ALGEBRAIC NUMBER THEORY, GU4043, SPRING 2024

GYUJIN OH

These notes are for GU4043, Algebraic Number Theory, taught in Spring 2024 semester at Columbia University. The reader is assumed to have taken the standard undergraduate courses in algebra such as groups, rings and Galois theory (a background in complex analysis and Fourier analysis will also be helpful but not necessary).

This notes contain more exposition of modern algebraic number theory such as class field theory and the arithmetic of cyclotomic fields, focusing one understanding the meaning of the statements rather than their difficult proofs. Some emphasis is also given on the classical aspects, such as binary quadratic forms, continued fractions and various reciprocity laws.

Contents

1. Lecture 1. Mordell's equations

Summary. Introduction; Mordell's equations; how to find integer solutions using quadratic reciprocity or unique factorization property.

Content. The **Mordell curves** or the **Mordell's equations** are equations of the form

$$y^2 = x^3 + n, \quad n \in \mathbb{Z}.$$

It's called a curve because the implicit equation draws a curve in the xy-plane. We can come up with some immediate number-theoretic questions like the following.

(1) Is there an integer solution?

(2) Is there a rational solution?

(3) How many integer solutions are there?

(4) How many rational solutions are there?

In fact, the Mordell curves are examples of **elliptic curves**, and finding the rational solutions to elliptic curves is a hard question related to a very subtle arithmetic invariant of an elliptic curve (this is the subject of the Birch–Swinnerton-Dyer conjectures). We will not talk about this, but we can talk something about the integer solutions, and finding (or not finding) them uses some elementary but crucial ideas in number theory, such as **unique factorization** and **quadratic reciprocity**.

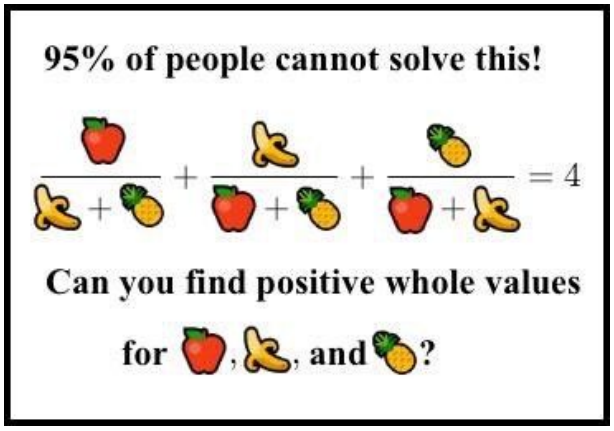


Figure 1. Finding a rational solution to an elliptic curve is very much related to the notorious "fruit equation meme".[1]

[1]The smallest solutions to this equation are

$$\text{apple} = 154476802108746166441951315019919837485664325669565431700026634898253202035277999,$$

$$\text{banana} = 368751317941299998271978115652254748254929799689719709962831374716372246340555 79,$$

$$\text{pineapple} = 437361267792869725786125260237139015281653755816161361862143799337842346777 2036.$$

Theorem 1.1. *The only integer solutions to* $y^2 = x^3 + 16$ *are* $(x, y) = (0, \pm 4)$.

Proof. We can write this as $x^3 = y^2 - 16 = (y-4)(y+4)$. If y is odd, then $(y-4, y+4) = 1$, so both $y-4$ and $y+4$ are odd cubes. No odd cubes differ by 8, so it is a contradiction. Thus, y is even, so x is even. Since x^3 is divisible by 8, y^2 is divisible by 8, so y is divisible by 4. Thus, $y^2 - 16$ is divisible by 16, so x^3 is divisible by 16, so x is divisible by 4. Letting $x = 4s$ and $y = 4t$, we get $4s^3 = t^2 - 1$, so t is odd, $t = 2n+1$. So $4s^3 = 4n^2 + 4n$, or $s^3 = n^2 + n = n(n+1)$. Since $(n, n+1) = 1$, this means both n, $n+1$ are cubes. The only possibilities of two cubes differing by 1 are $n = -1$ (so that $n+1 = 0$) and $n = 0$ (so that $n+1 = 1$). Thus $t = \pm 1$, $y = \pm 4$, and $x = 0$. □

Theorem 1.2. *The only integer solutions to* $y^2 = x^3 - 1$ *are* $(x, y) = (1, 0)$.

Proof. Note that $7 \pmod 8$ is not a square, so x is an odd number. Note also that $x^3 = y^2 + 1 = (y-i)(y+i)$ in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a UFD. Let d be a greatest common divisor of $y-i$ and $y+i$. Then, d divides $(y+i) - (y-i) = 2i$. Thus, $N(d) = d\overline{d} \in \mathbb{N}$ divides $N(2i) = 4$. Moreover, d divides $y-i$, so $N(d)$ divides $N(y-i) = (y-i)(y+i) = y^2 + 1 = x^3$, which is odd. Thus, $N(d) = 1$, so $d\overline{d} = 1$, which means d is a unit. By the unique factorization of $\mathbb{Z}[i]$, both $y-i$ and $y+i$ are cubes up to a unit. On the other hand, if $a + bi \in \mathbb{Z}[i]$ is a unit, then $N(a+bi) = 1$, so $a^2 + b^2 = 1$, so either $(a, b) = (0, \pm 1)$ or $(\pm 1, 0)$. This implies that the units of $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$. Since any unit of $\mathbb{Z}[i]$ is a cube, this implies that $y-i$ and $y+i$ are both cubes.

Now this means that there are $c, d \in \mathbb{Z}$ such that

$$y + i = (c + di)^3 = (c^3 - 3cd^2) + (3c^2 d - d^3)i$$

This implies that $d(3c^2 - d^2) = 3c^2 d - d^3 = 1$. Since d divides 1, $d = \pm 1$. If $d = 1$, $3c^2 - d^2 = 1$, or $3c^2 = 2$, which is a contradiction. If $d = -1$, $3c^2 - d^2 = -1$, or $3c^2 = 0$, so $c = 0$. Then, $y + i = (-i)^3 = i$, so $y = 0$ and $x = 1$. □

In the above proof, we used two ingredients, one being that $\mathbb{Z}[i]$ **is a UFD** and the other being the **characterization of the units of** $\mathbb{Z}[i]$. In the process, we also used the notion of the **norm**.

Theorem 1.3. *The only integer solutions to* $y^2 = x^3 - 2$ *are* $(x, y) = (3, \pm 5)$.

Proof. Note that $6 \pmod 8$ is not a square, so x is an odd number. Note also that $x^3 = y^2 + 2 = (y - \sqrt{-2})(y + \sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$. Since $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain, it is a UFD. Let d be a greatest common divisor of $y - \sqrt{-2}$ and $y + \sqrt{-2}$. Then, d divides $(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2}$, so $N(d) = d\overline{d}$ divides $N(2\sqrt{-2}) = 8$, where $\overline{a + b\sqrt{-2}} = a - b\sqrt{-2}$. On the other hand, $N(d)$ divides $N(y + \sqrt{-2}) = y^2 + 2 = x^3$, which is odd. So, $N(d) = 1$, which means that d is a unit. By the unique factorization of $\mathbb{Z}[\sqrt{-2}]$, both $y - \sqrt{-2}$ and $y + \sqrt{-2}$ are cubes up to a unit. On the other hand, if $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ is a unit, then $N(a + b\sqrt{-2}) = a^2 + 2b^2 = 1$, so $(a, b) = (\pm 1, 0)$. This means that the units of $\mathbb{Z}[\sqrt{-2}]$ are precisely $\{\pm 1\}$. Therefore, all the units of $\mathbb{Z}[\sqrt{-2}]$ are cubes, and $y - \sqrt{-2}$ and $y + \sqrt{-2}$ are both cubes.

Now this means that there are $c, d \in \mathbb{Z}$ such that

$$y + \sqrt{-2} = (c + d\sqrt{-2})^3 = (c^3 - 6cd^2) + (3c^2d - 2d^3)\sqrt{-2}$$

In particular, $1 = 3c^2d - 2d^3 = d(3c^2 - 2d^2)$. This implies that $d = \pm 1$. If $d = 1$, then $3c^2 - 2d^2 = 1$, so $c^2 = 1$, so $c = \pm 1$. Thus $y = \mp 5$ and $x = 3$. If $d = -1$, then $3c^2 - 2d^2 = -1$, so $3c^2 = 1$, which is a contradiction. □

As seen above, it is desirable to have a unique factorization property of rings like $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$. But most of the rings like this are not unique factorization domains.

Example 1.4. The ring $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, as

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}),$$

and 2 is an irreducible element in $\mathbb{Z}[\sqrt{-3}]$.

Proof of the fact that 2 is irreducible in $\mathbb{Z}[\sqrt{-3}]$. If $2 = xy$ for some non-units $x, y \in \mathbb{Z}[\sqrt{-3}]$, then using the norm $N(a + b\sqrt{-3}) = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2$, we have $4 = N(2) = N(x)N(y)$. Since x, y are nonunits and $N(x), N(y)$ are positive, this implies that $N(x) = N(y) = 2$. If $x = c + d\sqrt{-3}$, then $N(x) = c^2 + 3d^2$, which can never be $2 \pmod 3$, a contradiction.

However, $\mathbb{Z}[\sqrt{-3}]$ is not a UFD because we are looking at the wrong ring at the first place. In fact, the correct "number ring" for the field $\mathbb{Q}(\sqrt{-3})$ is not $\mathbb{Z}[\sqrt{-3}]$ but a slightly larger ring $\mathbb{Z}[\zeta_3]$ where

$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2},$$

is a primitive third root of unity. This contains $\mathbb{Z}[\sqrt{-3}]$ but is not equal to it. It is then true that $\mathbb{Z}[\zeta_3]$ is a UFD. We will see some justifications later on why $\mathbb{Z}[\sqrt{-3}]$ can never be a UFD in the first place.

On the other hand, even if we look at the correct number ring, it may still not be a UFD, and this is the case most of the time. However, an important idea is that the unique factorization of **ideals** is always true.

Another important theorem in algebraic number theory is the **quadratic reciprocity law**.

Definition 1.5 (Legendre symbol)**.** Let p be an odd prime number, and $a \in \mathbb{Z}$. Then,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \\ 0 & \text{if } p|a \end{cases}$$

We say that a is a quadratic residue mod p (quadratic nonresidue mod p, respectively) if a is a square mod p (not a square mod p, respectively).

Theorem 1.6 (Quadratic reciprocity law)**.** *Let p, q be distinct odd primes. Then,*

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

The quadratic reciprocity law, coupled with the following Theorem, enables us to compute any Legendre symbol inductively.

Theorem 1.7. *Let p be an odd prime number.*

(1) We have

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

(2) We have

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

There are many proofs to the quadratic reciprocity law. Later in the course we will see three proofs of the quadratic reciprocity law, one algebraic, one class-field theoretic, and one analytic.

Remark 1.8 (On the "reciprocity laws")**.** The word "reciprocity" generally means things like "you take what you give", "an eye for an eye", $\cdots$. The quadratic reciprocity law is called a reciprocity law because how a prime p treats another prime q (in terms of the Legendre symbol) is determined by how q treats p.

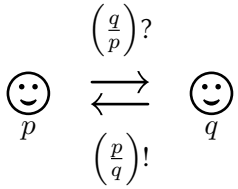


Figure 2. The quadratic reciprocity law.

In general, in algebraic number theory, if there is a **role-reversal** of some sort in some rule, we call it a **reciprocity law**. Although usually not stated in this way, another well-known instance of reciprocity law is Galois correspondence; here, a role-reversal happens if you pass a subfield of a Galois extension to the Galois group side, because the larger the field is, the smaller the Galois group is, and vice versa.

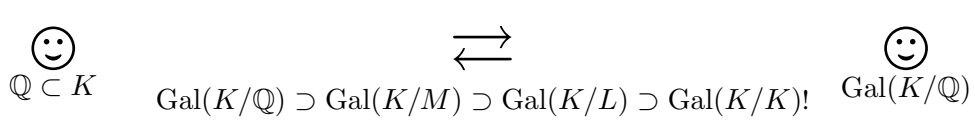


Figure 3. Galois correspondence as a reciprocity law.

We will see in this course that many big theorems in algebraic number theory are stated as reciprocity laws.

The quadratic reciprocity law, and more generally the notion of quadratic residues, can be found useful in the context of Mordell's equations.

Theorem 1.9. *There are no integer solutions to* $y^2 = x^3 + 7$.

Proof. If x is even, $y^2 \equiv 7 \pmod 8$, which is impossible. So, x is odd, and y is even. Write

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4).$$

Since $x^2 - 2x + 4 = (x-1)^2 + 3$ and since x is odd, $x^2 - 2x + 4 \equiv 3 \pmod 4$. This implies that $x^2 - 2x + 4$ has a prime factor $p \equiv 3 \pmod 4$. Because $p|(y^2+1)$, $\left(\frac{-1}{p}\right) = 1$, which contradicts $p \equiv 3 \pmod 4$. □

Theorem 1.10. *There are no integer solutions to* $y^2 = x^3 - 5$.

Proof. By considering mod 4, we note that y has to be even and $x \equiv 1 (\mathrm{mod}\, 4)$. Write

$$y^2 + 4 = x^3 - 1 = (x-1)(x^2 + x + 1).$$

Since $x \equiv 1 \pmod 4$, $x^2 + x + 1 \equiv 3 \pmod 4$, so there is a prime factor $p \equiv 3 \pmod 4$ dividing $y^2 + 4$. This implies that $\left(\frac{-4}{p}\right) = 1$, or $\left(\frac{-1}{p}\right) = 1$, which is a contradiction. □

Remark 1.11. As mentioned above, enumerating all the $\mathbb{Q}$-solutions to the Mordell equations are much more difficult. In fact, $y^2 = x^3 - 2$ has two $\mathbb{Z}$-solutions, $(3, \pm 5)$, while it has **infinitely many $\mathbb{Q}$-solutions**.

– –

Exercise 1.1. Let p be an odd prime, and $a \in \mathbb{Z}$. Using that $\mathbb{F}_p^\times$ is a cyclic group, show that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Exercise 1.2. This exercise aims to prove Fermat's theorem: an odd prime number $p \in \mathbb{N}$ is of the form $p = x^2 + y^2$ for some integers x, y if and only if $p \equiv 1 \pmod 4$.

(1) Show that $p = x^2 + y^2$ implies that $p \equiv 1 \pmod 4$.

(2) Conversely, if $p \equiv 1 \pmod 4$, then we have $\left(\frac{-1}{p}\right) = 1$, so there is an integer n such that $n^2 \equiv -1 \pmod p$. This implies that $p|(n^2+1)$.

By using the UFD property of $\mathbb{Z}[i]$, show that p has to be a reducible element in $\mathbb{Z}[i]$.

(3) Show that p being reducible in $\mathbb{Z}[i]$ implies that $p = x^2 + y^2$ for some integers x, y.

2. Lectures 2 and 3. Number fields, rings of integers

Summary. Number fields; quadratic fields; norms and traces of quadratic fields; Gauss's lemma; modules and algebras; integrality; integral closure; integral closure is a subring.

Content.

Definition 2.1 (Number fields)**.** A **number field** is a finite field extension K of the field of rational numbers $\mathbb{Q}$. The degree $[K:\mathbb{Q}]$ is called the **degree of a number field**.

The simplest examples (other than $\mathbb{Q}$) are **quadratic fields**.

Definition 2.2 (Quadratic fields)**.** A **quadratic field** is a degree 2 number field.

Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some integer d. (Why?)

We want to define the notion of "integers" inside any number field, just like $\mathbb{Z} \subset \mathbb{Q}$ for the field of rational numbers. We have also seen that somehow $\mathbb{Z}[\zeta_3]$ is better-behaved than $\mathbb{Z}[\sqrt{-3}]$. It turns out that the correct notion of "integers" for $K = \mathbb{Q}(\sqrt{-3})$ is those in $\mathbb{Z}[\zeta_3]$, not $\mathbb{Z}[\sqrt{-3}]$.

Definition 2.3 (Algebraic integers)**.** An element α in a number field K is an **algebraic integer** if it is a root of a **monic** polynomial $f(X) \in \mathbb{Z}[X]$ with integer coefficients, i.e. $f(\alpha) = 0$.

Example 2.4. Indeed, even though the expression

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2},$$

"looks like" it has a denominator, it is in fact an algebraic integer, as $\zeta_3^3 - 1 = 0$ (better: $\zeta_3^2 + \zeta_3 + 1 = 0$).

Let's go through a reality check:

Proposition 2.5. *A rational number $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if α is an integer, $\alpha \in \mathbb{Z}$.*

Proof. If $\alpha \in \mathbb{Z}$, then α is an algebraic integer, as it is a root of a monic integral polynomial $f(X) = X - \alpha$. Conversely, if $\alpha \in \mathbb{Q}$ is an algebraic integer, there is a monic integral polynomial $f(X) \in \mathbb{Z}[X]$ with $f(\alpha) = 0$. Suppose α is not an integer, and is denoted $\alpha = \frac{m}{n}$ where m, n are coprime integers with $n > 1$. Choose a prime factor p of n. Let $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d$. Then,

$$f(\alpha) = \frac{m^d + a_1 m^{d-1} n + \cdots + a_d n^d}{n^d} = 0,$$

so $m^d + a_1 m^{d-1} n + \cdots + a_d n^d = 0$. Thus, $m^d \equiv 0 \pmod{p}$, so $p | m$, which is a contradiction. □

What are the algebraic integers in a quadratic field $\mathbb{Q}(\sqrt{d})$?

Theorem 2.6. *Let $d \in \mathbb{Z} - \{0, 1\}$ be a square-free integer.*

(1) If $d \equiv 2, 3 \pmod{4}$, an element $\alpha \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}[\sqrt{d}] = \mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{d}$.

(2) If $d \equiv 1 \pmod 4$, an element $\alpha \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{d}}{2}$.

Before we move on to prove the Theorem, we review the useful notions of norms and traces for quadratic fields. The notion will later generalize to arbitrary number fields.

Definition 2.7 (Norms and traces, quadratic field case)**.** Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. For $\alpha = a + b\sqrt{d} \in K$, $a, b \in \mathbb{Q}$, the **conjugate of** α is $\overline{\alpha} = a - b\sqrt{d}$. The **norm of** α is $N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2$. The **trace of** α is $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2a$.

Note that, for $\alpha \in \mathbb{Q}(\sqrt{d})$, $N(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Q}$.

Proof of Theorem 2.6. Note that, if $\alpha \in \mathbb{Q}(\sqrt{d})$, α is a solution to a monic polynomial

$$p_\alpha(X) = X^2 - \mathrm{Tr}(\alpha)X + N(\alpha) = (X - \alpha)(X - \overline{\alpha}) \in \mathbb{Q}[X].$$

Thus, if $\mathrm{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$, then α is an algebraic integer. Thus, if $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$, then α is an algebraic integer. Furthermore, if $d \equiv 1 \pmod 4$ and $\alpha = a + b\frac{1+\sqrt{d}}{2} = \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{d}$, $a, b \in \mathbb{Z}$, then $\mathrm{Tr}(\alpha) = 2a + b \in \mathbb{Z}$, and

$$N(\alpha) = \left(a + \frac{b}{2}\right)^2 - d\left(\frac{b}{2}\right)^2 = a^2 + ab + \frac{(1-d)b^2}{4} \in \mathbb{Z}.$$

Therefore, we have shown one direction of the Theorem.

Conversely, suppose $\alpha \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer, so that there is a monic integral polynomial $f(X) \in \mathbb{Z}[X]$ with $f(\alpha) = 0$. We would like to show that $p_\alpha(X) \in \mathbb{Z}[X]$. If $\alpha \in \mathbb{Q}$ is actually a rational number, then we know that $\alpha \in \mathbb{Z}$ by the previous Proposition, so $p_\alpha(X) = (X - \alpha)(X - \overline{\alpha}) = (X - \alpha)^2$ is obviously an integer polynomial. Thus, suppose that $\alpha \notin \mathbb{Q}$, so that $p_\alpha(X)$ is actually irreducible in $\mathbb{Q}[X]$.

Now, suppose that $p_\alpha(X) \in \mathbb{Q}[X]$ is not integral, and let $M > 1$ be the common denominator of $\mathrm{Tr}(\alpha), N(\alpha) \in \mathbb{Q}$, so that $q_\alpha(X) := Mp_\alpha(X) \in \mathbb{Z}[X]$. Note that $q_\alpha(X)$ is an irreducible element in $\mathbb{Z}[X]$.

Since $0 = \overline{f(\alpha)} = f(\overline{\alpha})$, $p_\alpha(X)$ is a factor of $f(X)$ in $\mathbb{Q}[X]$. Thus,

$$f(X) = p_\alpha(X)r(X),$$

for some monic polynomial $r(X) \in \mathbb{Q}[X]$. Let $N \geq 1$ be the common denominator of the coefficients of $r(X)$, and let $s(X) := Nr(X) \in \mathbb{Z}[X]$. Then,

$$MNf(X) = q_\alpha(X)s(X),$$

is a factorization in $\mathbb{Z}[X]$. Note that $\mathbb{Z}[X]$ is a UFD, and by the definition of N, $(N, r(X)) = 1$, so this implies that $N | q_\alpha(X)$. Since $q_\alpha(X)$ is irreducible, $N = 1$. In particular, $r(X) \in \mathbb{Z}[X]$. Thus,

$$Mf(X) = q_\alpha(X)r(X),$$

is a factorization in $\mathbb{Z}[X]$. Since $(M, q_\alpha(X)) = 1$ by definition of M, M divides $r(X)$. This contradicts with the fact that $r(X)$ is a monic polynomial.

Therefore, we have just shown that, if $\alpha \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer, $p_\alpha(X) \in \mathbb{Z}[X]$. If we let $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$, this means that

$$2a, a^2 - db^2 \in \mathbb{Z}.$$

If $a \in \mathbb{Z}$, then $db^2 \in \mathbb{Z}$, and since d is square-free, this implies that b itself is an integer. If $a \notin \mathbb{Z}$ but $2a \in \mathbb{Z}$, then $a = \frac{x}{2}$ for some odd integer x. Thus,

$$\frac{x^2}{4} - db^2 \in \mathbb{Z}.$$

This implies that $b \notin \mathbb{Z}$ as well. Since $db^2 \in \frac{1}{4}\mathbb{Z}$, and since d is square-free, this implies that $b = \frac{y}{2}$ for some odd integer y. Then, we have

$$\frac{x^2 - dy^2}{4} \in \mathbb{Z},$$

or

$$x^2 \equiv dy^2 \pmod 4.$$

Note that as x, y are both odd, $x^2, y^2 \equiv 1 \pmod 4$, so this translates into $d \equiv 1 \pmod 4$. This implies that, if $a \notin \mathbb{Z}$, then d must be $1 \pmod 4$, and both a, b must be halves of odd integers. This implies the converse statement we want. □

From the above proof, it seems like the integrality of the minimal polynomial seems to be what's important for an algebraic number to be an algebraic integer. This is in fact true.

Theorem 2.8. *Let K be a number field, and let $\alpha \in K$ have the minimal polynomial $p_\alpha(X) \in \mathbb{Q}[X]$ over $\mathbb{Q}$. Then, α is an algebraic integer if and only if $p_\alpha(X) \in \mathbb{Z}[X]$.*

Proof. If $p_\alpha(X) \in \mathbb{Z}[X]$, then this gives a monic integer polynomial to which α is a root, so α is an algebraic integer. Conversely, suppose that α is an algebraic integer, so that there is a monic integer polynomial $f(X) \in \mathbb{Z}[X]$ to which α is a root. Then, by the UFD property of $\mathbb{Q}[X]$, as $p_\alpha(X) \in \mathbb{Q}[X]$ is irreducible, $p_\alpha(X)$ divides $f(X)$. Therefore,

$$f(X) = p_\alpha(X)r(X),$$

for some monic polynomial $r(X) \in \mathbb{Q}[X]$. Let $M \geq 1$ ($N \geq 1$, respectively) be the least common denominator of the coefficients of $p_\alpha(X)$ ($r(X)$, respectively). Then, $q_\alpha(X) := Mp_\alpha(X)$, $s(X) := Nr(X)$ are in $\mathbb{Z}[X]$, $(M, q_\alpha(X)) = 1$ and $(N, s(X)) = 1$, and $q_\alpha(X)$ is irreducible in $\mathbb{Z}[X]$. Then,

$$MNf(X) = q_\alpha(X)s(X).$$

Since $\mathbb{Z}[X]$ is also a UFD, as $(N, s(X)) = 1$, N divides $q_\alpha(X)$. Since $q_\alpha(X) \in \mathbb{Z}[X]$ is irreducible, N is a unit in $\mathbb{Z}[X]$, which implies that $N = 1$. Thus, we have

$$Mf(X) = q_\alpha(X)r(X).$$

By the same reasoning, M divides $r(X)$. As $r(X)$ is a monic polynomial, this implies that M divides 1, so $M = 1$. This implies that $p_\alpha(X) \in \mathbb{Z}[X]$, as desired. □

Remark 2.9. The above proof is based on what's usually referred as the **Gauss's lemma**:

Theorem 2.10 (Gauss's lemma)**.** *Let A be a UFD, and $f(X) \in A[X]$ be a **monic** polynomial. Then, $f(X)$ as a polynomial in $\mathrm{Frac}(A)[X]$ has a factorization into irreducible **monic** polynomials in $\mathrm{Frac}(A)[X]$.*

As a consequence, a monic polynomial $f(X)$ is irreducible in $A[X]$ if and only if $f(X)$ is irreducible in $\mathrm{Frac}(A)[X]$.

A famous corollary to this is the following, which has been implicitly used in the course all the time.

Corollary 2.11. *If A is a UFD, then $A[X]$ is also a UFD.*

From the previous examples, it seems like the collection of algebraic integers in a number field forms a **subring** of the number field. This is in fact true.

Theorem 2.12. *Let K be a number field. Then, the set of algebraic integers in K forms a subring of K.*

Definition 2.13 (Rings of integers)**.** The subring of algebraic integers of a number field K is called the **ring of integers** of K, and is denoted $\mathcal{O}_K$.

The ring of integers $\mathcal{O}_K$ is the correct notion of the integers inside K, generalizing $\mathbb{Z} \subset \mathbb{Q}$.

We will prove Theorem 2.12 by formulating this in a more general commutative algebra language. First, we will freely use the language of **modules** and **algebras**.

Definition 2.14 (Modules)**.** Let A be a commutative ring with 1. An A-**module** M is an abelian group (expressed additively) together with the notion of "scalar multiplication by elements in A,"

$$A \times M \xrightarrow{(a,m)\mapsto a\cdot m} M.$$

Namely, this "scalar multiplication" satisfies the following axioms.

(1) $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$, for $a \in A$, $m_1, m_2 \in M$.

(2) $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$, for $a_1, a_2 \in A$, $m \in M$.

(3) $(a_1 a_2) \cdot m = a_1 \cdot (a_2 \cdot m)$, for $a_1, a_2 \in A$, $m \in M$.

(4) $1 \cdot m = m$, for $m \in M$.

Roughly speaking, the notion of modules is a generalization of the notion of vector spaces, where we relax the field of scalars to be a commutative ring. Just like a vector space where you cannot "multiply" two vectors, you cannot "multiply" two elements in a module.

Example 2.15.

(1) For a field K, a K-module is the same notion as a K-vector space.

(2) A $\mathbb{Z}$-module is the same notion as an abelian group.

(3) For any commutative ring R with 1 and an ideal $I \subset R$, I is an R-module. There are many more R-modules than just ideals though.

(4) If R, S are commutative rings with 1 and if there is a ring homomorphism $f : R \to S$, then any S-module M can be also regarded as an R-module by defining

$$r \cdot m := f(r) \cdot m, \quad r \in R, m \in M.$$

Definition 2.16 (Various properties of modules)**.** Let A be a commutative ring with 1.

(1) For the A-modules M, N, a homomorphism of abelian groups $f : M \to N$ is a **homomorphism of A-modules** (or sometimes just called an A-**linear map**) if it respects the scalar multiplication – namely, for any $a \in A$ and $m \in M$, $f(a \cdot m) = a \cdot f(m)$.

(2) The two A-modules M, N are **isomorphic** if there is a bijective homomorphism of A-modules $f : M \to N$.

(3) For an A-module M, an abelian subgroup $N \subset M$ is an A-**submodule** if it is also closed under the scalar multiplication by A – namely, for any $a \in A$ and $n \in N$, $a \cdot n \in N$.

Given an A-submodule $N \subset M$, one can form the quotient group M/N which can be given an obvious A-module structure. This A-module is called the **quotient module**. The natural map $M \to M/N$ is a homomorphism of A-modules.

(4) Given a homomorphism of A-modules $f : M \to N$, the **kernel of** f, denoted $\ker f$, is defined as

$$\ker f := \{m \in M \mid f(m) = 0\} \subset M.$$

It is an A-submodule of M.

The **image of** f, denoted $\operatorname{im} f$, is defined as

$$\operatorname{im} f := \{f(m) \mid m \in M\} \subset N.$$

It is an A-submodule of N. The module version of one of the Isomorphism Theorems is that $\operatorname{im} f$ is isomorphic to the quotient $M/\ker f$ (Easy; exercise).

The quotient $N/\operatorname{im} f$ is called the **cokernel of** f, denoted $\operatorname{coker} f$.

(5) Given any set (may be infinite, may be finite) I and, for each $i \in I$, an A-module M_i, the **direct product** of M_i, denoted $\prod_{i \in I} M_i$, is the A-module defined by

$$\prod_{i \in I} M_i := \{(m_i)_{i \in I} \mid m_i \in M_i \text{ for all } i \in I\},$$

with natural addition and scalar multiplication. Namely, this is a collection of tuples of elements in M_i. If $I = \{1, \cdots, n\}$ is a finite set with cardinality n, we also just write it as $M_1 \times M_2 \times \cdots \times M_n$.

The **direct sum** of M_i, denoted $\bigoplus_{i\in I} M_i$, is the A-submodule of $\prod_{i\in I} M_i$ defined by

$$\bigoplus_{i\in I} M_i := \{(m_i)_{i\in I} \mid m_i \in M_i \text{ for all } i \in I,\ m_i = 0 \text{ for all but finitely many } i \in I\}.$$

If $I = \{1, \cdots, n\}$ is a finite set with cardinality n, we also just write it as $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.[2]

(6) An A-module M is **finitely generated** if there are finitely many elements $m_1, \cdots, m_N \in M$ such that any element $m \in M$ is expressed as an A-linear combination of $m_1, \cdots, m_N$. Namely, for any $m \in M$, there exist $a_1, \cdots, a_N \in A$ such that

$$m = a_1 m_1 + \cdots + a_N m_N.$$

(7) An A-module M is **free** if it is isomorphic to a direct sum of the copies of the ring A as an A-module. If it is isomorphic to a direct sum of finitely many copies, let's say n copies, of A, then we call n the **rank** of M.

(8) For the A-modules M, N, the set of all A-module homomorphisms from M, N is denoted by $\mathrm{Hom}_A(M, N)$. This has a natural structure of an A-module.

Definition 2.17 (Algebra)**.** Let A be a commutative ring with 1. An A-**algebra** is a ring B with 1 that is also an A-module such that

(1) the addition as a ring is the same as the addition as an A-module,

(2) and the scalar multiplication as an A-module is compatible with the multiplication as a ring, namely

$$a \cdot (b_1 b_2) = (a \cdot b_1) b_2 = b_1 (a \cdot b_2), \quad a \in A, b_1, b_2 \in B.$$

Roughly speaking, the notion of algebras is a generalization of the notion of field extensions; a field extension L of a smaller field K is indeed a K-vector space (=K-module) but also has a ring structure.

Example 2.18. If $f : R \to S$ is a homomorphism of commutative rings with 1, then S is naturally an R-algebra. Therefore, any commutative ring with 1 is a $\mathbb{Z}$-algebra.

Conversely, if S is an R-algebra, then there is a natural ring homomorphism $f : R \to S$ given by $f(r) = r \cdot 1$. Therefore, the R-algebra structure is more ore less the same as giving the ring homomorphism from R.

Definition 2.19 (Various properties of algebras)**.** Let A be a commutative ring with 1.

(1) For the A-algebras B_1, B_2, a map $f : B_1 \to B_2$ that is both a homomorphism of A-modules and a ring homomorphism is called a **homomorphism of A-algebras**.

[2]Note that, if I is finite, $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$. On the other hand, mathematicians still would like to distinguish a finite direct sum from a finite direct product for some reason.

(2) The two A-algebras B_1, B_2 are **isomorphic** if there is a bijective homomorphism of A-algebras $f : B_1 \to B_2$.

(3) For an A-algebra B, an A-**subalgebra** is a subring $B' \subset B$ that is also an A-submodule.

(4) An A-algebra B is **finitely generated** if there are finitely many elements $b_1, \cdots, b_N \in B$ such that any element $b \in B$ is expressed as an A-linear combination of finite products of $b_1, \cdots, b_N$ (i.e. a polynomial in $b_1, \cdots, b_N$, with coefficients in A). Namely, for any $b \in B$, there exists an expresion

$$b = \sum_{0 \le i_1, \cdots, i_N \le M} a_{i_1, \cdots, i_N} b_1^{i_1} \cdots b_N^{i_N}, \quad a_{i_1, \cdots, i_N} \in A.$$

(5) For an A-module M, the A-module $\mathrm{Hom}_A(M, M)$ can be given an A-algebra structure by declaring the composition of A-module homomorphisms as its ring multiplication. We denote this as $\mathrm{End}_A(M)$, and call it the **endomorphism algebra** of M.

Remark 2.20 (Warning)**.** By definition, an A-algebra B is also an A-module. However, the notion of being finitely generated as an A-algebra is different from being finitely generated as an A-module. In fact, being finitely generated as an A-module is a stronger condition than being finitely generated as an A-algebra.

For example, let K be a field. Then, the polynomial ring $K[X]$ is naturally a K-algebra. It is finitely generated as a K-algebra, as any element is a polynomial in a single element, X. However, it is **not finitely generated as a K-module**, which is the same as the dimension of $K[X]$ as a K-vector space is infinite.

Definition 2.21 (Integrality)**.** Let A, B be commutative rings with 1, and let $A \hookrightarrow B$ be an injective map of rings. Then, we say $b \in B$ is **integral over** A if there is a monic polynomial $f(X) \in A[X]$ such that $f(b) = 0$.

Example 2.22.

(1) If A, B are fields, then $b \in B$ is integral over A if and only if $b \in B$ is algebraic over A.

(2) If $A = \mathbb{Z}$ and B is a number field, $b \in B$ is integral over A if and only if b is an algebraic integer.

Definition 2.23 (Integral closure)**.** Let A, B be commutative rings with 1, and let $A \hookrightarrow B$ be an injective map of rings. Then, the **integral closure** of A in B is the set

$$\{b \in B \mid b \text{ is integral over } A\}.$$

We say A is **integrally closed** in B if the integral closure of A in B is A itself.

Using this notion, the ring of integers $\mathcal{O}_K$ in K is precisely the integral closure of $\mathbb{Z}$ in K. Thus, Theorem 2.12 will be an immediate corollary to the following Theorem.

Theorem 2.24. *Let A, B be commutative rings with 1, and let $A \hookrightarrow B$ be an injective map of rings.*

(1) *An element $b \in B$ is integral over A if and only if there is an A-subalgebra $R \subset B$ that contains b and is finitely generated as an A-module.*

(2) *The integral closure of A in B is a subring of B.*

Before giving the proof, let's try to understand what this means.

Example 2.25. Let us consider the simple situation of $\mathbb{Z} \subset \mathbb{Q}$. Since $\frac{1}{2} \in \mathbb{Q}$ is obviously not integral over $\mathbb{Z}$, as per Theorem 2.24(1), it should be the case that any $\mathbb{Z}$-subalgebra of $\mathbb{Q}$ containing $\frac{1}{2}$ is not a finitely generated $\mathbb{Z}$-module. In particular, the $\mathbb{Z}$-algebra generated by $\frac{1}{2}$,

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{n}{2^k} \mid n \in \mathbb{Z}, k \geq 1 \right\},$$

should not be a finitely generated $\mathbb{Z}$-module. Let's see why this is the case. Suppose that $\mathbb{Z}\left[\frac{1}{2}\right]$ is a finitely generated $\mathbb{Z}$-module. This means that there are finitely many elements in $\mathbb{Z}\left[\frac{1}{2}\right]$ so that any element in $\mathbb{Z}\left[\frac{1}{2}\right]$ could be expressed as a $\mathbb{Z}$-linear combination of those basis elements. However, it is obvious that this is false, as any $\mathbb{Z}$-linear combination of chosen finitely many elements must have a denominator which divides the common denominator of the basis elements, and there are elements in $\mathbb{Z}\left[\frac{1}{2}\right]$ with arbitrarily high powers of 2 in their denominators.

On the other hand, consider the situation of $\mathbb{Z} \subset \mathbb{Q}(\sqrt{2})$, and consider the $\mathbb{Z}$-subalgebra of $\mathbb{Q}(\sqrt{2})$ generated by $\sqrt{2}$, denoted $\mathbb{Z}[\sqrt{2}]$. Note that by definition this is a collection of elements of the form

$$a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \cdots, \quad a_0, a_1, \cdots \in \mathbb{Z},$$

but by the relation $\sqrt{2}^2 = 2$, any term involving a_n with $n \geq 2$ is actually redundant, and therefore $\mathbb{Z}[\sqrt{2}]$ is just a collection of elements of the form

$$a_0 + a_1\sqrt{2}, \quad a_0, a_1 \in \mathbb{Z},$$

so $\{1, \sqrt{2}\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\sqrt{2}]$, making it a finitely generated $\mathbb{Z}$-module. In fact, this is a **free** $\mathbb{Z}$-module, meaning that there is no $\mathbb{Z}$-linear relation between 1 and $\sqrt{2}$. We will see that this is in fact always true, that $\mathcal{O}_K$ **is always a free** $\mathbb{Z}$**-module** for any number field K.

Proof of Theorem 2.24.

(1) Consider the A-subalgebra of B generated b, denoted as $A[b]$. More precisely,

$$A[b] = \left\{ \sum_{n=0}^{N} a_n b^n \mid N \geq 0, a_n \in A \right\}.$$

Suppose that b is integral over A. Then, we claim that $A[b]$ is a finitely generated A-module. As b is integral over A, there must be some expression of the form

$$b^d = c_{d-1}b^{d-1} + \cdots + c_0, \quad c_{d-1}, \cdots, c_0 \in A.$$

Therefore, any sum of the form $\sum_{n=0}^{N} a_n b^n$ can be rewritten as an A-linear combination of $1, b, \cdots, b^{d-1}$ using the above expression by inductively reducing any d-th or higher power of b into an A-linear combinbation of lower powers of b. Thus, any element in $A[b]$ is able to be expressed as an A-linear combination of $1, b, \cdots, b^{d-1}$, which imlies that $A[b]$ is a finitely generated A-module.

To prove the converse, it is sufficient to prove that any element b of an A-subalgebra $R \subset B$, finitely generated over A, is actually integral over A. There should be finitely many elements $r_1, \cdots, r_N \in R$ such that any element in R can be expressed as an A-linear combination of $r_1, \cdots, r_N$. Therefore, for each $1 \leq i \leq N$, there must be $a_{i1}, \cdots, a_{iN} \in A$ such that

$$br_i = \sum_{j=1}^{N} a_{ij} r_j.$$

We can write this as a matrix form,

$$\begin{pmatrix} b & 0 & \cdots & 0 \\ 0 & b & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & b \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \cdots \\ r_N \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \cdots \\ r_N \end{pmatrix},$$

or

$$\begin{pmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1N} \\ -a_{21} & b - a_{22} & \cdots & -a_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{N1} & -a_{N2} & \cdots & b - a_{NN} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \cdots \\ r_N \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}.$$

Let the $N \times N$ matrix on the left hand side expression be denoted as M. Now, consider the **adjugate of** M, M^{adj}. The Cramer's rule in linear algebra says that

$$M^{\mathrm{adj}} M = \begin{pmatrix} \det M & 0 & \cdots & 0 \\ 0 & \det M & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \det M \end{pmatrix}.$$

This makes a perfect sense over any commutative ring, as there is no "denominator involved." Therefore, multiplying on the left by M^{adj}, we get

$$\begin{pmatrix} \det M & 0 & \cdots & 0 \\ 0 & \det M & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \det M \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \cdots \\ r_N \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}.$$

This implies that $(\det M) r_i = 0$ for any $1 \leq i \leq N$. Since $1 \leq A \subset R$, taking an appropriate linear combination, we have $\det M = 0$. On the other hand, $\det M = p(b)$,

where $p(X) \in A[X]$ is the characteristic polynomial of the $N \times N$ matrix,

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix},$$

and in particular $p(X) \in A[X]$ is a monic polynomial! Thus, b is integral over A.

(2) We have to show that, if $b, b' \in B$ are both integral over A, then both $b + b'$ and bb' are integral over A. Consider the A-subalgebra $A[b.b'] \subset B$ generated by b, b'. More precisely,

$$A[b, b'] = \left\{ \sum_{i,j}^{\text{finite}} a_{ij} b^i b'^j \mid a_{ij} \in A \right\}.$$

Since b, b' are both integral over A, there must be relations

$$b^d = c_{d-1} b^{d-1} + \cdots + c_0, \quad c_{d-1}, \cdots, c_0 \in A,$$

$$b'^{d'} = c'_{d'-1} b'^{d'-1} + \cdots + c'_0, \quad c'_{d'-1}, \cdots, c'_0 \in A.$$

This implies that any linear combination of the form $\sum_{i,j}^{\text{finite}} a_{ij} b^i b'^j$ can be expressed as a linear combination of $b^i b'^j$ with $i < d$, $j < d'$. Therefore, $A[b, b']$ is finitely generated as an A-module.

□

– –

Exercise 2.1. Show that every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some integer $d \in \mathbb{Z}$.

Exercise 2.2. Let A be a commutative ring with 1, and let M, N be A-modules. Find the natural A-module structure on the set $\mathrm{Hom}_A(M, N)$.

3. Lecture 4. Norms, traces, discriminants

Summary. Norms; traces; computing norms and traces; transitivity of norms and traces; norms and traces of algebraic integers; discriminant; computing discriminant; discriminant only depends on the $\mathbb{Z}$-module generated by the basis; formula for $D(1, \alpha, \cdots, \alpha^{n-1})$.

