p}$ splits in an abelian extension $L/K$ depends only on $\mathfrak{p}$ modulo a *ray class group*, since splitting behavior can be expressed in terms of the Artin map (Proposition 10.1.3). We show this characterization is unique to abelian extensions, and give some examples for splitting in nonabelian extensions.

5. **Maximal unramified abelian extension**: We characterize the maximal unramified abelian extension $H_K$ of a number field $K$, and show that all ideals of $K$ become principal in $H_K$. $H_K$ can be computed for quadratic extensions using the modular function $j$, which we show in Chapter 16.

6. **Primes representated by quadratic forms**: We relate quadratic forms to primes using the Gauss correspondence (Theorem 4.5.1), then use the Hilbert class field to characterize which primes are represented by a given quadratic form.

7. **Artin and Hecke $L$-functions**: We use class field theory to show that for abelian extensions, all Artin L-functions are Hecke L-functions. This is useful because it is relatively easy to show Hecke L-functions satisfy nice properties such as analytic continuation and functional equation. This was Emil Artin's original motivation for class field theory.

Finally, we describe how class field theory fits as the "1-dimensional case" of the Langlands program.

# §1 Reciprocity laws

sec:rec-laws First we interpret and generalize the Legendre symbol using class field theory. We derive a generalize reciprocity law using class field theory, and then specialize to quadratic, cubic, and biquadratic reciprocity.

Reciprocity laws take two forms. The first is as follows.

**Theorem 1.1** (Weak reciprocity)**:** thm:weak-rec Let $K$ be a number field containing all $n$th roots of unity. Let $p$ be a fixed prime. Then there exists a modulus $\mathfrak{m}$ and a finite subset $S \in I_K^{\mathfrak{m}}/P_{K,1}(\mathfrak{m})$, such that for all $p$ relatively prime to $\mathfrak{m}$,

$$p \text{ is a perfect } n\text{th power } \bmod q \iff (q \bmod P_{K,1}(\mathfrak{m})) \in S.$$

In fact, $S$ is the kernel of a certain homomorphism $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \to \mu_n$.

This tells us that whether $p$ is a perfect $n$th power modulo $q$, depends only on the modular properties of $q$, and is moreover characterized by a group homomorphism. However, it does not give an efficient method to actually determine whether $p$ is a perfect $n$th power modulo $q$. To get this we turn to strong reciprocity.

We know that the Legendre symbol $\left(\frac{\bullet}{p}\right)$ (and its generalizations to $n$th powers, $\left(\frac{\bullet}{p}\right)_n$), is a homomorphism in the upper component as well, so it is natural to relate these two homomorphisms: what is their ratio $\left(\frac{p}{q}\right)_n \left(\frac{q}{p}\right)_n^{-1}$? This will give us a natural algorithm to compute the Legendre symbol $\left(\frac{a}{p}\right)_n$. We will prove strong reciprocity at the end of this section, after we discuss the Hilbert symbol.

## 1.1 Weak reciprocity and the Legendre symbol

The key observations linking reciprocity to the Artin map are that $a$ is a perfect $n$th power modulo $\mathfrak{p}$ iff $a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}} \equiv 1 \pmod{\mathfrak{p}}$ (just like $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ in the quadratic case), and the homomorphism $a \mapsto a^{\frac{\mathfrak{N}p-1}{n}}$ can be linked to the Frobenius map.

**Definition 1.2:** Let $K$ be a number field containing an $n$th root of unity, and let $\mathfrak{p}$ be a prime ideal with $an \perp \mathfrak{N}\mathfrak{p}$. Define the **Legendre symbol** $\left(\frac{a}{\mathfrak{p}}\right)_n$ to be the unique $n$th root of unity $\zeta$ such that

$$\zeta \equiv a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}} \pmod{\mathfrak{p}}.$$

To see this is well-defined, note the following two points.

1. The $n$th roots of unity are distinct modulo $\mathfrak{p}$ because $n \perp \mathfrak{N}\mathfrak{p}$. Hence $\frac{\mathfrak{N}\mathfrak{p}-1}{n}$ is an integer.
2. $(a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}})^n = 1 \equiv 1 \pmod{\mathfrak{p}}$ by Fermat's little theorem so $a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}}$ is equivalent to a unique $n$th root of unity.

**Proposition 1.3:** Let $K$ be a number field containing an $n$th root of unity, let $\mathfrak{p}$ be a prime ideal with $an \perp \mathfrak{N}\mathfrak{p}$. Then $a$ is a perfect $n$th power modulo $\mathfrak{p}$ iff $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$.

*Proof.* Let the residue field of $\mathfrak{p}$ be $k$. As $k^\times$ has order $\mathfrak{N}\mathfrak{p} - 1$ and is generated by 1 element, $a$ is a perfect $n$th power modulo $\mathfrak{p}$ iff $a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}} = \left(\frac{a}{\mathfrak{p}}\right)_n = 1$. □

**Proposition 1.4:** $\left(\frac{a}{\mathfrak{p}}\right)$ is a group homomorphism factoring through $\mathcal{O}_K/\mathfrak{p}$.

*Proof.* Clear. □

How can class field theory give us an expression like this? Well, the Frobenius element corresponding to $\mathfrak{p}$ acts like taking the $\mathfrak{N}\mathfrak{p}$ power modulo $p$. How do we get to $a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}}$? By acting by the Frobenius on $\sqrt[n]{a}$ instead.

**Proposition 1.5:** pr:leg-cft The following holds:

$$\left(\frac{a}{\mathfrak{p}}\right)_n = \frac{[\psi_{L/K}(\mathfrak{p})](\sqrt[n]{a})}{\sqrt[n]{a}},$$

where $L = K(\sqrt[n]{a})$.

*Proof.* First note $\mathfrak{p} \nmid an$ implies that $K(\sqrt[n]{a})/K$ is unramified at $\mathfrak{p}$, by Theorem 8.2.5.

By definition $\psi_{L/K}(\mathfrak{p})$ is the homomorphism that sends $b$ to $b^{\mathfrak{N}\mathfrak{p}}$ modulo $\mathfrak{p}$. Thus

$$[\psi_{L/K}(\mathfrak{p})](\sqrt[n]{a}) \equiv \sqrt[n]{a}^{\mathfrak{N}\mathfrak{p}} \equiv a^{\frac{\mathfrak{N}\mathfrak{p}-1}{n}} \sqrt[n]{a} \pmod{\mathfrak{p}}.$$

But $\sqrt[n]{a}$ satisfies $X^n - a = 0$, so $(\mathfrak{p}, L/K)$ must send $\sqrt[n]{a}$ to $\zeta\sqrt[n]{a}$ where $\zeta$ is some root of unity. The above equation shows that we must have $\zeta = \left(\frac{a}{\mathfrak{p}}\right)_n$, as needed. □

We define $\left(\frac{a}{\mathfrak{b}}\right)_n$ for any $\mathfrak{b} \in I_K^{(na)}$ by extending multiplicatively the map $\left(\frac{a}{\bullet}\right)$, originally defined for primes $\mathfrak{p}$. Equivalently (by Proposition 1.5), define $\left(\frac{a}{\mathfrak{b}}\right) = \frac{[\psi_{L/K}(\mathfrak{b})](\sqrt[n]{a})}{\sqrt[n]{a}}$.[1]

We can now prove weak reciprocity.

[1]We can extend the definition to all prime elements $p$ by definining $\left(\frac{a}{p}\right)_n = \frac{\phi_{L/K}(i_v(p))(\sqrt[n]{a})}{\sqrt[n]{a}}$, then extend

*Proof of Theorem 1.1.* By Proposition 1.5,

$$eq:leg-symb-cft\left(\frac{a}{\mathfrak{p}}\right)_n=\frac{[\psi_{K(\sqrt[n]{a})/K}(\mathfrak{p})](\sqrt[n]{a})}{\sqrt[n]{a}}. \tag{15.1}$$

Taking $a=p$ and $\mathfrak{p}=(q)$, we get

$$\left(\frac{p}{q}\right)_n=\frac{[\psi_{K(\sqrt[n]{p})/K}(q)](\sqrt[n]{p})}{\sqrt[n]{p}}.$$

Let $\mathfrak{m}$ be the conductor of $K(\sqrt[n]{p})/K$. Since $\psi_{K(\sqrt[n]{p})/K}$ is an homomorphism on $I_K^{\mathfrak{m}}/i(P_{K,1}(\mathfrak{m}))$ (Theorem 10.4.1), its kernel contains $i(P_{K,1}(\mathfrak{m}))$. In other words, when $q\in i(P_{K,1}(\mathfrak{m}))$, then $\left(\frac{p}{q}\right)=\frac{[\psi_{K(\sqrt[n]{q})/K}(q)](\sqrt[n]{p})}{\sqrt[n]{p}}=\frac{\mathrm{id}(\sqrt[n]{p})}{\sqrt[n]{p}}=1$ and $p$ is a perfect $n$th power modulo $q$. □

## 1.2 Strong reciprocity and the Hilbert symbol

To prove strong reciprocity we need to actually compute (15.1). Supposing $\mathfrak{p}$ is a principal ideal $(b)$, our statement about reciprocity seems to suggest that $b$ and $a$ play similar roles in the equation:[2]

$$eq:leg-symb-cft2\left(\frac{a}{b}\right)_n=\frac{[\psi_{L/K}(b)](\sqrt[n]{a})}{\sqrt[n]{a}}. \tag{15.2}$$

However, (15.2) is not symmetric. We seek to symmetrize it.

But look at Proposition 12.2.2. Equation (15.1) is the character corresponding to the element $a\in K^\times$. Using the map in Kummer Theory, we can get the equation symmetric in $a$ and $b$. In fact, we did this already when we defined the Hilbert symbol.

If motivation was lacking when we defined the Hilbert symbol, hopefully this clears things up: it explains and clarify the duality in $a$ and $b$ observed above by making it symmetric in $a$ and $b$.

**Proposition 1.6:** pr:hilbert-is-rec Let $b\nmid n$ be prime in $K$ and $K_b$ the completion at $b$. Let $(,)_b : K_b^\times/K_b^{\times n}\times K_b^\times/K_b^{\times n}\to\mu_n$ denote the Hilbert symbol. Then for $a\perp b$,

$$(a,b)_{b,n}=\left(\frac{a}{b}\right)_n.$$

In general, if $K_\pi(\sqrt[n]{a})/K_\pi(a)$ is unramified,

$$(a,b)_{\pi,n}=\left(\frac{(-1)^{v(a)v(b)}a^{v(b)}b^{-v(a)}}{\pi}\right)_n.$$

where $(a,b)_{v,n}$ denotes $(a,b)_n$ when $a,b$ are considered in $K_v$.

the definition of $\left(\frac{a}{b}\right)_n$ to encompass any $b\in K^\times$ by multiplicativity. For instance, in the case $n=2$, this gives the Jacobi symbol. For $b=2$, $\left(\frac{a}{b}\right)$ tells us whether $a$ is a perfect square modulo *any power of* 2.

[2]Caution: we're using the Artin map on ideals; we write $\psi_{L/K}(b)$ to mean $\psi_{L/K}((b))$. In contrast, $\phi_{L/K}(b)=1$ since $b\in K$.

*Proof.* Proposition 1.5 and Proposition 13.6.3 give

$$\left(\frac{a}{b}\right)_n = \frac{[\psi_{L/K}(b)](\sqrt[n]{a})}{\sqrt[n]{a}} = \frac{[\psi_{L_b/K_b}(b)](\sqrt[n]{a})}{\sqrt[n]{a}} = (a,b)_{b,n}.$$

For the second part write $a = \pi^j u$ and $b = \pi^k u'$ where $u, u'$ are units, and use bilinearity 13.6.4 to compute

$$\begin{aligned}
(\pi^j u, \pi^k u') &= (\pi, \pi^k u')^j (u, \pi)^k && (u,u') = 1 \text{ since } K(\sqrt[n]{a}) \text{ unramified, } 13.6.5\\
&= (\pi, -\pi)^{jk} (\pi, (-1)^k u')^j \left(\frac{u}{\pi}\right)_n^k && \text{by the first part}\\
&= ((-1)^k u', \pi)^{-j} \left(\frac{u}{\pi}\right)_n^k && (\pi, -\pi) = 1,\ \text{Theorem 13.6.4(2)}\\
&= \left(\frac{(-1)^k u'}{\pi}\right)_n^{-j} \left(\frac{u}{\pi}\right)_n^k\\
&= \left(\frac{(-1)^{jk} u^k u'^{-j}}{\pi}\right)_n\\
&= \left(\frac{(-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)}}{\pi}\right)_n.
\end{aligned}$$

□

The last main ingredient is the product formula for Hilbert symbols.

**Theorem 1.7** (Product formula for Hilbert symbols)**:** thm:hilbert-prod Let $K$ be a number field containing the $n$th roots of unity. Then

$$\prod_{v \in V_K} (a,b)_v = 1.$$

*Proof.* Using the fact that the global Artin map can be written as the product of local Artin maps,

$$\prod_{v \in V_K} \phi_{K_v(\sqrt[n]{a})/K_v}(b) = \phi_K(b) = 1,$$

because $\phi_K$ is the identity on $K$. Now operate on this by the character $\chi(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \in K$ and use Proposition 13.6.3 to get

$$\prod_{v \in V_K} (a,b)_v = \prod_{v \in V_K} \chi(\phi_{K(\sqrt[n]{a})/K}(b)) = 1.$$

□

Combining Proposition 1.6 and 1.7 gives the strong reciprocity law.

**Theorem 1.8** (Strong reciprocity)**:** thm:strong-rec Let $K$ be a number field containing a primitive $n$th root of unity and suppose $a, b, n$ are pairwise relatively prime. Then

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{v \mid n\infty} (b, a)_{v,n}.$$

Suppose $b, n$ are relatively prime and $a$ is a prime dividing $n$. Then

$$\left(\frac{a}{b}\right)_n = \prod_{v \mid n\infty} (a, b)_{v,n}.$$

*Proof.* Suppose $a, b, n$ are pairwise relatively prime. For a number $c$ let $S(c)$ denote the finite places $v$ where $v(c) \neq 0$. We calculate $\left(\frac{a}{b}\right)_n$ and $\left(\frac{b}{a}\right)_n$ using multiplicativity. We have

$$\begin{aligned}
\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} &= \left(\frac{a}{\prod_{\pi \in S(b)} \pi^{v_\pi(b)}}\right)\left(\frac{b}{\prod_{\pi \in S(a)} \pi^{v_\pi(a)}}\right)^{-1} && (b) = \left(\prod_{\pi \in S(b)} \pi^{v_\pi(b)}\right), (a) = \left(\prod_{\pi \in S(a)} \pi^{v_\pi(a)}\right) \\
&= \prod_{v_\pi \in S(b)} \left(\frac{a}{\pi}\right)_n^{v_\pi(b)} \prod_{v_\pi \in S(a)} \left(\frac{b}{\pi}\right)_n^{-v_\pi(a)} \\
&= \prod_{v_\pi \in S(b)} \left(\frac{a}{\pi}\right)_n^{v_\pi(b)} \prod_{v_\pi \in S(a)} \left(\frac{b^{-v_\pi(a)}}{\pi}\right)_n \\
&= \prod_{v \in S(b)} (a, b)_v \prod_{v \in S(a)} (a, b)_v && \text{by Proposition 1.6} \\
&= \prod_{v \nmid n\infty} (a, b)_v && (a, b)_{\mathbb{C}} = 1,\ (a, b)_v = 1 \text{ when } a, b \in U_v,\ 13.6.5 \\
&= \prod_{v \mid n\infty} (b, a)_v
\end{aligned}$$

where in the last step we used the product formula 1.7, which tells us $\prod_{v \in V_K} (a, b)_v = 1$.

Now suppose $a$ is a prime dividing $n$. Then again using multiplicativity, Proposition 1.6, and the fact that $(a, b)_v = 1$ for $v \mid n\infty$, $n \nmid a$ (Corollary 13.6.5),

$$\left(\frac{a}{b}\right)_n = \prod_{v_\pi \in S(b)} \left(\frac{a}{\pi}\right)^{v_\pi(b)} = \prod_{v \in S(b)} (a, b)_v = \prod_{v \mid n\infty} (a, b)_v.$$

□

In practice, we can compute the action of the Hilbert symbol for each $v \mid n\infty$, since $K_v^\times / K_v^{\times n}$ is a finite set. We will carry out these computations in the cases $n = 2, 4$, for $K = \mathbb{Q}$ and $\mathbb{Q}(i)$.

## 1.3 Quadratic and biquadratic reciprocity

We derive quadratic and biquadratic reciprocity using Theorem 1.8.

**Theorem 1.9** (Quadratic reciprocity)**:** Let $p, q$ be odd primes. Then

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

*Proof.* The first follows from definition of the Legendre symbol. By strong reciprocity 1.8,

$$\left(\frac{2}{p}\right) = (2, p)_2$$
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (p, q)_2.$$

Let $U^{(i)}$ denote $1 + (2)^i$ in $\mathbb{Q}_2$.

1. We have $(2, p)_2 = 1$ iff $p$ is a norm from $\mathbb{Q}_2(\sqrt{2})$ (Theorem 13.6.4), iff $p$ is in the form $x^2 - 2y^2$ in $\mathbb{Q}_2$. Looking at this modulo 8, we must have $p \in \{1, 5\}2^{\mathbb{Z}}$. This is sufficient as we know $[\mathbb{Q}_2^\times : \mathrm{Nm}_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{2})^\times)] = [\mathbb{Q}_2(\sqrt{2}) : \mathbb{Q}_2] = 2$, so we must have $\mathrm{Nm}_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{2})^\times) = \{1, 5\}2^{\mathbb{Z}}$. Hence $(2, p)_2 = 1$ iff $p \equiv 1, 5 \pmod 8$, iff $\frac{p^2-1}{8}$ is even. This gives
$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

2. We have $(p, q)_2 = 1$ iff $q \in N := \mathrm{Nm}_{\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{p})^\times)$, iff $q$ is in the form $x^2 - py^2$.

   (a) If $p \equiv 1 \pmod 4$, then $x^2 - py^2$ can attain any odd residue modulo 8. Since $[Q : N] = [\mathbb{Q}_2(\sqrt{p}) : \mathbb{Q}_2] \le 2$, we have $U^{(3)}2^{2\mathbb{Z}} = \mathbb{Q}_2^{\times 2} \subseteq N$. Since $N$ contains all residues modulo 8, $U2^{2\mathbb{Z}} \subseteq N$. Hence $q \in N$, and $(p, q)_2 = 1$.

   (b) If $p \equiv 3 \pmod 4$, then $x^2 - py^2$ cannot be $3 \pmod 4$. Hence $N = U^{(2)}2^{\mathbb{Z}}$, and $q \in N$ iff $q \equiv 1 \pmod 4$. Hence $(p, q)_2 = 1$ iff $q \equiv 1 \pmod 4$.

It remains to note $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$ iff either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$. □

**Theorem 1.10** (Biquadratic reciprocity)**:** Suppose $p, q$ are primes in $\mathbb{Z}[i]$ with $p, q \equiv 1 \pmod{(1+i)^3}$. Then
$$\left(\frac{p}{q}\right)_4 = (-1)^{\frac{\mathfrak{N}p-1}{4}\cdot\frac{\mathfrak{N}q-1}{4}}\left(\frac{q}{p}\right)_4.$$

Note every prime contains an associate that is equivalent to $1 \pmod 4$.

*Proof.* Note $p \equiv 1 \pmod{(1+i)^3}$ means $p \equiv 1$ or $1 + 2i \pmod{(1+i)^3}$.

By strong reciprocity 1.8,

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4^{-1} = (q,p)_{2,4} = (p,q)_{2,4}^{-1}.$$

We have $(p,q)_{2,4} = 1$ iff $q \in \mathrm{Nm}_{\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{p})^\times)$. Consider 2 cases.

1. $\mathfrak{N}p \equiv 1 \pmod 8$. Equivalently (writing out $p = a+bi$ and calculating the norm), $p \equiv 1 \pmod 8$. We can calculate that $(1+i)^{3\mathbb{Z}}U^{(3)} \subseteq N := \mathrm{Nm}_{\mathbb{Q}_2(\sqrt{p},i)/\mathbb{Q}_2(i)}(\mathbb{Q}_2(\sqrt{p},i)^\times)$, so $q \in N$. (The calculations are lengthy, but here's the idea: by examining the structure of $\mathbb{Q}_2(i)$, or using Proposition 14.3.2, we find that $\mathbb{Q}_2(i)^{\times 4} = U^{(7)}(1+i)^{4\mathbb{Z}}$. Hence the norm group $N$ satisfies
$$U^{(7)}(1+i)^{4\mathbb{Z}} \subseteq N \subseteq \mathbb{Q}_2(i)^\times$$
and has index at most 4. Now calculate the norm of enough numbers in $\mathbb{Q}_2(\sqrt{p},i)$ until we can determine $(1+i)^{3\mathbb{Z}}U^{(3)} \subseteq N$. Using a computer algebra system is advised.)

2. $\mathfrak{N}p \equiv 5 \pmod 8$. Equivalently, $p \equiv 5 \pmod 8$. We can calculate that $(1+i)^{4\mathbb{Z}}U^{(3)} \subseteq \mathrm{Nm}_{\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{p})^\times)$ but $(1+2i)(1+i)^{4\mathbb{Z}}U^{(3)} \not\subseteq \mathrm{Nm}_{\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2}(\mathbb{Q}_2(\sqrt{p})^\times)$. Hence $(p,q)_4 = 1$ iff $q \equiv 1 \pmod 4$, i.e. iff $\mathfrak{N}q \equiv 1 \pmod 8$.

In the case where $\mathfrak{N}p, \mathfrak{N}q \equiv 5 \pmod 8$, we have $(p,q)_4^2 = (p,q^2)_4 = 1$ but $(p,q)_4 \neq 1$ so $(p,q)_4 = -1$. □

## 1.4 Reciprocity for odd primes

We give an algorithm for finding reciprocity laws for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ for $p$ prime, and then specialize to $p = 3$.

**Theorem 1.11:** thm:explicit-rec Let $p$ be an odd prime, let $K = \mathbb{Q}(\zeta_p)$, and let $v$ be the valuation corresponding to $1-\zeta_p$. Let $\pi = 1-\zeta_p$. Then the elements

$$\begin{aligned} &\pi \\ \eta_1 &= 1-\pi = \zeta_p \\ \eta_2 &= 1-\pi^2 \\ &\vdots \quad \vdots \\ \eta_p &= 1-\pi^p \end{aligned}$$

generate $K_v^\times/K_v^{\times p}$, and $(a,b)_v$ is the unique skew-symmetric pairing $K_v^\times \times K_v^\times \to \mu_p$ satisfying the following.

1. $(\eta_i,\eta_j)_v = (\eta_i,\eta_{i+j})_v(\eta_{i+j},\eta_j)_v(\eta_{i+j},\pi)_v^{-j}$.

2. $(\eta_i,\pi)_v = \begin{cases} 1, & 1 \le i \le p-1 \\ \zeta, & i = p. \end{cases}$

Moreover, if $i+j \geq p+1$, then $(a,b)_v = 1$ for all $a \in U^{(i)}$ and $b \in U^{(j)}$.

We start with the following lemma.

**Lemma 1.12:** Let $K$ be a number field containing $p$th roots of unity. Let $\zeta$ be a primitive $p$th root of unity, $\pi = 1-\zeta$, and $\mathfrak{p}$ a prime dividing $\pi$. Suppose $a = 1+\pi^p c$ with $\pi = 1-\zeta$ and $c \in \mathcal{O}_v$. Then for all $b$,

$$(a,b)_{\mathfrak{p}} = \zeta^{-\mathrm{Tr}_{k/\mathbb{F}_p}(\bar{c})v_{\mathfrak{p}}(b)}.$$

We will just need the case where $K = \mathbb{Q}(\zeta_p)$, in which case $k = \mathbb{F}_p$.

*Proof.* Because $a \notin \mathfrak{p}$, $K(\sqrt[p]{a})/K$ is unramified by Lemma 7.2.5. We have (cf. Proposition 6.2.2)

$$\begin{aligned} \frac{\zeta^p - 1}{\zeta - 1} &= 0 \\ \implies \frac{(1-\pi)^p - 1}{(1-\pi)-1} &= 0 \\ \implies \pi^{p-1} - p\pi^{p-2} + \cdots + p &= 0 \\ \implies \pi^{p-1} \equiv -p \pmod{p\pi} \end{aligned}$$

and we get

$$eq: explicit-rec1 \frac{\pi^{p-1}}{p} \equiv -1 \pmod{\mathfrak{p}}. \tag{15.3}$$

Let $\alpha = \sqrt[p]{a}$ be a $p$th root of $a$, and write $\alpha = 1+\pi x$, where $x \in L$. Now $\alpha^m - a = 0$ becomes $(1+\pi x)^p - (1+\pi^p c) = 0$. Hence $x$ is a zero of the polynomial $f(X) = \frac{1}{\pi^p}\left((1+\pi x)^p - (1+\pi^p c)\right)$. Using (15.4), we find that $f(X)$ is integral, so $x \in \mathcal{O}_L$, and that modulo $\pi$,

$$f(X) = \frac{1}{\pi^p}\left(\pi^p x^p + p\pi x - \pi^p c\right) \equiv x^p - x - c \pmod{\pi}$$

Let $\mathfrak{N}\mathfrak{p} = p^f$. Letting $\sigma$ be the Frobenius, we find that $\sigma(x) \equiv x^{p^f} \pmod{\mathfrak{p}}$. Note that

$$x^{p^j} \equiv (x+c)^{p^{j-1}} \equiv x^{p^{j-1}} + c^{p^{j-1}} \pmod{\mathfrak{p}}.$$

Hence by induction

$$eq: explicit-rec1 \sigma(x) = x^{p^f} = x + \bar{c} + \bar{c}^p + \cdots + \bar{c}^{p^{j-1}} = x + \mathrm{Tr}_{k/\mathbb{F}_p}(\bar{c}) \tag{15.4}$$

in $k$. Now by Proposition 13.6.3,

$$(a,b)_{\mathfrak{p}} = \frac{[\phi_{K_\pi(\alpha)/K_\pi}(b)](\alpha)}{\alpha} = \frac{\sigma^{v(b)}(\alpha)}{\alpha}$$

To get the second equality, note that by construction, $\phi_{K_\pi(\alpha)/K_\pi}(\pi)$ is the Frobenius element; as $K_\pi(\alpha)/K_\pi$ is unramified, $U_{K_\pi} \subseteq \ker \phi_{K_\pi(\alpha)/K_\pi}$ (Example 13.5.1), and the Artin map depends only on $v(b)$. We have

$$(a,b)_v = \zeta^n \text{ where } \zeta^n\alpha = \sigma^{v(b)}(\alpha);$$

to find $n$ we reduce both sides modulo $\mathfrak{p}\pi$. We calculate

$$\zeta\alpha \equiv (1-\pi)(1+\pi x) \equiv 1 + (x-1)\pi \pmod{\mathfrak{p}\pi} \tag{15.5}$$
$$\implies \zeta^n\alpha \equiv 1 + (x-n)\pi \pmod{\mathfrak{p}\pi} eq: explicit-rec2 \tag{15.6}$$
$$\sigma^{v(b)}(x) \equiv x + v(b)\mathrm{Tr}_{k/\mathbb{F}_p}(\bar{c}) \pmod{\pi} \qquad \text{by (15.4)} \tag{15.7}$$
$$\implies \sigma^{v(b)}(\alpha) \equiv 1 + (x + v(b)\mathrm{Tr}_{k/\mathbb{F}_p}(\bar{c}))\pi \pmod{\mathfrak{p}\pi}. eq: explicit-rec3 \tag{15.8}$$

Matching (15.6) and (15.8) gives $n = -v(b)\mathrm{Tr}_{k/\mathbb{F}_p}(\bar{c})$ and

$$(a,b)_v = \zeta^{-v(b)\mathrm{Tr}_{k/\mathbb{F}_p}(\bar{c})} \pmod{\pi}.$$

□

In particular, note that $(a,b)_v = 1$ if $a \equiv 1 \pmod{\pi^{p+1}}$. By nondegeneracy of the pairing (Theorem 13.6.4), we get that $a \in (K_v^\times)^p$. Hence $U^{(p+1)} \subseteq (K_v^\times)^p$.

*Proof of Theorem 1.11.* Note that $\eta_i$ generates $U^{(i)}/U^{(i+1)}$, and $\pi$ generates $K_\pi^\times/(K_\pi^\times)^p U^{(1)}$. As mentioned above, $U^{(p+1)} \subseteq (K_\pi^\times)^p$ so $\pi, \eta_1, \dots, \eta_p$ generate $K_\pi^\times/(K_\pi^\times)^p$. Since the group has order $\frac{p^2}{|p|_{v_\pi}} = p^{p+1}$ (Proposition 14.3.2), these generators are independent.

We use a relation between the $\eta_i, \eta_j$ to derive the first relation. Namely, we have $\frac{\eta_j}{\eta_{i+j}} + \pi^j \frac{\eta_i}{\eta_{i+j}} = 1$, so

$$\left(\frac{\eta_j}{\eta_{i+j}}, \pi^j \frac{\eta_i}{\eta_{i+j}}\right)_p = 1$$

by Theorem 6.4. Note $(a,-1) = 1$ for any $a$ because $-1$ is a $p$th power. Expanding the above bilinearity gives

$$\begin{aligned}
1 &= (\eta_j, \pi^j\eta_i)(\eta_{i+j}, \pi^j\eta_i)^{-1} \underbrace{(\eta_{i+j}, -\eta_{i+j})}_{1} \underbrace{(\eta_{i+j}, -1)}_{1} (\eta_j, \eta_{i+j})^{-1} \\
&= (\eta_j, \eta_i) \underbrace{(\eta_j, \pi^j)}_{=1,\, \eta_j + \pi^j = 1} (\eta_{i+j}, \pi)^{-j} (\eta_{i+j}, \eta_i)^{-1} (\eta_j, \eta_{i+j})^{-1} \\
&= (\eta_i, \eta_j)^{-1} (\eta_{i+j}, \pi)^{-j} (\eta_{i+j}, \eta_i)^{-1} (\eta_{i+j}, \eta_j) \\
\implies (\eta_i, \eta_j) &= (\eta_i, \eta_{i+j})(\eta_{i+j}, \eta_j)(\eta_{i+j}, \pi)^{-j}.
\end{aligned}$$

This shows item 1. For item 2, note for $1 \le i \le p-1$ that since $\eta_i + \pi^i = 1$,

$$1 = (\eta_i, \pi^i) = (\eta_i, \pi)^i \implies 1 = (\eta_i, \pi).$$

For $i = p$, we use the lemma to find

$$(\eta_p, \pi)_v = \zeta^{-\mathrm{Tr}_{k/\mathbb{F}_p}(-1)} = \zeta$$

because $k = \mathbb{F}_p$.

Note that if $i + j \geq p + 1$, then $\eta_{i+j} \in U^{(p+1)} \subseteq (K_v^\times)^p$ so item 1 gives that $(\eta_i, \eta_j) = 1$. Now as a skew-symmetric bilinear pairing $(\eta_i, \eta_j)$ is determined by items 1 and 2, because we can expand $(\eta_i, \eta_j)$ using item 1, then repeatedly expand factors (the indices increase each time) until we only have factors in the form $(\bullet, \pi)$, and use item 2 to get a value out. □

We now use this to derive cubic reciprocity.

**Theorem 1.13** (Cubic reciprocity)**:** thm:cubic-rec Let $K = \mathbb{Q}(\omega)$, where $\omega = \zeta_3 = \frac{-1+\sqrt{-3}}{2}$. For $a \equiv \pm 1 \pmod{3\mathcal{O}_K}$, write

$$a = \pm(1 + 3(m + n\omega)).$$

Then

$$\begin{aligned} \left(\frac{b}{a}\right)_3 &= \left(\frac{a}{b}\right)_3 & &\text{if } b \perp a,\ b \equiv \pm 1 \pmod{3\mathcal{O}_K} \\ \left(\frac{\omega}{a}\right)_3 &= \omega^{-m-n} \\ \left(\frac{1-\omega}{a}\right)_3 &= \omega^m. \end{aligned}$$

Note that if $q \not\equiv 1 \pmod 3$ is prime, then $3 \nmid |\mathbb{F}_q^\times|$ so any element of $\mathbb{F}_q^\times$ is a cubic residue. Note any element of $K$ relatively prime to 3 can be written in the from $\omega^i(1-\omega)^j a$ where $a \equiv \pm 1 \pmod{3\mathcal{O}_K}$.

*Proof.* First suppose $a, b \equiv 1 \pmod 3$. By Strong Reciprocity 1.8,

$$\left(\frac{a}{b}\right)_3 \left(\frac{b}{a}\right)_3^{-1} = (b, a)_3.$$

Note $a, b \in U^{(2)}$ so by Theorem 1.11, $(b, a)_3 = 1$. This shows the first equation.

For the second, letting $\pi = 1 - \omega$, note that

$$(1-\pi^2)^\alpha (1-\pi^3)^\beta = (1+3\omega)^\alpha (1+3(2\omega+1))^\beta \in [1 + 3(\beta + (2\beta+\alpha)\omega)]U^{(4)}$$

Setting $\alpha = n - 2m$ and $\beta = m$, we get

$$\begin{aligned} a &\in (1-\pi^2)^{n-2m}(1-\pi^3)^m U^{(4)} \\ (1-\pi^2)^{2m-n}(1-\pi^3)^{-m} &\in aU^{(4)} \end{aligned}$$

Now Theorem 1.11 tells us

$$\begin{aligned}(\omega, 1-\pi^2) &= (\eta_1, \eta_2) = (\eta_3, \pi)^{-2} = \omega \\ (\omega, 1-\pi^3) &= (\eta_1, \eta_3) = 1 \\ (\pi, 1-\pi^2) &= (\eta_2, \pi)^{-1} = 1 \\ (\pi, 1-\pi^3) &= (\eta_3, \pi)^{-1} = \omega^{-1}.\end{aligned}$$

Thus

$$\begin{aligned}\left(\frac{\omega}{a}\right) &= (\omega, (1-\pi^2)^{2m-n}(1-\pi^3)^{-m}) = \omega^{-m-n} \\ \left(\frac{\pi}{a}\right) &= (\pi, (1-\pi^2)^{2m-n}(1-\pi^3)^{-m}) = \omega^m.\end{aligned}$$

□

As an application, we show the following.

**Theorem 1.14:** thm:2cubic If $q \equiv 1 \pmod 3$ is a prime, then 2 is a cubic residue modulo $q$ iff $q$ is in the form

$$q = x^2 + 27y^2, \quad \text{for some } x, y \in \mathbb{Z}.$$

*Proof.* Since $q \equiv 1 \pmod 3$, $q$ splits in $\mathcal{O}_K$ as $\alpha\overline{\alpha}$. By multiplying by a root of unity, we may assume $\alpha \equiv 1 \pmod{3\mathcal{O}_K}$, i.e. $\alpha$ is in the form $\alpha = 3(x + y\omega) \pm 1$. In order for 2 to be a cubic residue, it must be a cubic residue modulo $\alpha$. If $a^3 \equiv 2 \pmod \alpha$, then $\overline{a}^3 \equiv 2 \pmod{\overline{\alpha}}$, so it would also be a cubic residue modulo $\overline{\alpha}$ and hence modulo $q$.

Now $\left(\frac{2}{\alpha}\right) = 1$ iff $\left(\frac{\alpha}{2}\right) = 1$, by Cubic Reciprocity 1.13. Since 2 remains inert in $\mathcal{O}_K$, and the only cube in $\mathbb{F}_4^\times$ is 1, we get that $\alpha$ must actually be in the form

$$\alpha = 6(x + y\omega) \pm 1.$$

Taking the norm gives

$$p = (6x + 3y \pm 1)^2 + 27y^2.$$

This is in the form $x'^2 + 27y'^2$; conversely, any prime in the form $x'^2 + 27y'^2$ must have $x' \equiv \pm 1 \pmod 3$, and hence is in the above form. □

# §2 Hasse-Minkowski Theorem

The global Artin map can be expressed as the product of local Artin maps. From class field theory, we get various "local-to-global" results such as the Hasse-Brauer-Noether Theorem 14.3.5 and the Hasse Norm Theorem 2.2. The most famous is the local-to-global principle for quadratic forms, the Hasse-Minkowski Theorem.

**Definition 2.1:** A quadratic form is said to **represent** $a$ if there is a solution to $q(X_1, \ldots, X_n) = a$ with $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. A quadratic form representing 0 is said to be **isotropic**.

(For a review of quadratic forms, see Chapter 4.)

Where class field theory comes in is that a quadratic form in 2 variables representing a number $a$ can be interpreted as a norm equation, $a = x^2 + by^2$. We can write this as $a = (x + y\sqrt{b})(x - y\sqrt{b}) = \mathrm{Nm}_{K(\sqrt{b})/K}(x + y\sqrt{b})$ when $\sqrt{b} \notin K$. Class field theory gives us a local-to-global theorem for norms, the Hasse Norm Theorem. This will prove the $n = 2$ case of Hasse-Minkowski. Then a series of elaborate reductions will prove the local-to-global principal for any number of variables.

## 2.1 Hasse norm theorem

**Theorem 2.2** (Hasse norm theorem)**:** thm:hasse-norm Suppose $L/K$ is cyclic. Then $a$ is a global norm iff it is a local norm everywhere: $a \in \mathrm{Nm}_{L/K} L^\times$ iff $a \in \mathrm{Nm}_{L^v/K_v} L^{v\times}$ for all $v \in V_K$.

Compare this to the proof of Theorem 14.3.5.

*Proof.* The forward direction is clear.

Let $G = G(L/K)$. Take the long exact sequence in Tate cohomology of

$$0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$$

to get the top row of the following.

$$\begin{tikzcd} eq : hasse - norm\ H_T^{-1}(G, \mathbf{C}_L) \arrow[r] \arrow[d, equal] & H_T^0(G, L^\times) \arrow[r] \arrow[d, equal] & H_T^0(G, \mathbb{I}_L) \arrow[r] \arrow[d, equal] & \cdots \\ 0 \arrow[r] & K^\times / \mathrm{Nm}_{L/K} L^\times \arrow[r, hook] & \bigoplus_{v \in V_K} K_v^\times / \mathrm{Nm}_{K_v}(L^{v\times}) & \end{tikzcd} \tag{15.9}$$

We explain the bottom row. First note the equalities of $H_T^0$ are by definition of $H_T^0$, plus Proposition 14.2.4. Next note cohomology is 2-periodic because $G$ is cyclic (Proposition 11.12.1), and $H_T^1(G, \mathbf{C}_L) = 0$ by Theorem 14.3.1 (HT90 for ideles), so

$$H_T^{-1}(G, \mathbf{C}_L) = H_T^1(G, \mathbf{C}_L) = 0.$$

Then (15.9) gives that the map $K^\times / \mathrm{Nm}_{L/K} L^\times \hookrightarrow \bigoplus_{v \in V_K} K_v^\times / \mathrm{Nm}_{K_v}(L^{v\times})$ is injective. If $a \in K^\times$ is a norm in every completion, then it is 0 in $\bigoplus_{v \in V_K} K_v^\times / \mathrm{Nm}_{K_v}(L^{v\times})$, hence 0 in $K^\times / \mathrm{Nm}_{L/K} L^\times$, hence a global norm. $\square$

## 2.2 Quadratic forms

We prove the following.

**Theorem 2.3** (Hasse-Minkowski)**:** hasse-minkowski Let $K$ be a number field. The following hold.

1. A quadratic form $f$ defined over $K$ represents $a$ iff $f$ represents $a$ in every completion $K_v$.

2. Two quadratic forms over $K$ are equivalent iff they are equivalent over every completion $K_v$.

First we note that item 1 implies item 2.

*Proof that 1 implies 2.* The forward direction is clear. For the reverse direction, induct on the rank $n$, $n = 0$ being the base case. Suppose $f, g$ are equivalent over every completion $K_v$. Suppose $f$ represents $a$. Then $f$ represents $a$ over every $K_v$. Since $g \sim f$ over every $K_v$, $g$ represents $a$ over every $K_v$. By item 1, $g$ represents $a$.

Thus we can write $f \sim aX^2 + f'$, $g \sim aX^2 + g'$. Now $aX^2 + f' \sim aX^2 + g'$ over every $K_v$ implies (see Serre [13, IV.1.7, Prop. 4]) $f' \sim g'$ over every $K_v$. By the induction hypothesis, $f' \sim g'$ over $K$. Thus $f \sim g$. □

Next we show that we can reduce item 1 to a statement about quadratic forms representing 0.

**Lemma 2.4:** Suppose $\operatorname{char}(K) \neq 2$. An nondegenerate isotropic quadratic form over $K$ represents all of $K$.

*Proof.* Let $B$ be the bilinear form associated to $q$. Suppose $\mathbf{x} \neq 0$ is such that $q(\mathbf{x}) = 0$. Since $q$ is nondegenerate, there exists $\mathbf{y}$ such that $B(\mathbf{x}, \mathbf{y}) \neq 0$. Then $q(\mathbf{x} + a\mathbf{y}) = a^2 q(\mathbf{y}) + 2aB(\mathbf{x}, \mathbf{y})$ attains every value as $a$ ranges over $K$. □

**Lemma 2.5:** A quadratic form $q(X_1, \ldots, X_{n-1})$ represents $a$ iff $q(X_1, \ldots, X_{n-1}) - aX_n^2$ represents 0.

*Proof.* For the forward direction, suppose $q(x_1, \ldots, x_{n-1}) = a$. Then $q(x_1, \ldots, x_{n-1}) - a \cdot 1^2 = 0$.

For the reverse direction, let $(x_1, \ldots, x_n)$ be a solution. If $x_n = 0$ then $q(x_1, \ldots, x_n) = 0$ so $q$ represents 0. Thus $q$ is isotropic and represents $a$. If $x_n \neq 0$ then $q\left(\frac{x_1}{x_n}, \ldots, \frac{x_{n-1}}{x_n}\right) = a$. □

Thus it suffices to prove item 1 of Hasse-Minkowski for $a = 0$. Specifically, item 1 for forms with $n$ variables is a consequence of item 1 for $a = 0$ for forms with $n+1$ variables. We now prove Hasse-Minkowski. Every quadratic form over a field not of characteristic 2 can be put in diagonal form, so it suffices to consider diagonal forms. By scaling, we may assume one of the coefficients is 1.

### 2.2.1 Proof for $n \leq 2$

For $n = 1$ the theorem is trivial. For $n = 2$, we need the following.

**Lemma 2.6:** An element $a \in K$ is a square iff it is a square in every completion $K_v$.

*Proof.* (cf. the proof of Proposition 14.2.8) The forward direction is clear.

So suppose $a$ is a square in every completion. Then $K_v(\sqrt{a}) = K$ so $\mathrm{Nm}_{K_v(\sqrt{a})/K_v} K_v(\sqrt{a})^\times = K_v^\times$. This shows $\mathrm{Nm}_{K(\sqrt{a})/K}(\mathbb{I}_{K(\sqrt{a})}) = \mathbb{I}_K$. By the first inequality 14.2.1,

$$[K(\sqrt{a}) : K] \le [\mathbb{I}_K : \mathrm{Nm}_{K(\sqrt{a})/K}(\mathbb{I}_{K(\sqrt{a})})] = 1$$

so $K(\sqrt{a}) = K$, i.e. $a$ is a square in $K$. □

Now a quadratic form

$$q(X, Y) = X^2 - aY^2$$

represents 0 iff $a$ is a square (it rearranges to $\left(\frac{X}{Y}\right)^2 = a$), so $q$ represents 0 over $K$ if it represents 0 over every $K_v$.

### 2.2.2 Proof for $n = 3$

As promised, we re-express the condition for $p(x)$ to represent 0 as a condition on norms.

**Lemma 2.7:** lem:3var-norm Let $K$ be any field. A quadratic form

$$q(X, Y, Z) = X^2 - bY^2 - cZ^2$$

represents 0 iff $c \in \mathrm{Nm}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$.

*Proof.* Note if $q(x, y, z) = 0$ with $z = 0$, then $b$ must be a perfect square. If $b$ is a perfect square then $K(\sqrt{b})/K$ is trivial and $c$ is trivially a norm.

So it suffices to consider solutions with $z \neq 0$ and $b$ not a perfect square. In this case,

$$x^2 - by^2 - cz^2 = 0$$

iff

$$c = \left(\frac{x}{z}\right)^2 - b\left(\frac{y}{z}\right)^2 = \left(\frac{x}{z} - \sqrt{b} \cdot \frac{y}{z}\right)\left(\frac{x}{z} + \sqrt{b} \cdot \frac{y}{z}\right) = \mathrm{Nm}_{K(\sqrt{b})/K}\left(\frac{x}{z} - \sqrt{b}\frac{y}{z}\right).$$

□

By the Hasse Norm Theorem 2.2, $c \in \mathrm{Nm}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$ if this is true for every completion $K_v$. Combined with the lemma above, this gives Hasse-Minkowski for $n = 3$.

We will need the following in the proof for $n \ge 5$.

**Lemma 2.8:** 3-qf-almost The form $f = X^2 - bY^2 - cZ^2$ represents 0 in a local field $K_v$ iff $(b, c)_v = 1$. Moreover, $f$ represents 0 in $K_v$ for all but a finite number of places $v$.

*Proof.* Note $f$ represents 0 iff $c \in \mathrm{Nm}_{K(\sqrt{b})}(K(\sqrt{b})^\times)$, which is equivalent to $(b, c)_v = 1$ by Theorem 13.6.4. Only finitely many of these are not equal to 1 by Corollary 13.6.5. □

### 2.2.3 Proof for $n = 4$

We reduce the $n = 4$ case to the $n = 3$ case (but for a different field extension) by the following string of equivalences. The brilliant idea here is to turn the quadratic form equation into a quotient of norms.

**Theorem 2.9:** hm4 For any field $K$, the following are equivalent, for $a, b, c \in K^\times$.

1. The form $f(X, Y, Z, T) = X^2 - bY^2 - cZ^2 + acT^2$ represents 0 in $K$.
2. $c$ is a product of norms from $K(\sqrt{a})$ and $K(\sqrt{b})$:
$$c \in \mathrm{Nm}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)\, \mathrm{Nm}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times).$$
3. $c \in \mathrm{Nm}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}(K(\sqrt{a}, \sqrt{b})^\times)$.
4. The form $g(X, Y, Z) = X^2 - bY^2 - cZ^2$ represents 0 in $K(\sqrt{ab})$.

*Proof.* (1) $\iff$ (2): If $(x, y, z, t)$ is a solution with $z^2 - at^2 = 0$, then $x^2 - by^2 = 0$ as well. Then $a, b$ are squares in $K$ and (2) is clear. So it suffices to consider solutions with $z^2 - at^2 \neq 0$. In that case,

$$x^2 - by^2 - cz^2 + act^2 = 0 \iff c = \frac{x^2 - by^2}{z^2 - at^2} = (x - \sqrt{b}y)(x + \sqrt{b}y)(z - \sqrt{a}t)^{-1}(z + \sqrt{a}t)^{-1},$$

and this has a solution iff (2) holds.

(4) $\iff$ (3): Applying Lemma 2.7, we see (4) is equivalent to $c$ being a norm from $K(\sqrt{b}, \sqrt{ab})/K(\sqrt{ab})$. But $K(\sqrt{b}, \sqrt{ab}) = K(\sqrt{a}, \sqrt{b})$.

(2) $\iff$ (3): This is the hard part. We consider the field extensions

$$\begin{tikzcd}[arrows=dash]
 & L := K(\sqrt{a}, \sqrt{b}) \arrow[dl] \arrow[d] \arrow[dr] & \\
L^\sigma = K(\sqrt{a}) \arrow[dr] & L^{\sigma\tau} = K(\sqrt{ab}) \arrow[d] & L^\tau = K(\sqrt{b}) \arrow[dl] \\
 & K &
\end{tikzcd}$$

If any of $a, b, ab$ is in $K^{\times 2}$ then the result is clear: If $a \in K^{\times 2}$ then both (2) and (3) are true for any $c$, since $K(\sqrt{a}) = K$ and $K(\sqrt{a}, \sqrt{b}) = K(\sqrt{ab})$. If $ab \in K^{\times 2}$ then $K(\sqrt{a}) = K(\sqrt{b})$ so both (2) and (3) are equivalent to $c \in \mathrm{Nm}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)$.

Now assume $a, b, ab \notin K^{\times 2}$. In this case $G(K(\sqrt{ab})/K) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ with the 3 subextensions corresponding to 3 subgroups. Let $\sigma$ be the non-identity element fixing $K(\sqrt{a})$, $\tau$ fix

$K(\sqrt{b})$ and $\rho = \sigma\tau$ fix $K(\sqrt{ab})$. (I.e. $\sigma$ switches $\pm\sqrt{b}$ and $\tau$ switches $\pm\sqrt{a}$.) We convert the statements in (2) and (3) into the language of Galois theory, using the fixed field theorem.

Note (2) is equivalent to the following:

$$(2)': \quad \text{There exist } x, y \in L, \quad \sigma(x) = x, \tau(y) = y, x\rho(x)y\rho(y) = c.$$

To go between these statements take

$$x' = z - \sqrt{a}t,\ y = x - \sqrt{b}y$$

and note $\rho$ conjugates both $\sqrt{a}$ and $\sqrt{b}$. Similarly, (3) is equivalent to the following.

$$(3)': \quad \text{There exists } z \in L, \quad z\rho(z) = c;$$

just take $z' = (x - \sqrt{b}y)(z - \sqrt{a}z)$. To go from $(2)'$ to $(3)'$ just take $z = xy$. To go back from $(3)'$ to $(2)'$ requires more work. Given $z$, let $u = \frac{z\cdot\sigma(z)}{c}$. Now $\sigma(u) = u$ and $u\rho(u) = \frac{z\rho(z)\sigma(z)\sigma(\rho(z))}{c^2} = 1$. Since $\sigma(u) = u$. i.e. $u \in K(\sqrt{a})$, and $G(K(\sqrt{a})/K) = \{1, \tau|_{K(\sqrt{a})}\}$, by Hilbert's Theorem 90 (12.1.1) there exists $x \in K(\sqrt{a})$ (i.e. $x$ satisfying $\sigma(x) = x$) such that $\frac{\tau(x)}{x} = u$. Set $y = \frac{\rho(z)}{x}$. We've chosen $x$ satisfying the conditions. For $y$, note

$$\begin{aligned}
\tau(y) &= \frac{\sigma(z)}{\tau(x)} & \qquad \tau\rho &= \sigma \\
&= \frac{\sigma(z)}{xu} & \frac{\tau(x)}{x} &= u \\
&= \frac{c}{xz} & u &= \frac{z\sigma(z)}{c} \\
&= \frac{\rho(z)}{x} = y & z\rho(z) &= c.
\end{aligned}$$

Finally, $xy\rho(xy) = \rho(z)\rho(\rho(z)) = c$. This shows $(2)' \implies (3)'$ and finishes the proof. $\square$

Now we show Hasse-Minkowski holds for $n = 4$. By (1) $\iff$ (4) in Theorem 2.9, Hasse-Minkowski for $f = X^2 - bY^2 - cZ^2 + acT^2$ over $K$ is equivalent to Hasse-Minkowski for $g = X^2 - bY^2 - cZ^2$ over $K(\sqrt{ab})$, and we have already proved Hasse-Minkowski for $n = 3$.

### 2.2.4 Proof for $n \geq 5$

We now prove Hasse-Minkowski for $n \geq 5$. We proceed by induction. The idea is to "replace" $aX_1^2 + bX_2^2$ by just $cX^2$.

Suppose it proved for $n - 1$, and write

$$f(X_1, \ldots, X_n) = aX_1^2 + bX_2^2 - g(X_3, \ldots, X_n).$$

Suppose $f$ represents 0 in each $K_v$. Then there exists $c_v$ such that

$$aX_1^2 + bX_2^2 = c_v = g(X_3, \ldots, X_n)$$

has a nontrivial solution in $K_v$. By Lemma 2.8, there exists a finite set $S$ such that $g$ represents all elements of $K_v$ when $v \notin S$. We only need to focus on $v \in S$.

Note $K_v^{\times 2}$ is open in $K_v^\times$ by Theorem 8.1.5. By the Weak Approximation Theorem 7.3.4, there exists $c$ such that $c \in c_v K_v^{\times 2}$ for all $v \in S$. Since $c_v$ is in the form $ax_1^2 + bx_2^2$, so is $c$. Then $c = g(X_3, \ldots, X_n)$ has a solution for all $v$.

Thus

$$h(X, X_3, \ldots, X_n) := cX^2 - g(X_3, \ldots, X_n)$$

represents 0 in all $K_v$. By the induction hypothesis, it represents 0 in $K$ as well. Then $f$ represents 0: if $c = ax_1^2 + bx_2^2$ then replace the solution $(x, x_3, \ldots, x_n)$ with $(xx_1, xx_2, x_3, \ldots, x_n)$. This finishes the proof.

We now use Hasse-Minkowski show that most quadratic forms in $n \geq 5$ variables represent 0.

**Lemma 2.10:** lots-rep-0 A form $f = X^2 - bX^2 - cZ^2 + acT^2$ represents every nonzero element over a local field $K$ unless $K = \mathbb{R}$ and $f$ is positive definite.

A form $f$ in $n \geq 5$ variables over $K$ represents 0 unless $K$ is real and $f$ is definite.

*Proof.* First we show that if $f$ does not represent 0 in $K$, then $a, b \notin K^{\times 2}$, $ab \in K^{\times 2}$, and $c \notin \mathrm{Nm}_{K(\sqrt{a})} K(\sqrt{a})^\times = \mathrm{Nm}_{K(\sqrt{b})} K(\sqrt{b})^\times$. If $a$ or $b$ is in $K^{\times 2}$ then $f$ clearly represents 0, so $a, b \notin K^{\times 2}$. By $\sim (1) \implies \sim (2)$ of Theorem 2.9, $c \notin \mathrm{Nm}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)\,\mathrm{Nm}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$. If $K(\sqrt{a}) \neq K(\sqrt{b})$, then the norm groups are distinct groups of index 2 in $K^\times$, by the correspondence between norm groups and extensions. Then their product must be all of $K^\times$, a contradiction. Hence, $K(\sqrt{a}) = K(\sqrt{b})$ and $ab \in K^{\times 2}$. Then $\sim (2)$ becomes simply $c \notin \mathrm{Nm}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)$.