Content. We would like to generalize the notion of norm and trace for quadratic fields to arbitrary number fields. A naive first guess will be, for α in a number field K,

$$N(\alpha) \stackrel{?}{=} \prod \text{conjugates of } \alpha, \quad \mathrm{Tr}(\alpha) \stackrel{?}{=} \sum \text{conjugates of } \alpha.$$

This is indeed a good definition if $K/\mathbb{Q}$ is **Galois**, but not so much when it is not. The correct definition is as follows.

Definition 3.1 (Norms and traces)**.** Let L/K be a finite extension of fields, and let $\alpha \in L$. The multiplication by α gives rise to a K-linear map,

$$m_\alpha : L \to L, \quad x \mapsto \alpha x.$$

The **norm** $N_{L/K}(\alpha) \in K$ and the **trace** $\mathrm{Tr}_{L/K}(\alpha) \in K$ are defined as

$$N_{L/K}(\alpha) := \det(m_\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) := \mathrm{Tr}(m_\alpha).$$

If the base field K is $\mathbb{Q}$, then one often omits the subscript for the norm and the trace.

You may compute these concretely by taking a basis and writing the multiplication map as a square matrix. The matrix itself may depend on the choice of the basis, but its determinant and trace do not depend on the choice.

Proposition 3.2 (Various properties of the norm and the trace)**.** *Let L/K be a finite extension of fields.*

(1) For $\alpha, \beta \in L$, we have

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta).$$

(2) The trace $\mathrm{Tr}_{L/K} : L \to K$ is a K-linear map.

*(3) Both the norm and the trace are **transitive**. Namely, if $M/L/K$ is a "tower" of finite extension of fields, then*

$$N_{M/K} = N_{L/K} \circ N_{M/L}, \quad \mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}.$$

(4) If L/K is Galois, then

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

(5) For $\alpha \in L$,

$$N_{L/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^{[L:K(\alpha)]}, \quad \mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)] \, \mathrm{Tr}_{K(\alpha)/K}(\alpha).$$

(6) In general, the norm and the trace may be computed as follows. Let $p_\alpha(X) \in K[X]$ be the minimal polynomial of α over K, and let M/K be the Galois closure of L/K. Let $\alpha_1 = \alpha, \cdots, \alpha_n$ be the roots of $p_\alpha(X)$ in M. Then,

$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \alpha_i \right)^{[L:K(\alpha)]}, \quad \mathrm{Tr}_{L/K}(\alpha) = [L : K(\alpha)] \sum_{i=1}^{n} \alpha_i.$$

In case when L/K is separable [3], the norm and the trace have the alternative description as follows. As above, let M/L be a field extension which is normal over K (e.g. the Galois closure of L/K, an algebraic closure of L, etc.). Then,

$$N_{L/K}(a) = \prod_{\text{all } K\text{-embeddings } \sigma: L \hookrightarrow M} \sigma(a), \quad \mathrm{Tr}_{L/K}(a) = \sum_{\text{all } K\text{-embeddings } \sigma: L \hookrightarrow M} \sigma(a).$$

Proof. [4]

(1) This follows immediately from that $m_{\alpha\beta} = m_\alpha \circ m_\beta$.

(2) This follows immediately from that the map

$$L \to \mathrm{End}_K(L), \quad \alpha \mapsto m_\alpha,$$

is a K-linear map. More concretely, this means that, given $\alpha, \beta \in L$ and $a, b \in K$,

$$m_{a\alpha+b\beta} = a m_\alpha + b m_\beta,$$

as K-linear maps from L to itself.

(3) The separable case is an easy consequence of (6). We will not care much about the inseparable case; for those who are curious, see the handout by Conrad.

More precisely, let F be a big enough field extension of M such that it is normal over K (e.g. an algebraic closure of M). Then, F/K is Galois, so for $\alpha \in M$, the formula in (6) in terms of Galois theory becomes [5]

$$N_{M/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(F/K)/\mathrm{Gal}(F/M)} \sigma(\alpha).$$

[3] You may safely assume that this is always the case in this course. For example, if K is either of characteristic 0 or a finite field, any field extension of K is separable over K.

[4] The logical order of dependence is a bit convoluted, because (3) and (4) will be proved as a consequence of (6). This is fine because the proof of (6) will not use (3) or (4).

[5] Here, $\mathrm{Gal}(F/K)/\mathrm{Gal}(F/M)$ is merely the set of left cosets, not a group, as M/K is not necessarily a Galois extension.

By the same reason,

$$N_{M/L}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(F/L)/\mathrm{Gal}(F/M)} \sigma(\alpha),$$

and

$$N_{L/K} \circ N_{M/L}(\alpha) = \prod_{\tau \in \mathrm{Gal}(F/K)/\mathrm{Gal}(F/L)} \tau \left(\prod_{\sigma \in \mathrm{Gal}(F/L)/\mathrm{Gal}(F/M)} \sigma(\alpha) \right)$$

$$= \prod_{\tau \in \mathrm{Gal}(F/K)/\mathrm{Gal}(F/L)} \prod_{\sigma \in \mathrm{Gal}(F/L)/\mathrm{Gal}(F/M)} \tau(\sigma(\alpha)).$$

It is now clear from the above expressions that $N_{M/K}(\alpha) = N_{L/K} \circ N_{M/L}(\alpha)$. The same proof works for the trace as well.

(4) This is a special case of (6).

(5) We can choose a K-basis of L in two stages: first, take a $K(\alpha)$-basis of L, say $\{e_1, \cdots, e_m\}$; then, if $n = [K(\alpha) : K]$, the collection $\{\alpha^i e_j\}_{0 \le i < n, 1 \le j \le m}$ is a K-basis of L. Under this basis, the $nm \times nm$ matrix representing $m_\alpha : L \to L$ is just the diagonal block matrix of m copies of the $n \times n$ matrix representing $m_\alpha : K(\alpha) \to K(\alpha)$. The desired statement now follows.

(6) As before, we will only prove the separable case. Without loss of generality, we can assume that M/K is the Galois closure of L/K. We first prove the case when $L = K(\alpha)$ and then prove the general case.

Note that, if $L = K(\alpha)$, then there is a very appealing K-basis of L, namely $\{1, \alpha, \cdots, \alpha^{n-1}\}$, where $n = [K(\alpha) : K]$. Let $p_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of α over K. Then, under the choice of this K-basis, m_α is given by the following $n \times n$ matrix:

$$m_\alpha = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

Thus, $\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_{n-1}$, and $N_{K(\alpha)/K}(\alpha) = (-1)^n a_0$.

Over M, the polynomial $p_\alpha(X)$ factorizes into $p_\alpha(X) = \prod_{i=1}^n (X - \alpha_i)$, with $\alpha_1 = \alpha$. Then, $-a_{n-1} = \sum_{i=1}^n \alpha_i$, and $(-1)^n a_0 = \prod_{i=1}^n \alpha_i$. Note that α_i's are precisely the possible

conjugates of α in M over K. Therefore, as specifying a K-embedding of $L = K(\alpha)$ into M is the same as specifying a K-conjugate of α in M,

$$N_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{n} \alpha_i = \prod_{\text{all } K\text{-embeddings } \sigma: K(\alpha) \hookrightarrow M} \sigma(\alpha), \quad \mathrm{Tr}_{K(\alpha)/K}(\alpha) = \sum_{i=1}^{n} \alpha_i = \sum_{\text{all } K\text{-embeddings } \sigma: K(\alpha) \hookrightarrow M} \sigma(\alpha).$$

As per (5), the general case will follow once we prove that there are exactly $[L : K(\alpha)]$ many different K-embeddings of $L \hookrightarrow M$ lifting a fixed K-embedding $K(\alpha) \hookrightarrow M$, or in other words, given a K-conjugate α_i of α, there are exactly $[L : K(\alpha)]$ many different K-embeddings of $L \hookrightarrow M$ sending α to α_i. Note that there is at least one embedding sending α to α_i, as $M/K(\alpha)$ is Galois, and $\#(\mathrm{Gal}(M/K)/\mathrm{Gal}(M/K(\alpha))) = n$. Now, given such embedding, the number of different K-embeddings of $L \hookrightarrow M$ sending α to α_i is really the same as the number of different $K(\alpha)$-embeddings of $L \hookrightarrow M$ sending α to α (by conjugating by a fixed element in $\mathrm{Gal}(M/K)$ sending α_i to α), which is the same as $\#(\mathrm{Gal}(M/K(\alpha))/\mathrm{Gal}(M/L)) = [L : K(\alpha)]$, as desired.

□

Proposition 3.3 (Norm and $\mathcal{O}_K$)**.** *Let K be a number field.*

(1) Let L/K be a finite extension. For any $\alpha \in \mathcal{O}_L$, $N_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$ are both in $\mathcal{O}_K$.

(2) For $\alpha \in \mathcal{O}_K$, $N(\alpha) = \pm 1$ if and only if $\alpha \in \mathcal{O}_K^\times$ is a unit [6]*.*

Proof.

(1) By Proposition 3.2(6), $N_{L/K}(\alpha)$ ($\mathrm{Tr}_{L/K}(\alpha)$, respectively) is a product (a sum, respectively) of conjugates of α. Since a conjugate of an algebraic integer is an algebraic integer, both $N_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$ are algebraic integers.

(2) Suppose that $\alpha \in \mathcal{O}_K^\times$. Then, there is another $\beta \in \mathcal{O}_K^\times$ such that $\alpha\beta = 1$. Then, $N(\alpha)N(\beta) = N(1) = 1$. However, as $N(\alpha), N(\beta) \in \mathbb{Z}$, it follows that $N(\alpha) = \pm 1$.

Conversely, suppose that $N(\alpha) = \pm 1$. By Proposition 3.2(5) and the proof of Proposition 3.2(6), this implies that the minimal polynomial $p_\alpha(X) \in \mathbb{Z}[X]$ of α over $\mathbb{Q}$ has the constant term equal to ± 1. Let $\widetilde{K}/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$, so that the minimal polynomial $p_\alpha(X)$ factorizes into $p_\alpha(X) = \prod_{i=1}^{n}(X - \alpha_i)$ for $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n \in \widetilde{K}$. As $p_\alpha(X) \in \mathbb{Z}[X]$ is also the minimal polynomial of α_i over $\mathbb{Q}$ (this is because $p_\alpha(X)$ is irreducible), it follows that α_i is integral over $\mathbb{Z}$, which means that $\alpha_i \in \mathcal{O}_{\widetilde{K}}$. Note that $\alpha_2\alpha_3 \cdots \alpha_n = \pm\alpha^{-1} \in K$, but also that $\alpha_2\alpha_3 \cdots \alpha_n \in \mathcal{O}_{\widetilde{K}}$. Therefore, α^{-1} is an element in K integral over $\mathbb{Z}$, so $\alpha^{-1} \in K$ is actually an element of $\mathcal{O}_K$. Therefore, $\alpha \in \mathcal{O}_K^\times$ is a unit.

□

[6] In general, for a commutative ring R with 1, we use the notation $R^\times$ for the group of (multiplicative) units in R.

The concept of norms and traces are extremely useful. One useful byproduct is the notion of the **discriminant** of a number field. For the rest of this lecture, we assume that we already know that, for a number field K, $\mathcal{O}_K$ is in fact a **finitely generated, free $\mathbb{Z}$-module of rank** $[K:\mathbb{Q}]$. This fact will be proved in the next lecture.

Definition 3.4 (Discriminant with respect to a $\mathbb{Q}$-basis)**.** Let K be a number field, $n = [K:\mathbb{Q}]$, and $\{e_1, \cdots, e_n\}$ be a $\mathbb{Q}$-basis of K. Then, the **discriminant** of K with respect to the basis $\{e_1, \cdots, e_n\}$ is

$$D(e_1, \cdots, e_n) := \det(\{\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j)\}_{1\le i,j\le n}) \in \mathbb{Q}.$$

Here, $\{\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j)\}_{1\le i,j\le n}$ represents an $n\times n$ matrix with its (i,j)-th entry equal to $\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j)$ (called the **Gram matrix**).

We note the following.

Proposition 3.5. *Let K be a number field, and let $\{e_1, \cdots, e_n\}$ be a $\mathbb{Q}$-basis of K. Let $L/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$, and let $\sigma_1, \cdots, \sigma_n$ be the distinct $\mathbb{Q}$-embeddings $K \hookrightarrow L$. Then,*

$$D(e_1, \cdots, e_n) = \det(\{\sigma_i(e_j)\}_{1\le i,j\le n})^2.$$

Proof. By Proposition 3.2(6),

$$\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j) = \sum_{k=1}^{n} \sigma_k(e_i e_j).$$

Therefore,

$$D(e_1, \cdots, e_n) = \det\left(\left\{\sum_{k=1}^{n} \sigma_k(e_i)\sigma_k(e_j)\right\}_{1\le i,j\le n}\right) = \det\left(\{\sigma_k(e_i)\}_{1\le i,k\le n}\{\sigma_k(e_j)\}_{1\le k,j\le n}\right)$$

$$= \det\left(\{\sigma_i(e_j)\}_{1\le i,j\le n}\right)^2.$$

□

Proposition 3.6. *If two $\mathbb{Q}$-bases $\{e_1, \cdots, e_n\}$ and $\{f_1, \cdots, f_n\}$ of K generate the same $\mathbb{Z}$-submodule of K, namely if*

$$\mathbb{Z}\cdot e_1 \oplus \cdots \oplus \mathbb{Z}\cdot e_n = \mathbb{Z}\cdot f_1 \oplus \cdots \oplus \mathbb{Z}\cdot f_n \subset K,$$

then

$$D(e_1, \cdots, e_n) = D(f_1, \cdots, f_n).$$

Proof. That the two $\mathbb{Q}$-bases generate the same $\mathbb{Z}$-module means that the change-of-basis matrix M between the two bases has the property that both M and M^{-1} have only integer entries. This means that $\det M$ and $\det M^{-1}$ are both integers. Since $\det M \det M^{-1} = 1$, this implies that $\det M = \pm 1$.

Let us be a little more precise. The matrix M has the (i,j)-th entry equal to a_{ij}, where

$$e_i = \sum_{j=1}^{n} a_{ij} f_j.$$

Therefore,

$$\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j) = \mathrm{Tr}_{K/\mathbb{Q}}(\sum_{k,l=1}^{n} a_{ik} f_k a_{jl} f_l).$$

Therefore,

$$\{\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j)\}_{1\le i,j\le n} = M\{\mathrm{Tr}_{K/\mathbb{Q}}(f_k f_l)\}_{1\le k,l\le n} M^T,$$

where M^T is the transpose of M. This implies that

$$D(e_1, \cdots, e_n) = (\det M) D(f_1, \cdots, f_n)(\det M^T) = (\det M)^2 D(f_1, \cdots, f_n) = D(f_1, \cdots, f_n),$$

as $\det M = \pm 1$. □

Therefore, assuming that $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$, we can define the discriminant of a number field by using the basis coming from $\mathcal{O}_K$.

Definition 3.7 (Discriminant of a number field)**.** Let K be a number field, and $n = [K : \mathbb{Q}]$. Let $\{e_1, \cdots, e_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$ (namely, $\mathcal{O}_K$ is generated by $\{e_1, \cdots, e_n\}$ as a $\mathbb{Z}$-module, and there is no $\mathbb{Z}$-linear relation between $e_1, \cdots, e_n$). Then, the **discriminant of** K, denoted $\mathrm{disc}(K)$, is defined as $D(e_1, \cdots, e_n)$. This is independent of the choice of a $\mathbb{Z}$-basis of $\mathcal{O}_K$ by Proposition 3.6.

The discriminant is a fundamental invariant of a number field that is later related to the notion of **ramification of primes**. On the other hand, at the moment, this is also useful in the computation of the ring of integers $\mathcal{O}_K$ in certain cases – so far we only explicitly know the ring of integers of $\mathbb{Q}$ and quadratic fields, and the general definition of $\mathcal{O}_K$ is pretty abstract.

One key trick to compute $\mathcal{O}_K$ using the discriminant is the following.

Proposition 3.8. *Let K be a number field of degree n, and $\{e_1, \cdots, e_n\}$ be a $\mathbb{Q}$-basis of K such that $e_1, \cdots, e_n \in \mathcal{O}_K$. Let*

$$S = \mathbb{Z} \cdot e_1 \oplus \cdots \oplus \mathbb{Z} \cdot e_n \subset \mathcal{O}_K,$$

be a $\mathbb{Z}$-submodule of $\mathcal{O}_K$. Then,

$$D(e_1, \cdots, e_n) = [\mathcal{O}_K : S]^2 \,\mathrm{disc}(K).$$

As a consequence, if $D(e_1, \cdots, e_n) = \mathrm{disc}(K)$, then $\{e_1, \cdots, e_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.

Proof. Let $f_1, \cdots, f_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then, this means that the change-of-basis matrix from $\{f_1, \cdots, f_n\}$ to $\{e_1, \cdots, e_n\}$ has integer entries (although its inverse may not have integer entries). Namely, there are relations

$$e_i = \sum_{j=1}^{n} a_{ij} f_j, \quad a_{ij} \in \mathbb{Z}.$$

Let M be the $n \times n$ matrix whose (i, j)-th entry is a_{ij}. Then, as in the proof of Proposition 3.6, $D(e_1, \cdots, e_n) = (\det M)^2 \,\mathrm{disc}(K)$. We want to show that $|\det M| = [\mathcal{O}_K : S]$.

This can be seen easily by what's known as the **elementary divisor theorem**, but let us sketch another elementary proof without using this theorem. We can think of an actual $\mathbb{Z}$-lattice (namely, a $\mathbb{Z}$-module) L generated by the vectors $\vec{v_i} = \langle a_{i1}, \cdots, a_{in} \rangle \in \mathbb{R}^n$, $i = 1, \cdots, n$. This is a sublattice of the integer lattice $\mathbb{Z}^n = \{(x_1, \cdots, x_n) \mid x_i \in \mathbb{Z}\} \subset \mathbb{R}^n$. Then, the index $[\mathcal{O}_K : S] = [\mathbb{Z}^n : L]$ is the ratio of the densities of the points in L and those of $\mathbb{Z}^n$, respectively. Namely, let's define D_R to be the open ball in $\mathbb{R}^n$ centered at the origin with radius R, and then we have

$$[\mathcal{O}_K : S] = [\mathbb{Z}^n : L] = \lim_{R \to \infty} \frac{\#(D_R \cap \mathbb{Z}^n)}{\#(D_R \cap L)}.$$

On the other hand, $\#(D_R \cap \mathbb{Z}^n)$ is roughly the volume of D_R, and similarly $\#(D_R \cap L)$ is roughly[7] the volume of D_R **divided by the parallelipiped** P **generated by** $\vec{v}_1, \cdots, \vec{v}_n$. Thus

$$[\mathcal{O}_K : S] = [\mathbb{Z}^n : L] = \lim_{R \to \infty} \frac{\mathrm{vol}(D_R)}{\frac{\mathrm{vol}(D_R)}{\mathrm{vol}(P)}} = \mathrm{vol}(P) = |\det M|,$$

as desired. □

Corollary 3.9. *Let K be a number field of degree n. If there is a $\mathbb{Q}$-basis $\{e_1, \cdots, e_n\}$ of K such that $e_1, \cdots, e_n \in \mathcal{O}_K$ and $D(e_1, \cdots, e_n)$ is a square-free integer, then $\{e_1, \cdots, e_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.*

We now have one strategy to compute $\mathcal{O}_K$: **find a nice $\mathbb{Q}$-basis of K consisted of algebraic integers, and hope that its discriminant is a square-free integer.**

Remark 3.10. There are certainly a lot of examples of number fields whose discriminants are not square-free, so that Corollary 3.9 is not applicable. For example, $\mathrm{disc}(\mathbb{Q}(\sqrt{2})) = 8$.

One particular example of a simple $\mathbb{Q}$-basis of K of algebraic integers is when $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$; then, one can take the $\mathbb{Q}$-basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$, where $n = [K : \mathbb{Q}]$. The discriminant with respect to this basis has a nice formula.

Proposition 3.11. *Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$, $n = [K : \mathbb{Q}]$, and let $p_\alpha(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Suppose that $p_\alpha(X)$ factors into $\prod_{i=1}^n (X - \alpha_i)$ over the Galois closure of $K/\mathbb{Q}$. Then,*

$$D(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(p'_\alpha(\alpha)).$$

[7] One can make this very precise, that

$$\left| \#(D_R \cap L) - \frac{\mathrm{vol}(D_R)}{\mathrm{vol}(P)} \right| < CR^{n-1},$$

for a very explicit constant C (note that $\mathrm{vol}(D_R)$ grows to the order of R^n). This kind of inequality has been proved by many mathematicians, starting from Gauss.

Proof. Note that

$$\begin{aligned}
D(1,\alpha,\cdots,\alpha^{n-1}) &= \det(\{\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{i+j})\}_{1\le i,j\le n}) \\
&= \det\left(\left\{\sum_{k=1}^{n}\alpha_k^{i+j}\right\}_{1\le i,j\le n}\right) \\
&= \det\left(\left\{\alpha_k^{i}\right\}_{1\le i,k\le n}\left\{\alpha_k^{j}\right\}_{1\le k,j\le n}\right) \\
&= \det\left(\{\alpha_i^j\}_{1\le i,j\le n}\right)^2 \\
&= \left(\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)\right)^2 \qquad \text{(Vandermonde matrix)} \\
&= (-1)^{\frac{n(n-1)}{2}}\prod_{1\le i,j\le n,\ i\ne j}(\alpha_i-\alpha_j) \\
&= (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}p'_\alpha(\alpha_i) \quad = \quad (-1)^{\frac{n(n-1)}{2}}N_{K/\mathbb{Q}}(p'_\alpha(\alpha)).
\end{aligned}$$

□

Remark 3.12. This together with the **primitive element theorem** implies that $\mathrm{disc}(K)$ is not zero (see Exercise 3.2).

Remark 3.13. The quantity $\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$ can be computed purely in terms of the coefficients of $p_\alpha(X)$ and $p'_\alpha(X)$ by computing the determinant of a large matrix called the **resultant**.

Example 3.14 (Discriminant of the quadratic fields)**.** Let's compute $\mathrm{disc}(\mathbb{Q}(\sqrt{d}))$, for a square-free nonzero integer d. Of course, the case of $d\equiv 1 \pmod 4$ is different from the case of $d\equiv 2,3 \pmod 4$.

(1) If $d\equiv 1 \pmod 4$, then $\mathrm{disc}(\mathbb{Q}(\sqrt{d})) = D(1,\alpha)$ where $\alpha=\frac{1+\sqrt{d}}{2}$. The minimal polynomial of α over $\mathbb{Q}$ is
$$p_\alpha(X) = X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X].$$
Thus, by Proposition 3.11,
$$\mathrm{disc}(\mathbb{Q}(\sqrt{d})) = D(1,\alpha) = -N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(2\alpha-1) = -N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\sqrt{d}) = d.$$

(2) If $d\equiv 2,3 \pmod 4$, then $\mathrm{disc}(\mathbb{Q}(\sqrt{d})) = D(1,\alpha)$ where $\alpha=\sqrt{d}$. The minimal polynomial of α over $\mathbb{Q}$ is
$$p_\alpha(X) = X^2 - d \in \mathbb{Z}[X].$$
Thus, by Proposition 3.11,
$$\mathrm{disc}(\mathbb{Q}(\sqrt{d})) = D(1,\alpha) = -N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(2\sqrt{d}) = 4d.$$

Example 3.15. Let $f(X) = X^3 - X - 1$. This is irreducible in $\mathbb{Q}[X]$, as it has no rational roots. Therefore, if we let α be a root of $f(X)$, then $K = \mathbb{Q}(\alpha)$ is a degree 3 number field, and by definition, the minimal polynomial of α is $f(X)$, which has integer coefficients, so $\alpha \in \mathcal{O}_K$. Let $\alpha_1 = \alpha, \alpha_2, \alpha_3$ be the three roots of $f(X)$ in the Galois closure of K. Since $f'(X) = 3X^2 - 1$,

$$N_{K/\mathbb{Q}}(f'(\alpha)) = N_{K/\mathbb{Q}}(3\alpha^2 - 1) = (3\alpha_1^2 - 1)(3\alpha_2^2 - 1)(3\alpha_3^2 - 1)$$

$$= 27\alpha_1^2\alpha_2^2\alpha_3^2 - 9(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2\alpha_3^2) + 3(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) - 1.$$

Note that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -1, \quad \alpha_1\alpha_2\alpha_3 = 1.$$

Thus,

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = 2,$$

$$\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2\alpha_3^2 = (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)^2 - 2\alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3) = 1.$$

Therefore, we have

$$N_{K/\mathbb{Q}}(f'(\alpha)) = 27 - 9 + 6 - 1 = 23,$$

so $D(1, \alpha, \alpha^2) = -23$, which is square-free. Therefore, we see that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

– –

Exercise 3.1. Let $f(X) = X^3 + aX + b$, $a, b \in \mathbb{Q}$, such that $f(X)$ is irreducible in $\mathbb{Q}[X]$ (i.e. $f(X)$ has no rational roots). Let α be a root of $f(X)$, and let $K = \mathbb{Q}(\alpha)$ be a degree 3 number field. Show that

$$D(1, \alpha, \alpha^2) = -27b^2 - 4a^3.$$

Exercise 3.2. Read the proof of the **Primitive Element Theorem**. Using the Primitive Element Theorem, we aim to prove that, for a number field K, $\mathrm{disc}(K) \neq 0$.

(1) Use the Primitive Element Theorem to show that one can find $\alpha \in \mathcal{O}_K$ satisfying $K = \mathbb{Q}(\alpha)$.

(2) Show that $D(1, \alpha, \cdots, \alpha^{n-1}) \neq 0$, where $n = [K : \mathbb{Q}]$. Deduce that $\mathrm{disc}(K) \neq 0$.

Exercise 3.3. Let $n > 1$ be an integer, and choose a primitive n-th root of unity $\zeta_n \in \mathbb{C}$. This is an algebraic integer, and the field $\mathbb{Q}(\zeta_n)$ is called the **n-th cyclotomic field**. We will focus on the case when $n = p^a$ is a prime power.

(1) Prove the **Eisenstein's irreducibility criterion**: given a polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X],$$

if there is a prime number p such that the following two Conditions are satisfied, then $f(X)$ is irreducible in $\mathbb{Z}[X]$ (and thus $\mathbb{Q}[X]$, by Gauss's Lemma).

Condition 1. p divides $a_{n-1}, a_{n-2}, \cdots, a_0$.

Condition 2. p^2 does not divide a_0.

(2) Using the Eisenstein's irreducibility criterion, show that the minimal polynomial of ζ_{p^a} over $\mathbb{Q}$ is

$$\Phi_{p^a}(X) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \cdots + X^{p^{a-1}} + 1.$$

This polynomial is called the **p^a-th cyclotomic polynomial.**

Hint. First, note that the minimal polynomial of ζ_{p^a} must divide

$$\frac{X^{p^a} - 1}{X^{p^{a-1}} - 1} = \Phi_{p^a}(X).$$

Then, use the Eisenstein's irreducibility criterion to $\Phi_{p^a}(X+1)$.

(3) Deduce that the conjugates of ζ_{p^a} are $\zeta_{p^a}^k$, $1 \leq k \leq p^a$, $(k,p) = 1$, and that $\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}$ is Galois with

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times.$$

In particular, $\mathbb{Q}(\zeta_{p^a})$ does not depend on the choice of a primitive p^a-th root of unity.

Exercise 3.4. Let p be a prime number, and $a \geq 1$.

(1) Compute $D(1, \zeta_{p^a}, \cdots, \zeta_{p^a}^{p^{a-1}(p-1)-1})$.

(2) Show that $N_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(1 - \zeta_{p^a}) = p$. Deduce that, for any $k \in (\mathbb{Z}/p^a\mathbb{Z})^\times$,

$$\frac{1 - \zeta_{p^a}^k}{1 - \zeta_{p^a}} \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}^\times.$$

This kind of a unit is called a **cyclotomic unit**.

(3) Let $p \geq 5$. Show that

$$\frac{1 - \zeta_{p^a}^2}{1 - \zeta_{p^a}} = 1 + \zeta_{p^a} \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}^\times,$$

is of infinite order. This shows that the multiplicative group of units $\mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}^\times$ as an abelian group is infinite.

Hint. We have a freedom to choose ζ_{p^a}. Choose $\zeta_{p^a} = e^{\frac{2\pi i}{p^a}}$, and show that $\left|1 + e^{\frac{2\pi i}{p^a}}\right| > 1$ (the absolute value as a complex number).

4. Lecture 5. Finiteness of $\mathcal{O}_K$

Summary. $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module; $\mathcal{O}_K^\vee$; the discriminant of a subfield divides the discriminant of a larger field; basis of $\mathcal{O}_{KL}$ in terms of bases of $\mathcal{O}_K$ and $\mathcal{O}_L$, if $\mathrm{disc}(K)$ and $\mathrm{disc}(L)$ are coprime.

Content. The following, as promised before, is another very important property of $\mathcal{O}_K$.

Theorem 4.1. *Given a number field K, its ring of integers $\mathcal{O}_K$ is a finitely generated, free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$. Equivalently, $\mathcal{O}_K \cong \mathbb{Z}^{\oplus[K:\mathbb{Q}]}$ as abelian groups.*

Proof. Recall the Fundamental Theorem of finitely generated abelian groups: a finitely generated abelian group G is always of the form

$$G \cong \mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}), \quad n_1|n_2|\cdots|n_k.$$

Let $n = [K:\mathbb{Q}]$, and choose a $\mathbb{Q}$-basis of K, $e_1, \cdots, e_n$. Certainly, any element $\alpha \in \mathcal{O}_K$ can be expressed as a $\mathbb{Q}$-linear combination of $e_1, \cdots, e_n$,

$$\alpha = a_1e_1 + \cdots + a_ne_n, \quad a_1, \cdots, a_n \in \mathbb{Q}.$$

Of course, $a_1, \cdots, a_n$ are not necessarily integers and merely rational numbers. However, if one could somehow show that the common denominator of $a_1, \cdots, a_n$ always divides some big integer d, then this implies that $a_1, \cdots, a_n \in \frac{1}{d}\mathbb{Z}$, so

$$(*) \qquad \mathcal{O}_K \subset \mathbb{Z} \cdot \frac{e_1}{d} \oplus \cdots \oplus \mathbb{Z} \cdot \frac{e_n}{d}.$$

Since $\frac{e_1}{d}, \cdots, \frac{e_n}{d}$ have no $\mathbb{Q}$-linear relation (they form a $\mathbb{Q}$-basis), they have no $\mathbb{Z}$-linear relation. Thus, $\mathbb{Z} \cdot \frac{e_1}{d} \oplus \cdots \oplus \mathbb{Z} \cdot \frac{e_n}{d}$ is a free abelian group (=$\mathbb{Z}$-module) of rank n.

This actually implies that $\mathcal{O}_K$ is a finitely generated free abelian group (=$\mathbb{Z}$-module): any abelian subgroup (=$\mathbb{Z}$-submodule) of a finitely generated free group does not have a non-trivial torsion element, so by the Fundamental Theorem invoked above, an abelian subgroup of a finitely generated free group is finitely generated and free.

Note also that for a sufficiently divisible integer N, $Na_i \in \mathcal{O}_K$. More precisely, we can let N be any integer divisible by the common denominator of the coefficients of the minimal polynomial of a_i over $\mathbb{Q}$ for each i. Thus, by replacing $a_1, \cdots, a_n$ with $Na_1, \cdots, Na_n$, we can assume that $a_1, \cdots, a_n \in \mathcal{O}_K$. Then, we have

$$\mathbb{Z} \cdot e_1 \oplus \cdots \oplus \mathbb{Z} \cdot e_n \subset \mathcal{O}_K.$$

Therefore, if we prove (19.9), then not only we prove $\mathcal{O}_K$ is a finitely generated free abelian group (=$\mathbb{Z}$-module), we have

$$n = \mathrm{rank}\, \mathbb{Z} \cdot e_1 \oplus \cdots \oplus \mathbb{Z} \cdot e_n \leq \mathrm{rank}\, \mathcal{O}_K \leq \mathrm{rank}\, \mathbb{Z} \cdot \frac{e_1}{d} \oplus \cdots \oplus \mathbb{Z} \cdot \frac{e_n}{d} = n,$$

so $\mathrm{rank}\, \mathcal{O}_K = n$. Thus, all we need to prove is (19.9).

Consider the symmetric bilinear pairing on K,

$$\langle , \rangle : K \times K \to \mathbb{Q}, \quad \langle x, y \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy).$$

Here, "symmetric" means that $\langle x, y \rangle = \langle y, x \rangle$, and "bilinear" means that $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ and $\langle x, y+z \rangle = \langle x, y \rangle = \langle x, z \rangle$. Anyway, it is clear that, if $x, y \in \mathcal{O}_K$, then $\langle x, y \rangle \in \mathbb{Z}$.

Now consider $x \in \mathcal{O}_K$. Then, as $\{e_1, \cdots, e_n\}$ is a $\mathbb{Q}$-basis of K, there are $c_1, \cdots, c_n \in \mathbb{Q}$ such that

$$x = c_1 e_1 + \cdots + c_n e_n.$$

We would like to bound the denominators of $c_1, \cdots, c_n$. Note that

$$\langle x, e_j \rangle = \sum_{i=1}^{n} c_i \langle e_i, e_j \rangle,$$

which can be written as a matrix form as

$$(**) \qquad \begin{pmatrix} \langle x, e_1 \rangle \\ \langle x, e_2 \rangle \\ \cdots \\ \langle x, e_n \rangle \end{pmatrix} = \begin{pmatrix} \langle e_1, e_1 \rangle & \langle e_2, e_1 \rangle & \cdots & \langle e_n, e_1 \rangle \\ \langle e_1, e_2 \rangle & \langle e_2, e_2 \rangle & \cdots & \langle e_n, e_2 \rangle \\ \cdots & \cdots & \cdots & \cdots \\ \langle e_1, e_n \rangle & \langle e_2, e_n \rangle & \cdots & \langle e_n, e_n \rangle \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \cdots \\ c_n \end{pmatrix}.$$

Let the $n \times n$ matrix in the middle (the **Gram matrix**) be denoted as M. Note that $\det M$ is precisely the discriminant $D(e_1, \cdots, e_n)$. By Proposition 3.8, this is a nonzero multiple of $\mathrm{disc}(K)$, which is also nonzero by Exercise 3.2. Therefore, M is an invertible matrix. Using $M^{-1} = \frac{1}{\det M} M^{\mathrm{adj}}$, we obtain

$$\frac{1}{\det M} M^{\mathrm{adj}} \begin{pmatrix} \langle x, e_1 \rangle \\ \langle x, e_2 \rangle \\ \cdots \\ \langle x, e_n \rangle \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ \cdots \\ c_n \end{pmatrix}.$$

Since $\begin{pmatrix} \langle x, e_1 \rangle \\ \langle x, e_2 \rangle \\ \cdots \\ \langle x, e_n \rangle \end{pmatrix}$ and M^{adj} both have the integer entries, the denominators of c_i divide $\det M$, which does not depend on x, and this is what we want. □

The proof of Theorem 4.1 gives a yet another interpretation of $\mathrm{disc}(K)$.

Definition 4.2 (Dual lattice). Let $\mathcal{O}_K^\vee = \{x \in K \mid \langle x, \alpha \rangle \in \mathbb{Z} \text{ for all } \alpha \in \mathcal{O}_K\}$.

This is an abelian group that obviously contains $\mathcal{O}_K$.

Theorem 4.3. *The abelian group $\mathcal{O}_K^\vee / \mathcal{O}_K$ is finite, and*

$$|\mathrm{disc}(K)| = |\mathcal{O}_K^\vee / \mathcal{O}_K|.$$

Proof. Consider the $\mathbb{Q}$-linear map $f : K \to \mathbb{Q}^n$ defined by

$$f(x) = \begin{pmatrix} \langle x, e_1 \rangle \\ \langle x, e_2 \rangle \\ \cdots \\ \langle x, e_n \rangle \end{pmatrix}.$$

This is an injective map of $\mathbb{Q}$-vector spaces of the same dimension, so it is bijective. By definition, the image of $\mathcal{O}_K^\vee$ under f is $\mathbb{Z}^n \subset \mathbb{Q}^n$. On the other hand, from the equation $(**)$, the image of $\mathcal{O}_K$ under f is $M\mathbb{Z}^n$, where $M = \{\langle e_i, e_j \rangle\}_{1 \leq i,j \leq n}$ is the Gram matrix. Therefore, $|\mathcal{O}_K^\vee / \mathcal{O}_K| = |\det M| = |\operatorname{disc}(K)|$. □

From this, we obtain another useful property of the discriminant which will be later useful in more sophisticated computation of $\mathcal{O}_K$.

Theorem 4.4. *Let L/K be a field extension of two number fields. Then,* $\operatorname{disc}(K)$ *divides* $\operatorname{disc}(L)$.

Proof. Let $\alpha \in \mathcal{O}_K^\vee \subset K$. Then, for any $\beta \in \mathcal{O}_L$,

$$\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta) = \operatorname{Tr}_{K/\mathbb{Q}}(\operatorname{Tr}_{L/K}(\alpha\beta)) = \operatorname{Tr}_{K/\mathbb{Q}}(\alpha \operatorname{Tr}_{L/K}(\beta)) \in \mathbb{Z},$$

as $\operatorname{Tr}_{L/K}(\beta) \in \mathcal{O}_K$. Thus, $\mathcal{O}_K^\vee \subset \mathcal{O}_L^\vee$. Note also that

$$\mathcal{O}_K = \mathcal{O}_L \cap \mathcal{O}_K \subset \mathcal{O}_L \cap \mathcal{O}_K^\vee \subset \mathcal{O}_L \cap K = \mathcal{O}_K,$$

so $\mathcal{O}_K = \mathcal{O}_L \cap \mathcal{O}_K^\vee$. Thus, we have an inclusion of finite abelian groups,

$$\mathcal{O}_K^\vee / \mathcal{O}_K \hookrightarrow \mathcal{O}_L^\vee / \mathcal{O}_L.$$

Theorem follows from Theorem 4.3. □

The proof of Theorem 4.1 has some other interesting consequences.

Corollary 4.5. *There is an algorithm (i.e. a deterministic procedure that is guaranteed to stop in a finite number of steps) that computes $\mathcal{O}_K$ for any number field K.*

Proof. In words, the algorithm is as follows.

(1) Choose a $\mathbb{Q}$-basis $e_1, \cdots, e_n$ of K.

(2) Compute the minimal polynomial $p_i(X) \in \mathbb{Q}[X]$ of e_i over $\mathbb{Q}$.

(3) Let N_i be the common denominator of the coefficients of $p_i(X)$. Then, $f_i := N_i e_i \in \mathcal{O}_K$.

(4) Compute $D = D(f_1, \cdots, f_n) \in \mathbb{Z} \backslash \{0\}$. By the proof of Theorem 4.1, we know that

$$\mathbb{Z} \cdot f_1 \oplus \cdots \oplus \mathbb{Z} \cdot f_n \subset \mathcal{O}_K \subset \mathbb{Z} \cdot \frac{f_1}{D} \oplus \cdots \oplus \mathbb{Z} \cdot \frac{f_n}{D}.$$

Now one notices that the index between the two abelian groups sandwiching $\mathcal{O}_K$ is (very big but still) finite:

$$\left[\left(\mathbb{Z}\cdot\frac{f_1}{D}\oplus\cdots\oplus\mathbb{Z}\cdot\frac{f_n}{D}\right):(\mathbb{Z}\cdot f_1\oplus\cdots\oplus\mathbb{Z}\cdot f_n)\right]=D^n<\infty.$$

Therefore, to determine $\mathcal{O}_K$, one has to check whether each of the D^n cosets belongs to $\mathcal{O}_K$. That is, for $1\leq i_1,\cdots,i_n\leq D$, check whether

$$\frac{i_1}{D}f_1+\cdots+\frac{i_n}{D}f_n,$$

is an algebraic integer.

This very long but still finite check will determine $\mathcal{O}_K$.

□

Of course, the above algorithm is **not at all practical**, as the discriminant is usually very big, and the algorithm needs a power of the discriminant many steps. In practice, when computing by hand, one usually relies on Corollary 3.9, or the knowledge of the ring of integers of a small number field combined with the following Proposition.

Proposition 4.6. *Let K, L be two number fields, both Galois over $\mathbb{Q}$, such that $K\cap L=\mathbb{Q}$. Let $\{e_1,\cdots,e_m\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$, and $\{f_1,\cdots,f_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$. If $(\mathrm{disc}(K),\mathrm{disc}(L))=1$, then*

$$\{e_if_j\}_{1\leq i\leq m,\ 1\leq j\leq n},$$

is a $\mathbb{Z}$-basis of $\mathcal{O}_{KL}$, and $\mathrm{disc}(KL)=\mathrm{disc}(K)^n\,\mathrm{disc}(L)^m$.

Proof. Note that $K\cap L=\mathbb{Q}$ implies that $[KL:\mathbb{Q}]=mn$, so $\{e_if_j\}_{1\leq i\leq m,\ 1\leq j\leq n}$ forms a $\mathbb{Q}$-basis of KL. Furthermore, $KL/\mathbb{Q}$ is Galois (an exercise in Galois theory). Let

$$\mathrm{Gal}(KL/L)=\{\sigma_1,\cdots,\sigma_m\},\quad \mathrm{Gal}(KL/K)=\{\tau_1,\cdots,\tau_n\},$$

so that

$$\mathrm{Gal}(KL/\mathbb{Q})=\{\sigma_i\tau_j\mid 1\leq i\leq m,\ 1\leq j\leq n\}.$$

Let $\alpha\in\mathcal{O}_{KL}$, and let

$$\alpha=\sum_{i,j}a_{ij}e_if_j,\quad a_{ij}\in\mathbb{Q}.$$

We want to show that $a_{ij}\in\mathbb{Z}$. Let

$$\beta_j=\sum_{i=1}^{m}a_{ij}e_i\in K,\quad 1\leq j\leq n.$$

Then, for $1\leq k\leq n$,

$$\tau_k(\alpha)=\sum_{j=1}^{n}\tau_k(\beta_jf_j)=\sum_{j=1}^{n}\beta_j\tau_k(f_j),$$

as τ_k fixes K. Therefore,

$$\begin{pmatrix} \tau_1(\alpha) \\ \tau_2(\alpha) \\ \cdots \\ \tau_n(\alpha) \end{pmatrix} = \begin{pmatrix} \tau_1(f_1) & \tau_1(f_2) & \cdots & \tau_1(f_n) \\ \tau_2(f_1) & \tau_2(f_2) & \cdots & \tau_2(f_n) \\ \cdots & \cdots & \cdots & \cdots \\ \tau_n(f_1) & \tau_n(f_2) & \cdots & \tau_n(f_n) \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{pmatrix}.$$

Let the $n \times n$ matrix in the middle be denoted as A. Then, by Proposition 3.5, $\mathrm{disc}(L) = \det(A)^2$. Thus,

$$A^{\mathrm{adj}} \begin{pmatrix} \tau_1(\alpha) \\ \tau_2(\alpha) \\ \cdots \\ \tau_n(\alpha) \end{pmatrix} = \det(A) \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdots \\ \beta_n \end{pmatrix}.$$

Note that both A^{adj} and $\begin{pmatrix} \tau_1(\alpha) \\ \tau_2(\alpha) \\ \cdots \\ \tau_n(\alpha) \end{pmatrix}$ have their entries in $\mathcal{O}_{KL}$, because a Galois conjugate of an algebraic integer is an algebraic integer. Therefore, $\det(A)\beta_j \in \mathcal{O}_{KL}$ for $1 \leq j \leq n$, which implies that $\mathrm{disc}(L)\beta_j \in \mathcal{O}_{KL}$. Now note that $\mathrm{disc}(L)\beta_j \in K$, so $\mathrm{disc}(L)\beta_j \in \mathcal{O}_K$, which means that

$$\mathrm{disc}(L)\beta_j = \sum_{i=1}^{m} \mathrm{disc}(L) a_{ij} e_i,$$

has the integer coefficients, namely $\mathrm{disc}(L)a_{ij} \in \mathbb{Z}$ for all i, j.

We can swap the roles of K and L and go through the argument as above, which will then yield $\mathrm{disc}(K)a_{ij} \in \mathbb{Z}$ for all i, j. Since $\mathrm{disc}(K)$ and $\mathrm{disc}(L)$ are coprime to each other, $a_{ij} \in \mathbb{Z}$ for all i, j, as desired.

To compute the discriminant, we again use Proposition 3.5. Namely, $\mathrm{disc}(KL) = \det(B)^2$, where B is the $mn \times mn$ matrix given by

$$B = \{\sigma_i \tau_j(e_k f_l)\}_{1 \leq i,k \leq m,\ 1 \leq j,l \in n}.$$

Here, we use the description of the elements of $\mathrm{Gal}(KL/\mathbb{Q})$ and the just-proven fact that $\{e_k f_l\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_{KL}$. Note that

$$\sigma_i \tau_j(e_k f_l) = \sigma_i(e_k)\tau_j(f_l),$$

so $B = C \otimes D$ is the tensor product of the two square matrices C and D, where C and D are the $m \times m$ and $n \times n$ matrices with entries

$$C = \{\sigma_i(e_k)\}_{1 \leq i,k \leq m}, \quad D = \{\tau_j(f_l)\}_{1 \leq j,l \leq n},$$

respectively. Thus,

$$\det(B) = \det(C)^n \det(D)^m.$$

Since Proposition 3.5 implies that $\mathrm{disc}(K) = \det(C)^2$ and $\mathrm{disc}(L) = \det(D)^2$, we get

$$\mathrm{disc}(KL) = \mathrm{disc}(K)^n \mathrm{disc}(L)^m.$$

□

Example 4.7. We know that all quadratic fields are Galois over $\mathbb{Q}$. Thus, for example, we can use Proposition 4.6 to compute the $\mathbb{Z}$-basis of the ring of integers of $\mathbb{Q}(i, \sqrt{-3})$, because $\mathrm{disc}(\mathbb{Q}(i)) = -4$ and $\mathrm{disc}(\mathbb{Q}(\sqrt{-3})) = -3$ by Example 3.14. Namely,

$$\mathrm{disc}(\mathbb{Q}(i, \sqrt{-3})) = \mathrm{disc}(\mathbb{Q}(i))^2 \,\mathrm{disc}(\mathbb{Q}(\sqrt{-3}))^2 = 16 \cdot 9 = 144,$$

and a $\mathbb{Z}$-basis of $\mathcal{O}_{\mathbb{Q}(i,\sqrt{-3})}$ can be taken to be

$$\left\{1, i, \frac{1+\sqrt{-3}}{2}, \frac{i-\sqrt{3}}{2}\right\}.$$

– –

Exercise 4.1. Let p be an odd prime. In Exercise 3.3, we proved that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$. As this Galois group is a cyclic group of even order, there is a unique nontrivial group homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$. By Galois theory, there is a corresponding subfield $K \subset \mathbb{Q}(\zeta_p)$, which is the unique quadratic subfield. Show that

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Hint. Use $\mathrm{disc}(K) | \,\mathrm{disc}(\mathbb{Q}(\zeta_p))$.

Exercise 4.2. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n with $\alpha \in \mathcal{O}_K$, such that the minimal polynomial $p_\alpha(X)$ of α over $\mathbb{Q}$ satisfies the Eisenstein's irreducibility criterion with a prime number p (we say that $p_\alpha(X)$ is **Eisenstein at** p in short).

(1) If $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ are integers such that

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in p\mathcal{O}_K,$$

then show that $a_0, a_1, \cdots, a_{n-1} \in p\mathbb{Z}$.
Hint. First, multiply the expression by α^{n-1} to show that $a_0 \in p\mathbb{Z}$. Then, inductively show that $a_1 \in p\mathbb{Z}$, $a_2 \in p\mathbb{Z}$, $\cdots$.

(2) If $x \in \mathcal{O}_K$ has an expression

$$x = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \quad b_0, \cdots, b_{n-1} \in \mathbb{Q},$$

show that each $b_i \in \mathbb{Q}$ has no p in its denominator.

(3) Prove that $(p, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$ by showing that there is no element of order p in the finite abelian group $\mathcal{O}_K/\mathbb{Z}[\alpha]$.

(4) Show that $\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} = \mathbb{Z}[\sqrt[5]{2}]$ as follows.

- Note that $[\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} : \mathbb{Z}[\sqrt[5]{2}]]$ divides $\mathrm{disc}(1, \sqrt[5]{2}, \cdots, \sqrt[5]{2^4})$, which has only 2 and 5 as prime factors (compute it).
- 2 does not divide $[\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} : \mathbb{Z}[\sqrt[5]{2}]]$ as the minimal polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}$, $X^5 - 2$, is Eisenstein at 2.
- 5 does not divide $[\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} : \mathbb{Z}[\sqrt[5]{2}]]$ as the minimal polynomial of $\sqrt[5]{2} - 2$ over $\mathbb{Q}$, $(X + 2)^5 - 2$, is Eisenstein at 5.

5. Lecture 6. Dedekind domains

Summary. Dedekind domains; prime and maximal ideals; Noetherian rings and modules; finitely generated module over a Noetherian ring is Noetherian; normal integral domain; $\mathcal{O}_K$ is a Dedekind domain.

Content. As we have seen before, the unique factorization property does not hold in general for $\mathcal{O}_K$. As the unique factorization property is an extremely useful arithmetic property to have for number-theoretic applications (e.g. the first Lecture), one may wonder how to retain the unique factorization property in general number fields. It turns out that the unique factorization property holds in great generality once we start to work with **ideals** instead of **numbers**.

Indeed, the notion of "a divides b" can be reinterpreted in ideal-theoretic terms as "b is an element of the ideal (a) generated by a", or even better as "$(b) \subset (a)$". Thus, the discussion of divisibility of numbers can all be recast in terms of the ideals. We will see that

- the notions like the prime numbers and the unique factorization property all translate very well in great generality in terms of ideals,
- and that the failure of the unique factorization of numbers is actually the failure of a general ideal being a **principal ideal** (i.e. $\mathcal{O}_K$ is not UFD if and only if $\mathcal{O}_K$ is not a PID, a **principal ideal domain**).

We will develop the theory of **Dedekind domains** in which the unique factorization of ideals holds, and will prove that the rings of integers of number fields $\mathcal{O}_K$ are always Dedekind domains.

Definition 5.1 (Dedekind domains)**.** A **Dedekind domain** is a **Noetherian**, **normal** integral domain which is not a field and whose **nonzero prime ideals are maximal**.

We will explain what these words (in particular "Noetherian" and "normal") mean in a second. First, recall the following notions.

Definition 5.2 (Prime and maximal ideals)**.** Let A be a commutative ring with 1.

(1) A proper ideal $I \subset A$ (i.e. $I \neq A$) is a **prime ideal** if the following condition holds: if $a, b \in A$ satisfies that $ab \in I$, then either $a \in I$ or $b \in I$ must hold.

In other words, I is a prime ideal if and only if the quotient ring A/I is an **integral domain** (Easy).

(2) A proper ideal $I \subset A$ is a **maximal ideal** if any proper ideal $I \subset J \subset A$ containing I must satisfy $I = J$.

In other words, I is a maximal ideal if and only if the quotient ring A/I is a **field** (Easy).

From above, it is immediate that **all maximal ideals are prime ideals**.

Definition 5.3 (Noetherian rings and modules)**.** Let A be a commutative ring with 1, and let M be an A-module.

(1) An A-module M is called **Noetherian** if it satisfies the **ascending chain condition**: for any increasing sequence of submodules of M,

$$M_1 \subset M_2 \subset M_3 \subset \cdots,$$

there is some $n > 0$ such that $M_n = M_{n+1} = M_{n+2} = \cdots$; i.e. any increasing chain of submodules eventually stabilizes.

(2) The commutative ring A is called **Noetherian** if A is Noetherian as an A-module. Equivalently[8], for any increasing sequence of ideals of A,

$$I_1 \subset I_2 \subset I_3 \subset \cdots,$$

there is some $n > 0$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$; i.e. any increasing chaing of ideals eventually stabilizes.

Example 5.4.

(1) Any field is a Noetherian ring, because the only ideals are either (0) or itself.

(2) The ring of rational integers, $\mathbb{Z}$, or more generally any PID is a Noetherian ring. This is because an ascending chain of ideals is the same as an infinite dividing chain of elements by taking their generators,

$$a_1 \text{ is divisible by } a_2 \text{ is divisible by } a_3 \text{ is divisible by } \cdots,$$

and as PID is a UFD, after taking the prime factorization of a_1, there are only finitely many prime factors you can strip away from a_1, so after a finite amount of steps, a_n, a_{n+1}, a_{n+2}, $\cdots$ will all be just off by a unit, which means that the ideals $(a_n) = (a_{n+1}) = (a_{n+2}) = \cdots$ are the same.

(3) An example of a non-Noetherian ring is the ring of all algebraic integers in $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, as it has an infinite increasing sequence of ideals,

$$(2) \subset (2^{1/2}) \subset (2^{1/4}) \subset \cdots.$$

Another example is the ring of all ($\mathbb{R}$-valued) continuous functions on $\mathbb{R}$ (with pointwise multiplication and addition), as it has an infinite increasing sequence of ideals $I_1 \subset I_2 \subset \cdots$, where

$$I_n = \{f : \mathbb{R} \to \mathbb{R} \text{ continuous} \mid f(x) = 0 \text{ for all } x \geq n\}.$$

The Noetherianity condition is very close to the notion of finite generation.

Proposition 5.5. *Let A be a commutative ring with 1, and let M be an A-module. Then, M is Noetherian if and only if every A-submodule of M is finitely generated.*

[8]This is because an A-submodule of A is precisely an ideal of A.

Corollary 5.6. *A commutative ring A with 1 is Noetherian if and only if every ideal is finitely generated.*

Proof of Proposition 5.5. Suppose that M is Noetherian, and let $N \subset M$ be an A-submodule. Suppose on the contrary that N is not finitely generated. Then, we can inductively choose the finitely generated submodules N_i of N as follows.

- Choose $n_1 \in N$, and let $N_1 = An_1 \subset N$.
- For each i, N_i is a finitely generated A-module, so $N_i \neq N$. Therefore, one can choose $n_{i+1} \in N \backslash N_i$, and the A-module

$$N_{i+1} = N_i + An_{i+1} \subset N,$$

  contains N_i. Also, as $n_{i+1} \in N_{i+1}$, $N_i \neq N_{i+1}$

This gives rise to an increasing sequence $N_1 \subset N_2 \subset \cdots$ of A-submodules of M that never stabilizes, which contradicts the Noetherianity of M.

Suppose for the converse that every A-submodule of M is finitely generated, and let $M_1 \subset M_2 \subset \cdots$ be an increasing sequence of A-submodules of M. Let

$$N := \bigcup_{a \geq 1} M_a.$$

One can check very easily that $N \subset M$ is in fact an A-submodule. Therefore, by the assumption, N is finitely generated, say by the elements $n_1, \cdots, n_k \in N$. Then, as $N = \bigcup_{a \geq 1} M_a$, for each n_i, there must be $a_i \geq 1$ such that $n_i \in M_{a_i}$. Taking $R = \max(a_1, \cdots, a_k)$,

$$n_1, n_2, \cdots, n_k \in M_R,$$

which means that the A-module generated by $n_1, \cdots, n_k$, which is N, is also contained in M_R. This means that $N = M_R$, so $M_R = M_{R+1} = M_{R+2} = \cdots$ stabilizes. □

Here are some useful ways to construct Noetherian rings and modules.

Theorem 5.7 (Finitely generated over Noetherian is Noetherian)**.** *Let A be a Noetherian ring.*

(1) A finitely generated A-module is Noetherian as an A-module.

(2) An A-algebra B that is finitely generated as an A-module is a Noetherian ring.

Proof.

(1) This is Exercise 5.1.

(2) Let $I_1 \subset I_2 \subset \cdots$ be an increasing sequence of ideals of B, or B-submodules of B. Then, these are also A-submodules of B. As B is a Noetherian A-module, this sequence must stabilize.

□

Corollary 5.8 ($\mathcal{O}_K$ is Noetherian)**.** *For a number field K, $\mathcal{O}_K$ is a Noetherian ring.*

Proof. By Theorem 4.1, $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, and $\mathbb{Z}$ is a Noetherian ring as it is a PID. Thus, by Theorem 5.7(2), $\mathcal{O}_K$ is a Noetherian ring. □

Now on to the normality:

Definition 5.9 (Normal integral domains)**.** An integral domain A is **normal** if A is integrally closed (recall Definition 2.23) in its field of fractions, $\mathrm{Frac}(A)$.

Example 5.10.

(1) Proposition 2.5 implies that $\mathbb{Z}$ is normal.

(2) More generally, one can easily prove that **any UFD is normal** by using the same proof as that of Proposition 2.5. This explains why $\mathbb{Z}[\sqrt{-3}]$ has no chance of being a UFD; it is not $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, so not normal!

Even though $\mathcal{O}_K$ is not in general a UFD, it is always normal!

Theorem 5.11 ($\mathcal{O}_K$ is normal)**.** *Let L/K be a field extension of two number fields. Then, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.*

In particular, setting $L = K$, this shows that $\mathcal{O}_K$ is normal.

Proof. Let $\alpha \in L$ be integral over $\mathcal{O}_K$. By Theorem 2.24(1), $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathcal{O}_K$-module. As $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, this implies that $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathbb{Z}$-module. This implies that $\mathbb{Z}[\alpha] \subset \mathcal{O}_K[\alpha]$ is a finitely generated $\mathbb{Z}$-module (=abelian group), or, in other words, α is integral over $\mathbb{Z}$. Thus, $\alpha \in \mathcal{O}_L$. Thus, the integral closure of $\mathcal{O}_K$ in L is contained in $\mathcal{O}_L$. The reverse containment is obvious. □

Now we can prove what we want.

Theorem 5.12 ($\mathcal{O}_K$ is Dedekind)**.** *For a number field K, $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Corollary 5.8 and Theorem 5.11 have already proved that $\mathcal{O}_K$ is a Noetherian, normal integral domain. It is obvious that $\mathcal{O}_K$ is not a field, so we only need to prove that all nonzero prime ideals of $\mathcal{O}_K$ are maximal.

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal. Then, there is some nonzero integer contained in $\mathfrak{p}$ (e.g. for $\alpha \in \mathfrak{p}$ nonzero, $N(\alpha) \in \mathfrak{p}$), so $\mathfrak{p}' := \mathfrak{p} \cap \mathbb{Z}$ is a nonzero ideal of $\mathbb{Z}$. Note that, by definition, the natural map

$$\mathbb{Z}/\mathfrak{p}' \to \mathcal{O}_K/\mathfrak{p},$$

is injective. This implies that $\mathbb{Z}/\mathfrak{p}'$ is a subring of an integral domain, so it is also an integral domain. Therefore, $\mathfrak{p}' \subset \mathbb{Z}$ is a nonzero prime ideal, generated by an actual prime number p. Therefore, $\mathbb{Z}/\mathfrak{p}' = \mathbb{F}_p$ is a finite field.

Now we use that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Let $e_1, \cdots, e_n \in \mathcal{O}_K$ generate $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Then, their natural images $e_1, \cdots, e_n \in \mathcal{O}_K/\mathfrak{p}$ generate $\mathcal{O}_K/\mathfrak{p}$ as a $\mathbb{Z}/\mathfrak{p}' = \mathbb{F}_p$-module. As $\mathcal{O}_K/\mathfrak{p}$ is an integral domain, by Exercise 5.2, this implies that $\mathcal{O}_K/\mathfrak{p}$ is a field, which means that $\mathfrak{p}$ is a maximal ideal. □

Next time, we will prove that Dedekind domains have **unique factorization of ideals**.

Theorem 5.13 (Dedekind domains have unique factorization of ideals)**.** *Let A be a Dedekind domain. Then, any nonzero ideal $I \subset A$ can be written as a product*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

of nonzero (not necessarily distinct) prime ideals, and this expression is unique up to rearrangement of the $\mathfrak{p}_i$'s.

Remark 5.14. In fact, this is an if-and-only-if statement!

– –

Exercise 5.1. In this exercise, we will prove the following

Theorem. For a Noetherian ring A, any finitely generated A-module is Noetherian.

(1) Let B be any commutative ring with 1 and M be a B-module. Let $N \subset M$ be a B-submodule, and let $M_1, M_2 \subset M$ be two B-submodules of M. Show that $M_1 = M_2$ if and only if $M_1 \cap N = M_2 \cap N$ and $\frac{M_1}{M_1 \cap N} = \frac{M_2}{M_2 \cap N}$ as B-submodules of $\frac{M}{M_1 \cap N}$.

(2) For any commutative ring B with 1, show that a B-module generated by a single element is of the form B/I for an ideal $I \subset B$.

(3) Prove the Theorem by induction on the number of generators of the module.

Exercise 5.2. In this exercise, we will prove the following

Theorem. Let F be a field, and A be a commutative F-algebra which is finitely generated as an F-module. Then, A is an integral domain if and only if A is a field.

As fields are integral domains, we only need to prove one direction. Suppose that A is an integral domain.

(1) Choose $a \in A$ nonzero. Show that the multiplication-by-a map $m_a : A \to A$ (i.e. $m_a(x) = ax$) is an **injective** F-linear map.

(2) Show that A as an F-vector space is of finite dimension. Deduce that m_a is surjective.

(3) Deduce that A is a field.

6. Lecture 7. Unique factorization of ideals

Summary. Fractional ideals; proof of unique prime ideal factorization of fractional ideals of Dedekind domains; gcd and lcm; Chinese Remainder Theorem; ideal class group; ideals in Dedekind domains are generated by at most two elements.

Content. In this lecture, we will prove the unique factorization of ideals in a Dedekind domain, Theorem 5.13. Recall that a product of two ideals I, J of a ring A is

$$IJ = \left\{ \sum_i^{\text{finite}} a_i b_i \mid a_i \in I,\ b_i \in J \right\},$$

which corresponds to a product of two numbers, and a sum is

$$I + J = \{a + b \mid a \in I,\ b \in J\},$$

which corresponds to taking the greatest common divisor of two numbers. We in fact prove slightly more, a unique factorization of **fractional ideals**.

Definition 6.1 (Fractional ideals)**.** Let A be a Dedekind domain. A **fractional ideal** of A is a finitely generated A-submodule of $\mathrm{Frac}(A)$. It is always of the form

$$d\mathfrak{a} = \{da \mid a \in \mathfrak{a}\}, \quad \mathfrak{a} \subset A \text{ ideal}, d \in \mathrm{Frac}(A).$$

It is always of the above form because any fractional ideal I, being a finitely generated $\mathcal{O}_K$-module, has some $a \in A$ such that $aI \subset A$ is an A-submodule, i.e. an ideal of A.

Definition 6.2. For a nonzero fractional ideal $I \subset \mathrm{Frac}(A)$, define

$$I^{-1} := \{a \in \mathrm{Frac}(A) \mid aI \subset A\},$$

which is a fractional ideal[9].

For two fractional ideals $I, J \subset \mathrm{Frac}(A)$, define

$$IJ := \left\{ \sum_i^{\text{finite}} a_i b_i \mid a_i \in I,\ b_i \in J \right\},$$

which is a fractional ideal (easy).

From this, one can define an integer power of a nonzero fractional ideal. Now we state the unique factorization of fractional ideals.

[9]It is obviously an A-module. Take $e \in I$ nonzero, then $I \subset (e)$, so $I^{-1} \subset (e)^{-1} = e^{-1}A$. Then, I^{-1} is an A-submodule of $e^{-1}A$, which is isomorphic to A as a A-module, so is a Noetherian A-module. Therefore, I^{-1} is finitely generated.

Theorem 6.3 (Unique factorization of fractional ideals)**.** *Let A be a Dedekind domain. Then, any nonzero fractional ideal $I \subset \mathrm{Frac}(A)$ has a* ***prime factorization***

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i},$$

where $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ are distinct prime ideals of A, and $e_1, \cdots, e_r$ are nonzero integers. The prime factorization of I is unique up to rearrangement of the $(\mathfrak{p}_i, e_i)$'s.

To prove this, we need several lemmas. From now on until the end of this section, A is a Dedekind domain.

Lemma 6.4. *Let $\mathfrak{a} \subset A$ be a nonzero ideal. Then, there is a finite collection of maximal ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_n \subset A$ such that $\prod_{i=1}^{n} \mathfrak{p}_i \subset \mathfrak{a}$.*

Proof. Suppose not. Then, such $\mathfrak{a}$ cannot be a maximal ideal (as otherwise $\mathfrak{a} = \mathfrak{a}$ satisfies the condition). As $\mathfrak{a} \neq (0)$, this implies that $\mathfrak{a}$ is not a prime ideal (by the definition of Dedekind domains). Thus, there are $a, b \in A$ such that $ab \in \mathfrak{a}$ while $a, b \notin \mathfrak{a}$. Thus, $\mathfrak{b}_1 = \mathfrak{a} + (a)$ and $\mathfrak{b}_2 = \mathfrak{a} + (b)$ are strictly bigger than $\mathfrak{a}$, and yet $\mathfrak{b}_1\mathfrak{b}_2 \subset \mathfrak{a}$. Since $\mathfrak{a}$ does not contain any finite product of maximal ideals, at least one of the two ideals $\mathfrak{b}_1, \mathfrak{b}_2$ satisfy this condition as well. Now we can iterate this process over and over again to obtain a strictly increasing chain of ideals, which contradicts the Noetherianity of A. □

Lemma 6.5. *Let $\mathfrak{a} \subset A$ be a proper ideal. Then, there is $c \in \mathrm{Frac}(A) \backslash A$ such that $c\mathfrak{a} \subset A$.*

Proof. Pick a nonzero $a \in \mathfrak{a}$. Then, by Lemma 6.4, $(a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some finite collection of maximal ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r \subset A$. Let r be the smallest possible such integer. As $\mathfrak{a} \subset A$ is proper, there is a maximal ideal $\mathfrak{p} \supset \mathfrak{a}$ containing $\mathfrak{a}$. Therefore,

$$\mathfrak{p} \supset \mathfrak{a} \supset (a) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

which implies that $\mathfrak{p} \supset \mathfrak{p}_i$ for some $\mathfrak{p}_i$ – if not, choose $a_i \in \mathfrak{p}_i \backslash \mathfrak{p}$, then $a_1 \cdots a_r \in \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{p}$ implies that some $a_i \in \mathfrak{p}$, a contradiction. Thus, $\mathfrak{p} = \mathfrak{p}_i$ for some $\mathfrak{p}_i$. After reindexing, without loss of generality, suppose that $i = 1$.

By the minimality of r, (a) does not contain $\mathfrak{p}_2 \cdots \mathfrak{p}_r$. Let $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \backslash (a)$. Then, as $b \notin (a)$, $\frac{b}{a} \in \mathrm{Frac}(A) \backslash A$. On the other hand, $\frac{b}{a}\mathfrak{a} \subset \frac{b}{a}\mathfrak{p}_1$. Since $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$, $b\mathfrak{p}_1 \subset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a)$, so $\frac{b}{a}\mathfrak{p}_1 \subset A$. □

Lemma 6.6. *Let $\mathfrak{a} \subset A$ be an ideal, and $a \in \mathfrak{a}$. Then, there is an ideal $\mathfrak{b} \subset A$ such that $\mathfrak{a}\mathfrak{b} = (a)$.*

Proof. Let $\mathfrak{b} = \{b \in A \mid b\mathfrak{a} \subset (a)\}$. This is an ideal of A that satisfies $\mathfrak{a}\mathfrak{b} \subset (a)$. Let $\mathfrak{c} = \frac{1}{a}\mathfrak{a}\mathfrak{b} \subset A$, which is an ideal. We want to show that $\mathfrak{a}\mathfrak{b} = (a)$, or equivalently, $\mathfrak{c} = A$. Suppose not. Then, by Lemma 6.5, there is $c \in \mathrm{Frac}(A) \backslash A$ such that $c\mathfrak{c} \subset A$. Thus, $\frac{c}{a}\mathfrak{a}\mathfrak{b} \subset A$, so $c\mathfrak{a}\mathfrak{b} \subset (a)$. Note also that $a \in \mathfrak{a}$ implies that $\mathfrak{b} \subset \mathfrak{c}$, so $c\mathfrak{b} \subset c\mathfrak{c} \subset A$. Therefore, for any $x \in c\mathfrak{b} \subset A$, $x\mathfrak{a} \subset (a)$, so $x \in \mathfrak{b}$. Thus, $c\mathfrak{b} \subset \mathfrak{b}$.

As $\mathfrak{b}$ is finitely generated, we can pick a generating set $b_1, \cdots, b_n \in \mathfrak{b}$. Then, $c\mathfrak{b} \subset \mathfrak{b}$ implies that there is an $n \times n$ matrix M with entries in A such that

$$c \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix} = M \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix}.$$

Thus

$$(\gamma I_n - M) \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}.$$

By multiplying on the left with $(\gamma I_n - M)^{\text{adj}}$, we get

$$\det(\gamma I_n - M) \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}.$$

This implies that $\det(\gamma I_n - M) = 0$, or $p_M(\gamma) = 0$, where $p_M(X) \in A[X]$ is the characteristic polynomial of M. This implies that $\gamma \in \text{Frac}(A)$ is integral over A. As A is normal, $\gamma \in A$, which is a contradiction. □

Lemma 6.7. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subset A$ be ideals such that $\mathfrak{ab} = \mathfrak{ac}$. Then, $\mathfrak{b} = \mathfrak{c}$.*

Proof. Using Lemma 6.6, let $\mathfrak{d} \subset A$ be an ideal such that $\mathfrak{ad} = (a)$. Then, $\mathfrak{ab} = \mathfrak{ac}$ implies that $a\mathfrak{b} = a\mathfrak{c}$, so $\mathfrak{b} = \mathfrak{c}$. □

Lemma 6.8. *If $\mathfrak{a}, \mathfrak{b} \subset A$ are ideals, $\mathfrak{a} \supset \mathfrak{b}$ if and only if there exists an ideal $\mathfrak{c} \subset A$ such that $\mathfrak{b} = \mathfrak{ac}$.*

Proof. If $\mathfrak{b} = \mathfrak{ac}$, then obviously $\mathfrak{a} \supset \mathfrak{b}$. Conversely, if $\mathfrak{a} \supset \mathfrak{b}$, then choose an ideal $\mathfrak{c} \subset A$ such that $\mathfrak{ac} = (a)$ as per Lemma 6.6. Then, $(a) \supset \mathfrak{bc}$, so $A \supset \frac{1}{a}\mathfrak{bc}$ is an ideal. Let $\mathfrak{d} = \frac{1}{a}\mathfrak{bc}$. Then, $\mathfrak{ad} = \frac{1}{a}\mathfrak{abc} = \frac{1}{a}(a)\mathfrak{b} = \mathfrak{b}$. □

Lemma 6.9. *For a maximal ideal $\mathfrak{p} \subset A$, $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

Proof. By definition, $\mathfrak{p}\mathfrak{p}^{-1} \subset A$ is an ideal that contains $\mathfrak{p}$. As $\mathfrak{p}$ is maximal, either $\mathfrak{p}\mathfrak{p}^{-1} = A$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, then by Lemma 6.6, there is an ideal $\mathfrak{a} \subset A$ such that $\mathfrak{ap} = (a)$. Then, $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ implies that $a\mathfrak{p}^{-1} = (a)$, or $\mathfrak{p}^{-1} = A$. This contradicts Lemma 6.5. □

We can now prove the unique factorization of fractional ideals.

Proof of Theorem 6.3. We first show that for any nonzero ideal $I \subset A$, there exists an expression $I = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ with $e_i \geq 0$. If not, then there is a nonempty collection of nonzero ideals of A without such expression. Such collection has a maximal member M as A is Noetherian. Note that $M \neq A$ as A is the empty product, so there is a maximal ideal $M \subset \mathfrak{p}$ containing M. By

Lemma 6.8, there exists an ideal $N \subset A$ such that $M = \mathfrak{p}N$. Thus, $N \supset M$; if $N \neq M$, then N is a product of prime ideals by the maximality of M, so $M = \mathfrak{p}N$ is a product of prime ideals. Thus, $N = M$, which means that $M = \mathfrak{p}M$. Thus, by Lemma 6.7, $\mathfrak{p} = A$, which is a contradiction.

Now let I be a nonzero fractional ideal. Then, it is of the form $I = \frac{1}{d}J$ for $d \in A$ and $J \subset A$ an ideal. Then $I = \prod_{i=1}^{r} \mathfrak{p}_i \prod_{j=1}^{s} \mathfrak{q}_j^{-1}$, where $J = \prod_{i=1}^{r} \mathfrak{p}_i$ and $(d) = \prod_{j=1}^{s} \mathfrak{p}_j$. Therefore, this proves the existence part of Theorem 6.3.

Suppose now that two prime ideal factorization expressions are equal to each other,

$$\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{s} \mathfrak{q}_j^{f_j}.$$

By rearranging, without loss of generality $e_i > 0$ for $i \leq r'$, $e_i < 0$ for $i > r'$, $f_j > 0$ for $j \leq s'$, $f_j < 0$ for $j > s'$. Then, we have

$$\prod_{i=1}^{r'} \mathfrak{p}_i^{e_i} \prod_{j=s'+1}^{s} \mathfrak{q}_j^{-f_j} = \prod_{i=r'+1}^{r} \mathfrak{p}_i^{-e_i} \prod_{j=1}^{s'} \mathfrak{q}_j^{f_j},$$

which uses Lemma 6.9. Thus, the uniqueness part of Theorem 6.3 follows from the uniqueness when the exponents are assumed to be nonnegative, namely

$$\prod_{i=1}^{r} \mathfrak{p}_i = \prod_{j=1}^{s} \mathfrak{q}_j,$$

implies that $r = s$ and $\mathfrak{p}_i$'s are permutations of $\mathfrak{q}_j$'s.

We prove this by the induction on $r + s$. The base case is $r + s = 0$, which is just $A = A$. In general, we have $\mathfrak{p}_1 \supset \prod_{i=1}^{r} \mathfrak{p}_i = \prod_{j=1}^{s} \mathfrak{q}_j$, so for some j, $\mathfrak{p}_1 \supset \mathfrak{q}_j$, so $\mathfrak{p}_1 = \mathfrak{q}_j$. Thus, we can use Lemma 6.7 to reduce $r + s$ to $r + s - 2$. This finshes the proof of Theorem 6.3. □

Now that we have the unique factorization of ideals, an analogue of prime factorization, we have various arithmetic consequences.

Definition 6.10. Let A be a Dedekind domain, and let $I, J \subset A$ be ideals. Then, the **greatest common divisor** of I, J, denoted $\gcd(I, J)$ or just (I, J), is defined as

$$\gcd(I, J) := I + J.$$

The **least common multiple** of I, J, denoted $\operatorname{lcm}(I, J)$, is defined as

$$\operatorname{lcm}(I, J) := I \cap J.$$

We say I, J are **relatively prime** (or **coprime**) if $(I, J) = A$ is the unit ideal. We say that I **divides** J if there is an ideal $I' \subset A$ such that $J = II'$ (by Lemma 6.7, this is equivalent to $I \supset J$).

It's easy to show that the notions defined in Definition 6.10 behave exactly as expected under the prime factorization of ideals. For example:

Proposition 6.11. *Two ideals $I, J \subset A$ are relatively prime to each other if and only if the ideal factorizations of I and J share no common prime ideal factor.*

Proof. This follows from that $\mathfrak{p} + \mathfrak{q} = (1)$ for any two differet maximal ideals $\mathfrak{p}, \mathfrak{q} \subset A$, which is obvious as $\mathfrak{p} + \mathfrak{q}$ is an ideal that contains $\mathfrak{p}$ and is strictly larger than $\mathfrak{p}$. □

Theorem 6.12 (Chinese Remainder Theorem)**.** *Let A be a Dedekind domain, and let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n \subset A$ are ideals that are pairwise relatively prime (i.e. $\gcd(\mathfrak{a}_i, \mathfrak{a}_j) = (1)$ for all $i \neq j$). Then, the natural map*

$$A/\prod_{i=1}^{n} \mathfrak{a}_i \to \prod_{i=1}^{n} A/\mathfrak{a}_i,$$

is an isomorphism.

Proof. The natural map arises from the natural map $A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$, and its kernel is precisely $\bigcap_{i=1}^{n} \mathfrak{a}_i$. Thus, to prove injectivity of the map, we need to show that

$$\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

By induction, we are left to prove the case of $n = 2$. Namely, if $\mathfrak{a} + \mathfrak{b} = (1)$, then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. One containment, $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$, is obvious, so we need to prove the other containment. Suppose $\alpha \in \mathfrak{a} \cap \mathfrak{b}$. Then, as $\mathfrak{a} + \mathfrak{b} = (1)$, there exist $x \in \mathfrak{a}$, $y \in \mathfrak{b}$ such that $x + y = 1$. Then,

$$\alpha = \alpha x + \alpha y, \quad \alpha x, \alpha y \in \mathfrak{ab}.$$

Thus, $\alpha \in \mathfrak{ab}$. This proves the reverse containment.

To prove surjectivity, we need to prove the surjectivity of $A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$. This means that, for any $1 \leq i \leq n$, there is $x \in A$ such that $x - 1 \in \mathfrak{a}_i$ and $x \in \mathfrak{a}_j$ for all $j \neq i$. Since $\mathfrak{a}_i + \mathfrak{a}_j = (1)$, we have $a_j \in \mathfrak{a}_i$, $b_j \in \mathfrak{a}_j$ such that $a_j + b_j = 1$. Let

$$x = \prod_{j \neq i} (1 - a_j) = \prod_{j \neq i} b_j.$$

Then, expanding $\prod_{j \neq i}(1 - a_j)$, it is obvious that $x - 1 \in \mathfrak{a}_i$. Furthermore, $x = \prod_{j \neq i} b_j \in \mathfrak{a}_j$ for all $j \neq i$, which is what we want. □

Theorem 6.13. *Let A be a Dedekind domain. Then, A is a UFD if and only if A is a PID.*

Proof. It is in general true that a PID is a UFD, so we only need to prove the converse. Suppose that A is a Dedekind domain which is also a UFD. Let $\mathfrak{a} \subset A$ be any nonzero proper ideal. By Lemma 6.6, there exist $a \in \mathfrak{a}$ and some ideal $\mathfrak{b} \subset A$ such that $\mathfrak{ab} = (a)$. Let

$$a = up_1 \cdots p_r,$$

be a prime factorization of a, which comes from that A is a UFD; $u \in A^\times$ is a unit, and $p_1, \cdots, p_r$ are prime elements in A. Then, each p_i generates a principal prime ideal (p_i), which is maximal

by the Dedekind-ness of A. Thus, the uniqueness of the prime factorization of ideals implies that $\mathfrak{ab} = (p_1) \cdots (p_r)$ means $\mathfrak{a}$ is a product of principal prime ideals, so a principal ideal. Thus, any nonzero proper ideal of A is principal, so A is a PID. □

From Theorem 6.13, one sees that, as promised, a Dedekind domain may not be a UFD because the prime factorization of ideals does not translate to the prime factorization of elements, and this is because not all ideals are principal. Thus, it is important to measure the "failure of being a UFD" = "failure of being a PID" in a precise manner.

Definition 6.14 (Ideal class group)**.** Let K be a number field. Then, the set of nonzero fractional ideals of $\mathcal{O}_K$ forms an abelian group, called the **ideal group** of K, J_K, where the multiplication is given by the multiplication of the fractional ideals. Inside J_K, there is an abelian subgroup of **principal ideals**, consisted of the fractional ideals of the form $a\mathcal{O}_K$ for $a \in K^\times$. The quotient group is called the **(ideal) class group** of K,

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

For an ideal $I \subset \mathcal{O}_K$, one writes $[I] \in \mathrm{Cl}(K)$ for the ideal class that I belongs to.

Thus, $\mathrm{Cl}(K) = \{1\}$ precisely if and only if $\mathcal{O}_K$ is a PID (=a UFD). The second milestone of the course will be to prove the following Theorem.

Theorem 6.15 (Finiteness of the class number; to be proved later)**.** *For any number field K, $\mathrm{Cl}(K)$ is always a finite abelian group.*

Finally, we record that, even though the Dedekind domains are not necessarily PIDs, they are not too far away from being PIDs.

Theorem 6.16 (Ideals in Dedekind domains are generated by two elements)**.** *Any ideal I in a Dedekind domain $A$is generated by two elements. In fact, one can take one of the two generating elements to be any nonzero element of I.*

Proof. Let A be a Dedekind domain, and $\mathfrak{a} \subset A$ be an ideal. Then, $\mathfrak{a}$ has a prime factorization

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}.$$

Choose any $a \in \mathfrak{a}$ nonzero. Then, $(a) \subset \mathfrak{a}$, so the prime factorization of (a), after rearranging, can be written as

$$(a) = \prod_{i=1}^{n} \mathfrak{p}_i^{f_i},$$

where $f_i \geq e_i$.

For each i, choose $x_i \in \mathfrak{p}_i^{e_i} \backslash \mathfrak{p}_i^{e_i+1}$, which is possible as $\mathfrak{p}_i^{e_i} \neq \mathfrak{p}_i^{e_i+1}$. Then, the Chinese Remainder Theorem, Theorem 6.12, implies that there is $x \in A$ such that $x \equiv x_i \pmod{\mathfrak{p}_i^{f_i}}$ for all $1 \leq i \leq n$. As $x_i \in \mathfrak{p}_i^{e_i}$, $x \in \mathfrak{p}_i^{e_i}$, so $x \in \mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$, which implies that $(a, x) \subset \mathfrak{a}$.

We claim that $(a, x) = \mathfrak{a}$. Note that, by definition, $(a, x) = (a) + (x) = \gcd((a), (x))$. Let (x) have the prime factorization

$$(x) = \prod_{i=1}^{n} \mathfrak{p}_i^{g_i} \times \prod_{j=1}^{m} \mathfrak{q}_j^{h_j} = \bigcap_{i=1}^{n} \mathfrak{p}_i^{g_i} \cap \bigcap_{j=1}^{m} \mathfrak{q}_j^{h_j},$$

where $\mathfrak{q}_j$'s are differet from $\mathfrak{p}_i$'s. Then,

$$\gcd((a), (x)) = \prod_{i=1}^{n} \mathfrak{p}_i^{\min(f_i, g_i)}.$$

Note that $g_i \geq 0$ is the integer such that $x \in \mathfrak{p}_i^{g_i}$ and $x \notin \mathfrak{p}_i^{g_i+1}$. Thus, $g_i \geq e_i$. If $f_i = e_i$, then $\min(f_i, g_i) = e_i$. If $f_i > e_i$, then $x \equiv x_i \pmod{\mathfrak{p}_i^{f_i}}$ and $x_i \notin \mathfrak{p}_i^{e_i+1}$ implies that $g_i = e_i$, so again $\min(f_i, g_i) = e_i$. Thus,

$$(a, x) = (a) + (x) = \gcd((a), (x)) = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} = \mathfrak{a}.$$

□

– –

Exercise 6.1. Let A be a Dedekind domain, and let $I, J \subset A$ be two nonzero ideals with the prime ideal factorization

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}, \quad J = \prod_{i=1}^{n} \mathfrak{p}_i^{f_i},$$

with $e_i, f_i \geq 0$ and $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ mutually distinct maximal ideals of A. Show that

$$\gcd(I, J) := I + J = \prod_{i=1}^{n} \mathfrak{p}_i^{\min(e_i, f_i)}, \quad \operatorname{lcm}(I, J) := I \cap J = \prod_{i=1}^{n} \mathfrak{p}_i^{\max(e_i, f_i)}.$$

Exercise 6.2. Let A be a Dedekind domain.

(1) Prove the **weak approxmiation theorem**:

> **Theorem.** Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be mutually distinct maximal ideals of A, and let $e_1, \cdots, e_n \in \mathbb{Z}$. Then, there exists a nonzero $b \in \operatorname{Frac}(A)$ such that the prime ideal factorization of the principal ideal (b) has $\mathfrak{p}_i$ appearing with multiplicity exactly e_i.

> **Hint.** It is sufficient to prove the theorem for $e_1, \cdots, e_n \geq 0$ with the extra requirement that $b \in A$. Show first that $\mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1} \subset A/\mathfrak{p}_i^{e_i+1}$ is nonzero. After that, one can use (a variant of) the Chinese Remainder Theorem, that $A \to \prod_{i=1}^{n} A/\mathfrak{p}_i^{e_i+1}$ is surjective.