Conversely, suppose $a, b \notin K^{\times 2}$, $ab \in K^{\times 2}$, and $c \notin \mathrm{Nm}_{K(\sqrt{a})} K(\sqrt{a})^\times = \mathrm{Nm}_{K(\sqrt{b})} K(\sqrt{b})^\times$. Let $N := \mathrm{Nm}_{K(\sqrt{a})/K}(K(\sqrt{a})^\times)$; as noted it has index 2 in $K^\times$. Then

$$\left\{x^2 - by^2 - cz^2 + act^2 : x, y, z, t \in K \text{ not all zero}\right\} = \{x^2 - by^2\} - c\{z^2 - at^2\} = N - cN$$

where $A \pm B$ denotes $\{a \pm b : a \in A, b \in B\}$. Since $c \notin N$, $0 \notin N - cN$. Since $N - cN$ is invariant under multiplication by elements of $N$, it is a union of cosets of $N$. Suppose that $N - cN \neq K^\times$. Then $N - cN$ is either $N$ or $cN$, and

$$\{N - cN, cN - c^2N\} = \{N, cN\}$$

so

$$N - cN + cN - c^2N = N + cN.$$

If $-1 \in N$, then $N + cN = N - cN$ is $cN$ or $N$, which is a contradiction because 0 is in the LHS above. Hence $-1 \notin N$. Then

$$(N - cN) - (cN - c^2N) \in \{N - cN, cN - N\} = \{N, cN\}$$

Now $c, -1 \notin N$ imply $-c \in N$, so $(N - cN) - (cN - c^2N) = N + N + N + N \in \{N, cN\}$. We have $1^2 + 1^2 + 1^2 + 1^2 = 2^2 \in N$ and $3^2 + 4^2 = 5^2$, so $N + N + N + N = N$ and

$N + N = N$ (as it is a union of cosets). This implies that there exists a choice of sign in $K$: $K^\times$ is the disjoint union of the closed semigroups $N$ of "positive" elements and $-N$ of "negative" elements. If $K$ is $p$-adic then this cannot happen as we must have $N \supseteq \overline{\mathbb{Z}} = K$ where $\overline{\bullet}$ denotes closure in the $v$-adic topology. The only possibility is $K = \mathbb{R}$. Because $N$ consists just of positive numbers, $f$ is positive definite. This proves the first part.

For the second part, write $f(X_1, \ldots, X_n) = g(X_1, \ldots, X_{n-1}) - a_n X_n^2$. By the first part, $g(X_1, \ldots, X_{n-1})$ represents every element of $K^\times$ unless $K \cong \mathbb{R}$ and $g$ is positive definite. (Just consider $g(X_1, \ldots, X_4, 0, \ldots, 0)$.) In the first case, $g$ represents $a_n$ so $f$ represents 0. In the second case, $g$ represents all positive reals, and $f$ fails to represents all reals iff $a_n$ is negative, i.e. $f$ is positive definite. $\square$

**Corollary 2.11:** A form $f$ in $n \geq 5$ variables represents 0 in $K$ unless there is a real place $v$ with $f$ positive definite in $K_v$.

*Proof.* This follows directly from Lemma 2.10 and the Hasse-Minkowski Theorem 2.3. $\square$

# §3 Chebotarev density theorem

**Definition 3.1:** The **density** of a set of primes $S$ in $K$ is $d$ if

$$d = \lim_{N \to \infty} \frac{|\{\mathfrak{p} \in S \mid \mathfrak{N}\mathfrak{p} \leq N\}|}{\{\mathfrak{p} \mid \mathfrak{N}\mathfrak{p} \leq N\}}.$$

The **Dirichlet density** of a set of primes $S$ in $K$ is $\delta$ if

$$\delta = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \frac{1}{\mathfrak{N}\mathfrak{p}^s}}{\ln \frac{1}{s-1}}.$$

(Note that $\sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}\mathfrak{p}^s} \sim \ln \frac{1}{s-1}$ as $s \to 1^+$ by a weak version of the prime number theorem for number fields.)

Note if a set of primes has density $d$, then it has Dirichlet density $d$ (an exercise in partial summation), but a set of primes having a Dirichlet density may not have a well-defined density.

**Theorem 3.2** (Chebotarev density theorem)**:** cdt Let $L/K$ be a finite Galois extension of number fields, and let $C$ be a conjugacy class $G$. The set of prime ideals $\mathfrak{p}$ of $K$ such that $(\mathfrak{p}, L/K) = C$ has density $\frac{|C|}{|G|}$.

In the special case that $G$ is abelian, the conjugacy classes are just elements and they occur with density $\frac{1}{|G|}$. An especially notable case is the following.

**Example 3.3** (Dirichlet)**:** Let $n \in \mathbb{N}$ and $k$ be relatively prime to $n$. Then the set

$$\{q \text{ prime } \mid q \equiv k \pmod{n}\}$$

has density $\frac{1}{\varphi(n)}$.

Indeed, Chebotarev gives that the density of $q$ where $(q, L/K)$ is a specific element is $\frac{1}{\varphi(n)}$. By Example 10.1.6, this gives that the density of $q$ being a specific (relatively prime) residue modulo $n$ is $\frac{1}{\varphi(n)}$.

**Example 3.4:** If $L/K$ is a Galois extension, then the density of primes of $K$ splitting in $L$ is $\frac{1}{[L:K]}$.

Indeed, a prime splits completely iff $(\mathfrak{p}, L/K) = 1$, by Proposition 10.1.3.

## 3.1 Proof

We prove a weaker form of the Chebotarev Density Theorem, with Dirichlet density. We will need the following.

**Theorem 3.5** (Dirichlet's theorem for number fields)**:** thm:dirichlet-nf Let $K$ be a number field, let $H$ be a congruence subgroup modulo $\mathfrak{m}$, and let $\mathfrak{K}$ be a class in $I_K^{\mathfrak{m}}/H$. The set of prime ideals $\mathfrak{p}$ of $K$ such that $\mathfrak{p} \in \mathfrak{K}$ has density $\frac{1}{[I_K^{\mathfrak{m}}:H]}$.

*Proof.* See Lang [8, VIII. §4] for the proof with Dirichlet density. □

In the proof below, we use "density" to mean "Dirichlet density."

*Proof of Chebotarev Density Theorem 3.2.* We can't deal with nonabelian extensions directly, so the idea is to reduce to the abelian case as follows. Consider $L/L^\sigma$; this is cyclic. A prime $\mathfrak{P}$ in $L$ with $(\mathfrak{P}, L/K) = \sigma$ descends to a prime $\mathfrak{P}'$ such that $(\mathfrak{P}', L/L^\sigma) = \sigma|_{L^\sigma}$. Since $L/L^\sigma$ is abelian, these primes $\mathfrak{P}'$ are characterzed by a modular condition, and we can find their density using Theorem 3.5. Then we will relate the density of primes with $(\mathfrak{p}, L/K) = C$ to the density of primes with $(\mathfrak{P}, L/K) = \sigma$.

$$\begin{tikzcd} & L \arrow[dl, dash] \arrow[dr, dash] & \\ K & & L^\sigma \end{tikzcd} \qquad \begin{tikzcd} & S_{L,\sigma} \arrow[dl, dash, "1:\frac{N}{|C|f}"'] \arrow[dr, dash, "1:1"] & \\ S & & S_{L'} \end{tikzcd}$$

Let

$$S = \{\mathfrak{p} : (\mathfrak{p}, L/K) = C\}.$$

Note that fixing $\sigma \in C$, $\mathfrak{p} \in S$ iff there exists $\mathfrak{P} \mid \mathfrak{p}$ in $L$ such that $(\mathfrak{P}, L/K) = \sigma$.

Suppose $\sigma \in C$ has order $f$. Then $L/L^\sigma$ is a cyclic extension of degree $f$. Let $\mathfrak{c}$ be the conductor of this extension. The Artin map gives an isomorphism

$$I_{L^\sigma}^{\mathfrak{c}}/H \xrightarrow{\cong} G(L/K^\sigma)$$

for some congruence subgroup $H$.

Let $S_{L,\sigma}$ be those primes in $L$ whose Frobenius element is $\sigma$:

$$S_{L,\sigma} = \{\mathfrak{P} : (\mathfrak{P}, L/K) = \sigma\}.$$

(Note that $\bigcup_{\sigma\in C} S_{L,\sigma}$ gives all primes above those in $S$.) Let $S_{L'}$ be those primes in $L' := L^\sigma$ below a prime in $L'$:

$$S_{L'} = \{\mathfrak{P} \cap L^\sigma : \mathfrak{P} \in S_{L,\sigma}\}.$$

We have a bijection $S_{L,\sigma} \cong S_{L'}$ by $\mathfrak{P} \mapsto \mathfrak{P} \cap L^\sigma$, because $\sigma$ generates the decomposition group $D_{L/K}(\mathfrak{P})$, and $L/L^{D_{L/K}(\mathfrak{P})}$ has no splitting.

Now the density depends only on primes of degree 1 over $\mathbb{Q}$. Since $H$ is a subgroup of index $f$ in $I_{L^\sigma}^{\mathfrak{c}}$, by Theorem 3.5, $S_{L'}$ has density $\frac{1}{f}$.

Given $\mathfrak{p}$ such that $(\mathfrak{p}, L/K) = C$, how many primes $\mathfrak{P}$ above $\mathfrak{p}$ satisfy $(\mathfrak{P}, L/K) = \sigma$? Choose $\mathfrak{P}_0$ above $\mathfrak{p}$. The primes above $\mathfrak{p}$ are $\tau\mathfrak{P}$ for $\tau \in G(L/K)$. Each prime is hit $|D_{L/K}(\mathfrak{P})| = f$ times. Now we have $(\tau\mathfrak{P}_0, L/K) = \sigma$ iff

$$\tau(\mathfrak{P}_0, L/K)\tau^{-1} = \sigma.$$

The number of such $\tau$ is equal to the order of the stabilizer of the conjugation action (i.e. the number of elements commuting with $\tau$) which is $N$ divided by the number of elements in an orbit, i.e. $\frac{N}{|C|}$. Hence the number of $\mathfrak{P}$ lying above $\mathfrak{p}$ with $(\mathfrak{P}, L/K) = \sigma$ is

$$\frac{N/|C|}{f} = \frac{N}{|C|f}.$$

The density of $S_{L,\sigma}$ is $\frac{1}{f}$. Now every $\frac{N}{|C|f}$ good primes in $L$ correspond to 1 good prime down below, so we get the desired density to be

$$\frac{1/f}{N/(|C|f)} = \frac{|C|}{N}.$$

□

## 3.2 Applications

Often, we will need Chebotarev just for the existence of infinitely many primes with $(\mathfrak{p}, L/K) = C$, or just for the existence of a prime after we exclude a set of zero density. Here is a typical application.

**Corollary 3.6:** cor:chebotarev-resfield1 Let $K$ be a number field. There exist infinitely many primes $p$ of $\mathbb{Q}$ such that there is a prime $\mathfrak{p} \mid p$ of $K$ with $(\mathfrak{p}, L/K) = C$ and $\mathfrak{N}\mathfrak{p} = p$.

*Proof.* Chebotarev's Theorem 3.2 says there is a positive Dirichlet density of primes $\mathfrak{p}$ with $(\mathfrak{p}, L/K) = C$. The Dirichlet density of primes $\mathfrak{p}$ with residue degree greater than 1 is 0, because a sum of terms of the form $\frac{1}{p^{fs}}$ with $f \geq 2$ converges. Hence infinitely many primes must remain. $\square$

**Definition 3.7:** For two sets $S, T$, we write $S \overset{\subseteq}{\sim} T$ to mean $S \subseteq T \cup A$ for some finite set $A$, i.e. we have inclusion except for finitely many elements. We write $S \approx T$ if $S \overset{\subseteq}{\sim} T$ and $S \overset{\supseteq}{\sim} T$.

**Definition 3.8:** Define

$$\mathrm{Spl}(M/K) = \{\mathfrak{p} \text{ prime of } K \text{ splitting completely in } M\}.$$
$$\widetilde{\mathrm{Spl}}(M/K) = \{\mathfrak{p} \text{ prime of } K \text{ unramified in } M, f(\mathfrak{P}/\mathfrak{p}) = 1 \text{ for some } \mathfrak{P} \text{ in } M\}.$$

If $\mathfrak{p}$ is unramified in $K$ and $f(\mathfrak{P}/\mathfrak{p}) = 1$, we say that $\mathfrak{P}$ is a **split factor** of $\mathfrak{p}$.

Note $\widetilde{\mathrm{Spl}}(M/K) = \mathrm{Spl}(M/K)$ if $M/K$ is Galois.

The following says that the primes that split in a Galois extension characterize the extension uniquely, as well as giving inclusions between extensions.

**Theorem 3.9:** split-chebotarev Let $L/K$ and $M/K$ be finite field extensions.

1. If $L/K$ is Galois, then $L \subseteq M$ iff $\widetilde{\mathrm{Spl}}(M/K) \overset{\subseteq}{\sim} \mathrm{Spl}(L/K)$.
2. If $M/K$ is Galois, then $L \subseteq M$ iff $\mathrm{Spl}(M/K) \overset{\supseteq}{\sim} \mathrm{Spl}(L/K)$.
3. If $L/K$ and $M/K$ are Galois, then $L = M$ if and only if $\mathrm{Spl}(M/K) \approx \mathrm{Spl}(L/K)$.

In (1) and (2), inclusions actually hold.

*Proof.*

1. Suppose $L \subseteq M$, and $\mathfrak{p} \in \widetilde{\mathrm{Spl}}(M/K)$. Say that $\mathfrak{P} \mid \mathfrak{p}$ and $f(\mathfrak{P}/\mathfrak{p}) = 1$. Let $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_K$. Then $f(\mathfrak{P}'/\mathfrak{p}) = 1$. Additionally, $e(\mathfrak{P}/\mathfrak{p}) = 1$ implies $e(\mathfrak{P}'/\mathfrak{p}) = 1$. Since $L/K$ is Galois, the ramification indices and residue field degrees are equal for all primes above $\mathfrak{p}$. Hence $\widetilde{\mathrm{Spl}}(M/K) \subseteq \mathrm{Spl}(L/K)$.

   Conversely suppose $\widetilde{\mathrm{Spl}}(M/K) \overset{\subseteq}{\sim} \mathrm{Spl}(L/K)$. Let $N/K$ be a Galois extension containing $L$ and $M$. It suffices to show $G(N/M) \subseteq G(N/L)$; then Galois theory gives $M \supseteq L$.

   Take any $\sigma \in G(N/M)$. By Chebotarev Density 3.2, there exist infinitely many primes $\mathfrak{p}$ in $K$ such that $(\mathfrak{p}, N/K) = [\sigma]$. For such a prime $\mathfrak{p}$, let $\mathfrak{P}$ be a prime lying above $\mathfrak{p}$ in $N$ such that $(\mathfrak{P}, N/K) = \sigma$ and let $\mathfrak{P}' = \mathfrak{P} \cap \mathcal{O}_M$. For such a prime we have

   $$\alpha \equiv \sigma(\alpha) \equiv \alpha^{\mathfrak{N}\mathfrak{p}} \pmod{\mathfrak{P}'}, \quad \alpha \in \mathcal{O}_M.$$

   The left equality holds because $\sigma$ fixes $M$ and the right equality holds by definition of $(\mathfrak{P}, N/K)$. Hence $\mathcal{O}_M/\mathfrak{P}' \subseteq \mathbb{F}_{\mathfrak{N}\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, and equality must hold. In other words,

$f(\mathfrak{P}'/\mathfrak{p}) = 1$. Hence $\mathfrak{p} \in \widetilde{\operatorname{Spl}}(M/K)$. Since $\widetilde{\operatorname{Spl}}(M/K) \precsim \operatorname{Spl}(L/K)$, we can take $\mathfrak{p}$ such that $\mathfrak{p} \in \operatorname{Spl}(L/K)$ as well. Then $\sigma|_L = 1$ hence $G(N/M) \subseteq G(N/L)$ and $M \supseteq L$.

2. Suppose $L \subseteq M$. Then any prime splitting completely in $M$ splits completely in $L$, so $\operatorname{Spl}(M/K) \subseteq \operatorname{Spl}(L/K)$.

   Conversely suppose $\operatorname{Spl}(M/K) \precsim \operatorname{Spl}(L/K)$. Let $L^{\text{gal}}$ be the Galois closure of $L$. Since $M/K$ is Galois, $\widetilde{\operatorname{Spl}}(M/K) = \operatorname{Spl}(M/K)$; we also have $\operatorname{Spl}(L/K) = \operatorname{Spl}(L^{\text{gal}}/K)$ (Any prime splitting completely in $L$ splits completely in the Galois closure, by exercise 2 in 2.8). Thus

   $$\widetilde{\operatorname{Spl}}(M/K) \subseteq \operatorname{Spl}(L^{\text{gal}}/K)$$

   and we can apply part 1 to get $L^{\text{gal}} \subseteq M$; *a fortiori* $L \subseteq M$.

3. Apply part 2 twice. $\square$

# §4 Splitting of primes

sec:splitting

## 4.1 Splitting of primes

**Theorem 4.1:** thm:splitting-of-primes Let $L/K$ be an extension of number fields.

1. If $L^{\text{gal}}/K$ is abelian, then there is a modulus $\mathfrak{m}$ and a congruence subgroup modulo $\mathfrak{m}$ such that

   $$\operatorname{Spl}(L/K) = \{\text{prime } \mathfrak{p} \in H\}.$$

2. If there exists $\mathfrak{K} \in C_K(\mathfrak{m}) = I_K^{\mathfrak{m}}/P_K(1, \mathfrak{m})$ such that

   $$\{\text{prime } \mathfrak{p} : \mathfrak{p} \pmod{P_K(1,\mathfrak{m})} = \mathfrak{K}\} \precsim \operatorname{Spl}(L/K),$$

   (i.e. all but finitely many primes satisfying a certain modular condition split) then $L^{\text{gal}}/K$ is abelian.

In other words the law of decomposition of primes in an extension $L/K$ is determined by modular conditions iff $L/K$ is an abelian extension.

*Proof.* [3] As $\operatorname{Spl}(L/K) = \operatorname{Spl}(L^{\text{gal}}/K)$, it suffices to consider $L/K$ Galois.

<u>Part 1:</u> By global class field theory, the kernel of the Artin map $I_K^{\mathfrak{m}} \to G(L/K)$ is a congruence subgroup $H$. But we have by Proposition 10.1.3 that $\mathfrak{p}$ splits completely iff $\psi_{L/K}(\mathfrak{p}) = (\mathfrak{p}, L/K) = 1$. Hence

$$H = \ker(\psi_{L/K}) = \operatorname{Spl}(L/K).$$

[3] This proof is from http://mathoverflow.net/questions/11688.

Part 2: Let $K_\mathfrak{m}$ be the ray class field of $K$ modulo $\mathfrak{m}$ and $M = LK_\mathfrak{m}$. There is a natural map

$$p = p_1 \times p_2 : G(M/K) \hookrightarrow G(K_\mathfrak{m}/K) \times G(L/K) \xrightarrow{\cong} C_K(\mathfrak{m}) \times G(L/K)$$

where the second map is given by $\psi_{L/K}^{-1}$ in the first component.

For all but finitely many primes, we have the following string of facts.

1. $\mathfrak{p} \in \mathfrak{K}$.

2. $\mathfrak{p} \in \mathrm{Spl}(L/K)$.

3. $(\mathfrak{p}, L/K) = 1$.

4. For any prime $\mathfrak{P} \mid \mathfrak{p}$ in $M$, $p((\mathfrak{P}, M/K)) = (\mathfrak{K}, 1)$.

(1) $\implies$ (2) is by assumption, (2) $\iff$ (3) is Proposition 10.1.3, and (3) $\iff$ (4) is by compatibility of the Frobenius elements (the map $G(M/K) \to G(L_\mathfrak{m}/K) \times G(L/K)$ is compatible with the map on residue fields $G(m/k) \to G(k_\mathfrak{m}/k) \times G(l/k)$).

Suppose $\sigma \in G(M/K)$ and $p(\sigma) = (\mathfrak{K}, g)$. By Chebotarev's Theorem there exist primes $\mathfrak{P} \mid \mathfrak{p}$ in $M$ and $K$, respectively, such that $(\mathfrak{P}, M/K) = \sigma$. But (1) $\implies$ (4) shows that $g = 1$. Hence

$$p(G(M/K)) \cap (\mathfrak{K}, G(L/K)) = \{(\mathfrak{K}, 1)\}.$$

Since $p$ is a group homomorphism that is surjective in the first component, $p(G(M/K)) \cap (\mathfrak{K}', G(L/K))$ must consist of 1 element for every $\mathfrak{K}'$, in particular for $\mathfrak{K}' = 1$. Thus if $p(\sigma) = (P_K(1, \mathfrak{m}), g)$, then $g = 1$. Given a prime $\mathfrak{p}$ splitting completely in $K_\mathfrak{m}$, i.e. $\mathfrak{p}$ such that $\mathfrak{p} \in P_K(1, \mathfrak{m})$, take any $\mathfrak{P} \mid \mathfrak{p}$ in $M$. Then $p(\mathfrak{P}, M/K) = (P_K(1, \mathfrak{m}), g)$ for some $g$, so $g = 1$ and

$$(\mathfrak{p}, L/K) = (\mathfrak{P}, M/K)|_L = p_2(\mathfrak{P}, M/K) = g = 1,$$

i.e. $\mathfrak{p}$ splits completely in $L$. Thus $\mathrm{Spl}(L_\mathfrak{m}/K) \underset{\sim}{\subsetneq} \mathrm{Spl}(L/K)$, showing by Theorem 3.9 that $L \subseteq L_\mathfrak{m}$. □

For nonabelian extensions, the set of primes that split has to be specified by more than just a modulo condition.

**Example 4.2:** ex:prime-split-nonab We show that a prime splits completely in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ iff $p \equiv 1 \pmod 3$ and $p$ is in the form $x^2 + 27y^2$.

Note that $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is the splitting field of $x^3 - 2 = 0$. For an unramified prime, $p$ splits completely iff the residue field extension has degree 1, i.e. $x^3 - 2$ splits completely in $\mathbb{F}_p$. This is true iff 2 is a cubic residue modulo $p$. As we saw in Theorem 1.14, this is true iff $p$ is of the form $x^2 + 27y^2$.

### 4.2 Roots of polynomials over finite fields

We can recast the problem of splitting behavior in terms of finding roots of univariate polynomials over finite fields. Let $L/K$ be a finite extension, and $f \in \mathcal{O}_K[X]$ be the minimal polynomial of a primitive element in $L/K$. Then Theorem 2.6.3 tells us that for a prime $\mathfrak{p}$ relatively prime to the conductor of $L/K$, the factorization of $f$ in $\mathcal{O}_K/\mathfrak{p}$ corresponds to the factorization of $\mathfrak{p}$. In particular, $\mathfrak{p}$ splits completely iff $f$ splits completely, and $\mathfrak{p}$ has a split factor iff $f$ has a root in $\mathcal{O}_K/\mathfrak{p}$.

**Definition 4.3:** Let $N_{\mathfrak{p}}(f)$ denote the number of zeros of $f$ in $\mathcal{O}_K/\mathfrak{p}$.

Thus we can rephrase Theorem 4.1 as follows.

**Theorem 4.4:** thm:roots-over-ff Let $f$ be an irreducible polynomial over $K$. Let $\alpha$ be a root of $f$ and $L$ be the Galois closure of $K(\alpha)$.

1. For all except a finite number of primes, $N_{\mathfrak{p}}(f) = m$ iff $\psi_{L/K}(\mathfrak{p}) = [\sigma]$ for some $\sigma \in G(L/K)$ fixes $m$ of the roots of $L$.

2. The sets $\{\mathfrak{p} : N_{\mathfrak{p}}(f) = m\}$ are given by modular conditions iff $L/K$ is abelian.

3. The density of primes $\mathfrak{p}$ such that $N_{\mathfrak{p}}(f) = m$ is $\frac{\{\sigma \in G(L/K) : \sigma \text{ fixes } m \text{ roots}\}}{[L:K]}$.

*Proof.* The first item follows from Theorem 2.6.3. The second item follows from this and Theorem 4.1. The third item follows from the Chebotarev Density Theorem 3.2. □

Even the reciprocity laws (at least, weak reciprocity) can be put in the same framework: in a field $K$ containing $n$th roots of unity, $a$ is a perfect $n$th power modulo $\mathfrak{p}$ iff $x^n - a$ splits completely modulo $\mathfrak{p}$ (the polynomial viewpoint), i.e. the prime $\mathfrak{p}$ splits completely in $K(\sqrt[n]{a})/K$ (the splitting viewpoint).

## §5 Hilbert class field

sec:hcf

**Definition 5.1:** The **Hilbert class field** of $K$ is the largest abelian field extension of $K$ unramified over $K$ at all places. (For infinite places this means that no real embedding becomes complex.) It is denoted $H_K$.

The **large Hilbert class field** of $K$ is the largest abelian field extension of $K$ unramified over $K$ at all finite places, with no restrictions for infinite places (i.e. they are allowed to ramify). It is denoted $H_K^+$.

Note if $K$ is already totally complex then $H_K = H_K^+$.

**Proposition 5.2:** pr:hcf The Hilbert class field and large Hilbert class field exist, and the global reciprocity map gives isomorphisms

$$G(H_K/K) \cong C_K$$
$$G(H_K^+/K) \cong C_K^+.$$

*Proof.* The Hilbert class field is exactly the ray class field corresponding to the modulus 1, and the narrow Hilbert class field is exactly the ray class field corresponding to the modulus $\mathfrak{m} = \prod_{v \text{ real}} v$. Indeed, by global class field theory the fields corresponding to congruence subgroups of $C_K(1)$ are just the fields unramified over $K$, and the fields corresponding to congruence subgroups of $C_K(\mathfrak{m})$ are just the fields unramified at every infinite place.

The global reciprocity map gives the desired isomorphisms. $\square$

The most interesting property of the Hilbert class field is the following.

**Theorem 5.3:** Let $K$ be a global field. Every fractional ideal of $K$ becomes principal in the Hilbert class field $L$ of $K$.

*Proof.* Let $M$ be the Hilbert class field of $L$. By Proposition 5.2, the global reciprocity map gives $C_K \xrightarrow{\cong} G(L/K)$ and $C_L \xrightarrow{\cong} G(M/L)$. We will transfer the map $C_K \to C_L$ to the Galois groups. By definition, $L$ is the maximal unramified *abelian* extension of $K$; since $M$ is also unramified over $K$, $L$ is the maximal *abelian* subextension of $M/K$. But by Galois theory, intermediate Galois extensions correspond to quotient groups of $G(M/K)$. This means that

$$G(L/K) = G(M/K)/G(M/L)$$

is the largest abelian quotient of $G(L/K)$. From group theory this means that $G(M/L)$ is the *derived subgroup* $(G(L/K))'$.