(2) Prove the **strong approximation theorem**:

Theorem. Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be mutually distinct maximal ideals of A, and let $e_1, \cdots, e_n \in \mathbb{Z}$. Then, there exists a nonzero $b \in \mathrm{Frac}(A)$ such that the prime ideal factorization of the principal ideal (b) has $\mathfrak{p}_i$ appearing with multiplicity exactly e_i, **and also such that all the other prime ideal factors of** (b) **have nonnegative multiplicities**.

Hint. Use the version of the weak approximation for $e_1, \cdots, e_n \geq 0$ and $b \in A$ to first find a denominator, and then to find an appropriate numerator.

7. Lectures 8 and 9. Splitting of rational primes

Summary. Ideal norm; splitting of rational primes in quadratic fields; ramification indices; residue degrees; unramified/ramified primes; the relation between "e, f, g"; Dedekind's criterion.

Content. We are now interested in how the prime factorization of ideals is done. The first thing to note is that every nonzero prime ideal in $\mathcal{O}_K$ is associated with a prime number.

Proposition 7.1. *Let K be a number field, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a nonzero prime ideal. Then, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime $p \in \mathbb{Z}$, and therefore, $\mathfrak{p}$ divides (p).*

Here, the **rational prime** means that a prime element in $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$, to distinguish it from the prime ideals/elements in a general number field. If $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, we call that $\mathfrak{p}$ **lies over** $(p) \subset \mathbb{Z}$ (or $p \in \mathbb{Z}$).

Proof. Since $\mathfrak{p}$ divides a principal ideal, and since any principal ideal (α) divides $(N_{K/\mathbb{Q}}(\alpha))$, $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. Furthermore, it is easy to see that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Thus, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime $p \in \mathbb{Z}$. □

The notion of **ideal norm** is very useful.

Definition 7.2 (Ideal norm)**.** Let K be a number field, and $\mathfrak{a} \subset \mathcal{O}_K$ be a nonzero ideal. Then, the **norm** of $\mathfrak{a}$ is defined as

$$N(\mathfrak{a}) := \#(\mathcal{O}_K/\mathfrak{a}),$$

which makes sense as $\mathcal{O}_K/\mathfrak{a}$ is a finite abelian group.

Theorem 7.3. *Let K be a number field.*

(1) If $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ are nonzero ideals, then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

(2) If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal that divides (p) for a rational prime $p \in \mathbb{Z}$, then $N(\mathfrak{p}) = p^a$ for some integer $a \geq 1$.

(3) For a nonzero $\alpha \in \mathcal{O}_K$, $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

Proof.

(1) By using the prime factorization of $\mathfrak{b}$, it is sufficient to prove it when $\mathfrak{b} = \mathfrak{p}$ is a prime ideal. Then,

$$N(\mathfrak{ap}) = \#(\mathcal{O}_K/\mathfrak{ap}) = \#(\mathcal{O}_K/\mathfrak{a}) \cdot \#(\mathfrak{a}/\mathfrak{ap}),$$

so it suffices to show that $\mathfrak{a}/\mathfrak{ap} \cong \mathcal{O}_K/\mathfrak{p}$ as finite abelian groups. Note that, as $\mathfrak{p}$ is a maximal ideal, $\mathcal{O}_K/\mathfrak{p}$ is a finite field. Also, $\mathfrak{a}/\mathfrak{ap}$ is naturally an $\mathcal{O}_K/\mathfrak{p}$-module, as multiplication by an element in $\mathcal{O}_K$ on $\mathfrak{a}/\mathfrak{ap}$ does not change when you change the element by an element in $\mathfrak{p}$. Thus, $\mathfrak{a}/\mathfrak{ap}$ is a nonzero vector space over the finite field $\mathcal{O}_K/\mathfrak{p}$.

Suppose on the contrary that $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathfrak{a}/\mathfrak{ap} > 1$. Then, there is a proper nontrivial $\mathcal{O}_K/\mathfrak{p}$-submodule $M \subset \mathfrak{a}/\mathfrak{ap}$. This translates into the strict containment of $\mathcal{O}_K$-submodules $\mathfrak{ap} \subsetneq \widetilde{M} \subsetneq \mathfrak{a}$. Since $\widetilde{M} \subset \mathcal{O}_K$ is an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$, it turns out that $\widetilde{M}$ is an ideal

of $\mathcal{O}_K$. Therefore, $\widetilde{M}$ is an ideal that divides $\mathfrak{a}\mathfrak{p}$ and is divisible by $\mathfrak{a}$, which by the unique factorization of ideals means that either $\widetilde{M} = \mathfrak{a}$ or $\widetilde{M} = \mathfrak{a}\mathfrak{p}$, and both cases are prohibited by the assumption, hence a contradiction. Thus, $\dim_{\mathcal{O}_K/\mathfrak{p}} \mathfrak{a}/\mathfrak{a}\mathfrak{p} = 1$, as desired.

(2) This follows from the fact that $\mathcal{O}_K/\mathfrak{p}$ is a field that is a field extension of $\mathbb{Z}/(p) = \mathbb{F}_p$, which can be easily checked.

(3) Consider the multiplication-by-α map $m_\alpha : \mathcal{O}_K \to \mathcal{O}_K$. It is an injective $\mathbb{Z}$-linear map (=homomorphism of abelian groups) whose cokernel has the size $N((\alpha))$, which is of course equal to $|\det(m_\alpha)| = |N_{K/\mathbb{Q}}(\alpha)|$.

□

Therefore, for $\mathfrak{a} \subset \mathcal{O}_K$, by looking at $N(\mathfrak{a})$, you are left with finitely many possibilities for the prime factors of $\mathfrak{a}$. Namely, take the prime factorization of the integer $N(\mathfrak{a})$, and for each prime factor $p|N(\mathfrak{a})$, the prime ideals of $\mathcal{O}_K$ lying over p may appear as a prime ideal factor of $\mathfrak{a}$.

Thus, the question is: what are the prime ideals of $\mathcal{O}_K$ that lie over $p \in \mathbb{Z}$? Namely, what is the prime factorization of $(p) \subset \mathcal{O}_K$? The prime factorization of $(p) \subset \mathcal{O}_K$ is often called as the **splitting** of p in K (i.e. how a prime ideal in a smaller field splits off as a product of prime ideals in a larger field).

Example 7.4 (Factorization of rational primes in quadratic fields)**.** Let us consider the simplest case, when $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field. Consider first the simplest case of $d \equiv 2, 3 \pmod 4$. Then, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, so as a ring, $\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - d)$. Thus,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[X]/(p, X^2 - d) \cong \mathbb{F}_p[X]/(X^2 - d).$$

Since $\mathbb{F}_p[X]$ is a UFD, we can talk about the prime factorization of $X^2 - d$ in $\mathbb{F}_p[X]$:

$$X^2 - d = \begin{cases} X^2 & \text{if } d \equiv 0 \pmod p \\ X^2 - d & \text{if } p \text{ is odd and } d \text{ is not a square mod } p \\ (X-a)(X+a) & \text{if } p \text{ is odd and } d \equiv a^2 \pmod p \\ (X-d)^2 & \text{if } p = 2. \end{cases}$$

Thus,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \begin{cases} \mathbb{F}_p[X]/(X^2) & \text{if } p = 2 \text{ or } d \equiv 0 \pmod p \\ \mathbb{F}_p \times \mathbb{F}_p & \text{if } p \text{ is odd and } d \text{ is a square mod } p \\ \mathbb{F}_{p^2} & \text{if } p \text{ is odd and } d \text{ is not a square mod } p. \end{cases}$$

We would like to use the above information in conjuction with the Chinese Remainder Theorem. Note that $N((p)) = |N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(p)| = p^2$, so (p) has at most two prime factors. Thus, there are three possibilities:

(1) $(p) = (p)$ itself is a prime ideal in $\mathcal{O}_K$;

(2) $(p) = \mathfrak{p}\mathfrak{p}'$ is a product of two different prime ideals;

(3) $(p) = \mathfrak{p}^2$ is a square of a prime ideal.

By the Chinese Remainder Theorem, these three cases are completely characterized by the ring structure of $\mathcal{O}_K/p\mathcal{O}_K$:

(1) (p) is a prime ideal in $\mathcal{O}_K$ if and only if $\mathcal{O}_K/p\mathcal{O}_K$ is a field;

(2) $(p) = \mathfrak{p}\mathfrak{p}'$ is a product of two different prime ideals if and only if $\mathcal{O}_K/p\mathcal{O}_K$ is a product of two fields;

(3) $(p) = \mathfrak{p}^2$ is a square of a prime ideal if neither of the above holds.

Thus, we see that the prime factorization of (p) in $\mathcal{O}_K$ is of the form

$$(p) = \begin{cases} (p) & \text{if } p \text{ is odd and } d \text{ is not a square mod } p \\ \mathfrak{p}\mathfrak{p}' & \text{if } p \text{ is odd and } d \text{ is a square mod } p \\ \mathfrak{p}^2 & \text{if } p = 2 \text{ or } d \equiv 0 \pmod{p}. \end{cases}$$

In fact, one can give a precise description of these prime factors using the Chinese Remainder Theorem.

Theorem 7.5 (Splitting of rational primes in quadratic fields)**.** *Let $d \equiv 2, 3 \pmod 4$ be a squarefree integer. Then, the prime factorization of $(p) \subset \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$, is given as follows.*

$$(p) = \begin{cases} (p) & \text{if } p \text{ is odd and } d \text{ is not a square mod } p \\ (p, \sqrt{d} + a)(p, \sqrt{d} - a) & \text{if } p \text{ is odd and } d \equiv a^2 \pmod{p} \\ (p, \sqrt{d} - d)^2 & \text{if } p = 2 \text{ or } d \equiv 0 \pmod{p}. \end{cases}$$

This will follow from the Chinese Remainder Theorem and the following lemma.

Lemma 7.6. *Let A be a commutative ring with 1, and let $I \subset A$ be an ideal. Then, the natural map*

$$\{\text{prime ideals of } A \text{ containing } I\} \to \{\text{prime ideals of } A/I\}, \quad \mathfrak{p} \mapsto \mathfrak{p}/I,$$

is a bijection.

Proof. It is easy to see that if $I \subset \mathfrak{p} \subset A$ is a prime ideal, then $\mathfrak{p}/I \subset A/I$ is also a prime ideal. Furthermore, $\mathfrak{p} \mapsto \mathfrak{p}/I$ is an injection, as in general the submodules of an A-module M containing an A-submodule $N \subset M$ are in one-to-one correspondence with the A-submodules of M/N.

Thus, we only need to prove the surjectivity. Namely, given a prime ideal $\overline{\mathfrak{p}} \subset A/I$, the ideal

$$\mathfrak{p} := \{a \in A \mid a \pmod I \in \overline{\mathfrak{p}}\} \subset A,$$

is a prime ideal. But this is obvious; if $xy \in \mathfrak{p}$, then $xy \pmod I \in \overline{\mathfrak{p}}$, so either $x \pmod I \in \overline{\mathfrak{p}}$ or $y \pmod I \in \overline{\mathfrak{p}}$, hence either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. □

Proof of Theorem 7.5. The general strategy is as follows.

- Describe the ring structure $\mathcal{O}_K/p\mathcal{O}_K$ explicitly.
- Find the prime ideals of $\mathcal{O}_K/p\mathcal{O}_K$, and backtrack to obtain the prime ideals of $\mathcal{O}_K$ containing (p).

Indeed, knowing what prime ideals contain (p) will give the factorization, because we already know the multiplicities of the prime factors in each case.

There is nothing to do in the first case of p odd and d non-square mod p. Suppose that we are in the second case, that p is odd and $d \equiv a^2 \pmod p$. Then, we have an explicit isomorphism

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[X]/(p, X^2-d) = \mathbb{F}_p[X]/(X^2-d) \xrightarrow{\sim} \mathbb{F}_p[X]/(X-a)\times\mathbb{F}_p[X]/(X+a) \cong \mathbb{F}_p\times\mathbb{F}_p,$$

where the first isomorphism is given by the natural map (this is the Chinese Remainder Theorem for $\mathbb{F}_p[X]$!). Note that the prime ideals of $\mathbb{F}_p\times\mathbb{F}_p$ are $((1,0)) = \mathbb{F}_p\times 0$ and $((0,1)) = 0\times\mathbb{F}_p$. In turn, we see that the prime ideals of $\mathbb{F}_p[X]/(X^2-d)$ are $(X-a)$ and $(X+a)$. Thus, the prime ideals of $\mathcal{O}_K = \mathbb{Z}[X]/(X^2-d)$ containing (p) are $(p, \sqrt{d}-a) = (p, X-a)$ and $(p, \sqrt{d}+a) = (p, X+a)$, as desired.

Finally, suppose that we are in the third case, that either $p = 2$ or $d \equiv 0 \pmod p$. In any case, then $X^2 - d \equiv (X-d)^2 \pmod p$, so we have an explicit isomorphism

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[X]/(p, X^2-d) = \mathbb{F}_p[X]/(X^2-d) = \mathbb{F}_p[X]/(X-d)^2 \xrightarrow{\sim} \mathbb{F}_p[X]/(X)^2,$$

where the last isomorphism is given by $X \mapsto X + d$. Note that any element in $\mathbb{F}_p[X]/(X)^2$ is of the form $a + bX$ for some $a, b \in \mathbb{F}_p$, and if $a \neq 0$, then $(a+bX)(a^{-1} - ba^{-2}X) = 1$, so $a + bX$ is a unit. Therefore, any prime ideal of $\mathbb{F}_p[X]/(X)^2$ must be contained in (X). The only ideals contained in (X) are (X) and (0), as $(X) \subset \mathbb{F}_p[X]/(X)^2$ is an $\mathbb{F}_p$-vector subspace of dimension 1. Note that (X) is indeed a prime ideal, as it is a maximal ideal, while (0) is not a prime ideal, as $X \cdot X \in (0)$ but $X \notin (0)$. Thus, the only prime ideal of $\mathbb{F}_p[X]/(X)^2$ is (X). Backtracking, the only prime ideal of $\mathcal{O}_K = \mathbb{Z}[X]/(X^2-d)$ containing (p) is $(p, \sqrt{d}-d) = (p, X-d)$. □

The case of $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1 \pmod 4$ will be dealt in Exercise 7.1.

Example 7.7. We can now systematically factorize any ideals $I \subset \mathcal{O}_K$ for a quadratic field K. Let us take the example of $K = \mathbb{Q}(\sqrt{-5})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The ring $\mathcal{O}_K$ is not a UFD, because we have two different prime factorizations of the same element

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Let's see how this can be explained with the prime ideal factorization of (6). From our recipe, we have the prime ideal factorizations of (2) and (3),

$$(2) = (2, \sqrt{-5}+5)^2 = (2, 1+\sqrt{-5})^2, \quad (3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}),$$

using that $-5 \equiv 1^2 \pmod 3$. Thus, the prime ideal factorization of (6) is given as

$$(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{r}, \quad \mathfrak{p} = (2, 1+\sqrt{-5}),\ \mathfrak{q} = (3, 1+\sqrt{-5}),\ \mathfrak{r} = (3, 1-\sqrt{-5}).$$

Let's see how the principal ideals $(1+\sqrt{-5})$ and $(1-\sqrt{-5})$ factor. Note that

$$N((1+\sqrt{-5})) = |N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(1+\sqrt{-5})| = 6,$$

so $(1+\sqrt{-5})$ must factor into a product of two prime ideals,

$$(1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3, \quad N(\mathfrak{p}_2) = 2,\ N(\mathfrak{p}_3) = 3.$$

We know already that the only prime ideal of $\mathcal{O}_K$ lying over 2 is $(2, 1+\sqrt{-5})$, so $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$. On the other hand, there are two choices for $\mathfrak{p}_3$, either $(3, 1+\sqrt{-5})$ or $(3, 1-\sqrt{-5})$. On the other hand, the factorization $(1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3$ implies that $\mathfrak{p}_3$ is the unique prime ideal of $\mathcal{O}_K$ lying over 3 such that $(1+\sqrt{-5}) \subset \mathfrak{p}_3$, or $1+\sqrt{-5} \in \mathfrak{p}_3$. Since obviously $1+\sqrt{-5} \in (3, 1+\sqrt{-5})$, we know that $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$. Thus, we know that

$$(1+\sqrt{-5}) = \mathfrak{p}\mathfrak{q} = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}).$$

Indeed, we can check manually that

$$\begin{aligned}(2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) &= (6, 3+3\sqrt{-5}, 2+2\sqrt{-5}, (1+\sqrt{-5})^2) \\ &= (6, 1+\sqrt{-5}, (1+\sqrt{-5})^2) \\ &= (1+\sqrt{-5}).\end{aligned}$$

By the same reasoning, we have

$$(1-\sqrt{-5}) = \mathfrak{p}\mathfrak{r} = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Thus, the factorization $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ in terms of the prime ideal factorization can be explained as

$$\mathfrak{p}^2\mathfrak{q}\mathfrak{r} = (\mathfrak{p}^2)\cdot(\mathfrak{q}\mathfrak{r}) = (\mathfrak{p}\mathfrak{q})\cdot(\mathfrak{p}\mathfrak{r}).$$

Now, inspired by the tools we used in the quadratic field case, we discuss the case of general number fields $\mathcal{O}_K$.

Definition 7.8 (Ramification indices, residue degrees, ramified/unramified primes)**.** Let K be a number field, and let p be a rational prime. In the factorization of $(p) \subset \mathcal{O}_K$,

$$(p) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ are mutually distinct prime ideals of $\mathcal{O}_K$, we call e_i the **ramification index** of $\mathfrak{p}_i$ over p. If $e_i > 1$ for some $\mathfrak{p}_i$, we say that p **ramifies** in K. Otherwise (i.e. $e_i = 1$ for all i), we say p is **unramified** in K.

We also have

$$\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_{p^{f_i}},$$

for some $f_i \geq 1$. We call f_i the **residue degree** of $\mathfrak{p}_i$.

The following is the fundamental relation between the residue degrees, the ramification indices, and $[K:\mathbb{Q}]$.

Theorem 7.9 (Relations on "e, f, g")**.** *If K is a number field and p is a rational prime with a prime factorization $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ in $\mathcal{O}_K$, we have*

$$\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}].$$

Proof. Since $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_{p^{f_i}}$, $N(\mathfrak{p}_i) = p^{f_i}$. Thus,

$$p^{[K:\mathbb{Q}]} = |N_{K/\mathbb{Q}}(p)| = N((p)) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = p^{\sum_{i=1}^{g} e_i f_i},$$

which gives the desired relation. □

We have some special adjectives for the extreme cases of e, f, g:

Definition 7.10 (Extreme cases of "e, f, g")**.** Let K be a number field, and let p be a rational prime that splits as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}.$$

- If we have $e_i = f_i = 1$ for all i (equivalently, $g = [K : \mathbb{Q}]$), then we say p **splits completely** in K.
- If we have $g = 1$ and $e_1 = 1$ (equivalently, $f_1 = [K : \mathbb{Q}]$), then we say p is **inert** in K.
- If we have $g = 1$ and $f_1 = 1$ (equivalently, $e_1 = [K : \mathbb{Q}]$), then we say p is **totally ramified** in K.

In the quadratic field case, we saw the following: if $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f(X))$ for some monic $f(X) \in \mathbb{Z}[X]$, then the prime factorization of (p) in $\mathcal{O}_K$ is governed by how $f(X) \pmod p$ factorizes in $\mathbb{F}_p[X]$. This is in fact true in general, and gives a very useful and versatile method to find a prime factorization.

Theorem 7.11 (Dedekind's criterion)**.** *Let K be a number field, and $\alpha \in \mathcal{O}_K$ be a primitive element (i.e. $K = \mathbb{Q}(\alpha)$). Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. If $p \in \mathbb{Z}$ is a rational prime such that $(p, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$, then we can find the prime factorization of (p) in terms of the factorization of $f(X) \pmod p$ in $\mathbb{F}_p[X]$. More precisely, let $\overline{f}(X) \in \mathbb{F}_p[X]$ be the mod p reduction of $f(X)$. Suppose that*

$$\overline{f}(X) = \overline{h}_1(X)^{e_1} \cdots \overline{h}_g(X)^{e_g},$$

is a prime factorization of $\overline{f}(X)$ in $\mathbb{F}_p[X]$, where $\overline{h}_i(X)$'s are distinct monic irreducible polynomials in $\mathbb{F}_p[X]$. For each $1 \le i \le g$, choose $h_i(X) \in \mathbb{Z}[X]$ a monic polynomial whose mod p reduction is equal to $\overline{h}_i(X)$. Then, $(p) \subset \mathcal{O}_K$ has a prime factorization

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \quad \mathfrak{p}_i := (p, h_i(\alpha)).$$

Furthermore, the residue degree of $\mathfrak{p}_i$ is equal to $\deg h_i(X)$.

Proof. Consider the natural inclusion map $\mathbb{Z}[\alpha] \to \mathcal{O}_K$, which is a $\mathbb{Z}$-algebra map. By taking mod p reduction, we get a natural $\mathbb{F}_p$-algebra map $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$. We claim that this is an isomorphism.

Indeed, both $\mathcal{O}_K/p\mathcal{O}_K$ and $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$ are $[K:\mathbb{Q}]$-dimensional $\mathbb{F}_p$-vector spaces, so to prove that the given map is bijective, it is sufficient to prove that the map is surjective. Let $x \in \mathcal{O}_K$. Then, as $\mathcal{O}_K/\mathbb{Z}[\alpha]$ is a finite abelian group, $[\mathcal{O}_K : \mathbb{Z}[\alpha]]x \in \mathbb{Z}[\alpha]$. As $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is coprime to p, there are integers $a, b \in \mathbb{Z}$ such that $a[\mathcal{O}_K : \mathbb{Z}[\alpha]] + bp = 1$. Then, $a[\mathcal{O}_K : \mathbb{Z}[\alpha]]x \in \mathbb{Z}[\alpha]$, so $(1-bp)x \in \mathbb{Z}[\alpha]$. The image of mod p reduction of $(1-bp)x \in \mathbb{Z}[\alpha]$ under the natural map $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \to \mathcal{O}_K/p\mathcal{O}_K$ is congruent to the mod p reduction of x, so this proves that any $x \in \mathcal{O}_K/p\mathcal{O}_K$ is in the image of the natural map, as desired.

This implies that the natural map gives rise to a ring isomorphism $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \xrightarrow{\sim} \mathcal{O}_K/p\mathcal{O}_K$. We now see that

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = \mathbb{Z}[X]/(p, f(X)) = \mathbb{F}_p[X]/(\overline{f}(X)) \xrightarrow{\sim} \prod_{i=1}^{g} \mathbb{F}_p[X]/(\overline{h}_i(X))^{e_i},$$

by Chinese Remainder Theorem.

We now wonder what the prime ideals of this product are.

Lemma 7.12. *For commutative rings A, B,*

$$\{\textit{prime ideals of } A \times B\} = \{\textit{prime ideals of } A\} \cup \{\textit{prime ideals of } B\},$$

where a prime ideal $\mathfrak{p} \subset A$ ($\mathfrak{q} \subset B$, respectively) corresponds to a prime ideal $\mathfrak{p} \times B \subset A \times B$ ($A \times \mathfrak{q} \subset A \times B$, respectively).

Proof. It is easy to see that the ideals of the form $\mathfrak{p} \times B$ for a prime ideal $\mathfrak{p} \subset A$ and $A \times \mathfrak{q}$ for a prime ideal $\mathfrak{q} \subset B$ are prime ideals of $A \times B$. Conversely, if $\mathfrak{r} \subset A \times B$ is a prime ideal, then it is an easy exercise that any ideal of $A \times B$ is of the form $I \times J$ for ideals $I \subset A$, $J \subset B$. Since $I = \mathfrak{r} \cap A \times 0$ and $J = \mathfrak{r} \cap 0 \times B$, $I \subset A$ satisfy $xy \in I$ implies either $x \in I$ or $y \in I$ and similarly for $J \subset B$. This implies that I is either a prime ideal or $I = A$, and similarly for J. If $I = A$ and $J = B$, then $I \times J$ is not a prime ideal by definition. If $I \subsetneq A$ and $J \subsetneq$ are both prime ideals, then for $x \in I$ and $y \in J$, $(x,1)(1,y) = (x,y) \in \mathfrak{r} = I \times J$ but $(x,1), (1,y) \notin \mathfrak{r} = I \times J$, so it contradicts with the primality of $\mathfrak{r}$. □

Now, in $\mathbb{F}_p[X]/(\overline{h}_i(X))^{e_i}$, any prime ideal must contain $\overline{h}_i(X)$, as $\overline{h}_i(X)^{e_i} = 0$ in this ring. However, as $(\overline{h}_i(X)) \subset \mathbb{F}_p[X]$ is a maximal ideal, $(\overline{h}_i(X)) \subset \mathbb{F}_p[X]/(\overline{h}_i(X))^{e_i}$ is the only prime ideal. Therefore, the prime ideals of $\prod_{i=1}^{g} \mathbb{F}_p[X]/(\overline{h}_i(X))^{e_i}$ are precisely

$$\mathbb{F}_p[X]/(\overline{h}_1(X))^{e_1} \times \cdots \times (\overline{h}_i(X))/(\overline{h}_i(X))^{e_i} \times \cdots \times \mathbb{F}_p[X]/(\overline{h}_g(X))^{e_g}, \quad 1 \le i \le g.$$

One sees easily that these correspond to the principal ideals

$$(\overline{h}_i(X)) \subset \mathbb{F}_p[X]/(\overline{f}(X)), \quad 1 \le i \le g$$

under the natural map. These correspond to the principal ideals

$$(h_i(\alpha)) \subset \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha], \quad 1 \le i \le g$$

and under the natural map these correspond to the principal ideals

$$(h_i(\alpha)) \subset \mathcal{O}_K/p\mathcal{O}_K, \quad 1 \le i \le g.$$

These correspond to the ideals

$$\mathfrak{p}_i := (p, h_i(\alpha)) \subset \mathcal{O}_K, \quad 1 \le i \le g.$$

Therefore, we see that $\mathfrak{p}_i$'s are precisely the prime factors in the prime factorization of $(p) \subset \mathcal{O}_K$. Let e_i' be the ramification index of $\mathfrak{p}_i$ in (p). By looking at the Chinese Remainder Theorem, we see that, inside $\mathcal{O}_K/p\mathcal{O}_K$, $\mathfrak{p}_i^{e_i'-1} \supsetneq \mathfrak{p}_i^{e_i'} = \mathfrak{p}_i^{e_i'+1}$. By looking at the corresponding ideals in $\mathcal{O}_K/p\mathcal{O}_K \cong \prod_{i=1}^g \mathbb{F}_p[X]/(\overline{h}_i(X))^{e_i}$, we see that $e_i' = e_i$. Finally, since $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_p[X]/(\overline{h}_i(X))$ is, as a $\mathbb{F}_p$-vector space, of dimension $\deg \overline{h}_i(X) = \deg h_i(X)$, we see that the residue deree of $\mathfrak{p}_i$ is precisely $\deg h_i(X)$. □

As we have

$$\operatorname{disc}(1, \alpha, \cdots, \alpha^{[K:\mathbb{Q}]-1}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \operatorname{disc}(K),$$

we have in many cases a way to compute the splitting of a rational prime p in a number field.

Example 7.13. Consider $K = \mathbb{Q}(\sqrt[3]{3})$. We don't really know whether $\mathcal{O}_K$ is equal to $\mathbb{Z}[\sqrt[3]{3}]$ (it is in fact equal to each other, by using the technique introduced in Exercise 4.2). On the other hand, we know that, from Exercise 3.1,

$$\operatorname{disc}(1, \sqrt[3]{3}, \sqrt[3]{3^2}) = -3^5.$$

Thus, by Dedekind's criterion, any prime $p \neq 3$ will factor in K precisely based on how the minimal polynomial $f(X) = X^3 - 3$ of $\sqrt[3]{3}$ factors mod p.

- Let $p = 2$. Then, $X^3 - 3 = (X-1)(X^2+X+1)$ is a prime factorization in $\mathbb{F}_2[X]$. Accordingly, we have a prime ideal factorization

  $$(2) = \mathfrak{p}_1\mathfrak{p}_2, \quad \mathfrak{p}_1 = (2, \sqrt[3]{3} - 1), \ \mathfrak{p}_2 = (2, \sqrt[3]{3^2} + \sqrt[3]{3} + 1).$$

  In this case, the residue degrees are $f_1 = 1, f_2 = 2$.

- Let $p = 7$. Note that no cube is congruent to 3 mod 7 ($1^3 \equiv 1$, $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv -1$ mod 7). Thus, $X^3 - 3$ is irreducible in $\mathbb{F}_7[X]$, which means that (7) remains a prime (i.e. 7 is **inert**) in K.

As mentioned above, using the technique introduced in Exercise 4.2, we can show that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{3}]$ as follows. Namely, we know that the only possible prime factor of $[\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{3}]]$ is 3, but $(3, [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{3}]]) = 1$ as the minimal polynomial $X^3 - 3$ of $\sqrt[3]{3}$ is **Eisenstein at** 3. This implies that $[\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{3}]] = 1$. This means that we can also use Dedekind's criterion to factor (3).

- Let $p = 3$. Then, $X^3 - 3 = X^3$ is a prime factorization in $\mathbb{F}_3[X]$. Accordingly, we have a prime ideal factorization

$$(3) = \mathfrak{q}^3, \quad \mathfrak{q} = (3, \sqrt[3]{3}).$$

  In other words, 3 is **totally ramified** in K.

Challenge. Can you find a rational prime $p \in \mathbb{Z}$ that **splits completely** in K?

Remark 7.14. The Dedekind's criterion can be enhanced into the **Dedekind index theorem**, which tells you exactly which prime p divides $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. The handout by Keith Conrad linked on the website shows that, if there is p dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, the Dedekind index theorem even gives a systematic construction of an algebraic integer $x \in \mathcal{O}_K$ such that $x \notin \mathbb{Z}[\alpha]$ but $px \in \mathbb{Z}[\alpha]$.

– –

Exercise 7.1. In this exercise, we will describe the prime ideal factorization of $(p) \subset \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$, in the case of $d \equiv 1 \pmod 4$ squarefree.

(1) Show that the minimal polynomial of $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ over $\mathbb{Q}$ is

$$f(X) = X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X].$$

  Deduce that $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p[X]/(f(X))$.

(2) If $p = 2$, then show that $f(X)$ is irreducible in $\mathbb{F}_p[X]$ if and only if $\frac{1-d}{4} \equiv 1 \pmod 2$.

(3) If p is an odd prime, show that $f(X)$ is irreducible in $\mathbb{F}_p[X]$ if and only if d is not a square mod p.

  Hint. $f(X) = \left(X - \frac{1}{2}\right)^2 - \frac{d}{4}$.

(4) Give a complete description of the prime ideal factorization of $(p) \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ in the case of $d \equiv 1 \pmod 4$ squarefree.

Exercise 7.2. Let $K/L/\mathbb{Q}$ be a tower of number fields (**not necessarily Galois**). Let $p \in \mathbb{Z}$ be a rational prime.

(1) If p is unramified in the bigger field K, show that p is also unramified in the smaller field L.

(2) If p splits completely in the bigger field K, show that p also splits completely in the smaller field L.

Exercise 7.3. Using Exercise 7.1, check that even in the case of $d \equiv 1 \pmod 4$ a square-free integer, for $(p, \mathrm{disc}(\mathbb{Q}(\sqrt{d}))) = 1$ and odd prime,

$$\mathrm{Fr}_p = \left(\frac{d}{p}\right) \in \{\pm 1\} = \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}).$$

8. Lecture 10. Galois action on the splitting of primes, the Frobenius

Summary. e, f, g when $K/\mathbb{Q}$ is Galois; decomposition group; inertia group; Frobenius element; Frobenius elements in the Galois groups of quadratic fields; Frobenius and splitting of primes.

Content. In the case of $K/\mathbb{Q}$ Galois, the splitting of a rational prime p in K has more structure, with respect to the action of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. It is easy to see that, for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, then $\sigma(\mathfrak{p}) \subset \mathcal{O}_K$ is also a prime ideal.

Therefore, if (p) has a prime ideal factorization in $\mathcal{O}_K$ as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

then by applying $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we obtain

$$(p) = \sigma(p) = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_g)^{e_g}.$$

As the prime ideal factorization of (p) is unique, this implies that σ gives rise to a permutation of the prime factors $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ of (p) in $\mathcal{O}_K$. Namely, we have an action of the group $\mathrm{Gal}(K/\mathbb{Q})$ on the set $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\}$,

$$\mathrm{Gal}(K/\mathbb{Q}) \times \{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\} \to \{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\}, \quad (\sigma, \mathfrak{p}_i) \mapsto \sigma(\mathfrak{p}_i).$$

Theorem 8.1. *The action of $\mathrm{Gal}(K/\mathbb{Q})$ on the set of prime ideals of $\mathcal{O}_K$ dividing (p) is transitive, i.e. for any $1 \le i, j \le g$, there is $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. Consequently, the ramification indices e_i of the prime ideal factors of (p) are all equal, and the residue degrees f_i of the prime ideal factors of (p) are all equal.*

Proof. Suppose the contrary that there exist $1 \le i, j \le g$ such that, for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$. By the Chinese Remainder Theorem (or the **weak approximation theorem** as in Exercise 6.2), there exists an element $x \in \mathcal{O}_K$ such that $x \in \mathfrak{p}_j$ but $x \notin \sigma(\mathfrak{p}_i)$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

Now consider $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. On one hand, $N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x) \in x\mathcal{O}_K$, so $N_{K/\mathbb{Q}}(x) \in \mathfrak{p}_j$. This implies that $N_{K/\mathbb{Q}}(x) \in \mathbb{Z} \cap \mathfrak{p}_j = p\mathbb{Z}$. On the other hand, this implies that

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(x) \in (p) \subset \mathfrak{p}_i,$$

so by the primality of $\mathfrak{p}_i$, there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(x) \in \mathfrak{p}_i$. This implies that $x \in \sigma^{-1}(\mathfrak{p}_i)$, which is a contradiction. □

As per Theorem 8.1, in the Galois $K/\mathbb{Q}$ case, we denote the common ramification indices (residue degrees, respectively) of the prime ideals dividing (p) as e (f, respectively). Then, Theorem 7.9 implies that, in the Galois case,

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

Now we can give more structure on the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ based on its action on the primes in K lying over p.

Definition 8.2 (Decomposition/inertia groups)**.** Let $K/\mathbb{Q}$ be Galois, and let $\mathfrak{p} \subset \mathcal{O}_K$ lie over a rational prime $p \in \mathbb{Z}$. Then, the **decomposition group** at $\mathfrak{p}$ over p is

$$D(\mathfrak{p}|p) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\},$$

which is naturally a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. The **inertia group** at $\mathfrak{p}$ over p is

$$I(\mathfrak{p}|p) = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(x) - x \in \mathfrak{p} \text{ for all } x \in \mathcal{O}_K\},$$

which is naturally a subgroup of $D(\mathfrak{p}|p)$ (check this).

Proposition 8.3. *Let $K/\mathbb{Q}$ be Galois, and let $\mathfrak{p} \subset \mathcal{O}_K$ lie over a rational prime $p \in \mathbb{Z}$. Then, for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,*

$$D(\sigma(\mathfrak{p})|p) = \sigma D(\mathfrak{p}|p)\sigma^{-1}, \quad I(\sigma(\mathfrak{p})|p) = \sigma I(\mathfrak{p}|p)\sigma^{-1}.$$

In particular, if $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, $D(\mathfrak{p}|p)$ and $I(\mathfrak{p}|p)$ do not depend on $\mathfrak{p}$ and only depend on p.

Proof. Immediate from the definitions. □

The inertia group can be thought in the following way. Note that

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}) := \{f : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p} \text{ an } \mathbb{F}_p\text{-algebra isomorphism}\},$$

is a group, with the group multiplication given by the composition of maps.

Theorem 8.4. *Let $K/\mathbb{Q}$ be Galois, with $\mathfrak{p}$ lying over p. There is a natural group homomorphism*

$$D(\mathfrak{p}|p) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}), \quad \sigma \mapsto \sigma \pmod{\mathfrak{p}}.$$

This group homomorphism is surjective, with the kernel equal to $I(\mathfrak{p}|p) \subset D(\mathfrak{p}|p)$.

Proof. It is immediate that, if $\sigma \in D(\mathfrak{p}|p)$, then as $\sigma(\mathfrak{p}) = \mathfrak{p}$, σ gives rise to an $\mathbb{F}_p$-algebra map $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$, which is in fact an isomorphism as $\sigma^{-1} \pmod{\mathfrak{p}}$ is its inverse. By definition, the kernel of this map is the inertia group $I(\mathfrak{p}|p)$.

Let $e_1, \cdots, e_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. To prove the surjectivity of this map, we want to show that, for any $g \in \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$, there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that, for any $a \in \mathcal{O}_K$, we have

$$\sigma(a) \equiv ga \pmod{\mathfrak{p}}.$$

This can be asserted if we have

$$\sigma(\overline{e}_i) = g\overline{e}_i,$$

where $\overline{e}_i \in \mathcal{O}_K/\mathfrak{p}$ is the mod $\mathfrak{p}$ reduction of e_i, for $1 \leq i \leq n$. Now consider a polynomial in $(n+1)$-variables,

$$f(Y, X_1, \cdots, X_n) := \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(Y - \sum_{i=1}^{n} \sigma(e_i) X_i \right) \in \mathcal{O}_K[Y, X_1, \cdots, X_n].$$

Note that, if $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, we have[10]

$$\tau(f(Y, X_1, \cdots, X_n)) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(Y - \sum_{i=1}^{n} \tau(\sigma(e_i)) X_i \right) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(Y - \sum_{i=1}^{n} \sigma(e_i) X_i \right),$$

because $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sigma \mapsto \tau\sigma} \mathrm{Gal}(K/\mathbb{Q})$ is a bijection of sets, we know that $f(Y, X_1, \cdots, X_n)$ has coefficients in $\mathcal{O}_K^{\mathrm{Gal}(K/\mathbb{Q})} = \mathcal{O}_K \cap K^{\mathrm{Gal}(K/\mathbb{Q})} = \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. Note now that, as there is a term in the product with $\sigma = 1$, we have

$$f(e_1 X_1 + \cdots + e_n X_n, X_1, \cdots, X_n) = 0.$$

This means that, under the natural map

$$\mathcal{O}_K[Y, X_1, \cdots, X_n] \twoheadrightarrow \mathcal{O}_K[Y, X_1, \cdots, X_n]/(Y - e_1 X_1 - \cdots - e_n X_n),$$

the element $f(Y, X_1, \cdots, X_n) \in \mathcal{O}_K[Y, X_1, \cdots, X_n]$ is sent to zero.

Let $\overline{f}(Y, X_1, \cdots, X_n) \in \mathbb{F}_p[Y, X_1, \cdots, X_n]$ be the mod p reduction of $f(Y, X_1, \cdots, X_n)$. Namely, let $\overline{f}(Y, X_1, \cdots, X_n)$ be the image of $f(Y, X_1, \cdots, X_n)$ under the natural map

$$\mathbb{Z}[Y, X_1, \cdots, X_n] \twoheadrightarrow \mathbb{F}_p[Y, X_1, \cdots, X_n].$$

Then, we have

$$\overline{f}(e_1 X_1 + \cdots + e_n X_n, X_1, \cdots, X_n) = 0 \in (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n],$$

which means that the element $f(Y, X_1, \cdots, X_n)$ is sent to zero in the bottom right corner of the diagram

$$\begin{array}{ccccc}
\mathbb{Z}[Y, X_1, \cdots, X_n] & \hookrightarrow & \mathcal{O}_K[Y, X_1, \cdots, X_n] & \twoheadrightarrow & \mathcal{O}_K[Y, X_1, \cdots, X_n]/(Y - e_1 X_1 - \cdots - e_n X_n) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{F}_p[Y, X_1, \cdots, X_n] & \hookrightarrow & (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n] & \twoheadrightarrow & (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n]/(Y - \overline{e}_1 X_1 - \cdots - \overline{e}_n X_n)
\end{array}$$

Here, the arrows that you take to arrive from the top left to the bottom right do not matter, as this is a **commutative diagram**; namely, the arrows you take do not matter (check it yourself). Applying $g \in \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$ on the bottom row, we have an even bigger commutative diagram,

$$\begin{array}{ccccc}
\mathbb{Z}[Y, X_1, \cdots, X_n] & \hookrightarrow & \mathcal{O}_K[Y, X_1, \cdots, X_n] & \twoheadrightarrow & \mathcal{O}_K[Y, X_1, \cdots, X_n]/(Y - e_1 X_1 - \cdots - e_n X_n) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{F}_p[Y, X_1, \cdots, X_n] & \hookrightarrow & (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n] & \twoheadrightarrow & (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n]/(Y - \overline{e}_1 X_1 - \cdots - \overline{e}_n X_n) \\
\| & & \sim \downarrow g & & \sim \downarrow g \\
\mathbb{F}_p[Y, X_1, \cdots, X_n] & \hookrightarrow & (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n] & \twoheadrightarrow & (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n]/(Y - g\overline{e}_1 X_1 - \cdots - g\overline{e}_n X_n)
\end{array}$$

[10]Here, $\tau(f(Y, X_1, \cdots, X_n))$ means that you apply τ to the coefficients of the polynomial.

where $f(Y, X_1, \cdots, X_n) \in \mathbb{Z}[Y, X_1, \cdots, X_n]$ is sent to 0 in the bottom right corner. On the other hand, when you go through the veritcal arrows and then the horizontal arrows, you notice that the image of $f(Y, X_1, \cdots, X_n)$ in the bottom middle entry is just

$$\overline{f}(Y, X_1, \cdots, X_n) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \left(Y - \sum_{i=1}^{n} \sigma(\overline{e}_i) X_i \right) \in (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n].$$

As $\mathcal{O}_K/\mathfrak{p}$ is a field, $(\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n]$ is a domain, so there exists some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\left(\sum_{i=1}^{n} g\overline{e}_i X_i \right) - \left(\sum_{i=1}^{n} \sigma(\overline{e}_i) X_i \right) = 0 \in (\mathcal{O}_K/\mathfrak{p})[Y, X_1, \cdots, X_n].$$

Therefore, $\sigma(\overline{e}_i) = g\overline{e}_i$ for all $1 \leq i \leq n$, which is what we wanted. □

Remark 8.5. In most texts in undergraduate algebraic number theory, this is proved using the notion of the decomposition fields, but this notion is barely used in practice.