The following diagram commutes by compatibility of the Artin map (the last diagram in Theorem 13.4.10 together with Theorem 14.5.1)

$$\begin{tikzcd}
C_K \arrow[r, "\phi_{L/K}", "\cong"'] \arrow[d] & G(L/K)^{\mathrm{ab}} \arrow[d, "V"] \\
C_L \arrow[r, "\phi_{M/L}", "\cong"'] & G(M/L)^{\mathrm{ab}}
\end{tikzcd}$$

where $V$ is the transfer.

However, the transfer map is 0 by Theorem 11.11.13 and the fact that $G(M/L) = G(L/K)'$. Hence the map $C_K \to C_L$ is trivial, i.e. every fractional ideal of $K$ becomes trivial in $L$. $\square$

# §6 Primes represented by quadratic forms

sec:primes-rep-q We now give a complete characterization of which primes can be represented by which binary (positive definite integral) quadratic forms. First consider the form $x^2+ny^2$.

A prime is in the form $p = x^2 + ny^2$ iff $p$ splits as $\mathfrak{p}\overline{\mathfrak{p}} = (x + y\sqrt{n})(x - y\sqrt{n})$ in $\mathbb{Z}[\sqrt{-n}]$, with its factors being principal ideals. We can think of this as saying that $\mathfrak{p}$ goes to 0 in the ideal class group of $\mathbb{Z}[\sqrt{-n}]$. Unfortunately, this is not the same class group as $C_K$. However, this class group is essentially a quotient of a ray class group (Theorem 4.6.2). But by class field theory, we can find a field extension $L$ such that the Artin map to $G(L/K)$ is an isomorphism. The primes in the kernel of the Artin map are exactly those that split completely in $L$, so this relates the equation $x^2+ny^2$ to the splitting of primes in the Hilbert class field.

**Definition 6.1:** Let $\mathcal{O}$ be an integral quadratic order and $f := \operatorname{disc}(\mathcal{O})$.

1. Suppose $f < 0$. The field $L$ corresponding to the congruence subgroup
$$P_K(\mathbb{Z}, f) := \{(a) \in I_K(f) : a \pmod f \in \mathbb{Z} \pmod f\} \subseteq I_K(f)$$
is called the **ring class field** of $\mathcal{O}$.

2. Suppose $f > 0$. The field $L$ corresponding to the congruence subgroup
$$P_K(\mathbb{Z}, \infty f) := \{(a) \in I_K(f) : a \pmod f \in \mathbb{Z} \pmod f\} \subseteq I_K(f)$$
is called the **ring class field** of $\mathcal{O}$.

The reason for this definition is that $I_K(f)/P_K(\mathbb{Z}, \infty f) \cong I(\mathcal{O})/P^+(\mathcal{O}) = C^+(\mathcal{O})$ via the map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$, by Theorem 4.6.2. (Ignore the $\infty$ when $K$ is imaginary; in this case $C^+(\mathcal{O}) = C(\mathcal{O})$.)

**Example 6.2:** When $\mathcal{O} = \mathcal{O}_K$, with $K/\mathbb{Q}$ a quadratic extension, then the ring class field is just the large Hilbert class field of $K$, because $I(\mathcal{O})/P^+(\mathcal{O}) = C_K^+$.

**Theorem 6.3:** thm:p=x2+ny2 Let $n \geq 1$. Let $Q$ be a quadratic form that corresponds to $\mathfrak{a} \subseteq R$ under the Gauss correspondence 4.5.1, let $K = \operatorname{Frac}(R)$, and let $p$ be an odd prime not dividing $f := \operatorname{disc}(R)$. Let $\mathfrak{b}$ be the ideal corresponding to $\mathfrak{a}$ under the map $I_K(f)/P_K(\mathbb{Z}, \infty f) \to I(\mathcal{O})/P^+(\mathcal{O}) = C^+(\mathcal{O})$. Let $L$ be the ring class field of $R$ and suppose $(L/K, \mathfrak{b}) = \sigma$. Then
$$f \text{ represents } \mathfrak{p} \iff (L/\mathbb{Q}, p) = [\sigma]$$
where $[\sigma]$ denotes the conjugacy class of $\sigma$ in $G(L/\mathbb{Q})$.

*Proof.* Let $K = \mathbb{Q}(\sqrt{-n})$. We have the following string of equivalences.

1. $Q$ represents $p$.

2. $pR = \mathfrak{p}\overline{\mathfrak{p}}$ in $R$ for some ideal $\mathfrak{p}$ in the same ideal class as $\mathfrak{a}$.

3. $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ for $\mathfrak{p} \sim \mathfrak{b}$ where the ideals are considered in $I_K(f)/P_K(\mathbb{Z}, \infty f)$.

4. $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ for $(L/K, \mathfrak{p}) = \sigma$.

5. $(L/\mathbb{Q}, p) = [\sigma]$.

The equivalence (1) $\iff$ (2) follows from Proposition 4.5.4. We have (2) $\iff$ (3) by Theorem 4.6.2, which gives an isomorphism $I_K(f)/P_K(\mathbb{Z}, \infty f) \to I(\mathcal{O})/P^+(\mathcal{O}) = C^+(\mathcal{O})$ by sending $\mathfrak{a}$ to $\mathfrak{a} \cap \mathcal{O}$. By definition of ring class field, the Artin map is an isomorphism $I_K(f)/P_K(\mathbb{Z}, \infty f) \to G(L/K)$, so (3) $\iff$ (4).

For (4) $\iff$ (5), note by definition of the Artin symbol that (4) is equivalent to

$$p \text{ splits in } \mathcal{O}_K \text{ and } \sigma(\alpha) \equiv \alpha^{|k|} \pmod{\mathfrak{P}} \text{ for all } \alpha \in L$$

where $\mathfrak{P}$ is any prime dividing $\mathfrak{p}$ in $L$. Since $p$ is unramified, $p$ splits in $\mathcal{O}_K$ iff $[k : \mathbb{F}_p] = 1$, iff $|k| = p$. Hence the above is equivalent to

$$\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$$

This says exactly that $(L/\mathbb{Q}, p) = [\sigma]$. $\square$

**Corollary 6.4:** Suppose $n \neq 0$ is an integer.

1. Let $L$ be the ring class field of $\mathbb{Z}[\sqrt{-n}]$. Then $p$ can be represented as

$$p = x^2 + ny^2, \quad x, y \in \mathbb{Z}$$

   if and only if $p$ splits completely in $L$.

2. For $-n \equiv 1 \pmod 4$, let $L'$ be the ring class field of $\mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right]$. Then $p$ can be represented as

$$p = x^2 + xy + \frac{1-n}{2}y^2$$

   iff $p$ splits completely in $L'$.

**Remark:** It is not hard to show that we can replace the conditions by the following uniform statement: $4p$ can be represented as $4p = x^2 + dy^2$ iff $p$ splits completely in the order of discriminant $-d$.

*Proof.* These quadratic forms correspond to the principal ideals in $\mathbb{Z}[\sqrt{-n}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right]$, respectively (Example 4.5.3), so the theorem says $p$ can be represented by the quadratic forms iff

$$(L/K, p) = 1.$$

This is true iff $\mathfrak{p}$ splits completely in $L$ (Proposition 10.1.3). $\square$

How is this useful? Algorithmically, there are fast ways to find solutions to $p = x^2 + ny^2$ (Cornacchia's algorithm), so we can obtain primes splitting completely in the Hilbert class field $H_K$. This means that the minimal polynomial of $H_K/K$ factors completely modulo $p$. As we will in Chapter 16, the roots are the $j$-invariants of CM elliptic curves; the fact that they are in $\mathbb{F}_p$ gives us an easy way to calculate the action of the class group on elliptic curves.

Additionally, this description of solutions to $p = x^2 + ny^2$ gives a way to find the density of primes represented by a quadratic form.

**Theorem 6.5:** thm:density-qform Let $Q$ be a primitive positive definite quadratic form of discriminant $D < 0$, and let $S$ be the set of primes represented by $Q$. Then the density of primes $d(S)$ represented by $S$ is

$$d(S) = \begin{cases} \frac{1}{2h(D)}, & Q \text{ properly equivalent to its opposite,} \\ \frac{1}{h(D)}, & \text{else,} \end{cases}$$

where $h(D)$ is the class number of the quadratic ring with discriminant $D$. In particular, $Q$ represents infinitely many prime numbers.

Note "$Q$ properly equivalent to its opposite" is equivalent to saying that the ideal class corresponding to $Q$ has order dividing 2.

**Example 6.6:** $h(-27) = 3$ so $\frac{1}{6}$ of all primes can be represented by the form $x^2 + 27y^2$.

In fact, the ring class field of $\mathbb{Z}[\sqrt{-27}]$ is $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$, so $p = x^2 + 27y^2$ iff $p$ splits completely in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. This shows Example 4.2 in a different way.

*Proof of Theorem 6.5.* Let $K$ be the quadratic field of discriminant $D$.

By Theorem 6.3, $p$ is represented by $Q$ iff $(L/\mathbb{Q}, p) = [\sigma]$ where $L$ is the ring class field of the order corresponding to $Q$ and $Q$ corresponds to $\sigma$ under the Gauss correspondence. We need to find $[\sigma]$, so we first need to understand $G(L/\mathbb{Q})$.

Since $C(\mathcal{O}) \cong I_K(f)/P_K(\mathbb{Z}, f) \cong G(L/K)$ via the Artin map,

$$[L : K] = |C(\mathcal{O})| = h(D) \implies [L : \mathbb{Q}] = 2h(D).$$

Next we show $G(L/\mathbb{Q}) = G(L/K) \rtimes G(K/\mathbb{Q})$ where, denoting complex conjugation by $\sigma \in G(K/\mathbb{Q})$, we have $\sigma\tau\sigma^{-1} = \tau^{-1}$ for all $\tau \in G(L/K)$. Let $\mathfrak{m}$ be the modulus corresponding to $f\mathcal{O}_K$, where $f$ is the conductor. By construction of $L$, it is the unique field such that $\ker(\psi_{L/K}) = P_K(\mathbb{Z}, f)$. However, because the Artin map commutes with Galois action (see the third diagram in Theorem 4.10),

$$\ker(\psi_{\sigma(L)/K}) = \sigma \ker(\psi_{L/K}) = \sigma P_K(\mathbb{Z}, f) = P_K(\mathbb{Z}, f).$$

Uniqueness hence gives $\sigma(L) = L$, i.e. $\sigma \in L$. Hence $|G(L/\mathbb{Q})| = 2|G(L/K)| = [L : \mathbb{Q}]$, giving that $L/\mathbb{Q}$ is Galois. Given $\tau \in G(L/K)$, by surjectivity of the Frobenius map 14.2.8,

$\tau = (L/K, \mathfrak{p})$ for some $\mathfrak{p}$. Then by Lemma 10.1.2,

$$\sigma\tau\sigma^{-1} = \sigma(L/K, \mathfrak{p})\sigma^{-1} = (L/K, \sigma\mathfrak{p}) = (L/K, \overline{\mathfrak{p}}) = (L/K, \mathfrak{p})^{-1} = \tau^{-1},$$

as needed.

From the structure of $G(L/\mathbb{Q})$, we see that the conjugacy class of any element $\sigma$ is $\{\sigma, \sigma^{-1}\}$. By the Chebotarev density theorem 10.3.2, the density of primes such that $(L/\mathbb{Q}, p) = [\sigma] = \{\sigma, \sigma^{-1}\}$ is hence

$$\frac{|[\sigma]|}{[L : \mathbb{Q}]} = \begin{cases} \frac{1}{2h(D)}, & \sigma = \sigma^{-1}, \\ \frac{1}{h(D)}, & \text{else,} \end{cases}$$

as needed. □

# §7 Introduction to the Langlands program

sec:intro-langlands In this section, we'll give the big picture, and be content with morally, rather than mathematically correct, statements.

Much of modern number theory is occupied with the relationship between the following three objects.

1. Algebraic varieties, i.e. polynomial equations.

2. Galois representations, i.e. continuous functions from $G(\overline{K}/K)$ to algebraic groups such as $GL_n(\mathbb{C})$.

3. Automorphic forms, i.e. continuous functions defined on an algebraic group on the ideles, such as $\mathrm{GL}_n(\mathbb{A}_K)$, and satisfying certain conditions.

The relationship between Galois representations and automorphic forms is known as the Langlands correspondence. More precisely, there is a conjectural correspondence

$$\left\{ \begin{array}{c} \text{cuspidal automorphic} \\ \text{representations of } \mathrm{GL}_n(\mathbb{A}_K) \\ \text{algebraic at } \infty \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{irreducible continuous} \\ G(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{C}) \ . \\ \text{algebraic at } \ell \end{array} \right\}$$

We can define $L$-series from both Galois representations and automorphic forms. $L$-series from Galois representations arise more naturally in number theory (because it is relatively easy to go from algebraic varieties to Galois representations), but as automorphic forms are analytic objects, $L$-series of automorphic forms are known to satisfy more properties. The Langlands correspondence allows us to show that $L$-series of Galois representations arise from automorphic forms, hence have nice analytic properties as well. This allows us to prove various results about algebraic varieties, such as density theorems on the number of solutions over finite fields, for example the Sato-Tate conjecture.

We first give some more precise definitions, then describe this relationship in the 1-dimensional abelian case (which we have in fact proved!), and then give an overview of how it generalizes.

## 7.1 Definitions

**Definition 7.1:** Let $k$ be a topological field (for instance, $\mathbb{C}$ or $\mathbb{Q}_\ell$), and let $V \cong k^n$ be a $n$-dimensional vector space over $k$. A $n$-dimensional **Galois representation** of $K$ over $k$ is a continuous homomorphism

$$\rho : G(K^s/K) \to \mathrm{GL}(V) = \mathrm{GL}_n(k).$$

Let $\mathfrak{p}$ be a prime of $K$. We say $\rho$ is **unramified** at $\mathfrak{p}$ if $I_\mathfrak{p}(K^s/K) \subseteq \ker(\rho)$.

Let $K$ be a number field. Let $\mathrm{Frob}(\mathfrak{p})$ be a Frobenius element of $\mathfrak{p}$ in $K_\mathfrak{p}$ (defined in $G(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ up to $I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$). Define the (modified) **characteristic polynomial** of $\rho$ at $\mathfrak{p}$ to be

$$P_\rho(X) := \det(1 - X \cdot \rho(\mathrm{Frob}(\mathfrak{p}))|V^{I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})}).$$

(Here, $V^{I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})}$ denotes the subspace of $V$ fixed by the inertia group. $P_\rho(X)$ is well-defined because $\mathrm{Frob}(\mathfrak{p})$ is defined up to $I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$, and $I(\overline{K_\mathfrak{p}}/K_\mathfrak{p}) \subseteq \ker(\rho|_{V^{I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})}})$. In particular, if $\rho$ is unramified at $\mathfrak{p}$, then $V = V^{I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})}$.)

We can now define the $L$-function associated to a Galois representation.

**Definition 7.2:** In the above, suppose $V$ is a complex vector space and $K$ is a number field. The **local $L$-factor** at a prime $\mathfrak{p}$ is

$$L_\mathfrak{p}(\rho, s) = P_\rho(\mathfrak{N}\mathfrak{p}^{-s})^{-1}.$$

The **Artin $L$-function** of $\rho$ is[4]

$$L(\rho, s) = \prod_\mathfrak{p} L_\mathfrak{p}(\rho, s).$$

We have the following conjecture.

**Conjecture 7.3** (Artin's conjecture)**:** Every Artin $L$-function has analytic continuation to $\mathbb{C}$ and satisfies a functional equation.

## 7.2 Class field theory is 1-dimensional Langlands

For a different take on some of these ideas, with concrete examples, see Dalawat [6].

### 7.2.1 Galois representations are automorphic representations

We rephrase global class field theory in the form that generalizes under the Langlands program.

[4]Sometimes infinite places are included. The factors at infinite places take more thought to define so we exclude them here.

**Theorem 7.4** (Rephrase of GCFT)**:** thm:rephrase-gcft There is a bijection between continuous homomorphisms $\chi : \mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^0} \to \mathbb{C}^\times$ and continuous homomorphisms $\rho : G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$, given by the following.

$$\{\chi : \mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^0} \to \mathbb{C}^\times\} \leftrightarrow \{\rho : G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})\}$$
$$\chi \mapsto \chi \circ \phi_K^{-1}$$

*Proof.* From Theorem 10.6.4, the Artin map gives a topological isomorphism $\mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^0} \to G(K^{\mathrm{ab}}/K)$. It remains to note that any function $G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$ factors through $G(\overline{K}/K)^{\mathrm{ab}} = G(K^{\mathrm{ab}}/K)$, since $\mathrm{GL}_1(\mathbb{C})$ is abelian. □

The functions on the left side have a special name.

**Definition 7.5:** A **Hecke character** is a continuous homomorphism $\mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^0} \to \mathbb{C}^\times$, or equivalently, a homomorphism

$$\chi : \mathbf{C}_K \to S^1 := \{x \in \mathbb{C} : |x| = 1\}$$

with finite image. The **conductor** of $\chi$ is the smallest modulus $\mathfrak{m}$ such that $\chi$ factors through $\mathbb{A}_K^\times/K^\times\mathbb{U}_K(1,\mathfrak{m}) \cong C_K(\mathfrak{m})$.

The homomorphisms $\chi : \mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^0} \to \mathbb{C}$ are "automorphic functions" on $\mathrm{GL}_1(\mathbb{A}_K)$, a.k.a. Hecke characters, and the homomorphisms $\rho : G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$ are 1-dimensional "Galois representations." Our correspondence is unsatisfactory, however, because we would like to get all continuous homomorphisms $\mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$, not just those factoring through $\mathbb{A}_K^\times/\overline{K^\times(K_\infty^\times)^0}$. Since $G(K^{\mathrm{ab}}/K)$ has the profinite topology, any continuous homomorphism $G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$ must have finite image, while functions $\mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ can have infinite image. To remedy this, we introduce functions $G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$ with infinite image (no longer continuous under the complex topology).

For simplicity, we just consider the case of $\mathbb{Q}$.

**Example 7.6:** We say a function $\pi : \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \to \mathbb{C}$ is **algebraic at** $\infty$ if $\pi(i_{\mathbb{R}}(x)) = \mathrm{sign}(x)^m|x|^n$ for some $m \in \{0,1\}$ and $n \in \mathbb{Z}$. We characterize all the continuous homomorphisms $\pi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ ("**Grössencharacters**") that are algebraic at $\infty$.

It is enough to introduce 1 more character. Let $\ell$ be a prime of $\mathbb{Q}$. Let $|\cdot| : \mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times$ denote the map $|\mathbf{x}| = \prod_{v\in V_{\mathbb{Q}}} |x_v|_v$, and define $\chi_\ell$ by

$$\chi_\ell :\ G(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow G(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = G(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \xrightarrow{\cong} \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times \twoheadrightarrow \mathrm{GL}_1(\mathbb{Z}_\ell).$$

(We say $\chi_\ell$ is "**algebraic at** $\ell$." Note there is a noncanonical field isomorphism $\overline{\mathbb{Q}_\ell} \cong \mathbb{C}$, so we can think of $\mathrm{GL}_1(\mathbb{Z}_\ell)$ as being "inside" $\mathrm{GL}_1(\mathbb{C})$.)

Every continuous homomorphism $\pi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ algebraic at $\infty$ is in the form $|\cdot|^n \cdot \chi$, where $\chi$ is a Hecke character. We can extend the correspondence in Theorem 7.4 by associating $|\cdot|$ with $\chi_\ell$:

$$\pi = |\cdot|^n \cdot \chi \leftrightarrow \chi_\ell^n \cdot (\chi \circ \phi_K^{-1})$$

where the right-hand side is now viewed in $\mathbb{Q}_\ell$ instead of $\mathbb{C}$.

### 7.2.2 Artin $L$-functions are Hecke $L$-functions

Associated to each Hecke character is a $L$-function.

**Definition 7.7:** Let $\chi$ be a Hecke character and $\mathfrak{m}$ be the conductor of $\chi$. The ***L*-function** associated to $\chi$ is

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

Because $\chi$ admits a modulus, Hecke $L$-series have nice analytic properties.

**Theorem 7.8** (Hecke, Tate)**:** thm:l-analytic-cont Every Hecke $L$-series admits an analytic continuation to $\mathbb{C}$ and satisfies a functional equation.

For the details, see Tate's thesis in [3].

**Theorem 7.9:** Any 1-dimensional Artin $L$-function is a Hecke $L$-function. Hence it has analytic continuation and satisfies a functional equation.

*Proof.* Let $\rho : G(\overline{K}/K) \to \mathrm{GL}_1(\mathbb{C})$ be a 1-dimensional representation. By Theorem 7.4, $\rho(\Phi_{\mathfrak{p}}) = \chi(\mathfrak{p})$ for some Hecke character $\chi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$. Let $\mathfrak{m}$ be the modulus of $\rho$; note it is also the conductor for $\chi$. Then

$$L(\rho, s) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\rho(\Phi_{\mathfrak{p}})\mathfrak{N}\mathfrak{p}^{-1}} = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})\mathfrak{N}\mathfrak{p}^{-s}} = L(\chi, s).$$

□

This theorem is another way of saying that the Artin map factors through a modulus, and this is basically what allowed us to get all the density results in this chapter.

### 7.2.3 Algebraic varieties and Galois representations

We give examples of how to get Galois representations from algebraic varieties.

First consider the variety $\overline{\mathbb{Q}}^\times = \left\{x \in \overline{\mathbb{Q}} : x \neq 0\right\}$. It is a group under multiplication, and the torsion points $\overline{\mathbb{Q}}^\times[m]$ are exactly the roots of unity $\mu_m$. We can define a Galois representation by considering the action of $G(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $l$-power roots of unity. Define the Tate module of $\overline{\mathbb{Q}}^\times$ by

$$T_\ell(\overline{\mathbb{Q}}^\times) = \varprojlim_n \overline{\mathbb{Q}}^\times[\ell^n] = \varprojlim_n \mu_{\ell^n} \cong \mathbb{Z}_\ell.$$

Then $G(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on $T_\ell(\overline{\mathbb{Q}}^\times)$ so we get a representation

$$\rho : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell(\overline{\mathbb{Q}}^\times)) \cong \mathrm{Aut}(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_1(\mathbb{Q}_\ell)$$

sending the element $\phi_{\mathbb{Q}}(p)$ to $p$. The corresponding $L$-function is just a translate of the $\zeta$ function, missing the factor $\ell$: $\prod_{p\neq\ell}\frac{1}{1-p^{1-s}}$. This construction is a good analogy for what we will eventually do with elliptic curves, although it is a bit too "trivial" to capture any significant number theory facts.

We give another example, with equations in 1 variable, which is a bit less natural but show more of the number theory. Consider the variety defined by $f(X)=0$ where $f\in K[X]$ is a irreducible polynomial. Let $\alpha$ be a root, and $L$ be the Galois closure of $K(\alpha)$ over $K$. Let $\alpha_1,\ldots,\alpha_n$ be the roots of $f$ in $L$. $G(\overline{K}/K)$ acts by permuting the $\alpha_i$, so we get a representation $G(\overline{K}/K)\to S_n$. We can embed $S_n$ in some general linear group, to get $\rho: G(\overline{K}/K)\to \mathrm{GL}_m(k)$ for some $k$. Then to find how many roots $f$ has modulo $\mathfrak{p}$, we can look at the trace of $\rho(\mathrm{Frob}(\mathfrak{p}))$.

For example, consider $f(X)=X^3-X-1$ over $\mathbb{Q}$. We get a representation $\rho: G(\overline{K}/K)\to S_3\to \mathrm{GL}_2(\mathbb{C})$, where we embed $S_3\hookrightarrow \mathrm{GL}_2(\mathbb{C})$ as follows: we have a natural permutation representation $S_3\hookrightarrow \mathrm{GL}_3(\mathbb{C})$; now take out the trivial representation to get $S_3\hookrightarrow \mathrm{GL}_2(\mathbb{C})$. From this description we have $N_p(f)=\mathrm{Tr}(\rho(\mathrm{Frob}(\mathfrak{p})))+1$, so we can get the number of solutions of $X^3-X-1\equiv 0 \pmod p$ from looking at the trace of Frobenius. Constructing the $L$-function, the trace of Frobenius becomes the coefficient of $\frac{1}{p^s}$. Now $\rho$ comes from an automorphic form, so $L$ comes from a 2-dimensional automorphic form, i.e. a modular form. We can write this modular form explicitly using theta functions or as an eta quotient. At the end of the day, we have this striking fact: For $p\neq 23$, the number of solutions of $X^3-X-1\equiv 0 \pmod p$ is $N_p(f)=a_p+1$, where $a_p$ is the coefficient of the modular form

$$q\prod_{k=1}^{\infty}(1-q^k)(1-q^{23k})=\frac{1}{2}\sum_{(x,y)\in\mathbb{Z}^2}(q^{x^2+xy+6y^2}-q^{2x^2+xy+3y^2})=\sum_{n=1}^{\infty}a_nq^n.$$

(See Serre's article [15].) In this example we have traced out a relationship

(algebraic variety)$\to$(Galois representation)$\to$(automorphic form).

## 7.3 Elliptic curves and 2-dimensional Langlands

### 7.3.1 Galois representations and automorphic representations

**Definition 7.10:** A 2-dimensional automorphic form is a continuous function $\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ satisfying certain conditions.

A large class of 2-dimensional automorphic forms can be related to modular forms. A holomorphic function $f(z):\mathcal{H}\to\mathbb{C}$ is a **modular function** of weight $k$ for a congruence subgroup $\Gamma\subseteq\mathrm{GL}_2(\mathbb{Z})$ if

$$f(\gamma z)=(cz+d)^kf(z)\text{ for all }\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma.$$

If $\Gamma=\Gamma_0(N):=\left\{M\in\mathrm{SL}_2(\mathbb{Z}):M\equiv\begin{pmatrix}*&*\\0&*\end{pmatrix}\pmod N\right\}$, we say $f$ is of **level** $N$. Here $\mathcal{H}$ denotes the upper half-plane $\{z:\Im(z)>0\}$ and $\gamma z=\frac{az+b}{cz+d}$.

A modular function is a **modular form** if it is holomorphic at cusps of $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. A **cusp form** is a modular form that vanishes at the cusps.

There is a way to go from modular forms to Galois representations; this is better understood than going in the opposite direction. One of the biggest theorems in the 2-D case is Serre's conjecture, now a theorem, that tells us that we can go from Galois representations to modular forms in certain cases.

**Definition 7.11:** We say a Galois representation is **modular** if there exists a cusp form $f$ of some level $N$ and a finite set $S$ such that

$$f = \sum_{n=1}^{\infty} a_n q^n, \qquad \mathrm{Tr}(\rho(\mathrm{Frob}(p))) = a_p \text{ for } p \notin S.$$

**Theorem 7.12** (Serre's conjecture; Khare, Wintenberger)**:** Any irreducible odd Galois representation $\rho : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is modular.

### 7.3.2 Elliptic curves and Galois representations

Given an elliptic curve, we can define a Galois representation by looking at its torsion points.

**Definition 7.13:** Let $E$ be an elliptic curve over a number field $K$. It is known that the $m$-torsion points $E[m]$ over $\overline{K}$ satisfy

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$

(See Silverman [16, III.6.4].)

Define the $\ell$-adic **Tate module** of $E$ by

$$T_\ell E := \varprojlim_n E[\ell^n] \cong \mathbb{Z}_\ell^2.$$

As $G(\overline{K}/K)$ acts on $E[\ell^n]$ for each $n$, it acts on $T_\ell E$, so we get a map

$$G(\overline{K}/K) \to \mathrm{Aut}\, T_\ell E = \mathrm{GL}_2(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell),$$

called the $\ell$-adic **Galois representation** of $E$.[5]

Thus we can define the $L$-series of an elliptic curve, by defining it as the $L$-series of the corresponding Galois representation. (Roughly speaking, this definition is independent of the choice of $\ell$.) We'll flesh out this definition in Section 16.7. Thus we have the (tentative) correspondences

$$eq : ec - lang(\text{Elliptic curves}) \dashrightarrow (\text{Galois representations}) \dashrightarrow (\text{cusp forms}) \tag{15.10}$$

$$eq : ec - lang2(L\text{-series of elliptic curve}) \dashrightarrow (L\text{-series of modular form}). \tag{15.11}$$

[5]Alternatively, let $V_\ell E := T_\ell E \otimes \mathbb{Q}$ and consider $G(\overline{K}/K)$ as acting on $V_\ell E$.

Again, more is known about $L$-series of modular forms since modular forms have nice analytic properties and transformation properties. The theory of Jacquet-Langlands establishes analytic continuation and functional equations for $L$-series coming from modular forms.

This relationships in (15.10) and (15.11) are involved in the proof of two big theorems.

1. We now know the dotted lines in (15.10) are true, thanks to the following.

   **Theorem 7.14** (Modularity Theorem; Taniyama-Shimura-Weil)**:** All elliptic curves are modular.

   The heart of this proof is in showing that the Galois representations associated to the elliptic curves come from modular forms. This theorem (or rather, its earlier version with semistable elliptic curves) is what allowed the proof of Fermat's last theorem: there is no nontrivial solution to $a^n + b^n = c^n$ for $n > 2$. A nontrivial solution would give rise to an elliptic curve associated to a modular form that does not exist.

2. By working with $L$-functions of the elliptic curves, and reinterpreting them as $L$-functions of certain automorphic forms as in (15.11), one can prove the following.

   **Theorem 7.15** (Sato-Tate conjecture; Barnet-Lamb, Geraghty, Harris, Taylor)**:** Let $E$ be an elliptic curve without complex multiplication, and let $E(\mathbb{F}_p)$ denote the set of solutions to $E$ over $\mathbb{F}_p$. The density of primes $p$ with $|E(\mathbb{F}_p)| \in [p+1+a\sqrt{p}, p+1+b\sqrt{p}]$, for $-1 \le a \le b \le 1$ is

   $$d(\{p : |E(\mathbb{F}_p)| \in [p+1+a\sqrt{p}, p+1+b\sqrt{p}]\}) = \frac{2}{\pi}\int_a^b \sqrt{1-x^2}\,dx.$$

   By the correspondence between elliptic curves and modular forms, another way to phrase this theorem is that the distribution of coefficients of certain modular forms is the same "semicircle" distribution.

   This theorem is like the elliptic curve analogue of the Dirichlet's theorem on the distribution of primes in congruence classes.

# §8 Problems

3.1 (from Serre, [15]) Using Chebotarev's Density Theorem, prove the following.

**Theorem:** Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $n \ge 2$. Let $N_p(f)$ denote the number of zeros of $f$ in $\mathbb{F}_p$. Then the set $P_0(f)$ of primes with $N_p(f) = 0$ has a density $c_0(f)$. Moreover, $c_0(f) \ge \frac{1}{n}$, with strict inequality if $n$ is not a prime power.

You may use the following theorem from group theory.

**Theorem** (Jordan)**:** Let $G$ is a group acting transitively on a finite set $S$ with $n \geq 2$ elements. There exists $g \in G$ having no fixed point in $S$. If $n$ is not a prime power, then there exist at least 2 such $g$.

3.2 (All primes divide some coefficient of $\Delta$) Let $\ell$ be a given prime, and $K_\ell$ be the maximal extension of $\mathbb{Q}$ ramified only at $\ell$. Given that there is a continuous homomorphism (a.k.a. Galois representation)

$$\tilde{\rho}_\ell : G(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

such that

$$\mathrm{Tr}(\tilde{\rho}_\ell(\mathrm{Frob}_{K_\ell/\mathbb{Q}}(p))) = \tau(p)$$

for all $p \neq \ell$, and that there is an element in $\mathrm{im}(\tilde{\rho}_\ell)$ with trace 0, prove that a positive proportion of primes $p$ have the property that

$$\ell \mid \tau(p).$$

*Note.* Here $\tau$ is *Ramanujan's tau function*, the coefficients of a certain modular form $\Delta$. For more on the relationship between Galois representations and congruences for coefficients of modular forms, see Birch and Swinnerton-Dyer [18].

4.1 In Section 4, we showed that $L/K$ is abelian iff the primes that split can be characterized by a modular condition. In this problem, we do more: given a Galois extension $L/K$, characterize the maximal abelian subextension by looking at the primes that split.

(a) Let $\mathfrak{m}$ be a modulus for $K$, and suppose $L/K$ is a Galois extension. Let $H_\mathfrak{m}$ be the subset of the ray class field $C_K(\mathfrak{m})$ defined as follows:

$$H_\mathfrak{m} = \{\mathfrak{K} : \text{There exists } \mathfrak{p} \in \mathfrak{K} \text{ such that } \mathfrak{p} \text{ splits completely in } L\}.$$

Show that $H_\mathfrak{m}$ is a subgroup of $C_K(\mathfrak{m})$.

(b) Suppose we are given the groups $H_\mathfrak{m}$ for all $\mathfrak{m}$. Characterize the maximal abelian subextension of $L/K$.

6.1 Prove an analogue of Theorem 6.5 for positive discriminants.

6.2 Let $n > 0$ be an integer such that $K = \mathbb{Q}(\sqrt{-n})$ is an imaginary quadratic field, and let

$$Q(x,y) = \begin{cases} x^2 + ny^2, & n \equiv 1 \pmod 4 \\ x^2 + xy + \frac{1-n}{2}y^2, & n \equiv 3 \pmod 4. \end{cases}$$

(a) Find a condition on $G(H_K/K)$ so that for all but a finite number of primes, the primes represented by $Q$ are given by a modulo condition. In other words, find all $n$ such that there exists $m$ and a set of residues $S$ modulo $m$ such that if $p \nmid m$, then $p$ is represented by $Q$ iff $p$ is congruent to a residue in $m$. (Hint: combine the results of Section 4 with Section 6.)

(b) Find some values of $n$ for which $|C(K)| \neq 1$ and such that the primes represented by $Q$ are given by a modulo condition.

(c) Suppose $G(H_K/K)$ satisfies the property you found in part 1. Characterize all $n$, not necessarily prime, such that $Q$ represents $n$. (For simplicity, you can just consider $n \perp m$.) Compare to the statement in Example 4.3.4.)

1. **(Genus theory)** It is useful to group the equivalence classes of quadratic forms with given discriminant into *genera* (plural of genus).

   **Definition 8.1:** Define a similarity relation between primitive quadratic forms of discriminant $d$ as follows. We say $Q_1 \sim Q_2$ if $Q_1$ and $Q_2$ represent the same values in $(\mathbb{Z}/d\mathbb{Z})^\times$. The similarity classes are called **genera**.

   In this problem you will find an easy way to characterize the genera of discriminant $d$.

   (a) Let $H$ be the subgroup of $C(d)$ such that $C(d)/H \cong C(d)[2]$ where $G[n]$ denotes the $n$-torsion subgroup of $G$.
   Prove that $Q_1, Q_2 \in C(d)$ are in the same genera iff $Q_1, Q_2$ are the same in $C(d)/H$.
   In particular, conclude that the number of genera is a power of 2.

   (b) Let $M$ be the ring class field of $K$ and let $L$ denote the subextension of $M/K$ such that $G(L/K) \cong C(d)[2]$. (That is, under the Galois correspondence, $L \subseteq M$ corresponds to $H \subseteq C(d) = G(M/K)$.) Prove that $L/\mathbb{Q}$ is the maximal abelian subextension of $M/\mathbb{Q}$.

   The fact that $L/K$ is abelian, while $M/K$ may not be, makes it much easier to prove results pertaining to a genus of quadratic forms rather than an equivalence class of quadratic forms.

2. (?) Let $f, g \in \mathbb{Q}[X]$ be two irreducible cubic polynomials. How can you determine algorithmically whether $f, g$ have roots $\alpha, \beta$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$? (from `http://math.stackexchange.com/questions/34522/cubic-polynomials-that-generate-rq=1`)

# Chapter 16
# Complex multiplication

ch:CM In this chapter, we combine class field theory with the theory of elliptic curves, first to characterize the maximal abelian extension of $K$, then to illustrate the relationships in Section 15.7 for CM elliptic curves. We will assume basic facts about elliptic curves (for an introduction see Silverman [16, Chapter III]).

We know that every elliptic curve over $\mathbb{C}$ has endomorphism ring either equal to $\mathbb{Z}$ or a quadratic order. In the second case, the elliptic curve is said to have **complex multiplication**. This gives the elliptic curve a lot more structure. On one hand, it is useful algebraically—as we will see, torsion points of a CM elliptic curve give abelian extensions of imaginary quadratic fields. In general, because of the added structure, much more is known about CM elliptic curves than other elliptic curves, and they can act as a kind of "testing ground" or "first case" of general conjectures.

On the other hand, CM elliptic curves have practical uses—for instance, if we take an CM elliptic curve corresponding to a specific endomorphism ring, we can easily compute its order. Hence we can generate an elliptic curve with near-prime order, useful in cryptography. This is much more efficient than generating random elliptic curves and using Schoof's algorithm to find their orders.

There are several big theorems about complex multiplication. In Section 2, we specialize our knowledge about the relationship between elliptic curves over $\mathbb{C}$ and complex tori to CM elliptic curves and build a toolbox of basic facts. However, since we are interested in number theory, we want to take curves defined over $\mathbb{C}$ and define them over $\overline{\mathbb{Q}}$ instead—which we do in Section 3. Once we have these basics, we can then prove the big theorems.

We suppose $E$ has CM by a quadratic order $\mathcal{O} \subset K$ (i.e. $\mathrm{End}(E) \cong \mathcal{O}$), where $K$ is a quadratic extension of $\mathbb{Q}$. Then the following hold.

1. The $j$-invariant $j(E)$ generates the *ring class field* of $\mathcal{O}$ over $K$. In particular, if $\mathcal{O} = \mathcal{O}_K$, then $j(E)$ generates the *Hilbert class field* of $K$, the maximal unramified abelian extension (Theorem 4.4):
$$K(j(E)) = H_K.$$
2. If $E$ is defined over $H_K$, and we adjoin certain functions of torsion points of $E$, then we get the *maximal abelian extension* of $K$ (Theorem 5.4):
$$K(j(E), h(E_{\text{tors}})) = K^{\text{ab}}.$$

Compare this with the Kronecker-Weber Theorem, which says the maximal abelian extension of $\mathbb{Q}$ is generated by roots of unity (torsion points of $\overline{\mathbb{Q}}^\times$).

3. $j(E)$ is moreover an *algebraic integer* (We omit this; see Silverman AT, [17, II.6].)

4. The action of the idele class group sending $K/\mathfrak{a}$ to $K/\mathbf{x}^{-1}\mathfrak{a}$ corresponds to the Galois action on the corresponding elliptic curves, where the Galois action is given by the Frobenius element of $\sigma$. This is the Main Theorem of Complex Multiplication 6.2, and plays an important part in taking moduli spaces initially defined only over $\mathbb{C}$ and defining them over algebraic number fields.

5. The $L$-series of a CM elliptic curve is particularly easy to understand, because it is a product of 2 Hecke $L$-series (Theorem 7.4).

Two "big ideas" we'll consistently see are the following.

1. We expect abelian extensions because for CM elliptic curves (with endomorphism ring $\mathcal{O}_K$, say), the image of the map $G(L/H_K) \hookrightarrow \mathrm{Aut}(E[m])$ commutes with $\mathcal{O}_K$, not just $\mathbb{Z}$ and hence must be abelian, with appropriate $L$.

2. We can use torsion points $E[m]$ to "keep book" on the action of Frobenius, in the same way that we used the roots of unity $\mu_m$ to keep book on the action of Frobenius on $G(\mathbb{Q}(\mu_m)/\mathbb{Q})$.

# §1 Elliptic curves over $\mathbb{C}$

The following theorem helps us understand elliptic curves over $\mathbb{C}$.

**Theorem 1.1:** thm:lattice-ec-eoc Let $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$, where $G_n$ is the Eisenstein series. Let $\Lambda$ be a lattice in $\mathbb{C}$ and $\wp$ be the associated Weierstrass $\wp$-function.

There is a complex analytic isomorphism between the complex torus $\mathbb{C}/\Lambda$ and the elliptic curve over $\mathbb{C}$,

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

given by

$$\Phi(z) = (\wp(z), \wp'(z)).$$

The map $\Phi$ gives an equivalence of categories between the following.

1. Objects: Complex tori $\mathbb{C}/\Lambda$, where $\Lambda$ is a lattice in $\mathbb{C}$.
   Maps: Multiplication-by-$\alpha$ $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ where $\alpha\Lambda_1 \subseteq \Lambda_2$.

2. Objects: Elliptic curves over $\mathbb{C}$.
   Maps: Isogenies.

*Proof.* Silverman [16, VI.5.1.1, 5.3] □

The endomorphism ring of a lattice $\Lambda \subset \mathbb{C}$ is either $\mathbb{Z}$ or an imaginary quadratic order, so the same is true of an elliptic curve $E$ over $\mathbb{C}$. If the endomorphism ring is a quadratic order $\mathcal{O}$, we say $E$ has **complex multiplication** by $\mathcal{O}$.

# §2 Complex multiplication over $\mathbb{C}$

sec:cm-C

## 2.1 Embedding the endomorphism ring

We know the endomorphism ring $\text{End}(E)$ of a CM elliptic curve corresponds to a quadratic order $\mathcal{O}$ but since any quadratic order has conjugation as an isomorphism, we need to specify a way to embed $\text{End}(E)$ into $\mathbb{C}$.

**Example 2.1:** ex:which-i Consider the curve $E : y^2 = x^3 + x$. We note that the endomorphisms

$$\phi_1(x, y) = (-x, iy)$$
$$\phi_2(x, y) = (-x, -iy)$$

both square to $-1$. Which one should we call $[i]$, multiplication by $i$?

Fortunately, we have a way of embedding $\text{End}(\Lambda)$ into $\mathbb{C}$, where $\Lambda$ is the lattice corresponding to $E$, because $\Lambda$ itself is in $\mathbb{C}$. This to give a canonical way of embedding $\text{End}(E)$ into $\mathbb{C}$.

**Proposition 2.2:** pr:normalize-cmec Let $E/\mathbb{C}$ be a CM elliptic curve with complex multiplication by $\mathcal{O}$. There is a unique isomorphism $[\cdot] : \mathcal{O} \xrightarrow{\cong} \text{End}(E)$ satisfying either of the following equivalent conditions.

1. $[\alpha]$ is the unique morphism making the following diagram commute, where the top map is multiplication by $\alpha$.

$$\begin{tikzcd} \mathbb{C}/\Lambda \arrow[r, "m_\alpha"] \arrow[d, "\Phi"] & \mathbb{C}/\Lambda \arrow[d, "\Phi"] \\ E_\Lambda \arrow[r, "{[\alpha]}"] & E_\Lambda \end{tikzcd}$$

2. For any invariant differential $\omega \in \Omega_E$, $[\alpha]^*\omega = \alpha\omega$.

Moreover, we have the following.

3. Define $[\cdot]_1$ and $[\cdot]_2$ for elliptic curves $E_1$ and $E_2$. For any morphism $\phi : E_1 \to E_2$,

$$\phi \circ [\alpha]_1 = [\alpha]_2 \circ \phi.$$

   In other words, multiplication by $\alpha$ commutes with all morphisms.

4. For any $\sigma \in \mathrm{Aut}(\mathbb{C})$,
$$[\alpha]_E^\sigma = [\sigma(\alpha)]_{\sigma(E)},$$
i.e. it commutes with Galois action.

The pair $(E, [\cdot])$ is called a **normalized** elliptic curve. After we prove this proposition, we will assume all CM elliptic curves are normalized.

*Proof.* The uniqueness and existence of $[\alpha]$ satisfying item 1 follows directly from the equivalence of categories (Theorem 1.1).

Define $[\alpha]$ as in item 1. For any invariant differential $\omega$ on $E_\Lambda$, since $\Phi$ is an analytic isomorphism, we can consider its pullback to $\mathbb{C}/\Lambda$; it will be $c\,dz$ for some $c$ (The space of invariant differentials on $\mathbb{C}/\Lambda$ is 1-dimensional.) Clearly, $m_\alpha^*(c\,dz) = c\,d(\alpha z) = \alpha c\,dz$. Transferring this to the bottom row of the commutative diagram gives $[\alpha]^*\omega = \alpha\omega$. For uniqueness, note the map

$$\begin{aligned} \mathrm{Hom}(E_1, E_2) &\hookrightarrow \mathrm{Hom}(\Omega_{E_2}, \Omega_{E_1}) eq : ec - diff - inj \\ \phi &\to \phi^* \end{aligned} \tag{16.1}$$

is injective when all isogenies $E_1 \to E_2$ are separable (in particular, in characteristic 0), i.e. the action of an isogeny of elliptic curves on an invariant differential completely determines the morphism. Taking $E_1 = E_2$ and considering the preimage of multiplication-by-$\alpha$ gives uniqueness in item 2.

A simple diagram chase shows that $(\phi \circ [\alpha]_1)^*$ and $([\alpha]_2 \circ \phi)^*$ act the same way on $\omega \in \Omega_{E_2}$. Then (16.1) gives item 3.

The proof of item 4 is similar. □

**Example 2.3:** The definition using differentials is useful for calculations. Revisiting the above Example 2.1, we see that we should let
$$[i](x, y) = (-x, iy).$$
Indeed, defining $[i]$ in this way, we check that
$$[i]^* \frac{dx}{y} = \frac{d(-x)}{iy} = i\frac{dx}{y}.$$

## 2.2 The class group parameterizes elliptic curves

Let $K$ be an imaginary quadratic field and $\mathcal{O}$ an order inside $K$.

**Definition 2.4:** Let $L$ be a field. Define
$$\begin{aligned} \mathrm{Ell}_L(\mathcal{O}) &= \{\text{elliptic curves } E/L \text{ with } \mathrm{End}(E) \cong \mathcal{O}\} \\ \mathcal{E}\mathrm{ll}_L(\mathcal{O}) &= \frac{\{\text{elliptic curves } E/L \text{ with } \mathrm{End}(E) \cong \mathcal{O}\}}{\text{isomorphism over } L}, \end{aligned}$$

i.e. $\mathcal{E}\text{ll}_L(\mathcal{O})$ is the set of elliptic curves over $L$ whose endomorphism ring is $\mathcal{O}$. If we omit $L$, we assume $L = \mathbb{C}$.

If $E \in \text{Ell}(\mathcal{O})$, then its corresponding lattice $\Lambda$ must be homothetic to a fractional ideal of $\mathcal{O}$: indeed, we can scale the lattice so that $1 \in \Lambda$; then $\mathcal{O} \subseteq \Lambda$ so $\Lambda \subseteq K$; since it is a lattice it must be a fractional $\mathcal{O}$-ideal. Now note an $\mathcal{O}$-ideal $\mathfrak{a}$ has endomorphism ring $\mathcal{O}$ iff $\mathfrak{a}$ is a *proper* ideal (see Definition 4.4.5).[1] Hence we get a correspondence between isomorphism classes of elliptic curves $[E] \in \mathcal{E}\text{ll}(\mathcal{O})$ and proper $\mathcal{O}$-ideals up to homothety. However, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic iff $\lambda\mathfrak{a} = \mathfrak{b}$ for some $\lambda$, i.e. iff they are equivalent in the class group. Thus the class group of $\mathcal{O}$ parameterizes all isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$. This is summarized in the following.

$$\mathcal{E}\text{ll}(\mathcal{O}) = \frac{\{\text{elliptic curves } E/\mathbb{C} \text{ with } \text{End}(E) \cong \mathcal{O}\}}{\text{isomorphism over } \mathbb{C}} = \frac{\{\text{proper fractional } \mathcal{O}\text{-ideal}\}}{\text{principal } \mathcal{O}\text{-ideals}} = C(\mathcal{O}).$$

We state this as a theorem.

**Theorem 2.5:** thm:ell=cl We have a bijection

$$\mathcal{E}\text{ll}(\mathcal{O}) \cong C(\mathcal{O})$$

where $[E] \in \mathcal{E}\text{ll}(\mathcal{O})$ is sent to a $[\mathfrak{a}]$, where $\mathfrak{a}$ is a fractional ideal homothetic to the lattice corresponding to $E$.

We get much more than this, however. $\mathcal{E}\text{ll}(\mathcal{O})$ is a priori just a set; however, $C(\mathcal{O})$ is a *group*. We can define the action of $I(\mathcal{O})$ on $\text{Ell}(\mathcal{O})$ since $I(\mathcal{O})$ acts on lattices. This action will descend to an action of $C(\mathcal{O})$ on $\mathcal{E}\text{ll}(\mathcal{O})$, since isomorphic elliptic curves correspond to equivalent ideals.

**Theorem 2.6:** There is a group action of $\text{Id}(\mathcal{O})$ on $\text{Ell}(\mathcal{O})$ given by

$$\mathfrak{a}E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

where $E_\Lambda$ denotes the elliptic curve corresponding to the lattice $\Lambda$.

This descends to a simply transitive group action of $C(\mathcal{O})$ on $\mathcal{E}\text{ll}(\mathcal{O})$.

*Proof.* Just check that if $\Lambda$ has endomorphism ring $\mathcal{O}$, then so does the lattice $\mathfrak{a}^{-1}\Lambda$. (Note that $\mathfrak{b}L$ is defined by $\{s\alpha : s \in \mathfrak{b}, \alpha \in L\}$.)

For the second part, note that $E_\Lambda \cong \mathfrak{a}E = E_{\mathfrak{a}^{-1}\Lambda}$ iff $\Lambda$ and $\mathfrak{a}^{-1}\Lambda$ are homothetic, i.e. $\mathfrak{a}$ is principal. □

**Remark:** Another way of saying that $C(\mathcal{O})$ acts simply transitively on $\mathcal{E}\text{ll}(\mathcal{O})$ is that $\mathcal{E}\text{ll}(\mathcal{O})$ is a **torsor** or **principal homogeneous space** for $C(\mathcal{O})$.

[1] When $R = \mathcal{O}_K$, all ideals are proper, so this distinction is not important. The reader unfamiliar with non-maximal orders can take $R = \mathcal{O}_K$ throughout.

This action will be fundamental to our understanding of CM elliptic curves. Later on we will relate this to the Galois action. The interplay between these two actions is the source for much of the richness of CM theory.

## 2.3 Ideals define maps

For any $n \in \mathbb{Z}$ and any elliptic curve $E$, $n$ defines the multiplication by $n$ map $[n] : E \to E$. When $E$ has CM, we saw in Theorem 2.2 that $\alpha \in \mathcal{O}$ defines (canonically) the multiplication by $\alpha$ map $[\alpha] : E \to E$. We now extend this to *ideals*: if $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal, $\mathfrak{a}$ determines a "multiplication by $\mathfrak{a}$" map. The only difference is that $[\mathfrak{a}]$ is now a map $E \to \mathfrak{a}E$.

**Definition 2.7:** Let $E \in \mathrm{Ell}(\mathcal{O})$ correspond to the lattice $\Lambda$. Let $\mathfrak{a}$ be a proper integral ideal of $\mathcal{O}$. We have $\mathfrak{a}R \subseteq R$, so $\mathfrak{a}$ determines a map $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$, sending $z \mapsto z$. Define the multiplication by $\mathfrak{a}$-map as the corresponding map on elliptic curves

$$[\mathfrak{a}] : E \to E_{\mathfrak{a}^{-1}\Lambda} = \mathfrak{a}E.$$

**Proposition 2.8:** pr:E[a] Do we need $R = \mathcal{O}_K$? Let $E \in \mathrm{Ell}(\mathcal{O}_K)$. We have the following.

1. The kernel of $[\mathfrak{a}]$ (the "$\mathfrak{a}$-torsion points") is
$$E[\mathfrak{a}] := \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\} \cong \mathcal{O}_K/\mathfrak{a}.$$
2. The degree of $[\mathfrak{a}]$ is
$$\deg([\mathfrak{a}]) = |E[\mathfrak{a}]| = \mathfrak{N}(\mathfrak{a}),$$
and in particular, $\deg([\alpha]) = |E[\alpha]| = \mathrm{Nm}_{K/\mathbb{Q}}(\alpha)$.

*Proof.* Silverman AT [17, pg. 102-3]. □

# §3 Defining CM elliptic curves over $\overline{\mathbb{Q}}$

sec:cm-Q We show that we do not lose anything if we just consider elliptic curves over $\overline{\mathbb{Q}}$ instead of over $\mathbb{C}$. To do this, we look at the $j$-invariants.

**Proposition 3.1:** pr:j-alg Suppose $E$ is an elliptic curve with CM by a quadratic order $\mathcal{O}$. Then $j(E) \in \overline{\mathbb{Q}}$, i.e. $j(E)$ is algebraic.

*Proof.* Let $\sigma$ be any automorphism of $\mathbb{C}$ over $\mathbb{Q}$. We look at how $\sigma$ acts on $j(E)$.

Note that $E^\sigma$ is defined by taking any equation for $E$ and operating on all the coefficients of $E$ by $\sigma$, so $\sigma(j(E)) = j(E^\sigma)$.

First note that $\mathrm{End}(E) \cong \mathrm{End}(E^\sigma)$ by the map $\phi \mapsto \phi^\sigma$. Hence $\mathrm{End}(\sigma(E)) = \mathcal{O}$ as well. But $C(\mathcal{O})$ is finite, and as $|C(\mathcal{O})| = |\mathcal{E}\mathrm{ll}(\mathcal{O})|$ (Theorem 2.5) we see that the $E^\sigma$ lie in finitely many isomorphism classes. Because isomorphic elliptic curves have the same $j$-invariant, there are a finite number of possibilities for $j(E^\sigma)$.

As $\{\sigma(j(E)) : \sigma \in \mathrm{Aut}(\mathbb{C})\}$ is finite, $j(E)$ must be algebraic. □

This allows us to prove the following.

**Theorem 3.2:** thm:ell-c-q We have

$$\mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathcal{O}) \cong \mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}).$$

*Proof.* We use the following properties of the $j$-invariant. ([16, III.1.4])

1. For every $j \in K$, there exists an elliptic curve $E/K$ with $j(E) = j$.

2. Let $K$ be an algebraically closed field and $E_1$, $E_2$ be elliptic curves defined over $K$. Then $E_1 \cong E_2$ over $K$ iff $j(E_1) = j(E_2)$. (The backwards direction does not necessarily hold if $K$ is not algebraically closed.)

We show that the map

$$eq : ellqc\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}) \to \mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathcal{O}) \tag{16.2}$$

is an isomorphism (of sets, in fact, of $C(\mathcal{O})$-modules). The map is well-defined, because any automorphism over $\overline{\mathbb{Q}}$ is an automorphism over $\mathbb{C}$.