Theorem 8.6. *Let $K/\mathbb{Q}$ be Galois, with $\mathfrak{p}$ lying over p. If p is unramified in K, then $I(\mathfrak{p}|p) = 1$. Therefore, if p is unramified in K, we have a natural isomorphism $D(\mathfrak{p}|p) \cong \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$.*

Proof. Note that $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{p^f}$, so $\mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}) = \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ is a cyclic group of order f. On the other hand, as the Galois group acts transitively on the set of g prime ideals lying over p, the order of $D(\mathfrak{p}|p)$ is $\frac{[K:\mathbb{Q}]}{g} = ef$. Thus, if $e = 1$, then the natural map $D(\mathfrak{p}|p) \to \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$ is a surjective map between two finite sets of the same cardinality, so is bijective. □

What Theorem 8.6 proves is that, if p is unramified in Galois $K/\mathbb{Q}$, then $D(\mathfrak{p}|p)$ is also a cyclic group of order f. Note that $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$, a cyclic group of order f, actually has a natural generator, called the **Frobenius automorphism**:

$$\mathrm{Fr}_p \in \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p), \quad \mathrm{Fr}_p(x) = x^p.$$

Exercise. Check that Fr_p is indeed a generator of $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$.

In terms of $\mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$, this corresponds to the element

$$\mathrm{Fr}_{\mathfrak{p}} \in \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}), \quad \mathrm{Fr}_{\mathfrak{p}}(x) = x^p.$$

Definition 8.7 (Frobenius element)**.** Let $K/\mathbb{Q}$ be Galois with a prime $p \in \mathbb{Z}$ unramified in K. Let $\mathrm{Fr}(\mathfrak{p}|p) \in D(\mathfrak{p}|p)$ be the element correspoding to $\mathrm{Fr}_{\mathfrak{p}} \in \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$ under the natural isomorphism $D(\mathfrak{p}|p) \cong \mathrm{Aut}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$. In other words, $\mathrm{Fr}(\mathfrak{p}|p) \in D(\mathfrak{p}|p)$ is the unique element such that

$$\mathrm{Fr}(\mathfrak{p}|p)(x) \equiv x^p \pmod{\mathfrak{p}},$$

for all $x \in \mathcal{O}_K$.

Proposition 8.8. *Let $K/\mathbb{Q}$ be Galois with a prime $p \in \mathbb{Z}$ unramified in K. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma \operatorname{Fr}(\mathfrak{p}|p)\sigma^{-1} = \operatorname{Fr}(\sigma(\mathfrak{p})|p)$. Therefore, $\operatorname{Fr}(\mathfrak{p}|p)$ lies in a single conjugacy class (i.e. a set of elements conjugate to each other) in $\mathrm{Gal}(K/\mathbb{Q})$ regardless of what $\mathfrak{p}$ is. The conjugacy class is often denoted as $\mathrm{Fr}_p \subset \mathrm{Gal}(K/\mathbb{Q})$ and called the **Frobenius conjugacy class**.*

In particular, if $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, $\operatorname{Fr}(\mathfrak{p}|p) \in \mathrm{Gal}(K/\mathbb{Q})$ does not depend on $\mathfrak{p}$ and only depends on p, in which case we denote the Frobenius element at p as $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$.

Proof. Easy exercise. □

The Frobenius elements are extremely important, as we will see in many instances.

Example 8.9. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 2, 3 \pmod 4$ a squarefree integer. We then know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, and we know that splitting of the rational primes:

$$(p) = \begin{cases} \mathfrak{p}^2 & \text{if } p = 2 \text{ or } d \equiv 0 \pmod p \\ (p) & \text{if } p \text{ is odd and } d \text{ is not a square mod } p \\ \mathfrak{p}\mathfrak{p}' & \text{if } p \text{ is odd and } d \text{ is a square mod } p. \end{cases}$$

Thus, p is unramified in K if and only if p is odd and p does not divide d. Note that $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q})$ abelian. Let's compute Fr_p for each unramified p.

- If p is odd and a square mod p, then p splits completely in K. Thus, $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$ is the unique element such that $\mathrm{Fr}_p(x) \equiv x^p \pmod{\mathfrak{p}}$ for a prime $\mathfrak{p}$ lying over p and $x \in \mathcal{O}_K$. We can take $\mathfrak{p} = (p, \sqrt{d} + a)$ for $d \equiv a^2 \pmod p$. Note that there are two elements in $\mathrm{Gal}(K/\mathbb{Q})$, 1 and σ, where $\sigma(\sqrt{d}) = -\sqrt{d}$. So, we wonder if $\sqrt{d}^p$ is congruent mod $(p, \sqrt{d} - a)$ to either $\sqrt{d}$ or $-\sqrt{d}$. This is the same as

  $$\pm 1 \overset{?}{\equiv} \sqrt{d}^{p-1} \pmod{(p, \sqrt{d} - a)}.$$

  If you unravel, this is asking what element does X^{p-1} correspond to in $\mathbb{F}_p[X]/(X - a)$, so really about what a^{p-1} is congruent to mod p, which is obviously 1 by Fermat's little theorem. Thus, this means that $\mathrm{Fr}_p = 1$.

- If p is odd and a non-square mod p, then p is inert in K. Thus, $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$ is the unique element such that $\mathrm{Fr}_p(x) \equiv x^p \pmod p$. Thus, we wonder if $\sqrt{d}^p$ is congruent mod p to either $\sqrt{d}$ or $-\sqrt{d}$. On the other hand, as $\sqrt{d}^{p-1} = d^{\frac{p-1}{2}} = -1$ as d is a non-square mod p, we have $\sqrt{d}^p = -\sqrt{d} \bmod p$. This means that $\mathrm{Fr}_p = \sigma$ is the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$.

In particular, one can concisely state the above results as follows. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$. Then, for $(p, \operatorname{disc}(\mathbb{Q}(\sqrt{d}))) = 1$ with $d \equiv 2, 3 \pmod 4$ squarefree (recall that in this case $\operatorname{disc}(\mathbb{Q}(\sqrt{d})) = 4d$),

$$\mathrm{Fr}_p = \left(\frac{d}{p}\right) \in \{\pm 1\} = \mathrm{Gal}(K/\mathbb{Q}).$$

One can easily check that this continues to hold when $d \equiv 1 \pmod 4$ (exercise).

The above example tells us that the splitting behavior of a rational prime is somehow related to what $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$ is. This is largely true in general, for example:

Theorem 8.10. *Let $K/\mathbb{Q}$ be Galois, with p a rational prime unramified in K. Then, $\mathrm{Fr}_p = 1 \in \mathrm{Gal}(K/\mathbb{Q})$[11] if and only if p splits completely in K.*

Proof. As the Frobenius element generates the decomposition group, $\mathrm{Fr}_p = 1$ means that the decomposition group $D(\mathfrak{p}|p)$ for any prime $\mathfrak{p}$ lying above p is a trivial group, which is the same as $f = 1$. Since $e = 1$ by assumption, this is equivalent to p splitting completely in K. □

The natural question is then **what does it mean for $\mathrm{Fr}_p = \sigma \in \mathrm{Gal}(K/\mathbb{Q})$ for an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$**? This is related to the **class field theory**, which we will briefly see in the section about the **Artin reciprocity**. As an example of how $\mathrm{Fr}(\mathfrak{p}|p)$ determines the prime splitting in general:

Theorem 8.11. *Let $K/\mathbb{Q}$ be Galois, with p a rational prime unramified in K. Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and $H \leq G$ be a subgroup, and let $L = K^H$ be the fixed field of H. Then, the splitting of the rational prime (p) in $\mathcal{O}_L$ can be described in terms of the Frobenius element in G as follows.*

- *Choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p.*
- *The Frobenius element $\mathrm{Fr}(\mathfrak{p}|p) \in G$ acts on the right on the set of right cosets $H\backslash G$ by $H\sigma \mapsto H\sigma\,\mathrm{Fr}(\mathfrak{p}|p)$.*
- *The set $H\backslash G$ splits into the orbits under the action of $\mathrm{Fr}(\mathfrak{p}|p)$ as*

$$H\backslash G = \{H\sigma_1, H\sigma_1\,\mathrm{Fr}(\mathfrak{p}|p), \cdots, H\sigma_1\,\mathrm{Fr}(\mathfrak{p}|p)^{m_1-1}\} \amalg \cdots \amalg \{H\sigma_r, H\sigma_r\,\mathrm{Fr}(\mathfrak{p}|p), \cdots, H\sigma_r\,\mathrm{Fr}(\mathfrak{p}|p)^{m_r-1}\}.$$

- *Then, the prime ideal factorization of (p) in $\mathcal{O}_L$ is*

$$(p) = \mathfrak{q}_1 \cdots \mathfrak{q}_r,$$

where $\mathfrak{q}_i = \sigma_i\mathfrak{p} \cap \mathcal{O}_L$. Moreover, $f(\mathfrak{q}_i|p) = m_i$.

Proof. It is true by generalities of prime ideals that $\mathfrak{q}_i = \sigma_i\mathfrak{p} \cap \mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$ lying over p, and that p is unramified in L. If $\mathfrak{q}_i = \mathfrak{q}_j$, then $\sigma_i\mathfrak{p}$ and $\sigma_j\mathfrak{p}$ are the prime ideals of $\mathcal{O}_K$ lying over the same prime ideal of $\mathcal{O}_L$. Since K/L is Galois, by the relative analogue of Theorem 8.1 (which we will develop in the later lectures), $\sigma_i\mathfrak{p} = \tau\sigma_j\mathfrak{p}$ for some $\tau \in \mathrm{Gal}(K/L) = H$. Thus, $\sigma_i^{-1}\tau\sigma_j \in D(\mathfrak{p}|p)$. Since $D(\mathfrak{p}|p)$ is a cyclic group generated by $\mathrm{Fr}(\mathfrak{p}|p)$, it follows that $\sigma_i^{-1}\tau\sigma_j = \mathrm{Fr}(\mathfrak{p}|p)^k$ for some $k \in \mathbb{N}$. This implies that $H\sigma_j = H\sigma_i\,\mathrm{Fr}(\mathfrak{p}|p)^k$, so $i = j$. This implies that $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$ are distinct prime ideals in $\mathcal{O}_L$.

Note that $\mathcal{O}_L/\mathfrak{q}_i \hookrightarrow \mathcal{O}_K/\sigma_i\mathfrak{p}$, which is a field extension of finite fields. Furthermore, $\mathcal{O}_L/\mathfrak{q}_i \cong \mathbb{F}_{p^{f(\mathfrak{q}_i|p)}}$, so an element in $x \in \mathcal{O}_K/\sigma_i\mathfrak{p}$ is an element of the subfield $\mathcal{O}_L/\mathfrak{q}_i$ if and only if $x^{p^{f(\mathfrak{q}_i|p)}} = x$. By definition, for $x \in \mathcal{O}_K$, $\mathrm{Fr}(\sigma_i\mathfrak{p}|p)^{f(\mathfrak{q}_i|p)}(x) \equiv x^{f(\mathfrak{q}_i|p)} \pmod{\sigma_i\mathfrak{p}}$. By the relative version of

[11] Note that Fr_p is usually well-defined up to conjugation, but $1 \in \mathrm{Gal}(K/\mathbb{Q})$ always forms a conjugacy class with a single element regardless of whether $\mathrm{Gal}(K/\mathbb{Q})$ is abelian or not.

Theorem 8.4, this implies that $\mathrm{Fr}(\sigma_i\mathfrak{p}|p)^{f(\mathfrak{q}_i|p)} = \mathrm{Fr}(\sigma_i\mathfrak{p}|\mathfrak{q}_i) \in H$ (the relative version of Frobenius; again, will be developed later). Therefore, $\mathrm{Fr}(\sigma_i\mathfrak{p}|p)^{f(\mathfrak{q}_i|p)} \in H$, or $\sigma_i \mathrm{Fr}(\mathfrak{p}|p)^{f(\mathfrak{q}_i|p)} \in H\sigma_i$, or $H\sigma_i \mathrm{Fr}(\mathfrak{p}|p)^{f(\mathfrak{q}_i|p)} = H\sigma_i$, which implies that $m_i \leq f(\mathfrak{q}_i|p)$. This implies that

$$[L:\mathbb{Q}] = |H\backslash G| = \sum_{i=1}^{r} m_i \leq \sum_{i=1}^{r} f(\mathfrak{q}_i|p) = [L:\mathbb{Q}],$$

so it follows that $m_i = f(\mathfrak{q}_i|p)$ for all $1 \leq i \leq r$, as desired. □

– –

Exercise 8.1. Let $K/\mathbb{Q}$ be a Galois extension. Suppose that there is a rational prime p which is inert in K. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group.

9. Lecture 11. Cyclotomic fields, the quadratic reciprocity law

Summary. Cyclotomic fields; rings of integers of cyclotomic fields; splitting of rational primes in cyclotomic fields; Frobenius elements in the Galois groups of cyclotomic fields; every quadratic fields are contained in cyclotomic fields; the first proof of the quadratic reciprocity law.

Content. We study the **cyclotomic fields** in more detail. Recall:

Definition 9.1. Let $m > 1$ be an integer. The m-**th cyclotomic field** is $\mathbb{Q}(\zeta_m)$, where $\zeta_m \in \mathbb{C}$ is a primitive m-th root of unity (for example, $\zeta_m = e^{\frac{2\pi i}{m}}$).

We have seen in Exercise 3.3 that, if $m = p^a$ is a prime power, then $\mathbb{Q}(\zeta_{p^a})$ is independent of the choice of primitive p^a-th root of unity in $\mathbb{C}$, has discriminant equal to $\pm$ of a power of p, and that is Galois over $\mathbb{Q}$ with the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times$.

Theorem 9.2. *Let $m = p^a$ be a prime power, and $K = \mathbb{Q}(\zeta_{p^a})$.*

(1) The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}]$.

(2) Any rational prime $\ell \neq p$ is unramified in K.

(3) The element $\pi := 1 - \zeta_{p^a}$ is an irreducible element in $\mathcal{O}_K$, and $(p) = (\pi)^{p^{a-1}(p-1)}$ is the prime ideal factorization of (p) in $\mathcal{O}_K$.

Proof. It is obvious that $\zeta_{p^a} \in \mathcal{O}_K$, so $\mathbb{Z}[\zeta_{p^a}] \subset \mathcal{O}_K$. We know from Exercise 3.4 that $D(1, \zeta_{p^a}, \cdots, \zeta_{p^a}^{p^{a-1}(p-1)-1})$ is $\pm$ a power of p, so for any $\ell \neq p$, $(\ell, [\mathcal{O}_K : \mathbb{Z}[\zeta_{p^a}]]) = 1$. Thus, the prime ideal factorization of (ℓ) in $\mathcal{O}_K$ can be computed by using the factorization of the minimal polynomial $\Phi_{p^a}(X) = \frac{X^{p^a}-1}{X^{p^{a-1}}-1}$ mod ℓ. Thus, ℓ is unramified in $\mathcal{O}_K$ if $\Phi_{p^a}(X)$ has no repeated roots mod ℓ. As $\Phi_{p^a}(X)$ divides $X^{p^a} - 1$, it is sufficient to prove that $X^{p^a} - 1$ has no repeated roots mod ℓ. This can be checked by whether $X^{p^a} - 1$ and its derivative has any common divisor mod ℓ. Note that the derivative of $X^{p^a} - 1$ is $p^a X^{p^a-1}$, so as p^a is not 0 mod ℓ, this obviously is coprime to $X^{p^a} - 1$ in $\mathbb{F}_\ell[X]$, which means that $X^{p^a} - 1$ has no repeated roots mod ℓ. Thus, ℓ is unramified in K, proving (2).

Note also that in Exercise 3.4 we showed that $N_{K/\mathbb{Q}}(\pi) = p$. This means that π is irreducible in $\mathcal{O}_K$, as otherwise its norm must be a composite number. Therefore, $(\pi) \subset \mathcal{O}_K$ is a prime ideal. Let us denote this as

$$\mathfrak{p} := (\pi).$$

Also, note that

$$p = \Phi_{p^a}(1) = \prod_{(i,p)=1,\ 1\leq i\leq p^a} (1 - \zeta_{p^a}^i) = \left(\prod_{(i,p)=1,\ 1\leq i\leq p^a} \frac{1 - \zeta_{p^a}^i}{\pi} \right) \pi^{p^{a-1}(p-1)},$$

and the big product is a **unit in** $\mathcal{O}_K$ by Exercise 3.4! Therefore, we have an equality of ideals

$$(p) = \mathfrak{p}^{p^{a-1}(p-1)},$$

in $\mathcal{O}_K$, and this is therefore the unique prime ideal factorization of (p) in $\mathcal{O}_K$. This proves (3).

What (3) implies is that p is **totally ramified** in K, so in particular $f = 1$, or

$$\mathbb{Z}/p \hookrightarrow \mathcal{O}_K/\pi\mathcal{O}_K,$$

is an isomorphism. This implies that the elements in $\mathcal{O}_K/\pi\mathcal{O}_K$ can be taken to have integers as representatives, or

$$\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K.$$

Thus, obviously,

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + \pi\mathcal{O}_K.$$

Multiplying by π, we get

$$\pi\mathcal{O}_K = \pi\mathbb{Z}[\zeta_{p^a}] + \pi^2\mathcal{O}_K.$$

Thus,

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + \pi\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + \pi\mathbb{Z}[\zeta_{p^a}] + \pi^2\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + \pi^2\mathcal{O}_K.$$

We can repeat this, to get

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + \pi^m\mathcal{O}_K,$$

for any $m \geq 1$. In particular, if you put $m = np^{a-1}(p-1)$, then as π^m is a unit times p^n, we get

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + p^n\mathcal{O}_K,$$

for any $n \geq 1$. On the other hand, by the proof of the finiteness of $\mathcal{O}_K$, we know that

$$D(1, \zeta_{p^a}, \cdots, \zeta_{p^a}^{p^{a-1}(p-1)-1})\mathcal{O}_K \subset \mathbb{Z}[\zeta_{p^a}],$$

so for a big enough n, $p^n\mathcal{O}_K \subset \mathbb{Z}[\zeta_{p^a}]$. Therefore, this proves that

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}] + p^n\mathcal{O}_K \subset \mathbb{Z}[\zeta_{p^a}],$$

which implies that $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^a}]$, proving (1). □

Now we can combine the prime-power cases to obtain a general statement.

Theorem 9.3. *Let $n > 1$ be an integer, and let ζ_n be a primitive n-th root of unity in $\mathbb{C}$, and $K = \mathbb{Q}(\zeta_n)$.*

(1) We have $[K : \mathbb{Q}] = \varphi(n)$,[12] and the conjugates of ζ_n are ζ_n^k for $1 \leq k \leq n$, $(k, n) = 1$. In particular, $K = \mathbb{Q}(\zeta_n)$ is independent of the choice of the primitive n-th root of unity ζ_n.

[12]This is the Euler totient function, defined by

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1),$$

when $n = p_1^{e_1} \cdots p_r^{e_r}$ is a prime factorization.

(2) The field extension $K/\mathbb{Q}$ is Galois, with the Galois group

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

(3) The minimal polynomial of ζ_n over $\mathbb{Q}$ is inductively defined as

$$\Phi_n(X) := \frac{X^n - 1}{\prod_{m|n,\ m\neq n} \Phi_m(X)} = \prod_{1\leq k\leq n,\ (k,n)=1} (X - \zeta_n^k) \in \mathbb{Z}[X].$$

*This is called the n-**th cyclotomic polynomial**.*

(4) The ring of integers of K is $\mathbb{Z}[\zeta_n]$.

(5) Any rational prime ℓ not dividing n does not divide $\mathrm{disc}(K)$, and is unramified in K.

(6) If $n = p^r m$ for $(m, p) = 1$, then the prime ideal decomposition of (p) in $\mathcal{O}_K$ is of the form

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{\varphi(p^r)},$$

for some g, where $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ are mutually distinct prime ideals in $\mathcal{O}_K$. In other words, $e = \varphi(p^r)$.

Proof. Let us prove this Theorem by induction on the number of prime factors of n. The base case of n being a prime power has already been proved. Suppose that $n = p^r m$ for $(m, p) = 1$. Note that $\zeta_n^{p^r}$ is a primitive m-th root of unity, while ζ_n^m is a primitive p^r-th root of unity. Thus,

$$\mathbb{Q}(\zeta_n) \supset \mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m).$$

As $(p^r, m) = 1$, there are $a, b \in \mathbb{Z}$ such that $ap^r + bm = 1$. Thus, $\zeta_n = \zeta_n^{ap^r+bm} = \zeta_m^a \zeta_{p^r}^b$, so

$$\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m).$$

Therefore, $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m)$, which is independendent of the choice of ζ_n. This implies that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is, as a compositum of two Galois extensions, Galois. Moreover, the field $\mathbb{Q}(\zeta_n)$ does not depend on the choice of ζ_n, as $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^r})\mathbb{Q}(\zeta_m)$ and the right hand side does not depend on any choice. Note also that there is a natural homomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a(\sigma),$$

where $\sigma(\zeta_n) = \zeta_n^{a(\sigma)}$ (note $\sigma(\zeta_n)$ must be a root of $X^n - 1$, so it should be a power of ζ_n). This is injective, as an automorphism of $\mathbb{Q}(\zeta_n)$ is determined by where ζ_n is sent to. As

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}][\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(p^r)\varphi(m) = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|,$$

the natural homomorphism is an isomorphism (here, we used that $\varphi(ab) = \varphi(a)\varphi(b)$ for $(a, b) = 1$). This proves (1) and (2).

By induction, we have

$$\prod_{m|n,\ m\neq n} \Phi_m(X) = \prod_{m|n,\ m\neq n} \prod_{1\leq k\leq m,\ (k,m)=1} (X-\zeta_m^k)$$

$$= \prod_{n=md,\ d\neq 1} \prod_{1\leq k'\leq n,\ (k',n)=d} (X-\zeta_n^{k'}) = \prod_{1\leq k'\leq n,\ (k',n)>1} (X-\zeta_n^{k'}),$$

so

$$\Phi_n(X) = \prod_{1\leq k\leq n,\ (k,n)=1} (X-\zeta_n^k).$$

Therefore, ζ_n is a root of $\Phi_n(X)$, and as $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n) = \deg \Phi_n(X)$, we see that $\Phi_n(X)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$, proving (3).

By induction, $\operatorname{disc}(\mathbb{Q}(\zeta_{p^r}))$ and $\operatorname{disc}(\mathbb{Q}(\zeta_m))$ are coprime to each other. Therefore, by Proposition 4.6,

$$\operatorname{disc}(\mathbb{Q}(\zeta_n)) = \operatorname{disc}(\mathbb{Q}(\zeta_{p^r}))^{\varphi(m)} \operatorname{disc}(\mathbb{Q}(\zeta_m))^{\varphi(p^r)}.$$

Furthermore, by induction, $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$ and $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$, so again by Proposition 4.6, $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, proving (4). Finally, by Dedekind's criterion, to prove that ℓ not dividing n is unramified in $\mathbb{Q}(\zeta_n)$, it is sufficient to prove that $\Phi_n(X)$ has no repeated roots mod ℓ. It is sufficient to prove that there is a polynomial divisible by $\Phi_n(X)$ with no repeated roots mod ℓ, so in particular it is sufficient to prove that X^n-1 has no repeated roots mod ℓ. This statement is equivalent to that X^n-1 and its derivative are coprime to each other mod ℓ, i.e.

$$\gcd(X^n-1 \pmod\ell, nX^{n-1} \pmod\ell) = 1.$$

This follows from that $\gcd(X^n-1 \pmod\ell, X \pmod\ell) = 1$ and $\gcd(X^n-1 \pmod\ell, n \pmod\ell) = 1$. Thus, we proved (4).

Finally, to prove (6), we have to show that $\Phi_n(X)$ mod p is the $\varphi(p^r)$-power of a polynomial with no repeated roots. Note first that

$$X^n-1 \equiv (X^m-1)^{p^r} \pmod p.$$

Therefore,

$$\frac{X^n-1}{X^{n/p}-1} \equiv (X^m-1)^{\varphi(p^r)} \pmod p.$$

Since

$$X^n-1 = \prod_{a|p^rm} \Phi_a(X),\ X^{n/p}-1 = \prod_{a|p^{r-1}m} \Phi_a(X),$$

therefore

$$\frac{X^n-1}{X^{n/p}-1} = \prod_{a|m} \Phi_{p^ra}(X).$$

Note that X^m-1 has no repeated roots mod p by the induction hypothesis on (5), and $\Phi_{p^ra}(X)$ for $a|m$, $a\neq m$, is the $\varphi(p^r)$-power of a polynomial with no repeated roots mod p by the induction hypothesis on (6). Therefore, $\Phi_n(X) = \Phi_{p^rm}(X)$ is also the $\varphi(p^r)$-power of a polynomial with no repeated roots mod p, proving (6). □

From the definition of the Frobenius element, the following Corollary is obvious.

Corollary 9.4. *For a rational prime ℓ not dividing n, $\mathrm{Fr}_\ell \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ corresponds to $\ell \in (\mathbb{Z}/n\mathbb{Z})^\times$ by the isomorphism in Theorem 9.3(2). Namely, $\mathrm{Fr}_\ell(\zeta_n) = \zeta_n^\ell$.*

Corollary 9.5 (Cyclotomic Reciprocity Law)**.** *Let p be an odd rational prime, and let q be any rational prime $\neq p$. Let $d|(p-1)$, and let $F_d \subset \mathbb{Q}(\zeta_p)$ be the unique subfield of degree d over $\mathbb{Q}$. Then, q is a d-th power mod p if and only if $\mathrm{Fr}_q = 1$ in $\mathrm{Gal}(F_d/\mathbb{Q})$ (i.e. if and only if q splits completely in F_d by Theorem 8.10).*

Proof. Note that $H := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/F_d) \subset G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is the unique cyclic subgroup of order $\frac{p-1}{d}$. Using Theorem 8.11, we know that q splits completely in F_d if and only if $H\sigma = H\sigma\,\mathrm{Fr}_{q,\mathbb{Q}(\zeta_p)}$ for all $\sigma \in G$, where $\mathrm{Fr}_{q,\mathbb{Q}(\zeta_p)} \in G$ is the Frobenius element of q in G. Since G is abelian, this is the same as $\mathrm{Fr}_{q,\mathbb{Q}(\zeta_p)} \in H$. Note that $\mathrm{Fr}_{q,\mathbb{Q}(\zeta_p)} \in G$ corresponds to $q \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $H \subset G$ corresponds to the cyclic subgroup of d-th powers in $(\mathbb{Z}/p\mathbb{Z})^\times$, the statement follows. □

Remark 9.6. Often the Cyclotomic Reciprocity Law means a special case of Corollary 9.5, that the cyclotomic polynomial $\Phi_p(X)$ factorizes into a product of distinct linear factors mod q if and only if $q \equiv 1 \pmod p$.

Now we are ready to prove the quadratic reciprocity law.

Theorem 9.7 (Quadratic reciprocity law)**.** *Let p be an odd prime.*

(1) We have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(2) We have

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

(3) If $q \neq p$ is an odd prime,

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

Proof. Let $q \neq p$ be a prime. Then, by Corollary 9.5, $\left(\frac{q}{p}\right) = 1$ if and only if q splits completely in the unique quadratic subfield K of $\mathbb{Q}(\zeta_p)$, which by Exercise 4.1 we know that $K = \mathbb{Q}(\sqrt{\epsilon p})$, where $\epsilon = 1$ if $p \equiv 1 \pmod 4$ and $\epsilon = -1$ if $p \equiv 3 \pmod 4$. By Exercise 7.3, we know that this happens if and only if $\left(\frac{\epsilon p}{q}\right) = 1$, or that

$$\left(\frac{q}{p}\right) = \left(\frac{\epsilon p}{q}\right),$$

or

$$\left(\frac{q}{p}\right)\left(\frac{\epsilon p}{q}\right) = 1.$$

Therefore, the statement of (3) in the case of either p or $q \equiv 1 \pmod 4$ follows from this (by possibly swapping the roles of p and q).

Now we prove (1) in the case of $p \equiv 1 \pmod 4$. As $p \neq 3$, we have

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right),$$

but also we have

$$\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right).$$

Therefore, it follows that $\left(\frac{-1}{p}\right) = 1$, as desired.

Now we prove (1) in the case of $p \equiv 3 \pmod 4$. Firstly, it is easy to see that $\left(\frac{-1}{3}\right) = -1$, as 2 is not a square mod 3. If $p \neq 3$, then we have

$$\left(\frac{3}{p}\right) = \left(\frac{-p}{3}\right) = \left(\frac{p}{3}\right)\left(\frac{-1}{3}\right) = -\left(\frac{p}{3}\right),$$

and

$$\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right).$$

Therefore, it follows that $\left(\frac{-1}{p}\right) = -1$ for all $p \equiv 3 \pmod 4$. This completely proves (1).

Now we prove the remaining cases of (3), that is that $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \equiv q \equiv 3 \pmod 4$. This follows easily from (1) as

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

Now it remains to prove (2). Note that $\left(\frac{2}{p}\right) = 1$ if and only if 2 splits completely in $K = \mathbb{Q}(\sqrt{\epsilon p})$. Note that $\epsilon p \equiv 1 \pmod 4$ by definition. By Exercise 7.1, 2 is inert in $\mathbb{Q}(\sqrt{\epsilon p})$ if and only if $\frac{1-\epsilon p}{4} \equiv 1 \pmod 2$, or $\epsilon p \equiv 5 \pmod 8$. Thus, $\left(\frac{2}{p}\right) = -1$ if and only if $\epsilon p \equiv 5 \pmod 8$, so either $p \equiv 5 \pmod 8$ or $p \equiv 3 \pmod 8$. Thus, (2) follows. □

Remark 9.8. We will later prove the quadratic reciprocity in a more "analytic way". Also, the relative theory of splitting gives us more generalized reciprocity laws like Fermat's "cubic reciprocity law."

Cyclotomic fields have a very special position in the theory of number fields. These are easy-to-write number fields whose Galois groups over $\mathbb{Q}$ are always abelian. In particular, any Galois subfield of a cyclotomic field is an **abelian extension of** $\mathbb{Q}$, namely a Galois extension of $\mathbb{Q}$ whose Galois group is an abelian group.

It is a very surprising and fundamental theorem that the converse direction is true!

Theorem 9.9 (Kronecker–Weber). *For any abelian extension $K/\mathbb{Q}$, there exists a cyclotomic field $\mathbb{Q}(\zeta_n)$ which contains K as a subfield.*

This Theorem is very difficult and requires the class field theory. We will see later how this follows from a big theorem of Artin reciprocity law (whose proof we will not be able to cover). On the other hand, we can see now that the quadratic fields version of the Kronecker–Weber theorem holds.

Proposition 9.10 (Kronecker–Weber for quadratic fields). *Let $K/\mathbb{Q}$ be a quadratic field. Then, there exists a cyclotomic field $\mathbb{Q}(\zeta_n)$ which contains K as a subfield.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ for a square-free integer d. Suppose first that d is odd. Let $d = \pm p_1 \cdots p_r$ be a prime factorization. Then, $\mathbb{Q}(\zeta_{p_i}) \supset \mathbb{Q}(\sqrt{\epsilon_i p_i})$ for some $\epsilon_i \in \{\pm 1\}$. Moreover, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$. As $\mathbb{Q}(\zeta_{4p_1\cdots p_r}) = \mathbb{Q}(\zeta_4)\mathbb{Q}(\zeta_{p_1})\cdots\mathbb{Q}(\zeta_{p_r})$ is a compositum, we have

$$\mathbb{Q}(\sqrt{-1}, \sqrt{\epsilon_1 p_1}, \cdots, \sqrt{\epsilon_r p_r}) \subset \mathbb{Q}(\zeta_{4p_1\cdots p_r}).$$

Therefore, both $\mathbb{Q}(\sqrt{\epsilon_1 \cdots \epsilon_r p_1 \cdots p_r})$ and $\mathbb{Q}(\sqrt{-\epsilon_1 \cdots \epsilon_r p_1 \cdots p_r})$ are inside $\mathbb{Q}(\zeta_{4p_1\cdots p_r})$. Thus, $K \subset \mathbb{Q}(\zeta_{4p_1\cdots p_r})$.

Now suppose that d is even. Let $d = \pm 2p_1 \cdots p_r$ be a prime factorization. Then, we look at $\mathbb{Q}(\zeta_8)$ instead – note that as $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^2$ is the Klein four group, there are three quadratic subfields (corresponding to the three order 2 quotients of the Klein four group) of $\mathbb{Q}(\zeta_8)$ by Galois theory. Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \langle \sigma_3, \sigma_5 \mid \sigma_3^2 = \sigma_5^2 = 1,\ \sigma_3\sigma_5 = \sigma_5\sigma_3 \rangle$, where $\sigma_i(\zeta_8) = \zeta_8^i$. Then, there are three order 2 subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$,

$$G_1 = \{1, \sigma_3\}, \quad G_2 = \{1, \sigma_5\}, \quad G_3 = \{1, \sigma_3\sigma_5\}.$$

We pick $\zeta_8 = \frac{1+i}{\sqrt{2}}$. Correspondingly, the fixed fields are

$$\begin{aligned}
\mathbb{Q}(\zeta_8)^{G_1} &= \{a + b(\zeta_8 + \zeta_8^3) + c(\zeta_8^2 + \zeta_8^6) + d(\zeta_8^5 + \zeta_8^7) + e\zeta_8^4 \mid a, b, c, d, e \in \mathbb{Q}\} \\
&= \{(a - e) + (b - d)\sqrt{2}i \mid a, b, c, d, e \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{-2}), \\
\mathbb{Q}(\zeta_8)^{G_2} &= \{a + b(\zeta_8 + \zeta_8^5) + c\zeta_8^2 + d(\zeta_8^3 + \zeta_8^7) + e\zeta_8^4 + f\zeta_8^6 \mid a, b, c, d, e, f \in \mathbb{Q}\} \\
&= \{(a - e) + (c - f)i \mid a, b, c, d, e, f \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{-1}), \\
\mathbb{Q}(\zeta_8)^{G_3} &= \{a + b(\zeta_8 + \zeta_8^7) + c(\zeta_8^2 + \zeta_8^6) + d(\zeta_8^3 + \zeta_8^5) + e\zeta_8^4 \mid a, b, c, d, e \in \mathbb{Q}\} \\
&= \{(a - e) + (b - d)\sqrt{2} \mid a, b, c, d, e \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2}).
\end{aligned}$$

In particular, both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ are inside $\mathbb{Q}(\zeta_8)$. Now, we use the same argument as above with $\mathbb{Q}(\zeta_{8p_1\cdots p_r})$ instead, we get the same result that both $\mathbb{Q}(\sqrt{2p_1 \cdots p_r})$ and $\mathbb{Q}(\sqrt{-2p_1 \cdots p_r})$ are inside $\mathbb{Q}(\zeta_{8p_1\cdots p_r})$, so $K \subset \mathbb{Q}(\zeta_{8p_1\cdots p_r})$. □

– –

Exercise 9.1. Let $K = \mathbb{Q}(\zeta_n)$ with $n > 2$.

(1) Show that there is no real embedding of K.

(2) Show that $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(\frac{2\pi i}{n}))$ is a subfield of K with $[K : K^+] = 2$.

(3) Show that every embedding $\iota : K^+ \hookrightarrow \mathbb{C}$ is a real embedding.

(4) Show that $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

10. Lectures 12 and 13. Finiteness of class number, binary quadratic forms

Summary. Geometry of numbers; Minkowski's theorem; proof of the finiteness of class number; binary quadratic forms; upper half plane.

Content. Our goal is to prove the following theorem.

Theorem 10.1 (Finiteness of the class number)**.** *Let K be a number field. Then, $\mathrm{Cl}(K)$ is a finite abelian group.*

As $\mathrm{Cl}(K)$ is obviously an abelian group by definition, the content is to prove that $\mathrm{Cl}(K)$ is finite. The order of $\mathrm{Cl}(K)$ is called the **class number** of K, and is denoted h_K.

The idea of the proof is to see a fractional ideal as a **lattice**. Recall that we know that any nonzero fractional ideal of K is a free $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$. The way that we proved certain domains are Euclidean domains is by embedding the domains into say $\mathbb{C}$ and use the distance of complex numbers. Similarly, for any fractional ideal $\mathfrak{a}$ of K, we can see this as a lattice in $\mathbb{R}^r \times \mathbb{C}^s$. Here, r, s are respectively the numbers of real and complex embeddings of K. These are more formally defined as follows.

Definition 10.2 (Real and complex embeddings)**.** Let K be a number field of degree n. Then,

$$\#\{\sigma : K \hookrightarrow \mathbb{C}\} = n.$$

An embedding $\sigma : K \hookrightarrow \mathbb{C}$ is a **real embedding** if the image of σ is contained in $\mathbb{R}$. The number of real embeddings of K is often denoted as r.

An embedding $\sigma : K \hookrightarrow \mathbb{C}$ is a **complex embedding** if it is not a real embedding. The number of complex embeddings is always an even number, as a complex embedding $\sigma : K \hookrightarrow \mathbb{C}$ comes in a pair of complex embeddings, with another complex embedding $\overline{\sigma} : K \hookrightarrow \mathbb{C}$ by taking the complex conjugate of σ. Let s be the half of the number of the complex embeddings of K. Clearly, $r + 2s = n$.

Definition 10.3 (Lattice)**.** Let V be a vector space over $\mathbb{R}$ of dimension n. A **lattice** L in V is a free $\mathbb{Z}$-submodule of rank n, namely

$$L = \mathbb{Z} \cdot v_1 \oplus \cdots \oplus \mathbb{Z} \cdot v_n,$$

where $v_1, \cdots, v_n$ are linearly independent vectors in V. Given this presentation, a **fundamental parallelopiped** is a set

$$D = \{a_1 v_1 + \cdots + a_n v_n \mid 0 \leq a_1, \cdots, a_n \leq 1\}.$$

Note that $\mathrm{vol}(D)$ is, unlike D, independent of the choice of the basis vectors $v_1, \cdots, v_n$.

Using these various embeddings, a fractional ideal of K can be seen as a lattice in some Euclidean space $\mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s} = \mathbb{R}^n$. The finiteness question is then reduced to the following type of question.

Question. In a lattice inside a Euclidean space, what is the smallest norm of a nonzero vector?

This kind of a technique where you transform a question about integers into a question about geometry is called the **geometry of numbers**. The specific question as above can be approached by **Minkowski's theorem**.

Theorem 10.4 (Minkowski's theorem)**.** *Let $L \subset V = \mathbb{R}^n$ be a lattice, and let $\mathrm{vol}(D)$ be the volume of a fundamental parallelopiped of L. Let $T \subset V$ be a compact, convex (i.e. $v, w \in T$ implies $\lambda v + (1-\lambda)w \in T$ for all $0 \leq \lambda \leq 1$) and symmetric (i.e. $v \in T$ implies $-v \in T$) subset. If*[13]

$$\mathrm{vol}(T) \geq 2^n \,\mathrm{vol}(D),$$

then T contains a nonzero element of L.

Proof. Let $\lambda > 1$ be a real number, and let $\lambda T = \{\lambda t \mid t \in T\}$. Then, $\mathrm{vol}(\lambda T) = \lambda^n \,\mathrm{vol}(T)$, so $\mathrm{vol}(\frac{\lambda}{2}T) > \mathrm{vol}(D)$. As $\mathbb{R}^n$ can be partitioned into

$$\mathbb{R}^n = \bigcup_{x \in L} (x + D),$$

we have

$$\mathrm{vol}\left(\frac{\lambda}{2}T\right) = \bigcup_{x \in L} \mathrm{vol}\left(\frac{\lambda}{2}T \cap (x + D)\right).$$

For $x \in L$, let $D_x \subset D$ be defined as

$$D_x = \left(\frac{\lambda}{2}T - x\right) \cap D.$$

As $\mathrm{vol}\left(\frac{\lambda}{2}T\right) = \sum_{x \in L} \mathrm{vol}(D_x) > \mathrm{vol}(D)$, there are two $x_1, x_2 \in L$ such that $D_{x_1} \cap D_{x_2} \neq \emptyset$. Then, there are $t_1, t_2 \in T$ such that $\frac{\lambda t_1}{2} - x_1 = \frac{\lambda t_2}{2} - x_2$, so $\frac{\lambda(t_1 - t_2)}{2} = x_1 - x_2 \in L \backslash \{0\}$. Since $-t_2 \in T$ by symmetry of T, $\frac{t_1 - t_2}{2} \in T$ by convexity of T. Thus, $\frac{\lambda(t_1 - t_2)}{2} \in \lambda T$. Thus, λT contains a nonzero element of L, for every $\lambda > 1$.

Suppose now that $T \cap L = \{0\}$. Then, even though $\frac{3}{2}T \cap L \neq \{0\}$, it is compact (since T is compact by assumption and L is closed as L is a homeomorphic image of $\mathbb{Z}^n \subset \mathbb{R}^n$ which is closed) and discrete (since L is discrete – again, L a homeomorphic image of $\mathbb{Z}^n \subset \mathbb{R}^n$, which is discrete), so finite. Let $\frac{3}{2}T \cap L = \{0, x_1, \cdots, x_m\}$. Then, by assumption, $x_i \notin \lambda_i T$ for some $\lambda_i > 1$. Taking $\lambda = \min(\lambda_1, \cdots, \lambda_m)$, we obtain a contradiction that $\lambda T \cap L = \{0\}$ for $\lambda > 1$. Thus, $T \cap L$ contains a nonzero element. □

In the above proof, we used the following little lemma in topology.

Lemma 10.5. *A compact discrete set is finite.*

Proof. Let S be a compact discrete set. For each $x \in S$, let $U_x := \{x\} \subset S$ which is an open subset (by discreteness). Then, $S = \bigcup_{x \in S} U_x$ is an open cover, so there is a finite subcover $U_{x_1}, \cdots, U_{x_r}$ for $x_1, \cdots, x_r$. This means that $S = \bigcup_{i=1}^r \{x_i\}$, so finite. □

[13] As we use the notion of the volume of T, to be very precise, we need that T is a Lebesgue-measurable set. In practice, T will be a finite intersection and union of the region defined by real analytic funcitons, so it is always Lebesgue measurable.

Now consider the r real embeddings of K,

$$\sigma_1, \cdots, \sigma_r : K \hookrightarrow \mathbb{R},$$

and the s pairs of complex embeddings of K,

$$\sigma_{r+1}, \overline{\sigma}_{r+1}, \cdots, \sigma_{r+s}, \overline{\sigma}_{r+s} : K \hookrightarrow \mathbb{C}.$$

Consider the map

$$\sigma = (\sigma_1, \cdots, \sigma_r, \sigma_{r+1}, \cdots, \sigma_{r+s}) : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s} = \mathbb{R}^n.$$

Proposition 10.6. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then, $\sigma(\mathfrak{a})$ is a lattice in $\mathbb{R}^n$. Furthermore, the volume of a fundamental parallelopiped is equal to $2^{-s}N(\mathfrak{a})\sqrt{|\operatorname{disc}(K)|}$.*

Proof. Let $\alpha_1, \cdots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Note that $\sigma(\mathfrak{a})$ is the $\mathbb{Z}$-module generated by the vectors $\sigma(\alpha_1), \cdots, \sigma(\alpha_n)$, or in terms of coordinates,

$$\sigma(\alpha_i) = (\sigma_1(\alpha_i), \cdots, \sigma_r(\alpha_i), \operatorname{Re}(\sigma_{r+1}(\alpha_i)), \operatorname{Im}(\sigma_{r+1}(\alpha_i)), \cdots, \operatorname{Re}(\sigma_{r+s}(\alpha_i)), \operatorname{Im}(\sigma_{r+s}(\alpha_i))).$$

Let A be the matrix whose i-th row is $\sigma(\alpha_i)$. Let B be the matrix whose i-th row is

$$(\sigma_1(\alpha_i), \cdots, \sigma_r(\alpha_i), \sigma_{r+1}(\alpha_i), \overline{\sigma_{r+1}(\alpha_i)}, \cdots, \sigma_{r+s}(\alpha_i), \overline{\sigma_{r+s}(\alpha_i)}).$$

Then, by Proposition 3.8,

$$|\det(B)|^2 = |D(\alpha_1, \cdots, \alpha_n)| = [\mathcal{O}_K : \mathfrak{a}]^2 |\operatorname{disc}(K)| \neq 0,$$

so $\det(B) \neq 0$. Through elementary column operations, it is easy to see that

$$\det(B) = (-2i)^s \det(A).$$

Therefore,

$$|\det(A)| = 2^{-s} N(\mathfrak{a}) \sqrt{|\operatorname{disc}(K)|},$$

which is nonzero. Therefore, $\sigma(\mathfrak{a})$ is a lattice. Also, since $\det(A)$ is the volume of a fundamental parallelopiped, we are done. □

The following is a key to the finiteness of the class number.

Proposition 10.7. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then, there is a nonzero element $\alpha \in \mathfrak{a} \backslash \{0\}$ such that*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} N(\mathfrak{a}) \sqrt{|\operatorname{disc}(K)|}.$$

Proof. Note that

$$|N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)|\cdots|\sigma_r(\alpha)||\sigma_{r+1}(\alpha)|^2\cdots|\sigma_{r+s}(\alpha)|^2 \le \frac{\left(\sum_{i=1}^r |\sigma_i(\alpha)| + 2\sum_{i=r+1}^{r+s}|\sigma_i(\alpha)|\right)^n}{n^n},$$

by the AM-GM inequality.

For any $y > 0$, let $B(y) \subset \mathbb{R}^r \times \mathbb{C}^s$ be the set of vectors

$$B(y) = \left\{(x_1, \cdots, x_r, x_{r+1}, \cdots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^r |x_i| + 2\sum_{i=r+1}^{r+s}|x_i| < y\right\}.$$

Thus, by Minkowski's theorem, if $\mathrm{vol}(B(y)) \ge 2^n \mathrm{vol}(D)$, for D a fundamental parallelopiped of $\sigma(\mathfrak{a})$, we have a nonzero element in $B(y) \cap \sigma(\mathfrak{a})$, which implies that there is a nonzero element $\alpha \in \mathfrak{a}\backslash\{0\}$ such that $|N_{K/\mathbb{Q}}(\alpha)| \le \frac{y^n}{n^n}$.

Computing $\mathrm{vol}(B(y))$ in terms of y is just a calculus exercise.

Lemma 10.8. *We have* $\mathrm{vol}(B(y)) = 2^r\left(\frac{\pi}{2}\right)^s \frac{y^n}{n!}$ *(as usual,* $n = r + 2s$*).*

Proof. This is the same as proving the volume of positive $x_1, \cdots, x_r$ is $\left(\frac{\pi}{2}\right)^s \frac{y^n}{n!}$. Furthermore, scaling $x_{r+1}, \cdots, x_{r+s}$ by 2, this is the same as proving that

$$\mathrm{vol}\left(\left\{(x_1, \cdots, x_{r+s}) \in \mathbb{R}^r_{\ge 0} \times \mathbb{C}^s \mid \sum_{i=1}^r x_i + \sum_{i=r+1}^{r+s}|x_i| < y\right\}\right) = (2\pi)^s \frac{y^n}{n!}.$$

For x_j, $j \ge r+1$, we use polar coordinates $x_j = r_j e^{i\theta_j}$, so that the integral we have to prove is

$$I_{r,s}(y) := \int_{x_1,\cdots,x_{r+s}\ge 0,\ x_1+\cdots+x_{r+s}\le y} x_{r+1}\cdots x_{r+s}dx_1\cdots dx_{r+s} = \frac{y^{r+2s}}{(r+2s)!}.$$

We prove this by induction. Note that

$$I_{r,s}(y) = \int_0^y x_{r+s}\int_0^{y-x_{r+s}} x_{r+s-1}\cdots\int_0^{y-x_{r+s}-\cdots-x_{r+2}} x_{r+1}\int_0^{y-x_{r+s}-\cdots-x_{r+1}}\cdots\int_0^{y-x_{r+s}-\cdots-x_1} dx_1dx_2\cdots dx_{r+s}.$$

Therefore, if $s \ge 1$,

$$I_{r,s}(y) = \int_0^y x_{r+s}I_{r,s-1}(y - x_{r+s})dx_{r+s}.$$

By induction,

$$I_{r,s}(y) = \int_0^y x\frac{(y-x)^{r+2s-2}}{(r+2s-2)!}dx = \int_0^y (y-x)\frac{x^{r+2s-2}}{(r+2s-2)!}dx = \int_0^y \frac{yx^{r+2s-2} - x^{r+2s-1}}{(r+2s-2)!}dx$$

$$= \frac{1}{(r+2s-2)!}\left(\frac{y^{r+2s}}{r+2s-1} - \frac{y^{r+2s}}{r+2s}\right) = \frac{1}{(r+2s-2)!}\frac{y^{r+2s}}{(r+2s-1)(r+2s)} = \frac{y^{r+2s}}{(r+2s)!}.$$

Therefore, we only need to prove the formula when $s = 0$. Again, then by induction

$$I_{r,0}(y) = \int_0^y I_{r-1,0}(y - x_r)dx_r = \int_0^y \frac{(y - x_r)^{r-1}}{(r-1)!}dx_r = \int_0^y \frac{x^{r-1}}{(r-1)!}dx = \frac{x^r}{r!},$$

so the formula follows from the base case

$$I_{1,0}(y) = \int_0^y dx_1 = y.$$

□

Therefore, if we take y such that

$$2^r \left(\frac{\pi}{2}\right)^s \frac{y^n}{n!} \geq 2^n 2^{-s} N(\mathfrak{a})\sqrt{|\operatorname{disc}(K)|},$$

then there is a nonzero element $\alpha \in \mathfrak{a}\backslash\{0\}$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{y^n}{n^n}$. We can take $y > 0$ be such that

$$y^n = n!\frac{2^{2s}}{\pi^s} N(\mathfrak{a})\sqrt{|\operatorname{disc}(K)|},$$

then it satisfies the desired inequality. Thus, we get the the desired upper bound on $|N_{K/\mathbb{Q}}(\alpha)|$.
□

We can now prove the finiteness of the class number, and actually can establish an explicit upper bound (even though the bound is too large to be useful in practice).

Theorem 10.9 (Finiteness of the class number, explicit version)**.** *Let K be a degree n number field.*

(1) For each $[\mathfrak{a}] \in \mathrm{Cl}(K)$, there exists an integral ideal representative $\mathfrak{a} \subset \mathcal{O}_K$ of $[\mathfrak{a}]$ (which is a priori a mere equivalence class of fractional ideals) such that

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|} =: B_K.$$

*The number on the right is called the **Minkowski bound**, B_K.*

(2) The class number h_K is finite. For example, there is an explicit bound

$$h_K \leq (\log_2 B_K + 2)^{nB_K}.$$

Proof. (1) Choose any integral ideal representative $\mathfrak{b}$ of $[\mathfrak{a}]^{-1}$ (this is possible because any fractional ideal is of the form $\mathfrak{b}/d$ for some $d \in \mathbb{Z}$ and $\mathfrak{b} \subset \mathcal{O}_K$). Then, by Proposition 10.7, there is $\beta \in \mathfrak{b}$ not zero such that $|N_{K/\mathbb{Q}}(\beta)| \leq B_K N(\mathfrak{b})$. Since $\mathfrak{b}$ divides (β), there exists an integral ideal $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{b} = (\beta)$. Therefore, $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$ is an integral ideal representing the equivalent class of $([\mathfrak{a}]^{-1})^{-1} = [\mathfrak{a}]$. Furthermore, as $N(\mathfrak{a})N(\mathfrak{b}) = N((\beta)) = |N_{K/\mathbb{Q}}(\beta)|$, we have

$$N(\mathfrak{a}) = \frac{|N_{K/\mathbb{Q}}(\beta)|}{N(\mathfrak{b})} \leq B_K,$$

as desired.

(2) It is sufficient to show that the number of integral ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $N(\mathfrak{a}) \leq B_K$ is finite (or, more precisely, bounded above by $(\log_2 B_K + 2)^{nB_K}$). Note that $N(\mathfrak{a}) = \prod_{i=1}^{r} p_i^{e_i} \leq B_K$ implies that very crudely there are B_K many primes p_i can appear in the prime factorization of $N(\mathfrak{a})$, and $0 \leq e_i \leq \log_2 B_K + 1$. For each p_i appearing in the prime factorization of $N(\mathfrak{a})$, the part of the prime ideal factorization of $\mathfrak{a}$ consisted of the primes lying over p_i should be of the form $\mathfrak{p}_{i,1}^{e_{i,1}} \cdots \mathfrak{p}_{i,s_i} S e_{i,s_i}$, where $f(\mathfrak{p}_{i,1}|p_i)e_{i,1} + \cdots + f(\mathfrak{p}_{i,s_i}|p_i)e_{i,s_i} = e_i$. Note that $s_i \leq n$, and $0 \leq e_{i,j} \leq e_i \leq \log_2 B_K + 1$, so there are at most $(\log_2 B_K + 2)^n$ many choices for the part of the prime ideal factorization of $N(\mathfrak{a})$ lying over p_i. Thus, there are at most $(\log_2 B_K + 2)^{nB_K}$ many integral ideals of norm $\leq B_K$. □

Remark 10.10. The Minkowski bound is quite large, but combined with other information like prime splitting, one often has good handle of the class group for small examples. On the other hand, the bound in Theorem 10.9(2) is useless in practice.

We will see later that the class **number** can be computed with analytic methods.

For the rest of this section, we will compute the class group for some examples, and exhibit how the knowledge of class number can be useful in number theoretic questions. A general procedure is as follows.

(1) By Minkowski bound, we have a surjective map of sets

$$\{\mathfrak{a} \subset \mathcal{O}_K,\ N(\mathfrak{a}) \leq B_K\} \twoheadrightarrow \mathrm{Cl}(K).$$

(2) The set on the left is finite. Furthermore, multiplicatively, it is generated by the maximal ideals of $\mathcal{O}_K$ of norm $\leq B_K$. In particular, you have to consider the prime ideals lying over a rational prime p for $p \leq B_K$, and the ideal classes of such finitely many prime ideals will generate $\mathrm{Cl}(K)$.

(3) The task is now to come up with the relations between the ideal classes of those prime ideals.

- The splitting of rational primes gives relations between ideal classes.
- To see whether a given (prime) ideal is a principal ideal, the task is to find (or prove the nonexistence of) a purported generator. The purported generator should have the norm equal to $\pm$ the norm of the ideal, so that should give you a clue.
- To come up with a relation between the prime ideals, you have to come up with a principal ideal whose prime factorization is given by the powers of the prime ideals of norm $\leq B_K$. This again can be guessed by first looking at $\alpha \in \mathcal{O}_K$ whose norm $N_{K/\mathbb{Q}}(\alpha)$ has only prime factors $\leq B_K$.
- You can always reuse the fact that any ideal class must be represented by an ideal $\mathfrak{a} \subset \mathcal{O}_K$ with $N(\mathfrak{a}) \leq B_K$.

(4) Showing that there are no more relations comes from showing that certain prime ideals are not principal.

Example 10.11. Let $K = \mathbb{Q}(\sqrt{14})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{14}]$. We will show that $h_K = 1$. By Theorem 10.9(1), for each $[\mathfrak{a}] \in \mathrm{Cl}(K)$, there is a representative $\mathfrak{a} \subset \mathcal{O}_K$ with

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\sqrt{4 \cdot 14} = \sqrt{14} \sim 3.7417.$$

To prove $h_K = 1$, or $\mathrm{Cl}(K) = 1$, it is sufficient to prove that any integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ with $N(\mathfrak{a}) = 2, 3$ is a principal ideal. Such an ideal is necessarily a prime ideal, and is a prime ideal that lies over either 2 or 3. So let's look at how (2) and (3) splits in K.

$$(2) = (2, \sqrt{14})^2, \quad (3) = (3).$$

In particular, there is no prime ideal with norm 3. So, the only ideal that has a possibility of being non-principal is $(2, \sqrt{14})$ (whose norm is indeed 2, as $N((2, \sqrt{14}))^2 = N(2) = 4$).

If it is indeed a principal ideal, then $(2, \sqrt{14}) = (\alpha)$ for $\alpha \in \mathcal{O}_K$ with $N(\alpha) = \pm 2$. So to investigate whether this ideal is principal or not, we need to look for an element $\alpha = x + \sqrt{14}y$ whose norm is ± 2, or $x^2 - 14y^2 = 2$. One immediately sees that $x = 4, y = 1$ is a possibility.

So is $(2, \sqrt{14})$ the same ideal as $(4 - \sqrt{14})$? Certainly $(4 - \sqrt{14}) \subset (2, \sqrt{14})$, and 2 is a multiple of $4 - \sqrt{14}$, as after all $(4 - \sqrt{14})(4 + \sqrt{14}) = 4^2 - 14 = 2$. So the problem is whether $\sqrt{14}$ is a multiple of $4 - \sqrt{14}$. One may just do the calculation of $\frac{\sqrt{14}}{4-\sqrt{14}}$ and get

$$\frac{\sqrt{14}}{4 - \sqrt{14}} = \frac{\sqrt{14}(4 + \sqrt{14})}{2} = \frac{14 + 4\sqrt{14}}{2} = 7 + 2\sqrt{14},$$

which indeed confirms our expectation.[14]

Remark 10.12 (Fun history **(non-examinable)**)**.** One may wonder whether one can show that $\mathbb{Z}[\sqrt{14}]$ is a PID by showing that it is a Euclidean domain. In fact, this is true, but with a funny twist.

Recall that so far we showed that something is a Euclidean domain by using the most natural and obvious notion of norm. In that regard, it is natural to believe that, if $\mathbb{Z}[\sqrt{14}]$ were to be a Euclidean domain, its division algorithm must use the (absolute value of the) quadratic norm. It is however known that the quadratic norm on $\mathbb{Z}[\sqrt{14}]$ **does not give rise to a division algorithm** (the ring of integers of a quadratic field whose absolute value of the norm gives a division algorithm is called **norm-Euclidean**; so it is shown that $\mathbb{Z}[\sqrt{14}]$ is not norm-Euclidean). In fact, [BSD] classified all norm-Euclidean quadratic fields, which is a finite list. On the other hand, [Har] shows that $\mathbb{Z}[\sqrt{14}]$ is Euclidean! So $\mathbb{Z}[\sqrt{14}]$ has a division algorithm, but a weird division algorithm. The situation is very interesting:

- [BSD] proves that there are finitely many norm-Euclidean quadratic fields: $\mathbb{Q}(\sqrt{d})$ with d in the following list:

$$-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

[14] Another way to do this is to use that, if $\sqrt{14} = (4 - \sqrt{14})c$ for some $c \in \mathcal{O}_K$, then $N(c) = \frac{N(\sqrt{14})}{N(4-\sqrt{14})} = \frac{-14}{2} = -7$. Then $c = d + \sqrt{14}e$ with $d^2 - 14e^2 = -7$. From this one can guess what d, e should be. This kind of approach may be useful for non-quadratic fields, whenever taking the inverse of an element is not so obvious to calculate.

- It is a classical problem raised by Gauss (**Gauss class number one problem**; solved by Baker and Stark) that there are only finitely many imaginary quadratic fields (i.e. $\mathbb{Q}(\sqrt{d})$ with $d < 0$) with class number 1. The list is $\mathbb{Q}(\sqrt{d})$ with d one of the following:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

  The standard proof of this uses **elliptic curves** (more precisely, the complex multiplication theory of elliptic curves).

- It is known that for $\mathbb{Q}(\sqrt{d})$ with $d = -19, -43, -67, -163$ (i.e. d in the second list but not in the first list), $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a PID but not a Euclidean domain.

- Gauss also conjectured that there are infinitely many real quadratic fields (i.e. $\mathbb{Q}(\sqrt{d})$ with $d > 0$) with class number one. This is a major **open problem**. **We don't even know whether there are infinitely many real quadratic fields with class number one.** There are more refined conjectures on the class numbers of real quadratic fields under the name of the **Cohen–Lenstra heuristics**.

- It is **conjectured that the ring of integers of every real quadratic field with class number one is a Euclidean domain**. It is known that the (generalized form of) **Riemann Hypothesis implies this statement**.

- Thus, for (supposedly) infintely many real quadratic fields, their rings of integers are Euclidean domains with weird division algorithms. In fact, the way that this is proven for a few examples is **not constructive**, i.e. **it is proven that there is a division algorithm but we do not know how to write down the division algorithm explicitly**. For example, this is the case for $\mathbb{Q}(\sqrt{69})$ where the existence of division algoritmh is proven indirectly in [Lut].

More examples like this are in the Exercises. We record two more examples indicating that this approach helps to determine the **class group**, not just the class number – in both examples, the class number is 4, but the group structures are different.

Example 10.13. Let $K = \mathbb{Q}(\sqrt{-14})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$. We will to show that $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$. The Minkowski bound is, for each $[\mathfrak{a}] \in \mathrm{Cl}(K)$, there is a representative $\mathfrak{a} \subset \mathcal{O}_K$ with

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\frac{4}{\pi}\sqrt{4 \cdot 14} \sim 4.764.$$

Thus, if $[\mathfrak{a}] \neq 1$, then $N(\mathfrak{a}) = 2, 3, 4$. Therefore, $\mathfrak{a}$ is either a prime ideal lying over either 2 or 3, or is a product of two prime ideals lying over 2. Let's see how (2) and (3) factorizes in $\mathcal{O}_K$:

$$(2) = (2, \sqrt{-14})^2, \quad (3) = (3, \sqrt{-14} + 1)(3, \sqrt{-14} - 1).$$

Let $\mathfrak{p}_2 = (2, \sqrt{-14})$, $\mathfrak{p}_3 = (3, \sqrt{-14} + 1)$, $\mathfrak{p}_3' = (3, \sqrt{-14} - 1)$. Then, $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. Thus, any nontrivial ideal class in $\mathrm{Cl}(K)$ is represented by either $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$ or $\mathfrak{p}_2^2$.

On the other hand, $\mathfrak{p}_2^2 = (2)$ is principal, so $\mathfrak{p}_2^2$ is not an option. Furthermore, $[\mathfrak{p}_2]^2 = 1$ and $[\mathfrak{p}_3][\mathfrak{p}_3'] = 1$, so $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$. Note also that $N_{K/\mathbb{Q}}(2-\sqrt{-14}) = 2^2+14 = 18 = 2\cdot 3^3$, so the prime ideal factorization of $(2-\sqrt{-14})$ is either $\mathfrak{p}_2\mathfrak{p}_3^2$, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$, or $\mathfrak{p}_2{\mathfrak{p}_3'}^2$. Note that $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3' = 3\mathfrak{p}_2$, and $2-\sqrt{-14}$ is not divisible by 3, this is not an option. Note that

$$\mathfrak{p}_3^2 = (3, \sqrt{-14}+1)^2 = (9, 3+3\sqrt{-14}, -13+2\sqrt{-14}),$$

$$\mathfrak{p}_2\mathfrak{p}_3^2 = (2,\sqrt{-14})(9, 3+3\sqrt{-14}, -13+2\sqrt{-14})$$
$$= (18, 6+6\sqrt{-14}, -26+4\sqrt{-14}, 9\sqrt{-14}, -42+3\sqrt{-14}, -28-13\sqrt{-14}),$$

and this contains $2-\sqrt{-14}$ as

$$2-\sqrt{-14} = 18-(-26+4\sqrt{-14})+(-42+3\sqrt{-14}),$$

so $(2-\sqrt{-14}) \subset \mathfrak{p}_2\mathfrak{p}_3^2$, which is an equality as both ideals have the same norm.[15] Thus, in $\mathrm{Cl}(K)$, $[\mathfrak{p}_3]^2[\mathfrak{p}_2] = 1$, so $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$. Therefore, $[\mathfrak{p}_3]$ generates $\mathrm{Cl}(K)$, whose order divides 4, as $[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = 1$.

To show that $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$, therefore, it is sufficient to show that $[\mathfrak{p}_2] = [\mathfrak{p}_3]^2$ is not trivial, or that $\mathfrak{p}_2$ is not a principal ideal. If $\mathfrak{p}_2 = (\alpha)$ for $\alpha = x+y\sqrt{-14}$, $x, y \in \mathbb{Z}$, then $N_{K/\mathbb{Q}}(\alpha) = \pm N(\mathfrak{p}_2) = \pm 2$, so $x^2+14y^2 = 2$. This is clearly impossible. Thus, $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$, as desired.

Example 10.14. Let $K = \mathbb{Q}(\sqrt{-30})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-30}]$. We will show that $\mathrm{Cl}(K) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. The Minkowski bound is, for each $[\mathfrak{a}] \in \mathrm{Cl}(K)$, there is a representative $\mathfrak{a} \subset \mathcal{O}_K$ with

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\frac{4}{\pi}\sqrt{4\cdot 30} \sim 6.974.$$

Thus, if $[\mathfrak{a}] \neq 1$, then $N(\mathfrak{a}) = 2, 3, 4, 5, 6$. Therefore, $\mathfrak{a}$ is either a prime ideal lying over either $2, 3, 5$, a product of two prime ideals lying over 2, or a product of two prime ideals lying over 2 and 3, respectively. Let's see how (2), (3) and (5) factorizes in $\mathcal{O}_K$:

$$(2) = (2,\sqrt{-30})^2, \quad (3) = (3,\sqrt{-30})^2, \quad (5) = (5,\sqrt{-30})^2.$$

Let $\mathfrak{p}_2 = (2,\sqrt{-30})$, $\mathfrak{p}_3 = (3,\sqrt{-30})$, $\mathfrak{p}_5 = (5,\sqrt{-30})$. Then, indeed $N(\mathfrak{p}_2) = 2$, $N(\mathfrak{p}_3) = 3$, $N(\mathfrak{p}_5) = 5$, so $\mathfrak{a}$ is either $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_2^2$, $\mathfrak{p}_5$, or $\mathfrak{p}_2\mathfrak{p}_3$. Note that $\mathfrak{p}_2^2 = (2)$ is principal, so this is not an option. Thus, $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, $[\mathfrak{p}_5]$, with $[\mathfrak{p}_2]^2 = [\mathfrak{p}_3]^2 = [\mathfrak{p}_5]^2 = 1$.

Note also that $N_{K/\mathbb{Q}}(\sqrt{-30}) = 30 = 2\cdot 3\cdot 5$, so the prime ideal factorization of $(\sqrt{-30})$ must be

$$(\sqrt{-30}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5.$$

Thus, $[\mathfrak{p}_5] = [\mathfrak{p}_5]^{-1} = [\mathfrak{p}_2][\mathfrak{p}_3]$. Therefore, $\mathrm{Cl}(K)$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$, both of order dividing 2. Note that $[\mathfrak{p}_2], [\mathfrak{p}_3] \neq 1$, or both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are nonprincipal. This is because, if there is $\alpha = x+y\sqrt{-30}$ where $(\alpha) = \mathfrak{p}_2$ or $\mathfrak{p}_3$, then $N_{K/\mathbb{Q}}(\alpha) = \pm 2$ or ± 3, but $N_{K/\mathbb{Q}}(\alpha) = x^2+30y^2$, so this is clearly impossible. So, $\mathrm{Cl}(K)$ is an abelian group generated by two order 2 elements

[15] This is a very explicit calculation, but you could pretty much bypass this - we know for sure that $(2-\sqrt{-14})$ is either $\mathfrak{p}_2\mathfrak{p}_3^2$ or $\mathfrak{p}_2{\mathfrak{p}_3'}^2$, and even if it is $\mathfrak{p}_2{\mathfrak{p}_3'}^2$, we can just replace $\mathfrak{p}_3$ with $\mathfrak{p}_3'$ and move on.

(which may be equal). Thus, either $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$ (which corresponds to $[\mathfrak{p}_2] = [\mathfrak{p}_3]$) or $\mathrm{Cl}(K) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ (which corresponds to $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$). Thus, what we want to show is that $[\mathfrak{p}_2] \neq [\mathfrak{p}_3]$, or $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3] = [\mathfrak{p}_2][\mathfrak{p}_3]^{-1} \neq 1$, or that $\mathfrak{p}_5$ is nonprincipal, This is again because $N_{K/\mathbb{Q}}(\alpha) = x^2 + 30y^2$ can never be equal to ± 5. Therefore, $\mathrm{Cl}(K) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Let's see why knowing the class number is useful in solving elementary number theory questions.

Example 10.15. Let's go back to the Mordell's equation, this time with $y^2 = x^3 - 14$. As seen above, if we were to make use of

$$x^3 = y^2 + 14 = (y + \sqrt{-14})(y - \sqrt{-14}),$$

then we face a problem as we just proved that $h_{\mathbb{Q}(\sqrt{-14})} = 4$. On the other hand, it is not a problem, because what we only need is actually that **the class number is not divisible by** 3. Let's see why, by mimicking the argument we had in the first lecture in the language of ideals.

Suppose there is a solution $x, y \in \mathbb{Z}$. If y is even, then x is also even, so writing $x = 2a$, $y = 2b$, we have

$$4b^2 = 8a^3 - 14,$$

which is a contradiction as the left side is divislbe by 4 while the right side is not. Thus, y is odd, and subsequently x is odd.

Similarly, y is not divisible by 7 – otherwise, x will also be divisible by 7, so $x^3 - y^2 = 14$ is divisible by at least 49, which is a contradiction.

Then, we have an equation

$$x^3 = (y + \sqrt{-14})(y - \sqrt{-14}),$$

or in terms of **ideals**,

$$(x)^3 = (y + \sqrt{-14})(y - \sqrt{-14}).$$

Suppose that the two ideals $(y + \sqrt{-14})$ and $(y - \sqrt{-14})$ have a common prime ideal factor $\mathfrak{p}$. Then, $\mathfrak{p}$ contains both $(y + \sqrt{-14})$ and $(y - \sqrt{-14})$, so $y + \sqrt{-14}, y - \sqrt{-14} \in \mathfrak{p}$. In particular, $2\sqrt{-14} \in \mathfrak{p}$. Thus, $\mathfrak{p}$ divides the principal ideal $(2\sqrt{-14})$, so $N(\mathfrak{p})$ divides $N((2\sqrt{-14})) = N_{\mathbb{Q}(\sqrt{-14})/\mathbb{Q}}(2\sqrt{-14}) = 56 = 2^3 \cdot 7$. Thus, either $\mathfrak{p}$ lies over 2 or 7. If $\mathfrak{p}$ lies over 2, then $y + \sqrt{-14}, y - \sqrt{-14} \in \mathfrak{p}$ implies that $x^3 = (y + \sqrt{-14})(y - \sqrt{-14}) \in \mathfrak{p}$, so $N(\mathfrak{p})$ divides $N_{\mathbb{Q}(\sqrt{-14})/\mathbb{Q}}(x)^3 = x^6$, which is odd, so this is impossible. Thus, $\mathfrak{p}$ must lie over 7 (and actually $N(\mathfrak{p}) = 7$). In particular, $\mathfrak{p}$ dividing $(2\sqrt{-14})$ implies that $\mathfrak{p}$ divides $(\sqrt{-14})$, or $\sqrt{-14} \in \mathfrak{p}$, which implies that $-14 \in \mathfrak{p}$. As $y + \sqrt{-14} \in \mathfrak{p}$, so $y \in \mathfrak{p}$. As y and 14 are coprime integers, 1 is a $\mathbb{Z}$-linear combination of y and 14, which implies that $1 \in \mathfrak{p}$, a contradiction again.

What we have proved is that $(y + \sqrt{-14})$ and $(y - \sqrt{-14})$ are coprime ideals, so by the unique factorization of ideals, $(y + \sqrt{-14})$ is a cube of an ideal, say $(y + \sqrt{-14}) = \mathfrak{a}^3$ for $\mathfrak{a} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-14})}$. Now, the upshot is, even though we don't know a priori whether $\mathfrak{a}$ is principal, $[\mathfrak{a}]^3 = 1$ in $\mathrm{Cl}(\mathbb{Q}(\sqrt{-14}))$, and as $\mathrm{Cl}(\mathbb{Q}(\sqrt{-14}))$ has no nontrivial 3-torsion element, $[\mathfrak{a}] = 1$, so $\mathfrak{a}$ is a **principal ideal**! Thus, $(y + \sqrt{-14}) = (c + d\sqrt{-14})^3$ for some $c, d \in \mathbb{Z}$ (as ideals), so $y + \sqrt{-14}$ is a unit times $(c + d\sqrt{-14})^3$, the kind of a statement that we would like to obtain in

the original UFD approach to the Mordell's equations. Note that a unit in $\mathbb{Z}[\sqrt{-14}]$ is ± 1, so this means $y + \sqrt{-14}$ is just a cube. So

$$y + \sqrt{-14} = (c + d\sqrt{-14})^3 = (c^3 - 42cd^2) + (3c^2d - 14d^3)\sqrt{-14},$$

so $1 = 3c^2d - 14d^3 = (3c^2 - 14d^2)d$. So, $d = \pm 1$, so $3c^2 - 14 = 3c^2 - 14d^2 = \pm 1$, or $3c^2 = 15$ or 13, which is impossible, a contradiction!

We would like to give a little context on how Gauss got interested in this problem: **binary quadratic forms**.

Definition 10.16 (Binary quadratic forms)**.** A **binary quadratic form** is an expression of the form

$$Q(X, Y) = aX^2 + bXY + cY^2, \quad a, b, c \in \mathbb{Z}.$$

Given a binary quadratic form Q, its **discriminant** is $d_Q := b^2 - 4ac$. A binary quadratic form Q is **nondegenerate** if $d_Q \neq 0$. A binary quadratic form Q is **positive definite** if $d_Q < 0$ and $a > 0$. A binary quadratic form Q is **primitive** if $\gcd(a, b, c) = 1$.

It is easy to see that, if Q is positive definite, then $Q(X, Y) > 0$ for any $X, Y \in \mathbb{R}$, $(X, Y) \neq (0, 0)$. Gauss was interested in the following problem:

Question. Given a primitive binary quadratic form Q, what is the set $\{Q(X, Y) \mid X, Y \in \mathbb{Z}\}$?

We say that an integer m is **represented** (**properly represented**, respectively) **by** $Q(X, Y)$ if $m = Q(X, Y)$ for some $X, Y \in \mathbb{Z}$ ($X, Y \in \mathbb{Z}$ with $(X, Y) = 1$, respectively).

Definition 10.17 ($\mathrm{SL}_2, \mathrm{GL}_2$)**.** Let A be a commutative ring with 1. Then, $\mathrm{GL}_2(A)$ (the **general linear group**) is the group of invertible 2×2 matrices with coefficient A. Also, $\mathrm{SL}_2(A)$ (the **special linear group**) is the group of 2×2 matrices with coefficients in A and determinant 1.

Definition 10.18. Two binary quadratic forms $Q(X, Y)$ and $Q'(X, Y)$ are **equivalent** (**strongly equivalent**, respectively) if there is $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ ($\mathrm{SL}_2(\mathbb{Z})$, respectively) such that $Q(X, Y) = Q'(aX + bY, cX + dY)$.

It is obvious that the numbers (properly) represented by two equivalent binary forms are the same. Note also that a matrix in $\mathrm{GL}_2(\mathbb{Z})$ has determinant $\mathbb{Z}^\times = \{\pm 1\}$, and $\mathrm{SL}_2(\mathbb{Z})$ is an index 2 normal subgroup of $\mathrm{GL}_2(\mathbb{Z})$. The nontrivial element in $\mathrm{GL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})$ is represented by $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Proposition 10.19. *For two equivalent binary quadratic forms $Q(X, Y)$ and $Q'(X, Y)$, $d_Q = d_{Q'}$.*

Proof. Exercise. □

Proposition 10.20. *An integer m is properly represented by some binary quadratic form of discriminant d if and only if d is a square modulo $4m$.*

Proof. If $m = ax^2 + bxy + cy^2$ for $a, b, c \in \mathbb{Z}$ with $(x, y) = 1$, then there are $p, q \in \mathbb{Z}$ such that $px - qy = 1$. Let $Z = xX + qY$ and $W = yX + pY$. Then, $Q(Z, W)$ in terms of X, Y is expressed as

$$Q(Z,W) = a(xX+qY)^2 + b(xX+qY)(yX+pY) + c(yX+pY)^2$$

$$= (ax^2+bxy+cy^2)X^2+(2axq+bxp+bqy+2cyp)XY+(aq^2+bpq+cp^2)Y^2 = mX^2+eXY+fY^2,$$

for some $e, f \in \mathbb{Z}$. Thus, $d = d_{Q(Z,W)} = e^2 - 4mf \equiv e^2 \pmod{4m}$, which implies that d is a square modulo $4m$.

Conversely, if d is a square modulo $4m$, then there is $b \in \mathbb{Z}$ such that $d \equiv b^2 \pmod{4m}$. Let $d = b^2 - 4mc$, $c \in \mathbb{Z}$. Then, m is properly represented by $Q(X, Y) = mX^2 + bXY + cY^2$, as $m = Q(1, 0)$. □

It is thus quite standard to determine whether m is properly represented by some binary quadratic form of discriminant d. The problem is then to determine how many equivalence classes of binary quadratic forms of discriminant d there are. In fact, it turns out that the equivalence classes of binary quadratic forms are closely related to the class group of a quadratic field.

Definition 10.21. A complex number $\gamma \in \mathbb{C}$ is a **quadratic number** if it is a root of a degree 2 irreducible polynomial $p_\gamma(X) \in \mathbb{Z}[X]$. If $p_\gamma(X) = aX^2 + bX + c$, then $\operatorname{disc}(\gamma) := b^2 - 4ac$.

Necessarily, for a quadratic number γ, $\gamma \in \mathbb{Q}(\sqrt{\operatorname{disc}(\gamma)})$ by the quadratic formula.

Theorem 10.22. *Let $K = \mathbb{Q}(\sqrt{n})$ be a quadratic field, with discriminant $d = \operatorname{disc}(K)$, and choose a complex embedding $K \hookrightarrow \mathbb{C}$ so that we see numbers in K as complex numbers. Then, there is a natural map*

$$\{\textit{quadratic numbers of discriminant } d\} \to \{\textit{fractional ideals of } K\},$$

given by

$$\gamma \mapsto \mathbb{Z} + \mathbb{Z}\gamma.$$

This gives rise to a bijection

$$\{\textit{quadratic numbers of discriminant } d\}/\sim \xrightarrow{\sim} \operatorname{Cl}(K),$$

where two numbers $\gamma_1 \sim \gamma_2$ are equivalent if $\gamma_1 = \frac{a\gamma_2+b}{c\gamma_2+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$.

Proof. Let γ be a quadratic number, so that it is a root of $aX^2 + bX + c = 0$ with $d = b^2 - 4ac$. We would first like to show that $\mathbb{Z} + \mathbb{Z}\gamma$ is a fractional ideal of K. Note that $a\gamma \in \mathcal{O}_K$, so it is sufficient to prove that $\mathbb{Z}a + \mathbb{Z}a\gamma \subset \mathcal{O}_K$ is an integral ideal. Note that $a\gamma$ is a root of the monic polynomial $X^2 + bX + ac = 0$ with integer coefficients, so $D(1, a\gamma) = b^2 - 4ac = d$. This implies that $\mathbb{Z} + \mathbb{Z}a\gamma \subset \mathcal{O}_K$ is actually an equality. Thus, to prove that $\mathbb{Z}a + \mathbb{Z}a\gamma \subset \mathcal{O}_K$ is an ideal, it suffices to prove that it is closed under the multiplication by $a\gamma$, which is obvious as $(a\gamma)^2 = a(-b\gamma - c) = -ac - ab\gamma$. Therefore, the natural map is indeed well-defined.

To show that the natural map induces a well-defined map from the equivalence classes of binary quadratic forms of discriminant d to $\mathrm{Cl}(K)$ that is furthermore an injection, we need to show that

$$\gamma' = \frac{a\gamma + b}{c\gamma + d} \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \Leftrightarrow \mathbb{Z} + \mathbb{Z}\gamma' = \mathbb{Z}\beta + \mathbb{Z}\beta\gamma \text{ for some } \beta \in K.$$

The forward direction is as follows. If $\gamma' = \frac{a\gamma+b}{c\gamma+d}$, then

$$\mathbb{Z} + \mathbb{Z}\gamma' = \frac{1}{c\gamma + d}(\mathbb{Z}(c\gamma + d) + \mathbb{Z}(a\gamma + b)).$$

Note that $d(a\gamma + b) - b(c\gamma + d) = (ad - bc)\gamma = \pm\gamma$, and $a(c\gamma + d) - c(a\gamma + b) = ad - bc = \pm 1$, so $\mathbb{Z}(c\gamma + d) + \mathbb{Z}(a\gamma + b) = \mathbb{Z} + \mathbb{Z}\gamma$, which is what we want.

The reverse direction is as follows. If $\mathbb{Z} + \mathbb{Z}\gamma' = \mathbb{Z}\beta + \mathbb{Z}\beta\gamma$, then there is $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \gamma' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \beta\gamma \\ \beta \end{pmatrix} = \begin{pmatrix} a\beta\gamma + b\beta \\ c\beta\gamma + d\beta \end{pmatrix}.$$

Thus, $\gamma' = \frac{\gamma'}{1} = \frac{a\beta\gamma+b\beta}{c\beta\gamma+d\beta} = \frac{a\gamma+b}{c\gamma+d}$, as desired.

To prove that the induced map is surjective, it suffices to prove that any ideal class $[\mathfrak{a}]$ of K is represented by $\mathbb{Z} + \mathbb{Z}\gamma$ for some $\gamma \in K$. This is easy: take a representative $\mathfrak{a}$, and take $r \in \mathfrak{a} \cap \mathbb{Q}$; then $\frac{1}{r}\mathfrak{a}$ is of the form as it has $\mathbb{Z}$ in it. This finishes the proof. □

To relate this with the binary quadratic forms, we need to divide into two cases, **imaginary quadratic fields** and **real quadratic fields**. In this notes, we will focus on the case of imaginary quadratic fields.

Theorem 10.23. *Let $K = \mathbb{Q}(\sqrt{n})$ be an **imaginary quadratic field**, so that its discriminant $d = \mathrm{disc}(K)$ is negative.*

Then, there is a natural bijection

$$\{\textit{strong equivalence classes of binary quadratic forms of discriminant } d\} \xrightarrow{\sim} \mathrm{Cl}(K),$$

given by

$$aX^2 + bXY + cY^2 \mapsto \mathbb{Z} + \mathbb{Z}\gamma,$$

where $\gamma = \frac{-b+\sqrt{d}}{2a}$ so that $a\gamma^2 + b\gamma + c = 0$.

Proof. Let's consider a complex embedding $K \hookrightarrow \mathbb{C}$ which sends $\sqrt{d}$ to $\sqrt{d} = \sqrt{|d|}i$, the purely imaginary number with positive imaginary part. It is clear that you have a natural map

$$\{\text{binary quadratic forms of discriminant } d\} \to \{\text{quadratic numbers of discriminant } d\},$$

$$aX^2 + bXY + cY^2 \mapsto \frac{-b + \sqrt{d}}{2a}.$$

Therefore, as per Theorem 10.22, it is sufficient to prove that this gives rise to a bijection

$$\{\text{strong equivalence classes of binary quadratic forms of discriminant } d\} \to \{\text{quadratic numbers of discriminant } d\}/\sim .$$

It is clear that the original natural map is injective. Also, it is clear that if $Q'(X,Y) = a'X^2 + b'XY + c'Y^2$ and $Q(X,Y) = aX^2 + bXY + cY^2$ are strongly equivalent, so that there is $A = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q'(X,Y) = Q(eX+fY, gX+hY)$, then if we denote the roots of $aX^2+bX+c=0$ as γ, γ', then the roots of $a'X^2+b'X+c'=0$ are $\frac{e\gamma+f}{g\gamma+h}$ and $\frac{e\gamma'+f}{g\gamma'+h}$. The natural map picks up the root that has the positive imaginary part (i.e. the root that is in $\mathbb{H}$), and it is easy to see that, if $\mathrm{Im}(z) > 0$, then $\mathrm{Im}\left(\frac{az+b}{cz+d}\right) > 0$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$. Thus, we see that the induced map on strong equivalence classes is well-defined. The induced map is furthermore injective as the original map is injective. To see that the induced map is surjective, we observe that the image of the original natural map is every quadratic number with positive imaginary part. As any quadratic number z with negative imaginary part is equivalent to $-z$, which has positive imaginary part, the induced map is surjective, thus bijective, as desired. □

Remark 10.24. The above proof used the distinction between the complex numbers with positive imaginary parts and those with negative imaginary parts, so it does not translate into real quadratic case. The real quadratic field version of the above theorem requires some modification. In particular, what corresponds to strong equivalence classes of binary quadratic forms are the classes in the **narrow class group**, which further takes the positivity of real numbers into consideration.