By Lemma 3.1, if $[E] \in \mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathcal{O})$ then $j(E) \in \overline{\mathbb{Q}}$. By item 1, there exists an elliptic curve $E'$ defined over $\overline{\mathbb{Q}}$ with $j(E') = j(E)$. Then $E'$ is isomorphic to $E$ over $\mathbb{C}$. Thus the map (16.2) above is surjective. It is injective because if $E, E'$ are defined over $\overline{\mathbb{Q}}$ and isomorphic over $\mathbb{C}$, then item 2 says $j(E) = j(E')$; and the other direction of item 2 says that $E \cong E'$ over $\overline{\mathbb{Q}}$. □

It is also important to know what fields we can define elliptic curves and isogenies over.

**Proposition 3.3:** Suppose $E$ is an elliptic curve with CM by $\mathcal{O} \subset K$, where $K$ is an imaginary quadratic field.

1. If $E$ is defined over $L$ then endomorphisms of $E$ can be defined over $LK$.

2. If $E_1, E_2$ are defined over $L$ then there exists a finite extension $M/L$, so that every isogeny $E_1 \to E_2$ is defined over $M$.

*Proof.* For item 1, note that all endomorphisms are in the form $[\alpha]$ and use Proposition 2.2(4).

For item 2, first we claim that any isogeny $\phi$ is defined over a finite extension of $L$. For any $\sigma \in \mathrm{Aut}(\mathbb{C})$ fixing $L$, $\phi^\sigma$ is a map $E_1 \to E_2$ having the same degree as $\phi$. Any isogeny is determined by its kernel, up to automorphism of $E_1$ and $E_2$. As $E_1$ has a finite number of subgroups of given index and $\deg(\phi) = \ker(\phi)$, there are finitely many isogenies of a given degree. Hence $\{\phi^\sigma : \sigma \in G(\mathbb{C}/L)\}$ is finite, showing $\phi$ is defined over a finite extension of $L$.

Now $\mathrm{Hom}(E_1, E_2)$ is a finitely generated group, so we can take the field of definition for a finite set of generators. □

# §4 Hilbert class field

## 4.1 Motivation: Class field theory for $\mathbb{Q}(\zeta_n)$ and Kronecker-Weber

sec:kw-cm

### 4.1.1 The case of $\mathbb{Q}$

First we give some motivation for the next two sections by making an analogy with class field theory for $\mathbb{Q}(\zeta_n)$. We can think of $\mu_n$, the $n$th roots of unity, as the analogue of $E[n]$: $\mu_n$ are the $n$-torsion points of the group variety $\overline{\mathbb{Q}}^\times$ under multiplication, and $E[n]$ are the $n$-torsion points of an elliptic curve. To emphasize this analogy, we write $K^\times[n]$ to denote the $n$th roots of unity in $\overline{K}$.

Recall how we established class field theory for $\mathbb{Q}(\zeta_n)$: given a prime $p$, we want to find $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$. To do this we looked at the action of $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ on $\mathbb{Q}^\times[n] = \mu_n$, by taking everything modulo $p$. We know by definition of $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ how it must act on the residue field extension $l/\mathbb{F}_p$ and hence on $\mathbb{F}_p^\times[n]$. Suppose $p \nmid n$. Because the maps

$$\begin{aligned} \mathbb{Q}^\times[n] &\hookrightarrow \mathbb{F}_p^\times[n] \\ \operatorname{End}(\mathbb{Q}^\times[n]) &\hookrightarrow \operatorname{End}(\mathbb{F}_p^\times[n]) eq:end-inj \end{aligned} \tag{16.3}$$

are injective (the first is because $p \nmid n$ and the second is a direct consequence of the first), once we know how $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts on $\mathbb{F}_p^\times[n]$, we know it acts on $\mathbb{Q}_p^\times[n]$, so we know exactly what automorphism it is:

$$(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})(\zeta_n) = \zeta_n^p.$$

In particular, since $\zeta_n$ is a $n$-torsion point (i.e. $\zeta_n^n = 1$) this only depends on $p \pmod n$. Hence we get the Artin map $\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ factoring through the modulus $\infty n$:[2]

$$\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} : I_{\mathbb{Q}}/I_{\mathbb{Q}}(1, n\infty) \xrightarrow{\cong} G(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Finally, since every modulus divides $\infty n$ for some $n$, we get the Kronecker-Weber Theorem

$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_\infty) = \mathbb{Q}(\mathbb{Q}^\times[\infty]).$$

In summary, we found the ray class groups and thus the maximal abelian extension by looking at how $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ acted on $\mathbb{Q}^\times[n]$:

*thm : max − ab − Q*

$$\begin{tikzcd} & \mathbb{Q}^\times[n] \arrow[r, dotted, "\widetilde{\bullet}", "\text{reduction}"'] & \mathbb{F}_p^\times[n] \\ & \circlearrowright & \circlearrowright \\ I_{\mathbb{Q}}/P_{\mathbb{Q}}(1, n\infty) \arrow[r, "\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}"] & G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \arrow[r, dotted, "\widetilde{\bullet}"] & G(\mathbb{F}_p(\zeta_n)/\mathbb{F}_p). \end{tikzcd} \tag{16.4}$$

[2]The $\infty$ is a technical detail coming from the fact that $\mathbb{Q}$ is totally real.

#### 4.1.2 The case of $K$

One big difference when we're working over an imaginary quadratic field $K$ is that while we had $C_{\mathbb{Q}} = 1$, we have $C_K$ is nontrivial in general. This corresponds to the fact that there is only 1 nonisomorphic "version" of $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times$, but multiple elliptic curves with endomorphism ring by the same order $\mathcal{O}$. Hence $G(K^{\text{ab}}/K)$ no longer operates on the same elliptic curve. Instead we have to analyze it in two steps.

1. Consider the action of $G(H_K/K)$ on $\mathcal{E}\text{ll}_{\overline{\mathbb{Q}}}(\mathcal{O})$, i.e. equivalence classes of elliptic curves with CM by $\mathcal{O}$.

2. Consider the action of $G(K^{\text{ab}}/H_K)$ on the torsion points $E_{\text{tors}}$ of a single elliptic curve.

In both cases, we will understand the action by looking at how the Frobenius elements of the Galois groups act.

#### 4.1.3 The case of $K$: Part 1

We have two natural actions on the set of elliptic curve $\mathcal{E}\text{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$, namely the action of $G(\overline{K}/K)$ and $C(\mathcal{O}_K)$. Our first task is to relate these, i.e. find a dotted map that preserves the action on $\mathcal{E}\text{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$:

$$eq : G - cl - compat \qquad \begin{tikzcd} & \mathcal{E}\text{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) & \\ G(\overline{K}/K) \arrow[ur, phantom, "\circlearrowright"] \arrow[rr, dotted] & & C(\mathcal{O}_K). \arrow[ul, phantom, "\circlearrowright"] \end{tikzcd} \tag{16.5}$$

We'll see that this map factors through $G(L/K)$ where $L = K(j(E))$. We have a map $\psi_{L/K} : I_K^{\mathfrak{f}}/P_K(1, \mathfrak{f}) \to G(L/K)$; we show that $\mathfrak{f} = 1$ and the composition of the two maps is an isomorphism, and that in fact we have

$$eq : G - cl - compat2 \qquad \begin{tikzcd} & & \mathcal{E}\text{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) & \\ I_K/P_K \arrow[r, "\Psi_{L/K}"] \arrow[rrr, dotted, bend right, "\mathfrak{a} \mapsto [\mathfrak{a}]"'] & G(L/K) \arrow[ur, phantom, "\circlearrowright"] \arrow[rr] & & C(\mathcal{O}_K). \arrow[ul, phantom, "\circlearrowright"] \end{tikzcd} \tag{16.6}$$

We establish (16.6) by looking at the reduction of the elliptic curves modulo some $\mathfrak{P}$.

Since $G(H_K/K) \cong C(\mathcal{O}_K)$ this will show that $L = H_K$, the Hilbert class field of $K$.

#### 4.1.4 The case of $K$: Part 2

We can now do the same thing we did with $\mathbb{Q}$, use the torsion points of elliptic curves to find the ray class fields and the maximal abelian extensions. We can't work directly over $K$ because $C_K$ is nonzero, but if we imitate the argument (with some modifications) over $\mathbb{Q}$ for

$H_K$ we will get the ray class fields of $K$. We let $L_n = K(j(E), h(E[n]))$ where $h$ is a Weber function (to be defined).

Let $l_n$, $l$ be the residue fields of $L_n$ and $H_K$ modulo some prime. We show $L_n$ is the ray class field for $(n)$ by constructing the diagram

$$eq:rcf-k \qquad \begin{tikzcd} & E[n] \arrow[r, dotted, "\widetilde{\bullet}", "\text{reduction}"'] & \widetilde{E}[n] \\ & \circlearrowright & \circlearrowright \\ \mathrm{Nm}_{H_K/K}(I_{H_K}^n)/P_K(1,n) \arrow[r, "\psi_{L_n/K}", "\cong"'] & G(L_n/H_K) \arrow[r, dotted, "\widetilde{\bullet}"] & G(l_n/l). \end{tikzcd} \tag{16.7}$$

We now carry out these two parts.

## 4.2 The Galois group and class group act compatibly

We establish the map in (16.5).

**Theorem 4.1:** thm:map-G-cl There exists a map $F : G(\overline{K}/K) \to C(\mathcal{O}_K)$ such that for *any* elliptic curve $E$,

$$[E^\sigma] = F(\sigma)E.$$

This map factors through $G(K^{\text{ab}}/K)$.

As a reminder, the action of $C(\mathcal{O}_K)$ on $\mathcal{E}\text{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$ is such that if $E = E_\Lambda$, then $F(\sigma)E = E_{F(\sigma)^{-1}\Lambda}$. Theorem 4.1 expresses a deep relationship because the left-hand side expresses an algebraic action, while the right-hand side expresses an analytic action, as it is defined on lattices and the map between $E$ and $\mathbb{C}/\Lambda$ is inherently analytic.

Proving this theorem essentially boils down to showing the Galois action commutes with the action on $C(\mathcal{O}_K)$.

**Proposition 4.2:** For all $E$,

$$\sigma([\mathfrak{a}][E]) = [\sigma(\mathfrak{a})][\sigma(E)].$$

*Proof.* Suppose $E$ corresponds to $\Lambda$, i.e. $E \cong \mathbb{C}/\Lambda\mathbb{C}$. Then we have the exact sequence

$$0 \to \Lambda \to \mathbb{C} \to E \to 0.$$

Then $\mathfrak{a}E$ corresponds to $\mathfrak{a}^{-1}\Lambda$. Take a resolution for $\mathfrak{a}$:

$$R^m \xrightarrow{A} R^n \to \mathfrak{a} \to 0.$$

Take a "Hom product" and use the Snake Lemma. See [17, II.2.5]. $\square$

*Proof of Theorem 4.1.* See [17, II.2.4]. $\square$

## 4.3 Hilbert class field

Before we proceed with finding the Hilbert class field, we need to show injectivity of the reduction map like in (16.3).

**Theorem 4.3:** thm:ec-hom-red Suppose $E_1$ and $E_2$ are elliptic curves defined over $L$ with good reduction at $\mathfrak{P}$. Then the reduction map

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\widetilde{E_1}, \widetilde{E_2})$$

is injective and preserves degrees.

*Proof.* See Silverman AT [17, pg. 124] (Also see Silverman's errata). □

Eventually rewrite this to work for all orders. The main theorem of this section is the following.

**Theorem 4.4** ($j(E)$ generates the Hilbert class field)**:** thm:j-generates-hilbert Let $E$ be an elliptic curve with CM by $\mathcal{O}_K$. Then

1. $K(j(E)) = H_K$, the Hilbert class field of $K$.
2. $G(\overline{K}/K)$ acts transitively on the isomorphism classes of curves in $\mathcal{E}\mathrm{ll}(\mathcal{O}_K)$.
3. For any ideal $\mathfrak{a} \in I_K$,
$$[E^{\psi_{H_K/K}(\mathfrak{a})}] = [\mathfrak{a}][E].$$
In particular, the action of Frobenius on the $j$-invariant is given by operating by $[\mathfrak{p}]$ on the elliptic curve:
$$[E^{(\mathfrak{p}, H_K/K)}] = [\mathfrak{p}][E].$$

*Proof.* Step 1: First we show the following: There exists a finite set of primes $S$ of $\mathbb{Z}$ such that for any $p \notin S$ that splits completely in $K$, $p = \mathfrak{p}\overline{\mathfrak{p}}$, we have

$$F((\mathfrak{p}, L/K)) = [\mathfrak{p}] \in C(\mathcal{O}_K).$$

This will show the dotted map in (16.6) is the identity for a large number of primes $\mathfrak{p}$.

We have the map $[\mathfrak{p}] : E \to \mathfrak{p}E$. We show that this is "like" the $p$th power Frobenius map. To do this, we show that it is inseparable of degree $p$ (this is why we needed $p$ to be split)[3], and then look at the $j$-invariants of the reduced maps modulo $\mathfrak{p}$.

As $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) = \mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathcal{O}_K)$ is finite, we can find a finite extension $L/K$ and representatives $E_1, \ldots, E_h$ of classes in $\mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathcal{O}_K)$, that are defined over $L$. Let $S$ be a set of primes containing the primes that satisfy one of the following conditions.

1. $p$ ramifies in $L$. (Primes that ramify always cause trouble.)

[3] If $\mathfrak{p}$ is not split, one can still show the map is inseparable of degree $p^2$, with some more work.

2. $E$ or some $E_i$ has bad reduction at some prime of $L$ lying over $p$.

3. $v_p(\mathrm{Nm}_{L/\mathbb{Q}}(j(E_i)-j(E_k))) \neq 0$ for some $i \neq k$. (This allows us to know what equivalence class an elliptic curve lies in, just by looking at its reduction modulo $p$.)

Let $\Lambda$ be the lattice such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, and let $\mathfrak{a}$ be an integral ideal relatively prime to $\mathfrak{p}$ such that $\mathfrak{a}\mathfrak{p} = (\alpha)$ is principal (This exists by Corollary 2.2.5). By the equivalence of categories 1.1, the following maps on complex tori correspond to isogenies of elliptic curves:

$$\begin{tikzcd}
\mathbb{C}/\Lambda \arrow[r, "i"] \arrow[d, "\Phi", "\cong"'] & \mathbb{C}/\mathfrak{p}^{-1}\Lambda \arrow[r, "i"] \arrow[d, "\Phi", "\cong"'] & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}^{-1}\Lambda \arrow[r, "{[\alpha]}", "\cong"'] \arrow[d, "\Phi", "\cong"'] & \mathbb{C}/\Lambda \arrow[d, "\Phi", "\cong"'] \\
E \arrow[r, "\phi_1"] & \mathfrak{p}E \arrow[r, "\phi_2"] & \mathfrak{a}\mathfrak{p}E \arrow[r, "\phi_3", "\cong"'] & E
\end{tikzcd}$$

Let the composition of the top maps be $f$ and the composition of the bottom maps be $g$.

Let $\omega$ be an invariant differential on $E$. Then $\omega' = \Phi^*\omega$ is an invariant differential on $\mathbb{C}/\Lambda$. It is in the form $c\,dz$. The composition of the top maps is just multiplication by $\alpha$, so $f^*\omega' = \alpha\omega'$. By commutativity, we get $g^*\omega = \alpha\omega$ as well.

Let $p \notin S$ and $\mathfrak{P} \mid \mathfrak{p} \mid p$ in $L$, $K$, $\mathbb{Q}$, respectively. Since $E$ has good reduction at $\mathfrak{P}$, we can reduce the elliptic curves and maps modulo $\mathfrak{P}$ to get

$$\widetilde{g}^*\widetilde{\omega} = \widetilde{\alpha}\widetilde{\omega} = 0$$

since $\mathfrak{P} \mid \alpha$. By a criterion for separability ($g$ is separable iff $g^*$ does not act as 0 on $\Omega_E$), $\widetilde{g}$ is inseparable. Now

$$\begin{aligned}
\deg(\phi_1) &= \mathfrak{N}\mathfrak{p} = p, \\
\deg(\phi_2) &= \mathfrak{N}\mathfrak{a} \perp p, \\
\deg(\phi_3) &= 1.
\end{aligned}$$

An inseparable map must have degree divisible by $p$, and the composition of separable maps is separable, so $\widetilde{\phi_1}$ must be inseparable.

Any inseparable map factors through the Frobenius map:

$$pE-factors-frob \begin{tikzcd}
\widetilde{E} \arrow[r, "\phi_p"] \arrow[dr, "\widetilde{\phi_1}"'] & \widetilde{E}^{(p)} \arrow[d, "\varepsilon", "\cong"'] \\
& \widetilde{\mathfrak{p}E}.
\end{tikzcd} \tag{16.8}$$

We have $p\deg(\varepsilon) = \deg(\phi_p)\deg(\varepsilon) = \deg(\widetilde{\phi_1}) = p$ so $\deg(\varepsilon) = 1$. This shows $\varepsilon$ is an isomorphism.

Thus we have

$$\widetilde{\mathfrak{p}E} \cong \widetilde{E}^{(p)}.$$

Now by definition of the Frobenius element (it is the $p$th power map modulo $\mathfrak{P}$), we have $j(\widetilde{E}^{(p)}) = j(\widetilde{E})^p = j(E)^{(\mathfrak{p},L/K)}$ modulo $\mathfrak{P}$. Putting everything together,

$$j(\mathfrak{p}E) \equiv j(\widetilde{E}^{(p)}) \equiv j(E^{(\mathfrak{p},L/K)}) \pmod{\mathfrak{P}}.$$

But we chose $p$ so that nonisomorphic curves have $j$-invariants that are not congruent modulo $p$ (item 3). Therefore, $\mathfrak{p}E \cong E^{(\mathfrak{p},L/K)}$. This shows that the action of $\mathfrak{p}$ is the same as the action of $(\mathfrak{p}, L/K)$, i.e. $F((\mathfrak{p}, L/K)) = [\mathfrak{p}]$.

Step 2: We show that $F : G(\overline{K}/K) \to C(\mathcal{O}_K)$ has kernel equal to $G(\overline{K}/K(j(E)))$, and so factors through $G(K(j(E))/K) \hookrightarrow C(\mathcal{O}_K)$. Indeed,

$$\begin{aligned}
\ker(F) &= \{\sigma : F(\sigma)E = E\} \\
&= \{\sigma : E^\sigma = E\} && \text{definition of } \sigma \\
&= \{\sigma : j(E)^\sigma = j(E)\} && j \text{ parameterizes isomorphism classes} \\
&= G(\overline{K}/K(j(E))).
\end{aligned}$$

We let $L = K(j(E))$.

Step 3: Let $\mathfrak{f}$ be the conductor of $L/K$. We extend Step 1 to all ideals $\mathfrak{a}$: for all $\mathfrak{a}$ we have

$$F((\mathfrak{a}, L/K)) = [\mathfrak{a}] \in C(\mathcal{O}_K);$$

in other words $\mathfrak{f} = 1$ and the following composition is the identity map.

$$eq : F(a) = [a] \quad \begin{tikzcd} I_K/P_K \arrow[r, "\psi_{L/K}"] \arrow[rr, bend right, dotted, "\cong"', "\mathrm{Id}"'] & G(L/K) \arrow[r, hook, "F"] & C(\mathcal{O}_K). \end{tikzcd} \tag{16.9}$$

Given $\mathfrak{a} \in I_K^{\mathfrak{f}}$, there are infinitely many $\mathfrak{p} \in I_K^{\mathfrak{f}}$ in the same class as $\mathfrak{a}$ with degree 1 by Corollary 15.3.6. Choose such a prime $\mathfrak{p}$, that does not divide a prime in $S$. Note $\mathfrak{a}, \mathfrak{p}$ differ by an ideal in $P_K(1, \mathfrak{f})$ so they have the same image by the Artin symbol. Step 1 shows that

$$F((\mathfrak{a}, L/K)) = F((\mathfrak{p}, L/K)) \overset{\text{Step 1}}{=} [\mathfrak{p}] = [\mathfrak{a}].$$

In particular, for any principal ideal $(\alpha) \in I_K^{\mathfrak{f}}$, we have $F(((\alpha), L/K)) = 1$. However, by definition the conductor is the smallest $\mathfrak{p}$ such that $\alpha \equiv 1 \pmod{\mathfrak{f}}$ implies $((\alpha), L/K) = 1$, so we must have $\mathfrak{f} = (1)$.[4] Thus the map $F : I_K^{\mathfrak{f}}/P_K(1, \mathfrak{f}) \to G(L/K)$ we had originally is actually just $F : I_K/P_K \to G(L/K)$, and we get (16.9).

[4]Technically, we only have $((\alpha), L/K) = 1$ for $(\alpha) \perp \mathfrak{f}$, and a priori $((\alpha), L/K)$ is not defined for $(\alpha) \perp \mathfrak{f}$. (We don't know $\mathfrak{f} = 1$ yet.) The proper way to conclude $\mathfrak{f} = (1)$ is transfer the problem over to ideles: We know $\psi_{L/K}(P_K^{\mathfrak{f}}) = 1$, so $\phi_{L/K}(K^\times \mathbb{U}_K^{\mathfrak{f}}) = 1$. By $\mathbb{I}_K^{\mathfrak{f}}/K(1, \mathfrak{f})\mathbb{U}_K(1, \mathfrak{f}) \cong \mathbb{I}_K/K^\times \mathbb{U}_K(1, \mathfrak{f})$ we conclude that $\phi_{L/K}(K^\times \mathbb{U}_K) = 1$. Hence $\mathfrak{f} = 1$.

Step 4: Since the conductor is divisible by exactly the ramifying primes, $L/K$ is unramified, and $L \subseteq H_K$. On the other hand, the map $F \circ \psi_{L/K} : I_K/P_K \to C(\mathcal{O}_K)$ is an isomorphism because $F \circ \psi_{L/K}$ is just the identity map. This gives $[L : K] = |C(\mathcal{O}_K)| = [H_K : K]$. Hence $L = H_K$. This shows item 1.

Step 5: Item 3 now follows immediately, since we already showed $E^{\psi_{L/K}(\mathfrak{a})} = [\mathfrak{a}]E$ and we now know $L = H_K$. Item 2 follows since the fact that the composition in (16.9) is an isomorphism means the map $F : G(L/K) \to C(\mathcal{O}_K)$ is surjective. Since $F$ transfers the action of $G(L/K)$ on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$ to $C(\mathcal{O}_K)$, and $C(\mathcal{O}_K)$ acts simply transitively on $\mathcal{E}\mathrm{ll}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$, we get that the same is true for $G(L/K)$. $\square$

# §5 Maximal abelian extension

We next carry out part 2 of our outline in Section 4.1. We construct the ray class fields for $K$, then take their compositum to get the maximal abelian extension.

**Definition 5.1:** Suppose $E$ has CM by an order in $K$, and $E$ is defined over $H_K$. A **Weber function** is an isomorphism $h : E/\operatorname{Aut}(1) \to \mathbb{P}^1$ defined over $H_K$. (So if $f : E \to E'$ is an automorphism, then $h(P) = h(f(P))$.)

We can always fix a concrete Weber function.

**Example 5.2:** The simplest Weber function is the following. If $E$ has the form

$$y^2 = x^3 + Ax + B, \quad A, B \in H_K,$$

then take

$$h(P) = \begin{cases} x, & AB \neq 0 \\ x^2, & B = 0 \\ x^3, & C = 0. \end{cases}$$

In the 3 cases, respectively, $\operatorname{Aut}(E)$ is 1, $\mathbb{Z}/2$ or $\mathbb{Z}/4$, and $\mathbb{Z}/3$ or $\mathbb{Z}/6$.

We can define a Weber function that is "model independent," i.e. doesn't change under if we change to an isomorphic elliptic curve, by

$$h(f(z)) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda), & j(E) \neq 0, 1728 \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z,\Lambda)^2, & j(E) = 1728 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z,\Lambda)^3, & j(E) = 0. \end{cases}$$

This is because the expressions have "weight 0."

The importance of the Weber function is given below. It would not be true if $h(P)$ were just defined as $h(x, y) = x$.

**Lemma 5.3:** lem:K-ab-ext Let $E$ be an elliptic curve with CM by $\mathcal{O}$.

1. The extension $K(j(E), E_{\text{tors}})/K(j(E))$ is abelian.
2. The extension $K(j(E), h(E_{\text{tors}}))/K$ is abelian.

The first statement is important because it tells us $G(\overline{K}/K(j(E)))$ acts in an abelian way on $E_{\text{tors}}$. Thus the "Galois representation" of the Galois group on $E_{\text{tors}}$ is abelian. Thus, as we will see, it will decompose into two Grössencharacters.

*Proof.* We have an injective map $G(K(j(E), E[m])/K(j(E))) \hookrightarrow \text{Aut}(E[m])$.[5] Now, the image of $G$ in $\text{Aut}(E[m])$ commutes with $\mathcal{O}_K$, so is contained in

$$\text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]) \cong \text{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(\mathcal{O}_K/m\mathcal{O}_K) \cong (\mathcal{O}_K/m\mathcal{O}_K)^\times$$

which is abelian.

For the second, suppose $\sigma, \tau \in G(K(j(E), h(E_{\text{tors}}))/K)$. We show that $\sigma\tau = \tau\sigma$. Since $K(j(E))/K$ is abelian, $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $j(E)$. Now $\sigma\tau\sigma^{-1}\tau^{-1}$ gives an automorphism of $E' = \tau\sigma(E)$ because

$$(\sigma\tau\sigma^{-1}\tau^{-1})\tau\sigma(E) = \sigma\tau(E) \cong \tau\sigma(E),$$

as the Galois action factors through $G(K^{\text{ab}}/K)$ and hence is abelian (Theorem 4.1) (alternatively, because $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $j(E)$). As $E$ is defined over $H_K$, we actually have equality.

Since $h$ is invariant under automorphism, for any $P \in E_{\text{tors}}$,

$$h(P) = h(\sigma\tau\sigma^{-1}\tau^{-1}P) = \sigma\tau\sigma^{-1}\tau^{-1}h(P).$$

(We know $h$ is defined over $H_K$ and $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $H_K = K(j(E))$.) Hence $\sigma\tau\sigma^{-1}\tau^{-1}$ fixes $h(E_{\text{tors}})$ as well, and $\sigma\tau\sigma^{-1}\tau^{-1} = 1$. $\square$

**Theorem 5.4:** thm:max-abe-ext-K Suppose $K$ is a quadratic imaginary field and $E$ has CM by $\mathcal{O}_K$.

1. For an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$, $L_{\mathfrak{a}} := H_K(h(E[\mathfrak{a}])) = K(j(E), h(E[\mathfrak{a}]))$ is the ray class field of $K$ modulo $\mathfrak{a}$.
2. The maximal abelian extension of $K$ is

$$K(j(E), h(E_{\text{tors}})).$$

*Proof.* Step 1: We need the following lemma.

**Lemma 5.5:** lem:comm-in-image Suppose $E$ is an elliptic curve defined over $L$ with CM by $\mathcal{O}_K$, and has good reduction at $\mathfrak{P}$. Let $\widetilde{E}$ be the reduction modulo $\mathfrak{P}$. Let $\theta : \text{End}(E) \to \text{End}(\widetilde{E})$ be the reduction map on endomorphisms. Then for any $\gamma \in \text{End}(\widetilde{E})$,

$$\gamma \in \text{im}(\theta) \iff \gamma \text{ commutes with every element in im}(\theta).$$

[5]Since $E[m] = \mathbb{Z}/m \times \mathbb{Z}/m$, if we choose a basis for $E[m]$, we have $\text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m)$, so we have a Galois representation.

*Proof.* Since $E$ has good reduction, the map $\mathrm{End}(E) \hookrightarrow \mathrm{End}(\widetilde{E})$ in injective. Consider 2 cases.

1. $\mathrm{End}(\widetilde{E})$ is a quadratic order. Then $\mathrm{End}(E) = \mathrm{End}(\widetilde{E})$ (as $\mathrm{End}(E)$ is a maximal order) so this case is clear.

2. $\mathrm{End}(\widetilde{E})$ is an order in a quaternion algebra. Then $\mathrm{End}(E) \otimes \mathbb{Q}$ is its own centralizer in the quaternion algebra $\mathrm{End}(\widetilde{E}) \otimes \mathbb{Q}$, by the Double Centralizer Theorem 12.4.11.

□

Step 2: We show that in general, we can lift the Frobenius map.

**Proposition 5.6:** pr:ec-lift-frob Suppose $E$ has CM by $\mathcal{O}_K$ and is defined over $H_K$. Let $\mathfrak{P} \mid \mathfrak{p} \mid p$ in $H_K$, $K$, $\mathbb{Q}$, respectively, with $\mathfrak{p}$ having degree 1 and $p \notin S$, $S$ being defined as in the proof of Theorem 4.4. Then the $p$th power Frobenius map can be lifted to a map on $E$, i.e. there is $\lambda$ making the following commute:

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^{(\mathfrak{p}, H_K/K)} \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\widetilde{\lambda}=\phi_p} & \widetilde{E}^{(p)}. \end{array}$$

Moreover, if $E$ corresponds to the complex torus $\mathbb{C}/\Lambda$, then up to isomorphism, $\lambda$ corresponds to the map $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$. (Recall that $E^{(\mathfrak{p}, H_K/K)} \cong \mathfrak{p}E$ by Theorem 4.4.)

*Proof.* We need to show $\phi_p$ is the reduction of some map; we do this by first reducing the problem to showing a certain endomorphism is in the image of $\theta$ and then showing the conditions of the previous lemma hold.

Again we use (16.8): $\widetilde{\phi_1} : \widetilde{E} \to \widetilde{\mathfrak{p}E}$ is "like" the Frobenius map. We know $\widetilde{\phi_1}$ is the reduction of a map, namely the map $\phi_1 : E \to \mathfrak{p}E$. Now note $\widetilde{\mathfrak{p}E} \cong \widetilde{E^{(\mathfrak{p}, L/K)}} = \widetilde{E}^{(p)}$, the first from Thm 4.4 and the second from definition of the Frobenius element.

Let $\sigma = (\mathfrak{p}, L/K)$. It remains to show that $\varepsilon : \widetilde{E^\sigma} \to \widetilde{\mathfrak{p}E} \cong \widetilde{E^\sigma}$ is the reduction of a map $\varepsilon'$, because then ${\varepsilon'}^{-1} \circ \phi_1$ will be the desired map. Let $\widetilde{[\alpha]} \in \mathrm{Aut}(\widetilde{E^\sigma})$ be the reduction of a map $[\alpha]$. To show $\varepsilon$ commutes with $[\alpha]$, we consider $\widetilde{\phi_1} = \varepsilon \circ \phi_p$, and consider how $[\alpha]$ "commutes" with $\widetilde{\phi_1}$ and $\phi_p$.

1. $\widetilde{\phi_1}$: By normalization (Proposition 2.2(3)), we know
$$\phi_1 \circ [\alpha]_E = [\alpha]_{E^\sigma} \circ \phi_1.$$

2. $\phi_p$: Note that for any morphism of varieties $f : V \to W$ over a field of characteristic $p$, the following commutes, where $\phi_V, \phi_W$ are the $p$th power Frobenius maps on $V$ and

$W$:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\phi_V"] & W \arrow[d, "\phi_W"] \\ V^{(p)} \arrow[r, "f^\sigma"] & W^{(p)} \end{tikzcd} \qquad \phi_W \circ f = f^\sigma \circ \phi_V.$$

Applying this to $[\alpha]_E$,

$$\phi_p \circ \widetilde{[\alpha]_E} = \widetilde{[\alpha]_E^\sigma} \circ \phi_p = \widetilde{[\alpha]_{E^\sigma}} \circ \phi_p,$$

where in the last step we used Theorem 2.2(4), noting $\sigma(\alpha) = \alpha$ since $\alpha \in K$ and $\sigma \in G(H_K/K)$.

Hence

$$\widetilde{[\alpha]_{E^\sigma}} \circ \underbrace{\varepsilon \circ \phi_p}_{\phi_1} \stackrel{1}{=} \varepsilon \circ \phi_p \circ \widetilde{[\alpha]_E} \stackrel{2}{=} \varepsilon \circ \widetilde{[\alpha]_{E^\sigma}} \circ \phi_p.$$

Cancelling $\phi_p$ gives $\widetilde{[\alpha]_{E^\sigma}} \circ \varepsilon = \varepsilon \circ \widetilde{[\alpha]_{E^\sigma}}$, so Lemma 5.5 shows $\varepsilon$ is the reduction of some $\varepsilon'$, as needed.

To finish, note that $\phi_1$ does indeed correspond to $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$. Hence $\lambda$ corresponds to $\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda$, up to some automorphism. □

Step 3: When $(\mathfrak{p}, H_K/K) = 1$, $\lambda$ is just an endomorphism of $E$, hence equals $[\alpha]$ for some $\alpha$. In fact, the following proposition shows it is $[\pi]$ for some $\pi$ generating $\mathfrak{p}$, so that multiplication by $\pi$ corresponds to the $p$th power Frobenius in the reduction.

**Proposition 5.7:** pr:pi-is-frob Suppose $E$ has CM by $\mathcal{O}_K$ and is defined over $H_K$. For all but finitely many degree 1 prime ideals $\mathfrak{p}$ with $(\mathfrak{p}, H_K/K) = 1$ (equivalently, such that $\mathfrak{p}$ is principal), there exists a unique $\pi$ such that $\mathfrak{p} = (\pi)$ and the following commutes.

$$\begin{tikzcd} E \arrow[r, "{[\pi]}"] \arrow[d] & E \arrow[d] \\ \widetilde{E} \arrow[r, "\phi_p"] & \widetilde{E}. \end{tikzcd}$$

*Proof.* Since $(\mathfrak{p}, H_K/K) = 1$, Proposition 5.6 gives a diagram

$$\begin{tikzcd} E \arrow[r, "\lambda"] \arrow[d] & E \arrow[d] \\ \widetilde{E} \arrow[r, "\phi_p"] & \widetilde{E}. \end{tikzcd}$$

for some $\lambda$. We know $\lambda$ is in the form $[\pi]$, and show $\pi$ satisfies the desired conditions. We have by Proposition 2.8 that

$$\mathrm{Nm}_{K/\mathbb{Q}}(\pi) = \deg([\pi]) = \deg(\phi) = p = \mathfrak{N}\mathfrak{p}$$

so either $(\pi) = \mathfrak{p}$ or $(\pi) = \overline{\mathfrak{p}}$. As always, when we're deciding between conjugates, normalization comes to the rescue. Take $\omega \in \Omega_E$ whose reduction modulo $\mathfrak{P}$ is nonzero. Normalization says that $[\pi]^*\omega = \pi\omega$ so

$$\widetilde{\pi}\widetilde{\omega} = \widetilde{[\pi]}^*\widetilde{\omega} = \phi_p^*\widetilde{\omega} = 0,$$

the last step since the Frobenius map is inseparable. We get $\mathfrak{P} \mid \pi$, forcing $(\pi) = \mathfrak{p}$.

For uniqueness, note the map

$$\mathcal{O}_K \xrightarrow[\cong]{[\cdot]} \mathrm{End}(E) \xrightarrow{\widetilde{E}} \mathrm{End}(\widetilde{E})$$

is injective for $E$ having good reduction at $\mathfrak{P}$ (Theorem 4.3). □

Step 4: Consider (16.7). We need to show that $P_K(1, \mathfrak{a})$ is exactly the kernel of the Artin map $\psi_{L_\mathfrak{a}/K}$. Note that $P_K(1, \mathfrak{a})$ and $\ker(\psi_{L_\mathfrak{a}/K})$ are both subgroups of $P_K^\mathfrak{a} = \ker(\psi_{H_K/K}) = \ker(\psi_{L_\mathfrak{a}/K}(\bullet)|_{H_K})$. It suffices to show that for all but finitely many primes $\mathfrak{p}$ of degree 1 such that $(\mathfrak{p}, H_K/K) = 1$, we have $\mathfrak{p} \in P_K(1, \mathfrak{a})$ iff $\mathfrak{p} \in \ker(\psi_{L_\mathfrak{a}/K})$.

Let $\mathfrak{p}$ satisfy the conditions of Proposition 5.7. Since the reduction of $\psi_{L/K}(\mathfrak{p})$ is the Frobenius map, we get that $\psi_{L/K}(\mathfrak{p}) = [\pi]$, for some $\pi$ such that $(\pi) = \mathfrak{p}$.[6] Since $(\mathfrak{p}, H_K/K) = 1$, we have the commutative diagram

$$eq:pi-is-frob \quad \begin{array}{ccc} E & \xrightarrow{\psi_{L/K}(\mathfrak{p})=[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi_p} & \widetilde{E}. \end{array} \tag{16.10}$$

We have the following string of equivalences, for all but finitely many degree 1 primes $\mathfrak{p}$ with $(\mathfrak{p}, H_K/K) = 1$,

1. $\mathfrak{p} \in P_K(1, \mathfrak{a})$.
2. $\mathfrak{p} = (\pi)$ where $\pi = u\alpha$ where $u$ is a unit and $\alpha \equiv 1 \pmod{\mathfrak{a}}$.
3. For all $\mathfrak{a}$-torsion points $P \in E[\mathfrak{a}]$, $h([\pi]P) = h(P)$.

3′. For all $\mathfrak{a}$-torsion points $P \in \widetilde{E}[\mathfrak{a}]$, $\widetilde{h}(\widetilde{[\pi]}\widetilde{P}) = \widetilde{h}(\widetilde{P})$.

4. $(\mathfrak{p}, L_\mathfrak{a}/K)$ fixes $h(E[\mathfrak{a}])$.
5. $\mathfrak{p} \in \ker(\psi_{L_\mathfrak{a}/K})$.

(1) $\iff$ (2) is clear.

[6]Note the analogy with the cyclotomic case. $\psi_{L/K}(\mathfrak{p})$ acts on torsion points as $[\pi]$, just as in the cyclotomic case it acted as the $p$th power map, that corresponds to $[p]$ if we consider the natural map $\mathbb{Z} \to \mathrm{End}(\mathbb{Q}(\zeta_n))$.

For (2) $\implies$ (3), note that for all $\mathfrak{a}$ torsion points $P \in E[\mathfrak{a}]$,

$$\begin{aligned} h([\pi]P) &= h([u][\alpha]P) \\ &= h([\alpha]P) && h \text{ is } \mathrm{Aut}(E)\text{-invariant} \\ &= h(P) && \alpha \equiv 1 \pmod{\mathfrak{a}} \text{ and } P \in E[\mathfrak{a}]. \end{aligned}$$

Note it is important that $h$ be $\mathrm{Aut}(E)$-invariant.

For (3′) $\implies$ (2), let $P \in E[\mathfrak{a}]$ be a torsion point. By [16, VII.3.1b], $E[\mathfrak{a}] \hookrightarrow \widetilde{E}[\mathfrak{a}]$ is injective for $\mathfrak{p} \nmid \mathfrak{a}$ and $E$ with good reduction at $\mathfrak{p}$. Since $h$ is an isomorphism (in particular, an injection) $E/\mathrm{Aut}(E) \to \mathbb{P}^1$, we get that $[\pi]P = [u]P$ for some $[u] \in \mathrm{Aut}(E)$. But $E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}$, so we can choose $u$ such that $\pi \equiv u \pmod{\mathfrak{a}}$. Then there exists $\alpha$ such that $\pi = u\alpha$, with $\alpha \equiv 1 \pmod{\mathfrak{a}}$.

For (3) $\implies$ (4), we calculate the action of $(\mathfrak{p}, L/K)$ on a torsion point $P \in E[\mathfrak{a}]$, in the reduced curve:

$$\widetilde{P^{(\mathfrak{p},L/K)}} = \phi_p(\widetilde{P}) = \widetilde{[\pi]P},$$

the second equality from Proposition 5.7. This allows us to understand the action on the nonreduced curve, since $E[\mathfrak{a}] \hookrightarrow \widetilde{E}[\mathfrak{a}]$ is injective for $\mathfrak{p} \nmid \mathfrak{a}$ and $\mathfrak{p}$ of good reduction. We get

$$P^{(\mathfrak{p},L/K)} = [\pi]P.$$

Thus (3) implies

$$\begin{aligned} h(P)^{(\mathfrak{p},L/K)} &= h(P^{(\mathfrak{p},L/K)}) && (\mathfrak{p}, L/K) \text{ fixes } H_K \text{ and } E \text{ defined over } H_K \\ &= h([\pi]T) \\ &= h(T) && \text{by (3).} \end{aligned}$$

Now we prove (4) $\implies$ (3′). Let $\sigma \in G(\overline{K}/K)$ be an automorphism such that $\sigma|_{K^{\mathrm{ab}}} = (\mathfrak{p}, K^{\mathrm{ab}}/K)$. Then for any $P \in E[\mathfrak{a}]$,

$$\widetilde{h}(\widetilde{[\pi]}\widetilde{P}) \overset{(16.10)}{=} \widetilde{h}(\phi(\widetilde{P})) = \widetilde{h(P^\sigma)} = \widetilde{h(P)}^{\sigma} = \widetilde{h}(\widetilde{P}),$$

the last two equalities since $\sigma|_H = 1$, $h$ is defined over $H$, and $\sigma|_{L_\mathfrak{a}}$ fixes $h(E[\mathfrak{a}])$ by assumption. Thus (3′) holds.

Now (4) $\iff$ (5) comes from the fact that $(\mathfrak{p}, L_\mathfrak{a}, K)$ already fixes $K(j(E))$, so to fix $L_\mathfrak{a}$ it only needs to fix $h(E[\mathfrak{a}])$.

<u>Step 7:</u> The maximal abelian extension is the union of the all ray class fields. Note every $\mathfrak{c}$ divides $n$ for some $n$ so we can just restrict to ray class fields corresponding to $(n)$ for some $n \in \mathbb{N}$:

$$K^{\mathrm{ab}} = \bigcup_n K(j(E), h(E[n])) = K(j(E), h(E_{\mathrm{tors}})).$$

$\square$

# §6 The Main Theorem of Complex Multiplication

Given $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$, consider the map $\sigma : E(\mathbb{C}) \to E^\sigma(\mathbb{C})$. We would like to know how this map acts on torsion points. This is since to get Galois representations of elliptic curves, we look at how $\sigma$ acts on torsion points—often specializing to torsion points that are a power of a prime.

Because we are considering CM elliptic curves, we can identify the torsion points with $K/\mathfrak{a}$, for some ideal $\mathfrak{a}$. Namely, given an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\cong} E(\mathbb{C})$, we can restrict it to $K/\mathfrak{a}$ to get

$$f|_{K/\mathfrak{a}} : K/\mathfrak{a} \xrightarrow{\cong} E_{\mathrm{tors}} \hookrightarrow E(\mathbb{C}).$$

The main theorem of complex multiplication tells us we can transfer the map $\sigma : E(\mathbb{C}) \to E^\sigma(\mathbb{C})$ via an *analytic isomorphism* to a multiplication-by-an-idele map $[\mathbf{x}^{-1}] : K/\mathfrak{a} \to K/\mathbf{x}^{-1}\mathfrak{a}$, where $\mathbf{x}$ and $\sigma$ are related in terms of the Artin map (to be made precise).

**Definition 6.1:** Let $\mathbf{x} = \prod_{\mathfrak{p}\in V_K^0} \mathfrak{p}^{m(\mathfrak{p})} \prod_{v\in V_K^\infty} v^{m(v)} \in \mathbb{I}_K$ be an idele. Let $\mathfrak{a}$ be an ideal, and define $\mathbf{x}\mathfrak{a}$ by

$$\mathbf{x}\mathfrak{a} = p(\mathbf{x})\mathfrak{a} = \left(\prod_{\mathfrak{p}\in V_K} \mathfrak{p}^{m(\mathfrak{p})}\right)\mathfrak{a}.$$

Define the map

$$eq:mult-idele-map[\mathbf{x}] : K/\mathfrak{a} \to K/\mathbf{x}\mathfrak{a} \tag{16.11}$$

as follows. Note $K/\mathfrak{a} \cong \prod_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}K_{\mathfrak{p}}$ by the Chinese Remainder Theorem, where $x$ is just identified with its images in the $K_{\mathfrak{p}}/\mathfrak{a}K_{\mathfrak{p}}$: $(x_{\mathfrak{p}})_{\mathfrak{p}\in V_K^0}$. Then (16.11) sends

$$eq:mult-by-idele(a_{\mathfrak{p}}) \mapsto (x_{\mathfrak{p}}a_{\mathfrak{p}}) \text{ where } \mathbf{x} = (x_{\mathfrak{p}}). \tag{16.12}$$

**Theorem 6.2** (Main Theorem of Complex Multiplication)**:** thm:mt-cm Suppose $E$ is an elliptic curve with CM by $\mathcal{O}_K$. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ and $\mathbf{x} \in \mathbb{I}_K$ be such that

$$\sigma|_{K^{\mathrm{ab}}} = \phi_K(\mathbf{x}).$$

Fix an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\cong} E(\mathbb{C})$. Then there exists a unique analytic isomorphism $f' : K/\mathbf{x}^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$ such that the following commutes:

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r, "\mathbf{x}^{-1}"] \arrow[d, "f"] & K/\mathbf{x}^{-1}\mathfrak{a} \arrow[d, "f'"] \\
E(\mathbb{C}) \arrow[r, "\sigma"] & E^\sigma(\mathbb{C}).
\end{tikzcd}$$

**Remark:** The map (16.12) can be a bit weird to think about: For instance, consider the simpler case $K = \mathbb{Q}$, $\mathfrak{a} = \mathbb{Z}$. Take the idele $\mathbf{x}$ with 1's everywhere except $x_5 = 2$. Then $[\mathbf{x}]$ sends $\frac{1}{2} \mapsto \frac{1}{2}, \frac{1}{3} \to \frac{1}{3}, \frac{1}{7} \to \frac{1}{7}$ and so forth but sends $\frac{1}{5} \to \frac{2}{5}$. So it is surprising that $\mathbf{x}^{-1} : K/\mathfrak{a} \to K/\mathbf{x}^{-1}\mathfrak{a}$ can be related analytically to $E(\mathbb{C}) \to E^\sigma(\mathbb{C})$.

Compare this theorem to Proposition 5.7. Rather tan just dealing with the Frobenius element of a prime, we deal with the Artin map of an idele.

*Proof.* Note uniqueness follows from the fact that topologically, the closure of $K/\mathbf{x}^{-1}\mathfrak{a}$ is $\mathbb{C}/\mathbf{x}^{-1}\mathfrak{a}$, and any continuous function is determined by its values on a dense set.

First we prove this for $E$ defined over $\mathbb{Q}(j(E))$ and $\mathfrak{a}$ integral. We do this in 2 steps. Step 1: Approximate $\sigma$ by a field automorphism $\lambda$ that is the Frobenius element of a prime $\mathfrak{p}$. (The Frobenius element is something much more concrete to work with than the abstract Artin map of an idele.) We will take better and better approximations, which determine the action on $E[m]$ for larger and larger $m$, and take an inverse limit.

So let $L'_m$ be the Galois closure of $K(j(E), E[m])/K$. By Corollary **??**.**??**, there are infinitely many primes with $\mathfrak{P} \mid \mathfrak{p}$ in $K$ and $L$ such that

$$(\mathfrak{P}, L/K) = \sigma|_{L'_m}, \quad \mathfrak{N}(\mathfrak{p}) = 1.$$

We can furthermore choose $\mathfrak{p}$ satisfying the following, because each condition excludes only finitely many primes.

1. $\mathfrak{p}$ is unramified in $L'_m$.

2. $\mathfrak{p} \notin S$, where $S$ is defined as in the proof of Theorem 4.4.

3. $\mathfrak{p} \nmid m$.

By Proposition 5.6, there exists a map $\lambda : E \to E^\sigma$ that reduces to $\phi_p$ modulo $\mathfrak{P}$. On $\widetilde{E}[m]$, both $\lambda$ and $\sigma$ act as $\phi_p$. Because $\mathfrak{P} \nmid m$ by item 3, the reduction map modulo $\mathfrak{P}$, $E[m] \to \widetilde{E}[m]$, is injective. Hence $\lambda$ and $\sigma$ act the same on $E[m]$:

$$eq : la = si\lambda|_{E[m]} = \sigma|_{E[m]} : E[m] \to E^\sigma[m]. \tag{16.13}$$

But we know how the map $\lambda$ acts: Proposition 5.6 tells us that the map $\lambda : E \to E^\sigma$ corresponds to the map on complex tori $i : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a}$.[7] Hence we have the commutative diagram

$$eq : mt - cm - 1 \quad \begin{array}{ccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{i} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\ \downarrow f & & \downarrow f'' \\ E(\mathbb{C}) & \xrightarrow{\lambda} & E^\sigma(\mathbb{C}) \end{array} \tag{16.14}$$

for some analytic isomorphism $f''$.

[7] The map $\sigma$ and $\mathbf{x}^{-1}$ appearing in the theorem statement are bijections, while $\lambda$ and $i$ are not. This is okay, though, because we only use $\lambda, i$ to approximate $\sigma$ on $m$-torsion, and $\lambda, i$ are injective on $m$-torsion, since $\mathfrak{P} \nmid m$.

Step 2: By Theorem 5.4, the ray class group modulo $m$ is $K_m = K(j(E), h(E[m]))$. Note $K_m \subseteq L'_m$. Now by assumption, $\mathfrak{p}$ was chosen so that the images of $\mathfrak{p}$ and $\mathbf{x}$ under the Artin map both project to $\sigma|_{K_m}$:

$$\phi_{K_m/K}(\mathbf{x}) = \sigma|_{K_m} = \psi_{K_m/K}(\mathfrak{p}) = \phi_{K_m/K}(i_{\mathfrak{p}}(\pi))$$

where $\psi$, $\phi$ denote the Artin map on ideals and on ideles, respectively, and $\pi$ is the uniformizer of $\mathfrak{p}$ in $K_{\mathfrak{p}}$. We have

$$\ker \psi_{K_m/K} = K^\times \mathbb{U}_K(1, m).$$

(See Definition 10.5.8 for notation.) This follows from the definition of the ray class field and from the correspondence between ray class groups in Definition 10.4.4 and idele class groups in Example 10.5.10. We have $\mathbf{x} \in i_{\mathfrak{p}}(\pi) \ker \phi_{K_m/K}$, giving

$$\mathbf{x} = \alpha \cdot i_{\mathfrak{p}}(\pi) \cdot \mathbf{u}, \quad \alpha \in K^\times, \quad \mathbf{u} \in \mathbb{U}_K(1, m).$$

We now compose (16.14) with the homothety $\alpha^{-1}$, and note $(\mathbf{x}) = (\alpha)\mathfrak{p}$, to get the desired map $\mathbb{C}/\mathbf{x}^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$:

$$eq:mt-cm-2 \quad \begin{array}{ccccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{i} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} & \xrightarrow{\alpha^{-1}} & \mathbb{C}/\mathbf{x}^{-1}\mathfrak{a} \\ \downarrow f & & \downarrow f'' & \swarrow f'_m & \\ E(\mathbb{C}) & \xrightarrow{\lambda} & E^\sigma(\mathbb{C}) & & \end{array} \tag{16.15}$$

Here, $f'_m(z) := f''(\alpha z)$.

This isn't quite what we want yet, though, because the top row is the map $\alpha^{-1}$ rather than the map $\mathbf{x}^{-1}$. We need to show that for $m$-torsion points, $\alpha^{-1}$ acts the same as $\mathbf{x}^{-1}$. Then we would have

$$\sigma(f(t)) = \lambda(f(t)) = f'_m(\alpha^{-1}t) = f'_m(\mathbf{x}^{-1}t), \quad t \in m^{-1}\mathfrak{a}/\mathfrak{a}.$$

The first equality is since $\sigma$, $\lambda$ were by construction the same on $E[m]$ (16.13), so $\sigma \circ f$ and $\lambda \circ f$ are the same on $m^{-1}\mathfrak{a}/\mathfrak{a}$. The second is by commutativity of (16.15).

To show the third equality, we note that

$$\begin{array}{rll} & f'_m(\alpha^{-1}t) = f'_m(\mathbf{x}^{-1}t) & \text{for all } t \in m^{-1}\mathfrak{a}/\mathfrak{a} \\ (f'_m \text{ bijective}) & \iff \alpha^{-1}t - \mathbf{x}^{-1}t \in \mathfrak{a} & \text{for all } t \in m^{-1}\mathfrak{a} \\ & \iff \alpha^{-1}t_{\mathfrak{q}} - x_q^{-1}t_{\mathfrak{q}} \in \mathfrak{a}_{\mathfrak{q}} & \text{for all } t \in m^{-1}\mathfrak{a},\ \mathfrak{q} \\ (\text{multiplying by } x_{\mathfrak{q}} = \alpha[i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}}u_{\mathfrak{q}}) & \iff [i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}}u_{\mathfrak{q}}t - t \in \mathfrak{a}_{\mathfrak{q}} & \text{for all } t \in m^{-1}\mathfrak{a}_{\mathfrak{q}} \\ & \iff ([i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}}u_{\mathfrak{q}} - 1)\mathfrak{a}_{\mathfrak{q}} \subseteq m\mathfrak{a}_{\mathfrak{q}} & \\ u_{\mathfrak{q}} \in \mathbb{U}_K(1, m) & \iff ([i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}} - 1)\mathfrak{a}_{\mathfrak{q}} \subseteq m\mathfrak{a}_{\mathfrak{q}}. & \end{array}$$

Consider 2 cases.

1. $\mathfrak{q} \neq \mathfrak{p}$. In this case, $[i_{\mathfrak{p}}(\pi)]_{\mathfrak{q}} = 1$, so this is trivial.

2. $\mathfrak{q} = \mathfrak{p}$: $[i_{\mathfrak{p}}(\pi)]_{\mathfrak{p}} = \pi$, and $\pi - 1$ is a unit. By assumption $\mathfrak{p} \nmid m$. hence $(\pi - 1)\mathfrak{a} = \mathfrak{a} = m\mathfrak{a}$.