This now gives several interesting arithmetic applications.

Example 10.25. We can provide another proof that an odd prime p is of the form $p = x^2 + y^2$, $x, y \in \mathbb{Z}$, if and only if $p \equiv 1 \pmod 4$. Note that by Proposition 10.20, p is represented by some binary quadratic form of discriminant -4 if and only if -4 is a square mod $4p$, or -1 is a square mod p, so by quadratic reciprocity, $p \equiv 1 \pmod 4$. Now, the strong equivalence classes of binary quadratic forms of discriminant -4 are in bijection with $\mathrm{Cl}(\mathbb{Q}(i))$, as $\mathrm{disc}(\mathbb{Q}(i)) = -4$. As $\mathrm{Cl}(\mathbb{Q}(i)) = 1$, it turns out that every binary quadratic form of discriminant -4 is strongly equivalent to each other, so in particular to $Q(X,Y) = X^2 + Y^2$. Thus, $p \equiv 1 \pmod 4$ if and only if p is (properly) represented by $Q(X,Y) = X^2 + Y^2$.

Example 10.26 (The case of x^2+5y^2)**.** Now consider the case of $K = \mathbb{Q}(\sqrt{-5})$, with discriminant $d = -20$. Then, for a prime p not dividing the discriminant (i.e. $p \neq 2, 5$), p is represented by some binary quadratic form with discriminant -20 if and only if -20 is a square mod $4p$, or -5 is a square mod p. On the other hand, the equivalence classes of binary quadratic forms of discriminant -20 are in bijection with $\mathrm{Cl}(K)$. What is $\mathrm{Cl}(K)$?

Note that the Minkowski bound gives that, if $\mathfrak{a}$ represents a nontrivial ideal class $[\mathfrak{a}] \in \mathrm{Cl}(K)$, then

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\frac{4}{\pi}\sqrt{20} \sim 2.847.$$

Therefore, $N(\mathfrak{a}) = 2$. Therefore, the only possibility of nonprincipal ideal can be found in the primes in K lying over 2. Note that $(2) = (2, \sqrt{-5}+1)(2, \sqrt{-5}-1)$, there is indeed a prime ideal of norm 2 lying over (2). Furthermore, it is not principal, as there is no norm ± 2 element in $\mathcal{O}_K$ (as $x^2 + 5y^2 \neq \pm 2$). Therefore, $h_K = 2$, with the nontrivial element in $\mathrm{Cl}(K)$ represented by the ideal $(2, \sqrt{-5}+1)$.

So, there are two strong equivalence classes of binary quadratic forms of discriminant -20. What are these? Note that the trivial ideal class is represented by $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$, and the nontrivial ideal class is represented by $\mathbb{Z} + \mathbb{Z}\frac{\sqrt{-5}+1}{2}$. Note that $\sqrt{-5}$ is a root of $X^2 + 5$, and $\frac{\sqrt{-5}+1}{2}$ is a root of $2X^2 - 2X + 3$. Thus, -5 is a square mod p, $p \neq 2, 5$, if and only if either $p = X^2 + 5Y^2$ or $p = 2X^2 - 2XY + 3Y^2$, for some $X, Y \in \mathbb{Z}$. Note that $p = 2X^2 - 2XY + 3Y^2$ is equivalent to $2p = 4X^2 - 4XY + 6Y^2 = (2X - Y)^2 + 5Y^2$, so -5 is a square mod p if and only if either $p = X^2 + 5Y^2$ or $2p = X^2 + 5Y^2$, for some $X, Y \in \mathbb{Z}$.

Note also that p and $2p$ cannot be simultaneously represented by $X^2 + 5Y^2$! Suppose not, then $2p^2 = p \cdot 2p = Z^2 + 5W^2$, or there is $\alpha = Z + W\sqrt{-5} \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha) = 2p^2$, and as -5 is a square mod p, $(p) = \mathfrak{p}_1\mathfrak{p}_2$ for prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \subset \mathcal{O}_K$ of norm p. Thus, (α) is a product of one prime ideal lying over 2 and two prime ideals lying over p. On the other hand, as $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$, $[\mathfrak{p}_1] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$, so the product of two prime ideals lying over p (can be the same, can be different) is principal. Thus, this implies that a prime ideal lying over 2 is principal, which is false, a contradiction.

In fact, Theorem 10.23 can be used to compute the class number of an imaginary quadratic field K. That is, you can compute the strong equivalence classes of binary quadratic forms of discriminant $\mathrm{disc}(K)$ in a systematic/algorithmic way.

For $K = \mathbb{Q}(\sqrt{m})$ with $-d = \mathrm{disc}(K) < 0$, given $aX^2 + bXY + cY^2$ of discriminant d, a root $\gamma \in K$ of $aX^2 + bX + c$ can be naturally regarded as a complex number that is not a real number. Thus, as per Theorem 10.22, one may translate the problem of finding $\mathrm{Cl}(K)$ as the problem of determining the strong equivalence classes of $\gamma \in K \backslash \mathbb{Q}$ under the action of $\mathrm{GL}_2(\mathbb{Z})$, where the action is as given in the proof of Theorem 10.22:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \gamma = \frac{a\gamma + b}{c\gamma + d}.$$

In terms of the complex numbers, we have established the following.

$$\#\,\mathrm{Cl}(K) = \#\left(\left\{ z = \frac{-b \pm \sqrt{d}i}{2a} \in \mathbb{C},\ a, b, c \in \mathbb{Z},\ -d = b^2 - 4ac \right\} / (z \sim \gamma \cdot z,\ \gamma \in \mathrm{GL}_2(\mathbb{Z})) \right).$$

Note that $[\mathrm{GL}_2(\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z})] = 2$ with $\mathrm{GL}_2(\mathbb{Z})/\,\mathrm{SL}_2(\mathbb{Z}) = \{1, \sigma\}$, $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $\sigma \cdot z = -z$. Thus, we can only consider the action of $\mathrm{SL}_2(\mathbb{Z})$ on those with positive imaginary part.

$$\left\{ z = \frac{-b \pm \sqrt{d}i}{2a} \in \mathbb{C},\ a, b, c \in \mathbb{Z},\ -d = b^2 - 4ac \right\} / (z \sim \gamma \cdot z,\ \gamma \in \mathrm{GL}_2(\mathbb{Z}))$$

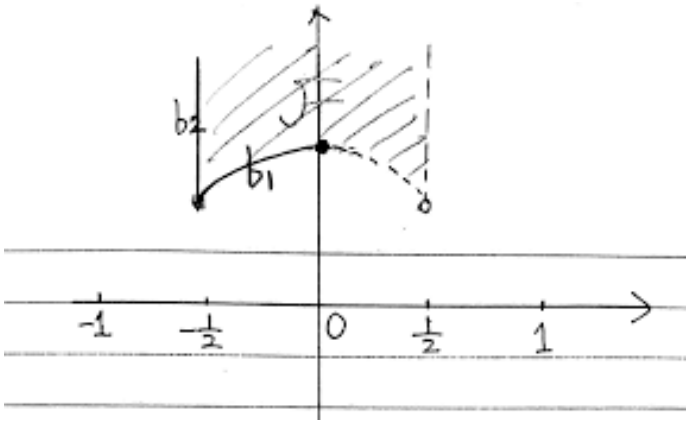
$$= \left\{ z = \frac{-b + \sqrt{d}i}{2a} \in \mathbb{C},\ a, b, c \in \mathbb{Z},\ -d = b^2 - 4ac \right\} / (z \sim \gamma \cdot z,\ \gamma \in \mathrm{SL}_2(\mathbb{Z}))$$

Definition 10.27 (The complex upper half plane)**.** Let $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \subset \mathbb{C}$. It is called the **complex upper half plane**.

In the same way, $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$, and the $\mathrm{SL}_2(\mathbb{Z})$-orbits on $\mathbb{H}$ have very natural representatives, called the **fundamental domain**.

Theorem 10.28. *Let $\mathcal{F} \subset \mathbb{H}$ be the subset defined as*

$$\mathcal{F} = \left\{ z \in \mathbb{H} \mid -\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2} \text{ and } |z| \geq 1; \text{ furthermore, } |z| > 1 \text{ if } \mathrm{Re}(z) > 0 \right\}.$$



*Then, for any $z \in \mathbb{H}$, there exists a **unique** $z' \in \mathcal{F}$ such that $z' = \gamma \cdot z$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. Note that the following matrices are elements of $\mathrm{SL}_2(\mathbb{Z})$:

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

These matrices act on $\mathbb{H}$ as:

$$Tz = z + 1, \quad Sz = -\frac{1}{z} = -\frac{\overline{z}}{|z|^2}.$$

Note that, if $z = x + yi$, then $Sz = -\frac{x-yi}{x^2+y^2} = -\frac{x}{x^2+y^2} + \frac{y}{x^2+y^2}i$. Thus, if $|z| < 1$, then $\mathrm{Im}(Sz) > \mathrm{Im}(z)$. More generally, for $z = x + yi$, it is straightforward to compute

$$\mathrm{Im}\left(\frac{az + b}{cz + d}\right) = \frac{y}{|cz + d|^2}.$$

Note that $\Lambda := \mathbb{Z} + \mathbb{Z}z$ is a lattice in $\mathbb{C}$, so in particular a discrete subset. Therefore, $\Lambda \backslash \{0\}$ has a vector of the minimal norm, $v \in \Lambda$, with $v = ez + f$, $e, f \in \mathbb{Z}$. Note that obviously $(e, f) = 1$, as otherwise one may divide v by the gcd and get a vector with a smaller norm. Also, as $1 \in \Lambda$,

$|v| \leq 1$. If $|v| = 1$, then it tells us that $\mathrm{Im}(\gamma \cdot z) \leq \mathrm{Im}(z)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so z is a number with the maximum imaginary part in the orbit $\mathrm{SL}_2(\mathbb{Z}) \cdot z$. If $|v| < 1$, then we may find $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that its bottom row is $(e\ f)$, and then $\mathrm{Im}(\gamma \cdot z) = \frac{\mathrm{Im}(z)}{|v|^2}$, and therefore $\gamma \cdot z$ is a number with the maximum imaginary part in the orbit $\mathrm{SL}_2(\mathbb{Z}) \cdot z$. In any case, there is a maximum out of all the imaginary parts of the complex numbers in the orbit $\mathrm{SL}_2(\mathbb{Z}) \cdot z$, and take a number $z' \in \mathrm{SL}_2(\mathbb{Z}) \cdot z$ realizing the maximum imaginary part.

Now one can apply an appropriate power of T so that $-\frac{1}{2} \leq \mathrm{Re}(T^m z') < \frac{1}{2}$. Then, $z'' = T^m z'$ also has the maximum imaginary part in the orbit $\mathrm{SL}_2(\mathbb{Z}) \cdot z$. As $\mathrm{Im}(Sz'') = \frac{\mathrm{Im}(Sz'')}{|z''|^2}$, it follows that $|z''| \geq 1$. The only possibility of $z'' \notin \mathcal{F}$ happens when $|z''| = 1$ and $\mathrm{Re}(z'') > 0$. In that case, $|Sz''| = 1$ but now $\mathrm{Re}(Sz'') = -\mathrm{Re}(z'') < 0$, so $Sz'' \in \mathcal{F}$. In any case, we have demonstrated that $\mathrm{SL}_2(\mathbb{Z}) \cdot z \cap \mathcal{F} \neq \emptyset$.

To show the uniqueness of the representative, it suffices to show that any two different numbers in $\mathcal{F}$ are not in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit. Suppose that $z_1, z_2 \in \mathcal{F}$ such that $z_2 = A \cdot z_1$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Without loss of generality, assume that $\mathrm{Im}(z_2) \geq \mathrm{Im}(z_1)$, so that $|cz_1 + d| \leq 1$. Note that, as $z_1 \in \mathcal{F}$, $\mathrm{Im}(z_1) \geq \frac{\sqrt{3}}{2}$. Therefore,

$$1 \geq |cz_1 + d| \geq |\,\mathrm{Im}(cz_1 + d)| = |c|\,\mathrm{Im}(z_1) \geq \frac{\sqrt{3}}{2}|c|,$$

or $|c| \leq \frac{2}{\sqrt{3}}$, which means that $|c| \leq 1$.

- If $c = 0$, then $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so $ad = 1$, which means that either A or $-A$ is of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. As $A \cdot z = (-A) \cdot z$, it follows that $z_2 = z_1 + n$, which means that $n = 0$, and $z_1 = z_2$.

- If $c = 1$, then $|z_1 + d| \leq 1$. By looking at the picture, this is possible only if either $d = 0$ and $|z_1| = 1$, or $d = 1$ and z_1 is the "left tip" of $\mathcal{F}$, namely $z_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

  If $d = 1$ and $z_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, then $\begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so $a - b = 1$, so $z_2 = \frac{az_1 + (a-1)}{z_1 + 1} = az_1^2 + (a-1)z_1 = -(a+1)z_1$. Therefore, $-(a+1) = 1$ is the only possibility, and $z_2 = z_1$.

  If $d = 0$, then $\begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ means $b = -1$, so $z_2 = a - \overline{z}_1$. Again, this kind of a thing is possible only if either $a = 0$ and $z_1, \overline{z}_1 \in \mathcal{F}$, so that $z_1 = i = z_2$, or $a = -1$ and z_1 is the left tip, so that $\overline{z}_1$ is the right tip and z_2 is again the left tip. In any case, $z_1 = z_2$.

- If $c = -1$, then one may replace A by $-A$ and use the argument of $c = 1$.

Therefore, in any case, $z_1 = z_2$, which shows the uniqueness. $\square$

Thus, we have

$$\mathrm{Cl}(K) = \left\{ z = \frac{-b+\sqrt{d}i}{2a} \in \mathbb{H},\ a,b,c \in \mathbb{Z},\ -d = b^2 - 4ac \right\} / (z \sim \gamma \cdot z,\ \gamma \in \mathrm{SL}_2(\mathbb{Z}))$$

$$= \left\{ z = \frac{-b+\sqrt{d}i}{2a} \in \mathcal{F},\ a,b,c \in \mathbb{Z},\ -d = b^2 - 4ac \right\}$$

$$= \left\{ z = \frac{-b+\sqrt{d}i}{2a},\ a,b,c \in \mathbb{Z},\ d = 4ac - b^2,\ -\frac{1}{2} \le -\frac{b}{2a} < \frac{1}{2},\ \frac{b^2+d}{4a^2} \ge 1, \text{ and if } b<0,\ \frac{b^2+d}{4a^2} > 1 \right\}$$

$$= \left\{ a,b,c \in \mathbb{Z},\ a,c>0,\ d = 4ac - b^2,\ -a < b \le a,\ c \ge a, \text{ and if } b<0, c>a \right\}.$$

Finding this set is a finite procedure, as

$$d = 4ac - b^2 > 4a^2 - a^2 = 3a^2,$$

so there are finitely many possibilities for a, so finitely many possibilities for b, and thus finitely many possibilities for c. Summarizing, we have the following algorithm for computing h_K for an imaginary quadratic field K.

Theorem 10.29 (Algorithm for computing the class number, imaginary quadratic fields)**.** *Let K be an imaginary quadratic field of discriminant $-d < 0$. Then, h_K can be computed as follows.*

1. *Start with $h = 0$. Run a loop for $a \in \mathbb{Z}$ with $1 \le a \le \sqrt{\frac{d}{3}}$.*
2. *For each such a, run a loop for $b \in \mathbb{Z}$ with $-a < b \le a$.*
3. *For each such b, check if $c := \frac{d+b^2}{4a}$ is an integer that is greater than or equal to a, and if $b < 0$, further check if $c > a$. If true, add 1 to h. If not, h stays the same.*
4. *After everything, the final value of h is h_K.*

It is also easy to find the representatives for each ideal class in $\mathrm{Cl}(K)$ from the above algorithm.

Remark 10.30. There is also a different story of finding representatives for the ideal classes of real quadratic fields, using continued fractions. You may find about this in the paper linked on the website.

– –

Exercise 10.1. Let $K = \mathbb{Q}(\sqrt{6})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$. We would like to show that $h_K = 1$, i.e. $\mathbb{Z}[\sqrt{6}]$ is a principal ideal domain.

(1) Use the Minkowski's bound to show that any ideal class has an integral ideal representative $\mathfrak{a}$ with $N(\mathfrak{a}) = 2$.

(2) Show that there is a unique prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ ideal lying over (2).

(3) Show that $\mathfrak{p}$ is principal by showing that $\mathfrak{p} = (2 + \sqrt{6})$. Conclude that $h_K = 1$.

Exercise 10.2. Let $K = \mathbb{Q}(\sqrt{10})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$. We would like to show that $h_K = 2$.

(1) Use the Minkowski's bound to show that any ideal class has an integral ideal representative $\mathfrak{a}$ with $N(\mathfrak{a}) \leq 3$.

(2) Show that there is a unique prime ideal $\mathfrak{p}_2 \subset \mathcal{O}_K$ lying over (2), with $N(\mathfrak{p}_2) = 2$.

(3) Show that there is no element $\alpha \in \mathcal{O}_K$ with norm ± 2. Conclude that $\mathfrak{p}_2$ is not a principal ideal, and its ideal class in $\mathrm{Cl}(K)$ is a nontrivial order 2 element.

Hint. Use that $\left(\frac{\pm 2}{5}\right) = -1$.

(4) Show that (3) splits completely in K, with $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, so that $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$.

(5) Using that $N_{K/\mathbb{Q}}(4 + \sqrt{10}) = 6$, deduce that the ideal classes of $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are both the same as the ideal class of $\mathfrak{p}_2$. Conclude that $h_K = 2$.

Hint. After possibly switching $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, $\mathfrak{p}_2\mathfrak{p}_3 = (4 + \sqrt{10})$, so $[\mathfrak{p}_2]^{-1} = [\mathfrak{p}_3]$ in $\mathrm{Cl}(K)$.

Exercise 10.3. Recall that, in the notes, it is proved that $h_{\mathbb{Q}(\sqrt{-14})} = 4$. Using this, we would like to know when a prime $p \neq 2, 7$ is of the form $p = x^2 + 14y^2$ for some integers $x, y \in \mathbb{Z}$.

Let $p \neq 2, 7$ be a rational prime number.

(1) Using the binary quadratic forms technique, show that p is properly represented by either $X^2 + 14Y^2$, $2X^2 + 7Y^2$, $3X^2 + 2XY + 5Y^2$, or $3X^2 - 2XY + 5Y^2$, if and only if -14 is a square modulo p.

(2) Show that if either $p = X^2 + 14Y^2$ or $p = 2X^2 + 7Y^2$, then $p \equiv 1$ or $7 \pmod 8$.

Hint. $n^2 \equiv 0, 1, 4 \pmod 8$.

(3) Show that $p = 3X^2 \pm 2XY + 5Y^2$ for some $X, Y \in \mathbb{Z}$ if and only if $3p = Z^2 + 14W^2$ for some $Z, W \in \mathbb{Z}$. Deduce that, if $p = 3X^2 \pm 2XY + 5Y^2$, then $p \equiv 3$ or $5 \pmod 8$.

(4) Show that $p = 2X^2 + 7Y^2$ for some $X, Y \in \mathbb{Z}$ if and only if $2p = Z^2 + 14W^2$ for some $Z, W \in \mathbb{Z}$.

(5) Combining the above, show that, for $p \neq 2, 7$,

$$\text{Either } p \text{ or } 2p = X^2 + 14Y^2 \Leftrightarrow p \equiv 1, 7 \pmod 8 \text{ and } p \equiv 1, 2, 4 \pmod 7.$$

(6) Show that the two cases in the left side of (5) are mutually exclusive, namely that there is no $p \neq 2, 7$ such that $X^2 + 14Y^2$ represents both p and $2p$.

Exercise 10.4. Let K be an imaginary quadratic field with $\mathrm{disc}(K) = -d < 0$. Recall that, in the notes, we have established

$$\mathrm{Cl}(K) = \left\{ z = \frac{-b + \sqrt{d}i}{2a} \in \mathbb{H},\ a, b, c \in \mathbb{Z},\ -d = b^2 - 4ac \right\} / (z \sim \gamma \cdot z,\ \gamma \in \mathrm{SL}_2(\mathbb{Z}))$$

$$= \left\{ a, b, c \in \mathbb{Z},\ a, c > 0,\ d = 4ac - b^2,\ -a < b \leq a,\ c \geq a, \text{ and if } b < 0, c > a \right\}.$$

For $z = \frac{-b+\sqrt{d}i}{2a} \in \mathbb{H}$ with $a, b, c \in \mathbb{Z}$ and $-d = b^2 - 4ac$, let $[z] \in \mathrm{Cl}(K)$ be its corresponding ideal class. For $a, b, c \in \mathbb{Z}$ with $a, c > 0$, $d = 4ac - b^2$, $-a < b \leq a$, $c \geq a$, and if $b < 0$, $c > a$, let $[a, b, c] \in \mathrm{Cl}(K)$ be its corresopnding ideal class.

(1) For $z = \frac{-b+\sqrt{d}i}{2a} \in \mathbb{H}$ with $a, b, c \in \mathbb{Z}$ and $-d = b^2 - 4ac$, show that $[-\overline{z}] = [z]^{-1}$ in $\mathrm{Cl}(K)$.

Hint. For $\mathfrak{a} \subset \mathcal{O}_K$, show that $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal, where $\overline{(\cdot)}$ is the nontrivial Galois conjugation of $K/\mathbb{Q}$.

(2) For $a, b, c \in \mathbb{Z}$ with $a, c > 0$, $d = 4ac - b^2$, $-a < b \leq a$, $c \geq a$, and if $b < 0$, $c > a$, show that $[a, b, c]^2 = 1$ in $\mathrm{Cl}(K)$ if and only if either $b = 0$, $b = a$ or $c = a$.

(3) Show that h_K is an odd number if and only if either $K = \mathbb{Q}(\sqrt{-1})$, $K = \mathbb{Q}(\sqrt{-2})$, or $K = \mathbb{Q}(\sqrt{-p})$ with p a rational prime $\equiv 3 \pmod 4$.

Hint. Divide into the cases where $K = \mathbb{Q}(\sqrt{m})$ with $m \equiv 1 \pmod 4$ and where $K = \mathbb{Q}(\sqrt{m})$ with $m \equiv 2, 3 \pmod 4$.

11. Lecture 14. Localization, discrete valuation rings

Summary. Localization; discrete valuation rings; some commutative algebra.

Content. We have studied the properties of number fields as extensions of $\mathbb{Q}$. On the other hand, a lot can be said about the situation where the smaller field is another field that is not necessarily $\mathbb{Q}$. We had however so far exploited the fact that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ and we can count integers. This is not the case for general rings of integers, so we need to develop some algebra to prove the analogues for this general situation.

The basic idea is that we may study a commutative ring one prime ideal at a time[16]. For each prime ideal, you may remove the other prime ideals from the ring, and the resulting ring is often easier to study.

How do we remove prime ideals from a ring? The idea comes from the notion of field of fractions. Note that by taking the field of fractions of an integral domain, you removed all the nonzero prime ideals from the integral domain. It turns out that a similar procedure, called the **localization**, can be used to remove the prime ideals in a more selective way.

Definition 11.1 (Localization)**.** Let A be a commutative ring with 1 which is also an integral domain. A subset $S \subset A - \{0\}$ is called a **multiplicative set** if it is closed under the multiplication, i.e. $s, s' \in S$ implies $ss' \in S$. For a multiplicative set $S \subset A - \{0\}$, we define a commutative ring[17] $S^{-1}A$ as

$$S^{-1}A := \left\{ \frac{a}{s} \in \mathrm{Frac}(A) \mid a \in A,\ s \in S \right\}.$$

Example 11.2. (1) For $a \in A - \{0\}$, the set $S = \{1, a, a^2, \cdots\}$ is clearly a multiplicative set. For such S, $S^{-1}A$ is also often denoted as $A[\frac{1}{a}]$.

(2) For a commutative subring $B \subset A$ with 1 (including the case $B = A$), and for a prime ideal $\mathfrak{q} \subset B$, the set $S = B - \mathfrak{q} \subset A - \{0\}$ is a multiplicative set (check this; exercise). For such S, $S^{-1}A$ is also often denoted as $A_{\mathfrak{q}}$, and is called the **localization of** A **at** $\mathfrak{q}$.

The reason why this construction is called a localization is because it can discard prime ideals as you would want.

Theorem 11.3. *Let A be a commutative integral domain with 1 and $S \subset A - \{0\}$ is a multiplicative set.*

(1) An ideal $J \subset S^{-1}A$ is always of the form $J = S^{-1}I := I \cdot S^{-1}A$, the ideal of $S^{-1}A$ generated by I, for some ideal $I \subset A$. Furthermore, one can take $I = J \cap A$.

(2) If A is Notherian, $S^{-1}A$ is Noetherian.

(3) If A is normal, $S^{-1}A$ is normal.

[16] This point of view is fundamental not just in algebraic number theory but also in any kind of algebraic theory, e.g. algebraic geometry.

[17] It is an easy exercise to check that this defines a subring of the field of fractions.

(4) There is a natural inclusion-preserving one-to-one correspondence

$$\{\textit{prime ideals of } S^{-1}A\} \leftrightarrow \{\textit{prime ideals } \mathfrak{p} \subset A \textit{ such that } \mathfrak{p} \cap S = \emptyset\},$$

such that the correspondence is given by

$$\mathfrak{p} \mapsto \mathfrak{p} \cap A,$$

$$\textit{The ideal generated by } \mathfrak{p} \hookleftarrow \mathfrak{p}.$$

(5) In (4), if $\mathfrak{p} \subset S^{-1}A$ corresponds to $\mathfrak{q} \subset A$, then

$$(S^{-1}A)/\mathfrak{p} \cong \overline{S}^{-1}(A/\mathfrak{q}),$$

where $\overline{S} \subset (A/\mathfrak{q}) - \{0\}$ is the image of S in $A/\mathfrak{q}$.

Proof. (1) Let $I = J \cap A$ for an ideal $J \subset S^{-1}A$. Then, as $I \subset J$, we have $S^{-1}I \subset J$. On the other hand, if $x \in J$, then $x = \frac{a}{s}$ for some $a \in A$ and $s \in S$. Thus, $sx = a \in J$, so $a \in I = J \cap A$. This means that $x \in S^{-1}I$. Thus, $J = S^{-1}I$.

(2) Let $J_1 \subset J_2 \subset \cdots$ be an ascending chain of ideals in $S^{-1}A$. Then, letting $I_n = J_n \cap A$, we have an ascending chain of ideals $I_1 \subset I_2 \subset \cdots$ in A, which must stabilize. As $J_n = S^{-1}I_n$, $J_1 \subset J_2 \subset \cdots$ must stabilize.

(3) Note that $F = \mathrm{Frac}(A) = \mathrm{Frac}(S^{-1}A)$. Let $x \in F$ be integral over $S^{-1}A$, which means that there is a monic polynomial $f(X) \in (S^{-1}A)[X]$ such that $f(x) = 0$. Let

$$f(X) = X^n + \frac{a_{n-1}}{s_{n-1}}X^{n-1} + \cdots + \frac{a_0}{s_0}, \quad a_{n-1}, \cdots, a_0 \in A, \quad s_{n-1}, \cdots, s_0 \in S.$$

Let $y = s_0 \cdots s_{n-1}x$. Then,

$$0 = f(x) = \frac{y^n}{s_0^n \cdots s_{n-1}^n} + \frac{a_{n-1}y^{n-1}}{s_0^{n-1} \cdots s_{n-1}^{n-1} \cdot s_{n-1}} + \cdots + \frac{a_0}{s_0} = \frac{y^n + \frac{a_{n-1}s_0 \cdots s_{n-1}}{s_{n-1}}y^{n-1} + \cdots + \frac{a_0 s_0^n \cdots s_{n-1}^n}{s_0}}{s_0^n \cdots s_{n-1}^n}.$$

Note that the numerator is a polynomial expression in y with coefficients in A, so y is integral over A. Thus, $y \in A$. Thus, $x = \frac{y}{s_0 \cdots s_{n-1}} \in S^{-1}A$.

(4) Let us first observe that the map is well-defined. Firstly, let $\mathfrak{p}$ be a prime ideal of $S^{-1}A$. Then, the natural map $A \to S^{-1}A/\mathfrak{p}$ has a kernel $A \cap \mathfrak{p}$, so $A/(A \cap \mathfrak{p}) \hookrightarrow S^{-1}A/\mathfrak{p}$ is an injection. Thus, $A/(A \cap \mathfrak{p})$ is a subring of $S^{-1}A/\mathfrak{p}$, which is an integral domain, so $A \cap \mathfrak{p}$ is also a prime ideal. Furthermore, as any element in S is invertible in $S^{-1}A$, S is disjoint from $\mathfrak{p}$, so $A \cap \mathfrak{p}$ is also disjoint from S.

Conversely, let $\mathfrak{p} \subset A$ be a prime ideal disjoint from S. Let $x = \frac{a}{b}, y = \frac{c}{d} \in S^{-1}A$, $a, c \in A$, $b, d \in S$, such that $xy = \frac{ac}{bd} \in S^{-1}\mathfrak{p}$. This means that $\frac{ac}{bd} = \frac{p}{q}$ for $p \in \mathfrak{p}$, $q \in S$, so $bdp = acq$. As $bdp \in \mathfrak{p}$, $acq \in \mathfrak{p}$, which means that either a, c, or q is in $\mathfrak{p}$. On the other

hand, as $q \in S$, $q \notin \mathfrak{p}$, so either $a \in \mathfrak{p}$ or $c \in \mathfrak{p}$, which means that either $x \in S^{-1}\mathfrak{p}$ or $y \in S^{-1}\mathfrak{p}$, which means that $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$.

We then need to show that the two maps are inverses to each other. Let $\mathfrak{p} \subset S^{-1}A$ be a prime ideal. Then, $\mathfrak{p} \cap A \subset \mathfrak{p}$ implies that $S^{-1}(\mathfrak{p} \cap A) \subset \mathfrak{p}$. On the other hand, if $x \in \mathfrak{p}$ is of the form $x = \frac{a}{b}$, $a \in A$, $b \in S$, then $bx = a \in \mathfrak{p}$, so $a \in \mathfrak{p} \cap A$, which mean that $x \in S^{-1}(\mathfrak{p} \cap A)$. Thus, $S^{-1}(\mathfrak{p} \cap A) = \mathfrak{p}$. On the other hand, if $\mathfrak{p} \subset A$ is a prime ideal disjoint from S, then as $\mathfrak{p} \subset S^{-1}\mathfrak{p}$, $\mathfrak{p} \subset (S^{-1}\mathfrak{p}) \cap A$. Conversely, if $x \in (S^{-1}\mathfrak{p}) \cap A$, this means that $x \in A$ but also $x = \frac{a}{b}$ where $a \in \mathfrak{p}$ and $b \in S$. This means that $a = bx$, so as $a \in \mathfrak{p}$, either $b \in \mathfrak{p}$ or $x \in \mathfrak{p}$. On the other hand, $b \in S$, so $b \notin \mathfrak{p}$. Thus, $x \in \mathfrak{p}$. This implies that $\mathfrak{p} = (S^{-1}\mathfrak{p}) \cap A$, as desired.

(5) We saw that $A/\mathfrak{q} \hookrightarrow (S^{-1}A)/\mathfrak{p}$ is an injection of integral domains. Thus, $\mathrm{Frac}(A/\mathfrak{q}) \subset \mathrm{Frac}((S^{-1}A)/\mathfrak{p})$ is a subfield. Under this, we see that any element in $\overline{S} \subset A/\mathfrak{q} \subset \mathrm{Frac}(A/\mathfrak{q}) \subset \mathrm{Frac}((S^{-1}A)/\mathfrak{p})$ is invertible in $(S^{-1}A)/\mathfrak{p}$ as it can be expressed as an element in S. Therefore, we have $\overline{S}^{-1}(A/\mathfrak{q}) \subset (S^{-1}A)/\mathfrak{p}$. Conversely, if $x \in (S^{-1}A)/\mathfrak{p}$, then it has a representative of the form $\frac{a}{s}$, $a \in A$, $s \in S$. Then, the corresponding $\overline{s} \in \overline{S}$ and $\overline{a} \in A/\mathfrak{q}$ will give rise to $\frac{\overline{a}}{\overline{s}} = \frac{a}{s}$.

□

Example 11.4. (1) If $a \in A - \{0\}$, then the prime ideals of $A[\frac{1}{a}]$ are precisely the prime ideals of A that do not contain a.

(2) If $B \subset A$ and $\mathfrak{q} \subset B$ a prime ideal, the prime ideals of $A_{\mathfrak{q}}$ are precisely the prime ideals of A lying over a prime ideal contained in $\mathfrak{q}$ (i.e. prime ideals $\mathfrak{p} \subset A$ such that $\mathfrak{p} \cap B \subset \mathfrak{q}$). In particular, if $B = A$, then $A_{\mathfrak{q}}$ has only one maximal ideal corresponding to $\mathfrak{q}$.

(3) If $S = A - \{0\}$, then $S^{-1}A = \mathrm{Frac}(A)$.

Definition 11.5 (Local ring)**.** A commutative ring A with 1 is **local** if it has exactly one maximal ideal $\mathfrak{m}$.

Definition 11.6 (Residue fields)**.** Let A be a commutative ring, and $\mathfrak{m}$ be a maximal ideal of A. The **residue field** of $\mathfrak{m}$ is the field $A/\mathfrak{m}$. If A is a local ring, then often we call the residue field of the unique maximal ideal of A just the residue field of A.

The following is immediate.

Proposition 11.7. *If A is a local ring with the unique maximal ideal $\mathfrak{m}$, then $A^\times = A - \mathfrak{m}$ (i.e. any element not in $\mathfrak{m}$ is invertible).*

From Theorem 11.3, we now know that if A is a Dedekind domain and if $\mathfrak{p}$ is a nonzero prime ideal, then $A_{\mathfrak{p}}$ is a local Dedekind domain.

Definition 11.8 (Discrete valuation rings)**.** A local Dedekind domain which is not a field (i.e. (0) is not the maximal ideal) is called a **discrete valuation ring**.

The advantage of the notion of discrete valuation rings is that there are multiple different persepectives on this notion.

Theorem 11.9. *Let A be an integral domain.*

(1) If A is a Dedekind domain with finitely many maximal ideals, then A is a principal ideal domain. In particular, discrete valuation rings are principal ideal domains.

(2) If A is a discrete valuation ring with the unique maximal ideal $\mathfrak{m}$, then every nonzero fractional ideal of A is of the form $\mathfrak{m}^n$ for some $n \in \mathbb{Z}$.

(3) If A is a local principal ideal domain which is not a field, A is a discrete valuation ring.

Proof. (1) Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be the maximal ideals of A. Then, by the weak approximation theorem and the unique factorization of ideals, for each $e_1, \cdots, e_r \geq 0$, there is $a \in A$ such that $(a) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$. This implies that in fact each $\mathfrak{p}_i$ is a principal ideal, so any ideal, which is a product of $\mathfrak{p}_i$'s, is principal.

(2) This is an immediate consequence of the unique factorization of ideals.

(3) Let A be a local principal ideal domain which is not a field. To show that A is a discrete valuation ring, we need to show that A is normal and the nonzero prime ideals are maximal.

Suppose $x = \frac{a}{b} \in \mathrm{Frac}(A)$, $a, b \in A$, $\gcd(a, b) = 1$ (meaning that (a, b) is the unit ideal), is integral over A. We want to show that $x \in A$. Let $\mathfrak{m}$ be the unique maximal ideal. If $b \notin \mathfrak{m}$, then b is invertible, so $x \in A$, which is what we want. Thus, let's assume that $b \in \mathfrak{m}$. Then, there exist $a_{n-1}, \cdots, a_0 \in A$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, or $a^n + a_{n-1}a^{n-1}b + \cdots + a_0 b^n = 0$. This implies that $a^n \in (b) \subset \mathfrak{m}$. As $\mathfrak{m}$ is a prime ideal, this implies that $a \in \mathfrak{m}$, so $(a, b) \subset \mathfrak{m}$, which is a contradiction. Thus, b has to be not in $\mathfrak{m}$, and $x \in A$, as desired.

Suppose that $\mathfrak{p} \subset A$ is a nonzero prime ideal. As A is a PID, $\mathfrak{p} = (a)$ for some $a \in A$ not zero, which has to be irreducible. Let $\mathfrak{m} = (b)$. Then, as $\mathfrak{p} \subset \mathfrak{m}$, $a = bc$ for some $c \in A$. This implies that either b is a unit or c is a unit. Since $(b) = \mathfrak{m}$ is not the whole A, it follows that c is a unit, so $(a) = (b)$, or $\mathfrak{p} = \mathfrak{m}$. This implies that $\mathfrak{m}$ is the only nonzero prime ideal of A. This finishes the proof that A is a discrete valuation ring.

□

Definition 11.10 (Uniformizer)**.** As per Theorem 11.9(1), a discrete valuation ring is a principal ideal domain. A generator of the unique maximal ideal of a discrete valuation ring is called a **uniformizer**.

Example 11.11 (Examples of discrete valuation rings)**.**

(1) The localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at $(p) \subset \mathbb{Z}$ is by definition a discrete valuation ring. Its unique maximal ideal is $p\mathbb{Z}_{(p)}$, and p is a uniformizer.

(2) The ring of formal power series $\mathbb{C}[[X]]$, defined as

$$\mathbb{C}[[X]] := \left\{ \sum_{n=0}^{\infty} a_n X^n \mid a_0, a_1, \cdots \in \mathbb{C} \right\},$$

with the usual multiplication and addition of infinite series, is a discrete valuation ring. This is because it is local with the unique maximal ideal (X) (i.e. any infinite series with nonzero constant coefficient is invertible), and more generally any element $f \in \mathbb{C}[[X]]$ can be written uniquely as $f = X^n u$ for u invertible and $n \geq 0$, so that there is a discrete valuation on $\mathrm{Frac}(\mathbb{C}[[X]])$ (as we will see in a moment). In this case, X is a uniformizer.

From Theorem 11.9(2), one can define a **discrete valuation**, $v : \mathrm{Frac}(A) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$, as $v(0) = \infty$ and $v(x) \geq 0$ is such that the fractional ideal $A \cdot x$ is equal to $\mathfrak{m}^{v(x)}$. More generally, one has the following definition.

Definition 11.12 (Discrete valuation)**.** Let F be a field. A **discrete valuation** on F is a map $v : F \to \mathbb{Z} \cup \{\infty\}$ such that the following conditions hold.

(1) $v(xy) = v(x) + v(y)$.

(2) $v(x + y) \geq \min(v(x), v(y))$.

(3) $v(x) = \infty$ if and only if $x = 0$.

A discrete valuation is **normalized** if there exists $a \in F$ such that $v(a) = 1$.

The following explains the terminology "discrete valuation ring".

Theorem 11.13. *Let A be an integral domain such that there is a discrete valuation v on $\mathrm{Frac}(A)$ and $A = \{x \in \mathrm{Frac}(A) \mid v(x) \geq 0\}$. Then, A is a discrete valuation ring.*

More concretely, if there is a non-zero non-invertible element $\pi \in A$ such that every element $a \in A$ can be written uniquely as $a = \pi^n u$ for some $n \geq 0$ and u invertible, then A is a discrete valuation ring, and π is a uniformizer.

Proof. First, note that any discrete valuation $v : \mathrm{Frac}(A) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is of the form $v = dw$ for $d \geq 1$ and a normalized discrete valuation w. This is because the image of v in $\mathbb{Z}$ forms a subgroup of $\mathbb{Z}$, so it is of the form $d\mathbb{Z}$ for some $d \geq 1$. Therefore, we can assume that the given discrete valuation is normalized.

As per Theorem 11.9(3), we would like to show that A is a local principal ideal domain. Let $I = \{a \in A \mid v(a) \geq 1\}$. This is an ideal as v is additive, and $x \in A - I$ is invertible, as $v(x^{-1}) = 0$, so $x^{-1} \in A$. Thus, I is the unique maximal ideal, and A is local. This in particular means that, if $a, b \in A$ are such that $v(a) \leq v(b)$, then $v\left(\frac{b}{a}\right) \geq 0$, so $\frac{b}{a} \in A$. Thus, for any ideal J of A, let $m = \min(v(x) \mid x \in J)$, which exists as the set is bounded below, and if we take any $y \in J$ such that $v(y) = m$, then any element in J is a multiple of m, so $(m) = J$. Therefore, A is a local principal ideal domain, so a discrete valuation ring. Taking $\pi \in A$ such that $v(\pi) = 1$, we get the concrete description. □

The usefulness of the discrete valuation ring is that it basically retains all the information about the specific prime that we care about, but also the such rings have much nicer properties like being a principal ideal domain. The following is another useful lemma that appears a lot in algebra.

Lemma 11.14 (Nakayama's lemma)**.** *Let A be a local commutative ring, and $I \subsetneq A$ be a proper ideal. Let M be a finitely generated A-module. If N is an A-submodule of M such that $N + IM = M$, then $N = M$. In particular, if $IM = M$, then $M = 0$.*

Proof. Suppose first that $IM = M$, but $M \neq 0$. Let M be generated by $e_1, \cdots, e_n \in M$, and take the basis so that n is minimal. By assumption, $n \geq 1$. As $M = IM$, there is an expression

$$e_1 = x_1 e_1 + \cdots + x_n e_n, \quad x_1, \cdots, x_n \in I.$$

Thus

$$(1 - x_1)e_1 = x_2 e_2 + \cdots + x_n e_n.$$

Let $\mathfrak{m}$ be the unique maximal ideal of A. Since $x_1 \in I \subset \mathfrak{m}$, $1 - x_1 \notin \mathfrak{m}$, so $1 - x_1 \in A^\times$ is a unit. Thus, e_1 is an A-linear combination of $e_2, \cdots, e_n$, which contradicts the minimality of n.