Step 3: We now show that the maps $f'_m$ are all actually the same for $m \geq 3$. Indeed, $f'_m|_{E[m]} = f'_{mn}|_{E[m]}$ by construction, so $f'_m, f'_{mn}$ differ by an automorphism that fixes $E[m]$. This automorphism must be $[\zeta]$ for some element of norm 1 in $K$, and $f'_m = [\zeta] \circ f'_{mn}$. Since $f'_m, f'_{mn}$ are isomorphisms, this says

$$E[m] \subseteq \ker[1 - \zeta]$$

The only possibilities are $\zeta$ a 4th or 6th root of unity, and if $\zeta \neq 1$, then $[1 - \zeta]$ has norm at most 4. So for $m \geq 3$, $\zeta = 1$, and $f'_m = f'_{mn}$.

Step 4: Finally, we show the theorem holds for general $E/L$. Any elliptic curve $E$ has a model $E'$ defined over $M' = \mathbb{Q}(j(E))$, corresponding to a complex torus $\mathbb{C}/\mathfrak{a}'$ with $\mathfrak{a}'$ an integral ideal (see the left face below). Let $E \to E'$ be an isomorphism and $K/\mathfrak{a} \to K/\mathfrak{a}'$ be the corresponding map on torsion. Then the existence of $f'_{E'}$ for $E'/L$ gives the existence of $f'_E$ for $E/L$, by choosing $f'_E$ to make the below diagram commute.

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[rr, "\mathbf{x}^{-1}"] \arrow[dr, "\cong"] \arrow[dd, "f_E"'] & & K/\mathbf{x}^{-1}\mathfrak{a} \arrow[dr, "\cong"] \arrow[dd, dotted, "f'_E"] & \\
& K/\mathfrak{a}' \arrow[rr, "\mathbf{x}^{-1}"] \arrow[dd, "f_{E'}"] & & K/\mathbf{x}^{-1}\mathfrak{a}' \arrow[dd, "f'_{E'}"] \\
E(\mathbb{C}) \arrow[rr, "\sigma"] \arrow[dr] & & E^{\sigma}(\mathbb{C}) \arrow[dr, "\cong"] & \\
& E'(\mathbb{C}) \arrow[rr] & & E'^{\sigma}(\mathbb{C}).
\end{tikzcd}$$

□

## 6.1 The associated Grössencharacter

The Main Theorem involved 2 different elliptic curves, and 2 different analytic isomorphisms. In the special case that $\sigma$ fixes $E$, the curves will be the same, and by nudging the map upstairs by a constant depending on $\mathbf{x}$, we can restate the theorem using a consistent choice of $f$. (Compare to how we specialized from Proposition 5.6 to 5.7.) The action of $\phi_L(\mathbf{x})$ on the elliptic curve will "essentially" correspond to multiplication by $\chi_{E/L}$ on $K/\mathfrak{a}$.

**Theorem 6.3** (Grössencharacter of an elliptic curve)**:** thm:grossen-ec Let $E/L$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, and suppose $K \subseteq L$. Let $\mathbf{x} \in \mathbb{I}_L$ and $\mathbf{y} = \mathrm{Nm}_{L/K}(\mathbf{x}) \in \mathbb{I}_K$. Then there exists a unique $\alpha = \alpha_{E/L}(x) \in K^{\times}$ with the following properties.

1. $\alpha\mathcal{O}_K = (\mathbf{y})$.

2. For any fractional ideal $\mathfrak{a} \subseteq K$ and any analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$, the following commutes.

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\alpha\mathbf{y}^{-1}"] \arrow[d, "f"] & K/\mathfrak{a} \arrow[d, "f"] \\ E(L^{\mathrm{ab}}) \arrow[r, "\phi_L(\mathbf{x})"] & E(L^{\mathrm{ab}}). \end{tikzcd}$$

Moreover, defining $\chi_{E/L} : \mathbb{I}_L \to \mathbb{C}^\times$ by

$$\chi_{E/L}(\mathbf{x}) := \alpha_{E/L}(\mathbf{x})[\mathrm{Nm}_{L/K}(\mathbf{x}^{-1})]_\infty,$$

$\chi_{E/L}$ is a Grössencharacter of $K$, and $\chi_{E/L}$ is ramified at $\mathfrak{P}$ (i.e. $\chi_{E/L}(U_\mathfrak{P})$ is not identically 1) iff $E$ has bad reduction at $\mathfrak{P}$.

*Proof.* Part 1: Since $f$ is an isomorphism, uniqueness is clear. To construct $\alpha$, choose any $\sigma \in \mathrm{Aut}(\mathbb{C}/L)$ such that $\sigma|_{L^{\mathrm{ab}}} = \phi_L(\mathbf{x})$. We use Theorem 6.2 with $\sigma$ and $\mathbf{y} \in \mathbb{I}_K$, noting the following points.

1. $E^\sigma = E$ since $E$ is defined over $L$ and $\sigma$ fixes $L$.

2. The image of $f$ is contained in $E(L^{\mathrm{ab}})$ as $E_{\mathrm{tors}} \in E(L^{\mathrm{ab}})$ by Lemma 5.3.

3. By compatibility of the Artin map, $\phi_L(\mathbf{x})|_{K^{\mathrm{ab}}} = \phi_K(\mathrm{Nm}_{L/K}\,\mathbf{x}) = \phi_K(\mathbf{y})$.

We obtain an analytic map $f'$ making the following commute.

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\mathbf{y}^{-1}"] \arrow[d, "f"] & K/\mathbf{y}^{-1}\mathfrak{a} \arrow[d, "f'"] \\ E(L^{\mathrm{ab}}) \arrow[r, "\phi_L(\mathbf{x})"] & E(L^{\mathrm{ab}}). \end{tikzcd}$$

Because

$$\mathbb{C}/\mathbf{y}^{-1}\mathfrak{a} \cong E^\sigma(\mathbb{C}) \cong E(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a},$$

we have that $\mathbf{y}^{-1}\mathfrak{a}$ is homothetic to $\mathfrak{a}$, i.e. there exists $\beta$ so that $\beta$ takes $K/\mathbf{y}^{-1}\mathfrak{a}$ back to $K/\mathfrak{a}$. Defining $f''(x) = f'(\beta^{-1}x)$, we have that it differs from $f$ by some automorphism $[\zeta]$: $f \circ [\zeta] = f''$. Let $\alpha = \beta\zeta$. Then we can extend the above diagram as follows.

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\mathbf{y}^{-1}"] \arrow[d, "f"] & K/\mathbf{y}^{-1}\mathfrak{a} \arrow[r, "\alpha"] \arrow[d, "f'"] & K/\mathfrak{a} \arrow[dl, "f"] \\ E(L^{\mathrm{ab}}) \arrow[r, "\phi_L(\mathbf{x})"] & E(L^{\mathrm{ab}}) & \end{tikzcd}$$

As $\alpha\mathbf{y}^{-1}\mathfrak{a} = \mathfrak{a}$, we get $(\alpha) = (\mathbf{y})$.

To see that $\alpha$ is independent of $f$ and the ideal $\mathfrak{a}$, let $f'$ be another analytic isomorphism $K/\mathfrak{a}' \to E(L^{\text{ab}})$. Let the map $K/\mathfrak{a}' \to K/\mathfrak{a}$ be multiplication-by-$\gamma$. Then $f(\gamma x)$ is also an analytic isomorphism $K/\mathfrak{a}' \to E(L^{\text{ab}})$. Hence $\gamma^{-1} f^{-1} \circ f'$ is an automorphism $[\zeta]$ of $K/\mathfrak{a}'$, i.e. $f'(x) = f([\zeta]\gamma x)$. Thus $\phi_L(\mathbf{x})[f'(x)] = f'(\alpha \mathbf{y}^{-1} x)$ as well.

Part 2: $\alpha_{E/L}$ and hence $\chi_{E/L}$ is a homomorphism since it's clear that $\phi_L(\mathbf{x}\mathbf{x}') \circ f = f \circ \alpha\alpha' \mathbf{y}\mathbf{y}'^{-1}$, and $\phi_L(\mathbf{x}^{-1}) \circ f = f \circ \alpha^{-1}\mathbf{y}$.

We need to check that $\chi_{E/L}(L^\times) = 1$ and that $\chi_{E/L}$ factors through a modulus.

For the first point, note $\phi_L(L^\times) = 1$, the identity element of $G(L^{\text{ab}}/L)$. Let $i : K^\times \to \mathbb{I}_K$, $L^\times \to \mathbb{I}_L$ be the diagonal maps, and suppose $\mathbf{x} = i(x)$. We have $\mathbf{y} = \mathrm{Nm}_{L/K}(i(x)) = i(\mathrm{Nm}_{L/K}(x))$. Then $\alpha$ is just the element such that $\alpha \, \mathrm{Nm}_{L/K}(x)^{-1}$ induces the identity map, i.e. $\alpha = \mathrm{Nm}_{L/K}(x) = [\mathrm{Nm}_{L/K} \mathbf{x}]_\infty$, so $\chi_{E/L}(\mathbf{x}) = 1$.

For the second point, fix $m \ge 3$ ($m = 3$ works fine). We'll show that for any idele $\mathbf{x}$ in a small enough open subset of finite index, $\phi_L(\mathbf{x})$ acts just like multiplication by $\alpha_{E/L}(\mathbf{x})$ *and* fixes $E[m]$, without the extra $\mathrm{Nm}_{L/K}(\mathbf{x})_\infty$ factor, so that $\alpha$ will actually be 1.

Let $B_m$ be the kernel of the Artin map $\mathbb{I}_L \to G(L(E[m])/L)$ (abelian by Lemma 5.3), so that it induces an isomorphism

$$eq:LEm \quad \phi_{L(E[m])/L} : \mathbb{I}_L/B_m \xrightarrow{\cong} G(L(E[m])/L). \tag{16.16}$$

We show that

$$U_m := B_m \cap L^\times \left(\mathrm{Nm}_{L/K}^{-1} \mathbb{U}_K(1,m)\right) \subseteq \ker \chi_{E/L}.$$

This is of finite index in $\mathbb{I}_L$ since $B_m$ is open of finite index in $\mathbb{I}_L$ and $K^\times \mathbb{U}_K(1,m)$ is open of finite index in $\mathbb{I}_K$.

Fixing an analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \xrightarrow{\cong} E(\mathbb{C})$, we get that for any $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$ and any $\mathbf{x} \in U_m$, $f(t) \in E[m]$ so

$$\begin{aligned} f(t) &= f(t)^{\phi_L(\mathbf{x})} && \text{by (16.16) and } \mathbf{x} \in B_m \\ &= f(\alpha \, \mathrm{Nm}_{L/K}(\mathbf{x})^{-1} t) && \text{by the Main Theorem 6.2} \\ &= f(\alpha t) && t \in m^{-1}\mathfrak{a}/\mathfrak{a} \text{ and } \mathrm{Nm}_{L/K}(\mathbf{x})_\mathfrak{p} \equiv 1 \pmod{m\mathcal{O}_{K_\mathfrak{p}}} \text{ for all } \mathfrak{p}. \end{aligned}$$

Thus multiplication by $\alpha$ fixes $m^{-1}\mathfrak{a}/\mathfrak{a}$, i.e. $\alpha \equiv 1 \pmod{m\mathcal{O}_K}$. Note $\mathrm{Nm}_{L/K}(\mathbf{x})^{-1} \in \mathbb{U}_K(1,m)$, so

$$(\alpha) = (\mathbf{y}) = (\mathrm{Nm}_{L/K}(\mathbf{x})) = \mathcal{O}_K$$

and $\alpha$ is a unit. Together with $\alpha \equiv 1 \pmod{m\mathcal{O}_K}$, we get $\alpha = 1$.[8]

Part 3: The relationship between ramification and bad reduction hinges on the Néron-Ogg-Shafarevich Criterion. See [17, pg. 169-170]. □

Note that if $\chi_{E/L}$ is unramified at $\mathfrak{P}$, then $\chi_{E/L}(i_\mathfrak{P}(U_\mathfrak{P})) = 1$, so it makes sense to talk about $\chi_{E/L}(\mathfrak{P})$ (defined as $\chi_{E/L}(i_\mathfrak{P}(\pi))$ for any uniformizer $\pi$).

[8] Any number in the form $m\tau + 1$, $\tau \in \mathcal{O}_K$ with norm 1 has norm at least $(\mathrm{Nm}_{K/\mathbb{Q}}(m) - 1)^2 - 1$, by the triangle inequality. In order for it to have norm 1, $\tau = 0$.

**Proposition 6.4:** Let $E/L$ be an elliptic curve with CM by $\mathcal{O}_K$, with $K \subseteq L$. Let $\mathfrak{P}$ be a prime of $L$ of good reduction, let $\widetilde{E}$ be the reduction of $E$ modulo $\mathfrak{P}$. Let $\phi_{\mathfrak{P}}$ be the Frobenius on $\widetilde{E}$. Then the following commutes.

$$\begin{tikzcd} E \arrow[r, "{[\chi_{E/L}(\mathfrak{P})]}"] \arrow[d] & E \arrow[d] \\ \widetilde{E} \arrow[r, "\phi_{\mathfrak{P}}"] & \widetilde{E} \end{tikzcd}$$

*Proof.* Let $\pi$ be a uniformizer of $L_{\mathfrak{P}}$, and let $\varpi = i_{\mathfrak{P}}(\pi)$. Note that $\varpi_\infty = 1$. Hence $\mathrm{Nm}_{L/K}(\varpi)_\infty = 1$, giving

$$\chi_{E/L}(\mathfrak{P}) = \chi_{E/L}(\varpi) = \alpha_{E/L}(\varpi).$$

If $m$ is an integer such that $\mathfrak{P} \nmid m$, then $\mathrm{Nm}_{L/K}(\varpi)$ fixes $m^{-1}\mathfrak{a}/\mathfrak{a}$ (since it is 1 at all $\mathfrak{Q}$ with $\mathfrak{Q} \mid m$). Then

$$\begin{aligned} f(t)^{\phi_L(\varpi)} &= f([\alpha_{E/L}(\varpi)]\,\mathrm{Nm}_{L/K}(\varpi)^{-1}t) && \text{definition of } \alpha_{E/L} \\ &= f([\chi_{E/L}(\mathfrak{P})]\,\mathrm{Nm}_{L/K}(\varpi)^{-1}t) && \\ &= [\chi_{E/L}(\mathfrak{P})]f(\mathrm{Nm}_{L/K}(\varpi)^{-1}t) && f \text{ preserves the action of } \mathcal{O}_K \\ &= [\chi_{E/L}(\mathfrak{P})]f(t) && \mathrm{Nm}_{L/K}(\varpi) \text{ fixes } m^{-1}\mathfrak{a}/\mathfrak{a}. \end{aligned}$$

Modulo $\mathfrak{P}$, $\phi_L(\varpi)$ is just the $q$th power Frobenius map, so we get

$$\phi_{\mathfrak{P}}|_{\widetilde{E}[m]} = \widetilde{[\chi_{E/L}(\mathfrak{P})]}|_{E[m]}.$$

Since an isogeny is determined by its action on $E[m]$ for $m \to \infty$ (the kernel of a nonzero isogeny is finite), we get that this is true for $E$, not just $E[m]$, as needed. $\square$

To study the Galois representation $G(\overline{K}/H_K) \to \operatorname{Aut} E_{\text{tors}}$ of $E$, we reduce modulo a prime $\mathfrak{P}$ of $L$, and show that on this reduced curve, the $q$th power Frobenius acts exactly as multiplication by the Grössencharacter. In particular, the $q$th power Frobenius is represented by multiplication by $\chi_{E/L}(\mathfrak{P})$ when we think of $E_{\text{tors}}$ as $K/\mathfrak{a}$. Thinking of $E_{\text{tors}}$ as a 2-dimensional space $\mathbb{Q}^2$, this says exactly that the eigenvalues of the Frobenius acting on $E_{\text{tors}}$ is exactly $\chi_{E/L}(\mathfrak{P})$ and $\overline{\chi}_{E/L}(\mathfrak{P})$. Typically we just restrict our attention to $\ell$-power torsion points for some $\ell$.

# §7 $L$-series of CM elliptic curve

sec:l-series-cmec

## 7.1 Defining the $L$-function

We define the $L$-series of an elliptic curve as the $L$-series of the corresponding Galois representation.

**Definition 7.1:** df:E-L1 Let $E$ be an elliptic curve defined over $K$, and $\rho_\ell$ the associated Galois representation $G(\overline{K}/K) \to \operatorname{Aut} V_\ell E \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$.

Define the **local $L$-factor** of $E$ at a prime $\mathfrak{p}$ of $K$ as follows. Choose $\ell$ such that $\mathfrak{p} \nmid \ell$, and let

$$L_\mathfrak{p}(E, s) := L_\mathfrak{p}(\rho_\ell, s) = \det(1 - q^{-s} \operatorname{Frob}(\mathfrak{p}) | (V_\ell E)^{I_\mathfrak{p}})^{-1},$$

where $q = \mathfrak{N}\mathfrak{p}$ and $I_\mathfrak{p}$ is the inertia subgroup of $G(\overline{K}/K)$. (Choose an embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.) The **$L$-series** of $E$ is the product of local factors

$$L_\mathfrak{p}(E/K, s) := \prod_\mathfrak{p} L_\mathfrak{p}(E, s).$$

**Remark:** This is (almost) the same as saying: fix a prime $\ell$ and let $L(E/K, s) := L(\rho_\ell, s)$. The only difference is that we run into trouble with the local factor $L_\mathfrak{p}(\rho_\ell, s)$ on the right hand side, so we have to choose a different $\ell'$ and let this local factor be $L_\mathfrak{p}(\rho_{\ell'}, s)$ instead.

The following is an equivalent definition (that is more concrete).

**Definition 7.2:** df:E-L2 Let $N$ be the conductor[9] of the elliptic curve $E$. Define the local $L$-factor by

$$L_\mathfrak{P}(E, s) = 1 - a_q q^{-s} + \chi(q) q q^{-2s}, \quad a_q = q + 1 - |E(\mathbb{F}_q)|, \quad \chi(q) = \begin{cases} 1, & m \perp N \\ 0, & \text{else} \end{cases}$$

where $q = \mathfrak{N}\mathfrak{p}$. Thus

$$L_v(E, s) = \begin{cases} 1 - a_q q^{-s} + q q^{-2s}, & \text{good reduction} \\ 1 - q^{-s}, & \text{split multiplicative reduction} \\ 1 + q^{-s}, & \text{non-split multiplicative reduction} \\ 1, & \text{additive reduction.} \end{cases}$$

Note that $a_q$, the "trace of Frobenius," is related to the number of points of $E$ over $\mathbb{F}_q$. Hence the $L$-function contains information about the number of points of $E$ over each $\mathbb{F}_q$.

Showing that these two definitions are equivalent requires us to show that $(V_\ell E)^{I_\mathfrak{p}}$ is 2, 1, or 0-dimensional when $E$ has good, multiplicative, and additive reduction, respectively. The general idea is that the action of $I_\mathfrak{p}$ on $V_\ell E$ contains exactly the information lost by looking at the reduced elliptic curve, since $I_\mathfrak{p}$ is exactly the kernel of $D_\mathfrak{p}(\overline{K}/K) \to G(\overline{k}/k)$, so nontrivial action of $I_\mathfrak{p}$ corresponds to bad reduction.

In the CM case, we cannot have multiplicative reduction, so the $L$-series is particularly simple. We will show that the two definitions are equivalent in this case.

[9] $N$ is divisible by exactly the primes of bad reduction

**Theorem 7.3:** thm:cmec-no-mr Let $E/K$ be a CM elliptic curve. Then $E$ cannot have multiplicative reduction at any prime.

*Proof.* An elliptic curve $E$ has potential good reduction iff its $j$-invariant is integral [16, VII.5.5]. CM have integral $j$-invariants, so have potential good reduction, i.e. have good or multiplicative reduction. □

*Proof that Definitions 7.1 and 7.2 are equivalent in the CM case.* Suppose $E$ has CM by an order $\mathcal{O}$ in $K$, and $E$ is defined over $L$. By Néron-Ogg-Shafarevich, $I_{\mathfrak{p}}$ acts trivially on $V_\ell E$ iff $E$ has good reduction at $\mathfrak{p}$. Let $q = \mathfrak{N}\mathfrak{p}$.

In the case of good reduction we need to show $\det(1-q^{-s}\operatorname{Frob}(\mathfrak{p})|V_\ell E) = 1-a_q a^{-s}+qq^{-2s}$. Every endomorphism $\phi$ on $E$ satisfies $\phi^2 - \operatorname{Tr}(\phi)\phi + \deg(\phi) = 0$, where $\operatorname{Tr}(\phi) = 1+\deg(\phi) - \deg(1-\phi)$. Since $\operatorname{Frob}(\mathfrak{p})$ acts as the Frobenius morphism $\phi_{\mathfrak{p}}$, its characteristic polynomial is

$$\det(\lambda - \operatorname{Frob}(\mathfrak{p})) = \lambda^2 - \operatorname{Tr}(\phi_{\mathfrak{p}})\lambda + \deg(\phi_{\mathfrak{p}}).$$

But

$$\begin{aligned}
\deg(\phi_{\mathfrak{p}}) &= q \\
\operatorname{Tr}(\phi_{\mathfrak{p}}) &= 1 + \deg(\phi_{\mathfrak{p}}) - \deg(1-\phi_{\mathfrak{p}}) \\
&= q + 1 - \ker(1-\phi_{\mathfrak{p}}) \\
&= q + 1 - |E(\mathbb{F}_q)|.
\end{aligned}$$

(This part of the proof doesn't use the fact that $E$ has CM.)

Since $E$ has no multiplicative reduction by Theorem 7.3, it remains to prove that $W := (V_\ell E)^{I_{\mathfrak{p}}} = 0$ when $E$ has multiplicative reduction. We know by Néron-Ogg-Shafarevich that $\dim(W) \le 1$. But because $E$ is CM, $V_\ell E \cong (\varprojlim_n \ell^{-n}\mathfrak{a}/\mathfrak{a}) \otimes \mathbb{Q}$ has the structure of a $\mathcal{O}_K \otimes \mathbb{Q}_\ell$-vector space. If $a \in W$, then for any $\alpha \in K$, $\alpha a \in W$ because $[\alpha]$ commutes with the Galois action. Hence $W$ is not just a $\mathbb{Q}_\ell$-subspace of $V$, but also a $\mathcal{O}_K \otimes \mathbb{Q}_\ell$-subspace. Hence its dimension over $\mathbb{Q}_\ell$ is even, and must be 0. □

## 7.2 Analytic continuation

**Theorem 7.4** (Deuring)**:** thm:cmec-l Let $E/L$ be an elliptic curve with CM by $\mathcal{O}_K$ with $K \subseteq L$.Then

$$L(E/L,s) = L(s,\psi_{E/L})L(s,\overline{\psi_{E/L}}).$$

**Corollary 7.5** (Analytic continuation of $L$-function for CM elliptic curves)**:** cor:cmec-l-ac Let $E/L$ be an elliptic curve with CM by $\mathcal{O}_K$. Then $L$ admits an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating its values at $s$ and $2-s$.

This theorem for general elliptic curves is very deep (it follows from the Modularity Theorem and the analytic properties of $L$-functions associated to modular forms).

*Proof of Theorem 7.4.* By Theorem 7.3, $E$ has no multiplicative reduction. Let $\mathfrak{P}$ be a prime, and consider 2 cases.

1. $E$ has good reduction at $\mathfrak{P}$. Choose any $\ell$ not dividing $\mathfrak{P}$. The characteristic polynomial of the action of $\phi_{\mathfrak{P}}$ on $V_\ell E$ is $\det(\lambda - \phi_{\mathfrak{P}}|V_\ell E)$. However, if we make the identification $E_{\text{tors}} \cong K/\mathfrak{a}$, we have

   $$V_\ell E = \varprojlim \ell^{-n}\mathfrak{a}/\mathfrak{a},$$

   and we know that $\phi_{\mathfrak{P}}$ acts on $E_{\text{tors}} \cong K/\mathfrak{a}$ as multiplication by $\chi_{E/L}(\mathfrak{P})$. Therefore, the eigenvalues of the action of $\phi_{\mathfrak{P}}$ on $V_\ell E$ are just $\chi_{E/L}(\mathfrak{P})$ and $\overline{\chi}_{E/L}(\mathfrak{P})$, and

   $$\det(\lambda - \phi_{\mathfrak{P}}|V_\ell E) = (\lambda - \chi_{E/L}(\mathfrak{P}))(\lambda - \overline{\chi}_{E/L}(\mathfrak{P})).$$

   Taking $\lambda = p^s$ and dividing by $p^{2s}$ gives

   $$L_{\mathfrak{P}}(E/L, s) = \det(1 - p^{-s}\phi_{\mathfrak{P}}|V_\ell E) = L_{\mathfrak{P}}(s, \chi_{E/L})L(s, \overline{\chi}_{E/L}).$$

2. $E$ has bad reduction at $\mathfrak{P}$. Then $\chi_{E/L}(\mathfrak{P}) = 0$ by definition, and $L_{\mathfrak{P}}(E/L, s) = 1 = (1 - \chi_{E/L}(\mathfrak{P}))(1 - \overline{\chi}_{E/L}(\mathfrak{P})) = L_{\mathfrak{P}}(s, \chi_{E/L})L(s, \overline{\chi}_{E/L})$.

Multiplying together all the local factors gives the result. $\square$

*Proof of Corollary 7.5.* The $L$-functions of Grössencharacters have analytic continuation (Theorem 15.7.8, which works for Grössencharacters as well). Thus the result follows directly from Theorem 7.4. $\square$

Thus we have carried out the program in Section 15.7 for CM elliptic curves, to get the correspondences.

$$\text{(CM Elliptic curves)} \to \text{(Galois representation)} \to \text{(2 Grössencharacters)}$$

Remember Grössencharacters are 1-dimensional automorphic representations. If we wanted a modular form, we can use the technique of *automorphic induction* to construct a modular form from 2 Grössencharacters.

# Bibliography


[1] M. Bhargava. Higher composition laws i: A new view on gauss composition, and quadratic generalizations. *Annals Math.*, 159(1):217–250, Jan. 2004.

[2] H. Cartan and S Eilenberg. *Homological Algebra*, volume 19. Princeton Math Series, 1956.

[3] J. Cassels and A. Frohlich, editors. *Algebraic Number Theory*. Academic Press, 1969.

[4] P. Cohn. *Further Algebra and Applications*. Springer, 2003.

[5] D. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley & Sons, Inc., 1989.

[6] C. Dalawat. Splitting primes, March 2011.

[7] P. Etingof. Introduction to representation theory.

[8] S. Lang. *Algebraic Number Theory*. Number 110 in GTM. Springer, 1994.

[9] J. Milne. *Class Field Theory*. 4.00 edition, 2008.

[10] J. Milne. *Algebraic Number Theory*. www.jmilne.org/math/, 3.02 edition, 2009.

[11] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[12] J. Rotman. *An Introduction to Homological Algebra*. Springer, 2009.

[13] J.-P. Serre. *A Course in Arithmetic*. Number 7 in GTM. Springer, 1973.

[14] J.-P. Serre. *Local Fields*. Number 67 in GTM. Springer, 1979.

[15] J.-P. Serre. On a theorem of jordan. *Bull. Amer. Math. Soc.*, 40(4):429–440, 2003.

[16] J. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in GTM. Springer, 1986.

[17] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151 in GTM. Springer, 1994.

[18] H. P. F. Swinnerton-Dyer. On l-adic representations and congruences for coefficients of modular forms. 1972.

# Index