Now in the general case, suppose that $N + IM = M$. Let $m \in M$. Then $m = n + \sum_i a_i m_i$ for some $n \in N$, $a_i \in A$, $m_i \in M$. Thus, $m + N = \sum_i a_i(m_i + N)$, so $m + N \in M/N$ is actually an element of $I(M/N)$. Thus, $I(M/N) = M/N$, so by the special case as above, $M/N = 0$, so $M = N$, as desired. □

– –

Exercise 11.1. For a rational prime $p \in \mathbb{Z}$, let $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ be the map defined as follows.

– For $n \in \mathbb{Z}$, $v_p(n) \geq 0$ is such that $p^{v_p(n)} \mid n$ but $p^{v_p(n)+1} \nmid n$.

– For $\dfrac{n}{m} \in \mathbb{Q}$, $n, m \in \mathbb{Z}$, define $v_p\left(\dfrac{n}{m}\right) = v_p(n) - v_p(m)$.

(1) Show that v_p is a normalized discrete valuation on $\mathbb{Q}$.

(2) Show conversely that any normalized discrete valuation v on $\mathbb{Q}$ is equal to v_p for some rational prime p.

Hint. Show that $v(1) = 0$, and $v(n) \geq 0$ for all $n \in \mathbb{Z}$. Then, show that $I = \{n \in \mathbb{Z} \mid v(n) > 0\}$ is a prime ideal of $\mathbb{Z}$.

Exercise 11.2. Let A be an integral domain, and let $S \subset A - \{0\}$ be a multiplicative set. Let B be a commutative ring, and let $f : A \to B$ be a ring homomorphism, such that $f(s)$ is a unit in B for every $s \in S$. Show that there exists a **unique** ring homomorphism $g : S^{-1}A \to B$ where the composition of g with the natural map $A \to S^{-1}A$, $a \mapsto \frac{a}{1}$, recovers $f : A \to B$.[18]

Exercise 11.3. Let $\mathbb{Z}_p$ (the p-**adic integers**) be the set defined as follows.

$$\mathbb{Z}_p := \{(a_1, a_2, \cdots) \mid a_n \in \mathbb{Z}/p^n\mathbb{Z},\ a_{n+1} \pmod{p^n} = a_n\}.$$

Namely, $\mathbb{Z}_p$ is the collection of compatible sequences of mod p^n congruence classes.

[18] In general, this kind of a statement is called the **universal property**.

(1) Endow $\mathbb{Z}_p$ with a commutative ring structure, where the addition and the multiplication are defined entrywise (e.g. $(a_1, a_2, \cdots) + (b_1, b_2, \cdots) = (a_1 + b_1, a_2 + b_2, \cdots)$). Show that $\mathbb{Z}_p$ is a discrete valuation ring.

(2) Consider the natural ring homomorphism $\mathbb{Z} \to \mathbb{Z}_p$, $n \mapsto [n] := (n, n, \cdots)$. Show that, for any $n \in \mathbb{Z}$ coprime to p, $[n]$ is a unit in $\mathbb{Z}_p$. Deduce that this gives rise to a natural injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$.

(3) Show that the natural injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ is not surjective. Deduce that $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p)$ is strictly bigger than $\mathbb{Q}$.

12. Lecture 15. Relative splitting of primes

Summary. Relative version of the relation on "e, f, g"; relative version of Dedekind's criterion; relative discriminant; ramification and discriminant; different.

Content. Now we apply the theory of localizations and discrete valuation rings to the study of **relative splitting of prime ideals**. This means that we study, given an extension of number fields K/L and a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_L$, how $\mathfrak{p}\mathcal{O}_K$ (the ideal of $\mathcal{O}_K$ generated by $\mathfrak{p}$) splits in $\mathcal{O}_K$. The key is that the prime ideals of $\mathcal{O}_{K,\mathfrak{p}}$ are precisely the prime ideals of $\mathcal{O}_K$ lying over $\mathfrak{p}$. In fact, the prime ideal factorization can be completely seen on the level of $\mathcal{O}_{K,\mathfrak{p}}$.

Theorem 12.1. *Let K/L be a finite extension of number fields, and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_L$. Suppose that $\mathfrak{p}\mathcal{O}_K$ has the prime ideal factorization*

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}.$$

(1) For $1 \leq i \leq g$, the natural map $\mathcal{O}_K \to \mathcal{O}_{K,\mathfrak{p}}$ induces an isomorphism $\mathcal{O}_K/\mathfrak{q}_i \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}}$.

(2) Inside $\mathcal{O}_{K,\mathfrak{p}}$, which is a Dedekind domain, the prime ideal factorization of $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is

$$\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = (\mathfrak{q}_1\mathcal{O}_{K,\mathfrak{p}})^{e_1} \cdots (\mathfrak{q}_g\mathcal{O}_{K,\mathfrak{p}})^{e_g}.$$

(3) If we let $f_i = [\mathcal{O}_K/\mathfrak{q}_i : \mathcal{O}_L/\mathfrak{p}]$[19], then

$$\sum_{i=1}^{g} e_i f_i = [K : L].$$

The relation (3) is the "relative" version of the "relation on e, f, g."

Proof.

(1) Note that, by Theorem 11.3(5), $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}} \cong \overline{S}^{-1}(\mathcal{O}_K/\mathfrak{q}_i)$, where $\overline{S}$ is the image of $S = \mathcal{O}_L - \mathfrak{p}$ in $\mathcal{O}_K/\mathfrak{q}_i$. Since $\mathfrak{p} = \mathfrak{q}_i \cap \mathcal{O}_L$, this means that any $x \in S$ is sent to a nonzero element in $\mathcal{O}_K/\mathfrak{q}_i$. Since $\mathcal{O}_K/\mathfrak{q}_i$ is a field, any nonzero element is invertible, so $\overline{S}^{-1}(\mathcal{O}_K/\mathfrak{q}_i) \cong \mathcal{O}_K/\mathfrak{q}_i$. It is easy to check that in fact the natural map is an isomorphism.

(2) The equality of ideals is clear, and that this is the prime ideal factorization follows from the fact that $\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}}$ is a prime ideal of $\mathcal{O}_{K,\mathfrak{p}}$.

(3) The crucial fact is that, even though $\mathcal{O}_L$ is not in general a principal ideal domain, $\mathcal{O}_{L,\mathfrak{p}}$, being a discrete valuation ring, is a principal ideal domain! Then we hope to mimic the proof when $L = \mathbb{Q}$ which may have used some special facts about $\mathcal{O}_L = \mathbb{Z}$.

[19] If $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $f_i = \frac{f(\mathfrak{q}_i|p)}{f(\mathfrak{p}|p)}$, where $f(\mathfrak{q}_i|p)$ and $f(\mathfrak{p}|p)$ are the residue degrees of $\mathfrak{q}_i|p$ and $\mathfrak{p}|p$, respectively. This is therefore the "relative residue degree".

Recall that we proved the relation on e, f, g originally using the order of the residue field $\mathcal{O}_K/\mathfrak{q}_i$'s. Similarly, we would like to use the Chinese Remainder Theorem,

$$\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \xrightarrow{\sim} \prod_{i=1}^{g} \mathcal{O}_{K,\mathfrak{p}}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i}.$$

Note that both sides are $\mathcal{O}_L/\mathfrak{p}$-modules, or if we denote $\mathcal{O}_L/\mathfrak{p}$ simply as k, a finite field, then both sides are k-vector spaces. Thus, we would like to use the equality of the k-dimensions of both sides.

Firstly, I claim that $\dim_k \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = [K : L]$. Note that $\mathcal{O}_{K,\mathfrak{p}}$ is already an $\mathcal{O}_{L,\mathfrak{p}}$-module. Since $\mathcal{O}_{L,\mathfrak{p}}$ is a PID, we can try to use the general theory of modules over PID. The details are laid out in the handout by Brian Conrad in the main webpage, but the upshot is that basically there is a structure theorem for the finitely generated modules over a PID just like the structure theorem of finitely generated abelian groups (=$\mathbb{Z}$-modules), in that if A is a PID and M is a finitely generated A-module, then M is of the form

$$M \cong A^{\oplus r} \times A/(a_1) \times \cdots \times A/(a_n).$$

In particular, if M is a torsion-free A-module (i.e. if $m \in M$ and $a \in A$ satisfies $am = 0$, then either $m = 0$ or $a = 0$), then M is a free A-module. Clearly, being the integral domain, $\mathcal{O}_{K,\mathfrak{p}}$ is a torsion-free $\mathcal{O}_{L,\mathfrak{p}}$-module, so as an $\mathcal{O}_{L,\mathfrak{p}}$-module, $\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_{L,\mathfrak{p}}^{\oplus r}$ for some r. You may localize the both sides of the isomorphism by inverting $\mathcal{O}_{L,\mathfrak{p}} - \{0\}$, and obtain $\mathrm{Frac}(\mathcal{O}_{K,\mathfrak{p}}) \cong \mathrm{Frac}(\mathcal{O}_{L,\mathfrak{p}})^{\oplus r}$ as $\mathrm{Frac}(\mathcal{O}_{L,\mathfrak{p}})$-modules (=vector spaces). Since $\mathrm{Frac}(\mathcal{O}_{K,\mathfrak{p}}) = \mathrm{Frac}(\mathcal{O}_K) = K$ and $\mathrm{Frac}(\mathcal{O}_{L,\mathfrak{p}}) = \mathrm{Frac}(\mathcal{O}_L) = L$, this implies that $K \cong L^{\oplus r}$ as L-vector spaces, so $r = [K : L]$. From this, $\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_{L,\mathfrak{p}}^{\oplus[K:L]}$ as $\mathcal{O}_{L,\mathfrak{p}}$-modules, and after taking reduction modulo $\mathfrak{p}$, we obtain $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \cong (\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}})^{\oplus[K:L]}$ as $\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$-modules, but by (1), we have $\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}} \cong \mathcal{O}_L/\mathfrak{p} = k$, so $[K : L] = \dim_k \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$.

Next, I claim that $\dim_k \mathcal{O}_{K,\mathfrak{p}}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i} = e_i f_i$. Note that we have a chain of k-subspaces

$$\mathcal{O}_{K,\mathfrak{p}}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i} \supset (\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i} \supset \cdots \supset (\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i-1}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i} \supset 0,$$

so it suffices to show that

$$\dim_k(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a-1}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i} - \dim_k(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{e_i} = f_i.$$

By taking the quotient vector space (=quotient module), this is equivalent to

$$\dim_k(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a-1}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a} = f_i.$$

Note that this is not just a $k = \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$-module, but also a module over $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_K/\mathfrak{q}_i$, which is also another field which we denote as k'. By definition, $[k' : k] = f_i$. Thus, our ultimate goal is to prove that

$$\dim_{k'}(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a-1}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a} = 1.$$

We now use that $\mathcal{O}_{K,\mathfrak{p}}$ is a PID (not a discrete valuation ring as it has in general more than one maximal ideal, but still there are finitely many). Therefore, $\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}} = (\pi_i)$ for some $\pi_i \in \mathcal{O}_{K,\mathfrak{p}}$. Thus, there is a k'-linear map

$$\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}} \to (\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a-1}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^a, \quad x \mapsto \pi_i^{a-1}x.$$

This is clearly well-defined and surjective (by $(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a-1} = (\pi_i^{a-1})$), so to show that it is an isomorphism, we only need to show that $(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^{a-1}/(\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}})^a \neq 0$ (because the k'-dimension of the source, $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}}$, is 1). This is equivalent to $(\pi_i^{a-1}) \neq (\pi_i^a)$, which is obvious as $\mathcal{O}_{K,\mathfrak{p}}$ is an integral domain and $\mathfrak{q}_i\mathcal{O}_{K,\mathfrak{p}}$ is a proper ideal. Thus, we get the desired relation.

□

Following Theorem 12.1, we make the following definition.

Definition 12.2 (Ramification indices/residue degrees)**.** Let K/L be a finite extension of number fields, and let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_K$ such that $\mathfrak{q} \cap \mathcal{O}_L = \mathfrak{p}$. Then $e(\mathfrak{q}|\mathfrak{p})$, the **ramification index**, is the power of $\mathfrak{q}$ in the prime ideal factorization of $\mathfrak{p}\mathcal{O}_K$. The **residue degree**, $f(\mathfrak{q}|\mathfrak{p})$, is defined as $f(\mathfrak{q}|\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{q} : \mathcal{O}_L/\mathfrak{p}]$.

Definition 12.3 (Ideal norm)**.** Let K/L be a finite extension of number fields, and let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_K$, with $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_L$. Then, the **ideal norm** $N_{K/L}(\mathfrak{q})$ is defined as

$$N_{K/L}(\mathfrak{q}) := \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}.$$

From this, one defines the ideal norm for all fractional ideals of K by extending the definition multiplicatively.

Definition 12.4 (Unramified, ramified, etc.)**.** Let K/L be a finite extension of number fields, and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_L$. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_g$ be the prime ideals of $\mathcal{O}_K$ lying over $\mathfrak{p}$.

- We say that $\mathfrak{p}$ is **unramified in** K if $e(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all $1 \leq i \leq g$. Otherwise, we say that $\mathfrak{p}$ is **ramified in** K.
- We say that $\mathfrak{p}$ **splits completely in** K if $e(\mathfrak{q}_i|\mathfrak{p}) = f(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all $1 \leq i \leq g$ (equivalently, $g = [K : L]$).
- We say that $\mathfrak{p}$ is **inert in** K if $g = 1$ and $e(\mathfrak{q}_1|\mathfrak{p}) = 1$ (equivalently, $f(\mathfrak{q}_1|\mathfrak{p}) = [K : L]$).
- We say that $\mathfrak{p}$ is **totally ramified in** K if $g = 1$ and $f(\mathfrak{q}_1|\mathfrak{p}) = 1$ (equivalently, $e(\mathfrak{q}_1|\mathfrak{p}) = [K : L]$).

Once you look at the proof of Dedekind's criterion, Theorem 7.11, one can realize that the proof is just immediately generalized to the relative case.

Theorem 12.5 (Dedekind's criterion, relative version)**.** *Let K/L be a finite extension of number fields, and let $\alpha \in \mathcal{O}_K$ be a primitive element (i.e. $K = L(\alpha)$). Let $f(X) \in \mathcal{O}_L[X]$ be the minimal polynomial of α over L. If $p \in \mathbb{Z}$ is a rational prime such that $(p, [\mathcal{O}_K : \mathcal{O}_L[\alpha]]) = 1$, then for a prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ lying over p with residue field $k = \mathcal{O}_L/\mathfrak{p}$, we can find the prime factorization of $\mathfrak{p}\mathcal{O}_K$ in terms of the factorization of $f(X) \pmod{\mathfrak{p}}$ in $k[X]$. More precisely, let $\overline{f}(X) \in k[X]$ be the mod $\mathfrak{p}$ reduction of $f(X)$. Suppose that*

$$\overline{f}(X) = \overline{h}_1(X)^{e_1} \cdots \overline{h}_g(X)^{e_g},$$

is a prime factorization of $\overline{f}(X)$ in $k[X]$. For each $1 \leq i \leq g$, choose $h_i(X) \in \mathcal{O}_L[X]$ a monic polynomial whose mod $\mathfrak{p}$ reduction is equial to $\overline{h}_i(X)$. Then, $\mathfrak{p}\mathcal{O}_K$ has a prime factorization

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}, \quad \mathfrak{q}_i := (\mathfrak{p}, h_i(\alpha)).$$

Furthermore, the residue degree is $f(\mathfrak{q}_i|\mathfrak{p}) = \deg h_i(X)$.

Proof. Let me point out what new part we need. The idea is to mimic the proof of Theorem 7.11 for completeness, with $\mathbb{Z}$ replaced by $\mathcal{O}_L$.

Consider the natural inclusion map $\mathcal{O}_L[\alpha] \to \mathcal{O}_K$, which is an $\mathcal{O}_L$-algebra map. By taking mod $\mathfrak{p}$ reduction, we get a natural k-algebra map $\mathcal{O}_L[\alpha]/\mathfrak{p}\mathcal{O}_L[\alpha] \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. We claim that this is an isomorphism.

Note that, if $x \in \mathcal{O}_K$, then $[\mathcal{O}_K : \mathcal{O}_L[\alpha]]x \in \mathcal{O}_L[\alpha]$. As p and $[\mathcal{O}_K : \mathcal{O}_L[\alpha]]$ are coprime, there are $n, m \in \mathbb{Z}$ such that $np + m[\mathcal{O}_K : \mathcal{O}_L[\alpha]] = 1$. Therefore, $x = m[\mathcal{O}_K : \mathcal{O}_L[\alpha]]x + pnx$ implies that $x \in \mathcal{O}_L[\alpha] + p\mathcal{O}_K$. Thus, $\mathcal{O}_K = \mathcal{O}_L[\alpha] + p\mathcal{O}_K$. Since $p\mathcal{O}_K \subset \mathfrak{p}\mathcal{O}_K$, we have $\mathcal{O}_K = \mathcal{O}_L[\alpha] + \mathfrak{p}\mathcal{O}_K$. Therefore, $\mathcal{O}_L[\alpha] \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is surjective, with the kernel $\mathcal{O}_L[\alpha] \cap \mathfrak{p}\mathcal{O}_K$. This obviously contains $\mathfrak{p}\mathcal{O}_L[\alpha]$, and if any $x \in \mathcal{O}_L[\alpha] \cap \mathfrak{p}\mathcal{O}_K$ so that $x = \sum_{i=1}^k a_i b_i$, $a_i \in \mathfrak{p}$ and $b_i \in \mathcal{O}_K$, then

$$x = npx + m[\mathcal{O}_K : \mathcal{O}_L[\alpha]]x,$$

and $x \in \mathcal{O}_L[\alpha]$ implies $npx \in p\mathcal{O}_L[\alpha] \subset \mathfrak{p}\mathcal{O}_L[\alpha]$, and

$$[\mathcal{O}_K : \mathcal{O}_L[\alpha]]x = \sum_{i=1}^k a_i [\mathcal{O}_K : \mathcal{O}_L[\alpha]]b_i \in \mathfrak{p}\mathcal{O}_L[\alpha],$$

as $[\mathcal{O}_K : \mathcal{O}_L[\alpha]]b_i \in \mathcal{O}_L[\alpha]$ for all i. Thus, $x \in \mathfrak{p}\mathcal{O}_L[\alpha]$, which implies that $\mathcal{O}_L[\alpha] \cap \mathfrak{p}\mathcal{O}_K = \mathfrak{p}\mathcal{O}_L[\alpha]$. This implies that $\mathcal{O}_L[\alpha]/\mathfrak{p}\mathcal{O}_L[\alpha] \xrightarrow{\sim} \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, as desired.

We can now use the Chinese Remainder Theorem,

$$\mathcal{O}_L[\alpha]/\mathfrak{p}\mathcal{O}_L[\alpha] \cong \mathcal{O}_L[X]/(\mathfrak{p}, f(X)) \cong k[X]/(\overline{f}(X)) \xrightarrow{\sim} \prod_{i=1}^g k[X]/(\overline{h}_i(X))^{e_i},$$

and proceed just as in the proof of Theorem 7.11. □

Corollary 12.6. *Let K/L be a finite extension of number fields. Then, there are at most finitely many prime ideals of $\mathcal{O}_L$ that are ramified in K.*

Proof. There are only finitely many prime ideals on $\mathcal{O}_L$ on which we cannot use Dedekind's criterion. Away from them, the unramifiedness is detected by whether $\overline{f}(X)$ has a factor with multiplicity greater than one. This would be avoided if the roots of $f(X)$ in the Galois closure of K are all different modulo the prime ideal that we are dividing. There are finitely many roots, thus finitely many differences, thus finitely many prime ideals dividing the differences. Thus, away from those finitely many exceptions, the prime ideal has to be unramified in K. □

Example 12.7. Let's consider the case of a quadratic extension of a quadratic field, say $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $L = \mathbb{Q}(\sqrt{5})$. We can take $\alpha = \sqrt{2}$ so that $K = L(\alpha)$, and its minimal polynomial over L is $f(X) = X^2 - 2$. Also, K is the compositum of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, whose discriminants are 8 and 5, so in particular

$$\mathcal{O}_K = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \sqrt{2} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{5}}{2} \oplus \mathbb{Z} \cdot \frac{\sqrt{2}+\sqrt{10}}{2} = \mathcal{O}_L[\sqrt{2}].$$

Let $p \neq 5$ be a rational prime. Then p is inert in L if and only if either $p = 2$ or p is odd and $\left(\frac{5}{p}\right) = -1$, and p splits completely in L if and only if p is odd and $\left(\frac{5}{p}\right) = 1$.

In the first case, take $(p) \subset \mathcal{O}_L$. Then, $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_{p^2}$. If $p = 2$, then we see that $f(X) = X^2 - 2 = X^2$ in $\mathbb{F}_{p^2}[X]$, so we have

$$2\mathcal{O}_K = (2, \sqrt{2})^2 = (\sqrt{2})^2.$$

If p is odd and nonsquare mod p, then we want to know when $X^2 - 2$ has a root in $\mathbb{F}_{p^2}$. Note that this would imply that $X^2 - 2$ has a root in $\mathbb{F}_p$ just by seeing it mod p. Conversely, a root of $X^2 - 2$ in $\mathbb{F}_p$ will imply that there is a root of $X^2 - 2$ in $\mathbb{F}_{p^2}$. Thus, $X^2 - 2$ is irreducible in $\mathbb{F}_{p^2}$ if and only if $\left(\frac{2}{p}\right) = -1$. Thus

$$p\mathcal{O}_K = p\mathcal{O}_K,$$

if $\left(\frac{5}{p}\right) = \left(\frac{2}{p}\right) = -1$, and

$$p\mathcal{O}_K = (p, \sqrt{2} - a)(p, \sqrt{2} + a),$$

if $\left(\frac{5}{p}\right) = -1$ and $a^2 \equiv 2 \pmod{p}$.

If p splits completely in $\mathcal{O}_L$, then

$$p\mathcal{O}_L = \left(p, \frac{1+\sqrt{5}}{2} - \frac{p+1}{2} - b\right)\left(p, \frac{1+\sqrt{5}}{2} - \frac{p+1}{2} + b\right) = \mathfrak{p}_1\mathfrak{p}_2,$$

where $\frac{5}{4} \equiv b^2 \pmod{p}$. For $\mathfrak{p} = \mathfrak{p}_1$ or $\mathfrak{p}_2$, $\mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_p$. Thus, whether $\mathfrak{p}_1$ or $\mathfrak{p}_2$ splits or not in K depends on whether $X^2 - 2$ has a root in $\mathbb{F}_p$ or not, as before. Thus,

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{p}\mathcal{O}_K,$$

if $\left(\frac{5}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$, and

$$\mathfrak{p}\mathcal{O}_K = (\mathfrak{p}, \sqrt{2} - a)(\mathfrak{p}, \sqrt{2} + a),$$

if $\left(\frac{5}{p}\right) = 1$ and $a^2 \equiv 2 \pmod{p}$.

We now observe that actually the discriminant can be made relative as an ideal, and how the (relative) discriminant have something to do with ramified primes.

Definition 12.8. Let A be a Dedekind domain with $F = \mathrm{Frac}(A)$, and let F'/F be a degree n field extension with A' the integral closure of A in F'. For $x_1, \cdots, x_n \in A'$, define

$$D(x_1, \cdots, x_n) = \det(\{\mathrm{Tr}_{F'/F}(x_i x_j)\}_{1 \le i,j \le n}).$$

We define the (relative) **discriminant** of A' over A, $\mathrm{disc}(A'/A)$, as the A-module generated by $\{D(x_1, \cdots, x_n) \mid x_1, \cdots, x_n \in A'\}$. As $\mathrm{disc}(A'/A)$ is an A-submodule of A, it is an ideal of A. If F', F are number fields with $A = \mathcal{O}_F$ and $A' = \mathcal{O}_{F'}$, we also use the notation $\mathrm{disc}(F'/F)$.

There are some other cases where you can define the discriminant.

Definition 12.9 (Variant of Definition 12.8)**.** Let A be an integral domain, and let A' be a commutative A-algebra which is also a free A-module of rank n. Then, for $a \in A'$, define

$$\mathrm{Tr}_{A'/A} = \mathrm{tr}(m_a), \quad N_{A'/A} = \det(m_a),$$

where $m_a : A' \to A'$ is the multiplication-by-a map. Then, one may define D and the discriminant of A'/A using the trace $\mathrm{Tr}_{A'/A}$.

It is easy to see that the above two definitions coincide when A is a Dedekind domain, and A' is the integral closure of A in a field extension of $\mathrm{Frac}(A)$. We have the expected properties.

Theorem 12.10. *Let A be a Dedekind domain with $F = \mathrm{Frac}(A)$, F'/F be a degree n field extension, and A' be the integral closure of A in F'.*

(1) Let K/F' be a large enough field extension for which there are n distinct F-embeddings $\sigma_1, \cdots, \sigma_n : F' \hookrightarrow K$. Then,

$$D(x_1, \cdots, x_n) = \det(\{\sigma_i(e_j)\}_{1 \le i,j \le n})^2.$$

(2) If S is a multiplicative subset of A, then $\mathrm{disc}(S^{-1}A'/S^{-1}A) = S^{-1}\,\mathrm{disc}(A'/A)$.

(3) Suppose further than A' is a free A-module. If $\mathfrak{p} \subset A$ is a maximal ideal, then

$$\mathrm{disc}((A'/\mathfrak{p}A')/(A/\mathfrak{p})) = \begin{cases} A/\mathfrak{p} & \text{if } \mathrm{disc}(A'/A) \text{ is coprime to } \mathfrak{p} \\ 0 & \text{if } \mathfrak{p} \text{ divides } \mathrm{disc}(A'/A). \end{cases}$$

(4) For a number field F, $\mathrm{disc}(F/\mathbb{Q}) = \mathrm{disc}(F)\mathbb{Z}$.

Proof.

(1) The proof we had before works verbatim.

(2) If $x_1, \cdots, x_n \in A'$, then $D(x_1, \cdots, x_n) \in \mathrm{disc}(S^{-1}A'/S^{-1}A)$, so $S^{-1}\,\mathrm{disc}(A'/A) \subset \mathrm{disc}(S^{-1}A'/S^{-1}A)$. Conversely, if $x_1, \cdots, x_n \in S^{-1}A'$, there exist $s \in S$ such that $sx_1, \cdots, sx_n \in A'$, and $D(x_1, \cdots, x_n) = s^{-2n}D(sx_1, \cdots, sx_n) \in S^{-1}\,\mathrm{disc}(A'/A)$, so $\mathrm{disc}(S^{-1}A'/S^{-1}A) \subset S^{-1}\,\mathrm{disc}(A'/A)$. These two together prove the desired result.

(3) Let $k = A/\mathfrak{p}$ be the residue field. As $[F' : F] = n$, if A' is a free A-module, A' is of rank n. Thus, $\dim_k A'/\mathfrak{p}A' = n$. Then, for any $x_1, \cdots, x_n \in A'$, $D(x_1, \cdots, x_n) \pmod{\mathfrak{p}} = D(x_1 \pmod{\mathfrak{p}}, \cdots, x_n \pmod{\mathfrak{p}})$, so $\mathrm{disc}((A'/\mathfrak{p}A')/(A/\mathfrak{p}))$ contains the image of $\mathrm{disc}(A'/A)$ under the map $\mathrm{disc}(A'/A) \subset A \twoheadrightarrow A/\mathfrak{p}$. Thus, this proves the first case when $\mathrm{disc}(A'/A)$ is coprime to $\mathfrak{p}$. On the other hand, if $\mathfrak{p}$ divides $\mathrm{disc}(A'/A)$, then for any $\overline{x}_1, \cdots, \overline{x}_n \in A'/\mathfrak{p}A'$, lift them to $x_1, \cdots, x_n \in A'$, then $D(\overline{x}_1, \cdots, \overline{x}_n) = D(x_1, \cdots, x_n) \pmod{\mathfrak{p}} = 0$, so $\mathrm{disc}((A'/\mathfrak{p}A')/(A/\mathfrak{p})) = 0$ in this case, as desired.

(4) This follows from the usual relation between the $\mathrm{disc}(F)$ and D of the random linearly independent elements in $\mathcal{O}_F$.

□

This actually proves a statement that we suspected for a while (and something that could be proved way before elementarily). The virtue of this wait is that we can reduce a hard theorem into a manageable piece.

Theorem 12.11 (Discriminant detects ramified primes)**.** *Let K/L be an extension of number fields. Then, for a prime ideal $\mathfrak{p} \subset \mathcal{O}_L$, $\mathfrak{p}$ divides $\mathrm{disc}(K/L)$ if and only if $\mathfrak{p}$ ramifies in K.*

In particular, a rational prime p ramifies in a number field F if and only if p divides $\mathrm{disc}(F)$.

Proof. Note that the prime splitting of $\mathfrak{p}$ in $\mathcal{O}_K$ is detected even after localization at $\mathfrak{p}$, and also $\mathrm{disc}(K/L)$ retains its factor of $\mathfrak{p}$ even after localization at $\mathfrak{p}$. Thus, we only need to show the analogous statement for the case when the base is a discrete valuation ring! To be more precise, $\mathfrak{p}$ divides $\mathrm{disc}(K/L) = \mathrm{disc}(\mathcal{O}_K/\mathcal{O}_L)$ if and only if $\mathfrak{p}$ divides $\mathrm{disc}(\mathcal{O}_K/\mathcal{O}_L)_{\mathfrak{p}} = \mathrm{disc}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}})$, and $\mathfrak{p}$ is ramified in K if and only if $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ has a prime factor of multiplicity greater than one. Moreover, as $\mathcal{O}_{L,\mathfrak{p}}$ is a discrete valuation ring, it is a PID, so $\mathcal{O}_{K,\mathfrak{p}}$ is a free $\mathcal{O}_{L,\mathfrak{p}}$-module. Thus, by Theorem 12.10(3), $\mathfrak{p}$ divides $\mathrm{disc}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}})$ if and only if $\mathrm{disc}(\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}, \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}) = 0$. Moreover, $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ has a prime factor of multiplicity greater than one if and only if, by the Chinese Remainder Theorem, the ring $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is a product of rings which are either fields or **not reduced**:

Definition 12.12 (Reduced rings)**.** A commutative ring A is called **reduced** if $a^N = 0$ for some $a \in A$, $N \geq 1$ implies that $a = 0$.

Let $k = \mathcal{O}_L/\mathfrak{p} = \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ be the residue field, which is a finite field. Then, $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is a free k-module (=k-vector space) of rank $[K : L]$ which is also a k-algebra. Thus, the Theorem will follow from the following

Proposition 12.13. *Let k be a finite field, and let A be a commutative k-algebra which is finitely generated as a k-module (i.e. $\dim_k A$ is finite), and is a product of fields and non-reduced k-algebras. Then, A is reduced if and only if $\mathrm{disc}(A/k) \neq 0$.*

Proof. If A is not reduced (i.e. there is a non-reduced factor), take a nonzero nilpotent element $a \in A$. Then, for any $b \in A$, ab is also nilpotent, so m_{ab} is a nilpotent matrix, so $\mathrm{Tr}_{A/k}(ab) = 0$. By completing a into a k-basis of A, we see that $\mathrm{disc}(A/k) = 0$.

If A is reduced, this means that there are no non-reduced factors, so A is a product of fields. Namely, $A = k_1 \times \cdots \times k_r$ where k_r/k is a finite extension of finite fields. It is easy to see (check; Exercise) that $\mathrm{disc}(\prod_{i=1}^r k_i/k) = \prod_{i=1}^r \mathrm{disc}(k_i/k)$, so it suffices to show that $\mathrm{disc}(k_i/k) \neq 0$. This is basically equivalent to saying that k_i/k is separable, which is indeed true in the case of field extensions between finite fields. □

□

There is a slight refinement of the discriminant that arguably has more straightforward properties, called the **different**.

Definition 12.14 (Different)**.** Let A be a Dedekind domain with $F = \mathrm{Frac}(A)$, and let F'/F be a finite extension of fields with A' the integral closure of A in F'. The A-**linear dual** of A', denoted $A'^\vee$, is defined as

$$A'^\vee := \{x \in F' \mid \mathrm{Tr}_{F'/F}(xa) \in A \text{ for all } a \in A'\}.$$

As $A'^\vee$ is an A'-submodule of F', it is a fractional ideal of A'. The **different** $\mathrm{diff}(A'/A)$ is defined as

$$\mathrm{diff}(A'/A) := (A'^\vee)^{-1} = \{x \in F' \mid xA'^\vee \subset A'\}.$$

In the cases when A, A' are rings of integers of number fields, we also use the notation $\mathrm{diff}(F'/F)$.

Theorem 12.15. *Let A be a Dedekind domain with $F = \mathrm{Frac}(A)$, F'/F be a finite extension of fields, and A' be the integral closure of A in F'.*

(1) The different $\mathrm{diff}(A'/A)$ is an ideal of A'.

(2) A fractional ideal $\mathfrak{a}$ of A' divides $\mathrm{diff}(A'/A)$ if and only if $\mathrm{Tr}_{F'/F}(\mathfrak{a}^{-1}) \subset A$. Equivalently, $A'^\vee$ is the maximal fractional ideal of A whose elements have the traces in A.

(3) Let S be a multiplicative subset of A. Then,

$$\mathrm{diff}(S^{-1}A'/S^{-1}A) = S^{-1}\,\mathrm{diff}(A'/A).$$

(4) Let F''/F' be another finite extension of fields, with A'' the integral closure of A in F''. Show that the different is multiplicative in towers, in the sense that

$$\mathrm{diff}(A''/A) = \mathrm{diff}(A''/A')(\mathrm{diff}(A'/A)A'').$$

Proof.

(1) It suffices to prove that $\mathrm{diff}(A'/A) \subset A'$. Note that $A' \subset A'^\vee$. Therefore, if $x \in \mathrm{diff}(A'/A)$, the $A' \supset xA'^\vee \supset xA'$. This implies that $x \in A'$.

(2) Note that $\mathfrak{a}$ divides $\operatorname{diff}(A'/A)$ means $\operatorname{diff}(A'/A) \subset \mathfrak{a}$, or in terms of the fractional ideals, $\mathfrak{a}^{-1} \subset A'^{\vee}$. Note that $\mathfrak{a}^{-1} \subset A'^{\vee}$ implies that $\operatorname{Tr}_{F'/F}(\mathfrak{a}^{-1}) \subset A$. Conversely, suppose $\operatorname{Tr}_{F'/F}(\mathfrak{a}^{-1}) \subset A$. Note that if two fractional ideals $\mathfrak{b}, \mathfrak{c}$ of A' satisfy $\operatorname{Tr}_{F'/F}(\mathfrak{b}) \subset A$, $\operatorname{Tr}_{F'/F}(\mathfrak{c}) \subset A$, then obviously $\operatorname{Tr}_{F'/F}(\mathfrak{b}+\mathfrak{c}) \subset A$. Therefore, there is a fractional ideal I of A which is maximal among all fractional ideals of A whose elements have $\operatorname{Tr}_{F'/F}$ valued in A. Note that $I \supset A'^{\vee}$. On the other hand, if $x \in I$, then $xa \in I$ for all $a \in A'$, so $\operatorname{Tr}_{F'/F}(xa) \in A$ for all $a \in A'$, so $x \in A'^{\vee}$. Thus, $I \subset A'^{\vee}$, so $I = A'^{\vee}$. Thus $\mathfrak{a}^{-1} \subset I = A'^{\vee}$.

(3) Note that $A'^{\vee}$ is also clearly an A'-module. We first want to show that $S^{-1}(A'^{\vee}) = (S^{-1}A')^{\vee}$. If $x \in A'^{\vee}$, then $\operatorname{Tr}_{F'/F}(xa) \in A$ for all $a \in A'$. Then for $\frac{a}{s} \in S^{-1}A'$, $s \in S$, $\operatorname{Tr}_{F'/F}(x\frac{a}{s}) = \frac{\operatorname{Tr}_{F'/F}(xa)}{s} \in S^{-1}A$, so $x \in (S^{-1}A')^{\vee}$. Thus, $S^{-1}(A'^{\vee}) \subset (S^{-1}A')^{\vee}$. Conversely, suppose that $x \in (S^{-1}A')^{\vee}$. Since A is Noetherian, A' is a finitely generated A-module. Take the generators $a_1, \cdots, a_r \in A'$. Then, $\operatorname{Tr}_{F'/F}(xa_j) \in S^{-1}A$ for $1 \le j \le r$, so $\operatorname{Tr}_{F'/F}(xa_j) = \frac{a'_j}{s'_j}$ for some $a'_j \in A$, $s'_j \in S$. Thus, $\operatorname{Tr}_{F'/F}((s'_1 \cdots s'_r x)a_j) = a'_j s'_1 \cdots s'_{j-1} s'_{j+1} \cdots s'_r \in A$. This implies that $s'_1 \cdots s'_r x \in A'^{\vee}$, so $x \in S^{-1}(A'^{\vee})$. This proves $(S^{-1}A')^{\vee} \subset S^{-1}(A'^{\vee})$.

Now we have

$$\operatorname{diff}(S^{-1}A'/S^{-1}A) = \{x \in F' \mid x \cdot S^{-1}(A'^{\vee}) \subset S^{-1}A'\}.$$

For $x \in \operatorname{diff}(A'/A)$, $xA'^{\vee} \subset A'$, so $x \cdot S^{-1}(A'^{\vee}) \subset S^{-1}A'$, which implies that $S^{-1}\operatorname{diff}(A'/A) \subset \operatorname{diff}(S^{-1}A'/S^{-1}A)$. Conversely, if $x \in \operatorname{diff}(S^{-1}A'/S^{-1}A)$, then $x \cdot S^{-1}(A'^{\vee}) \subset S^{-1}A'^{\vee}$. As A' is Noetherian, $A'^{\vee}$ is a finitely generated A'-module, whence has a finite basis $a_1, \cdots, a_k \in A'^{\vee}$. Then, $xa_i \in xA'^{\vee} \subset xS^{-1}(A'^{\vee}) \subset S^{-1}A'$, so $xa_i = \frac{a'_i}{s'_i}$ for $a'_i \in A'$, $s'_i \in S$. Thus $s'_1 \cdots s'_k x a_i \in A'$. Thus, $s'_1 \cdots s'_k x A'^{\vee} \subset A'$, so $s'_1 \cdots s'_k x \in \operatorname{diff}(A'/A)$. Thus, $x \in S^{-1}\operatorname{diff}(A'/A)$, so $\operatorname{diff}(S^{-1}A'/S^{-1}A) \subset S^{-1}\operatorname{diff}(A'/A)$.

(4) Let ${A''}^{\vee}_{A}$ be the A-linear dual of A'',

$${A''}^{\vee}_{A} := \{x \in F'' \mid \operatorname{Tr}_{F''/F}(xa) \in A \text{ for all } a \in A''\},$$

and ${A''}^{\vee}_{A'}$ be the A'-linear dual of A'',

$${A''}^{\vee}_{A'} := \{x \in F'' \mid \operatorname{Tr}_{F''/F'}(xa) \in A' \text{ for all } a \in A''\}.$$

By definition, as $\operatorname{Tr}_{F'/F}(A') \subset A$ and as Tr is transitive, ${A''}^{\vee}_{A'} \subset {A''}^{\vee}_{A}$.

By taking the inverse, what we need to prove is

$${A''}^{\vee}_{A} = {A''}^{\vee}_{A'}(A'^{\vee}A'') = A'^{\vee}{A''}^{\vee}_{A'},$$

where $A'^{\vee}A''$ is the fractional ideal of A'' generated by $A'^{\vee}$. If $x \in {A''}^{\vee}_{A'}$ and $y \in A'^{\vee}$, then for all $a \in A''$,

$$\operatorname{Tr}_{F''/F}(xya) = \operatorname{Tr}_{F'/F}(\operatorname{Tr}_{F''/F'}(xya)) = \operatorname{Tr}_{F'/F}(y \operatorname{Tr}_{F''/F'}(xa)),$$

as $y \in F'$. Since $x \in A''^{\vee}_{A'}$, $\mathrm{Tr}_{F''/F'}(xa) \in A'$. Since $y \in A'^{\vee}$, $\mathrm{Tr}_{F'/F}(ya') \in A$ for any $a' \in A'$, so in particular when $a' = \mathrm{Tr}_{F''/F'}(xa)$. Thus, $\mathrm{Tr}_{F''/F}(xya) \in A$, which implies that $xy \in A''^{\vee}_{A}$. This implies that $A'^{\vee}A''^{\vee}_{A'} \subset A''^{\vee}_{A}$.

Conversely, we want to show that $A''^{\vee}_{A} \subset A'^{\vee}A''^{\vee}_{A'}$, or equivalently $\mathrm{diff}(A'/A)A''^{\vee}_{A} \subset A''^{\vee}_{A'}$. Let $x \in \mathrm{diff}(A'/A)$ and $y \in A''^{\vee}_{A}$. Let $a \in A''$, and consider $\mathrm{Tr}_{F''/F'}(xya) = x\,\mathrm{Tr}_{F''/F'}(ya)$. Note that $\mathrm{Tr}_{F'/F}(\mathrm{Tr}_{F''/F'}(ya)) = \mathrm{Tr}_{F''/F}(ya) \in A$, so if we let $\mathfrak{a}$ be the fractional ideal of A' generated by $\mathrm{Tr}_{F''/F'}(ya)$, $a \in A''$, then $\mathfrak{a} \subset A'^{\vee}$ by (2). Thus, $\mathrm{Tr}_{F''/F'}(ya) \in A'^{\vee}$. Since $xA'^{\vee} \subset A'$, $x\,\mathrm{Tr}_{F''/F'}(ya) \in A'$. Thus, $\mathrm{Tr}_{F''/F'}(xya) \in A'$, so $xy \in A''^{\vee}_{A'}$, as desired.

□

The following is a generalization of Theorem 4.3, and gives a way to compute the discriminant in towers when combined with Theorem 12.15.

Theorem 12.16. *Let K/L be an extension of number fields. Then, the different and the discriminant are related as*

$$\mathrm{disc}(K/L) = N_{K/L}(\mathrm{diff}(K/L)).$$

Proof. We can compute both sides after localizing at each prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$. In that case, $\mathcal{O}_{L,\mathfrak{p}}$ is a discrete valuation ring, so a PID, and $\mathcal{O}_{K,\mathfrak{p}}$ is a free $\mathcal{O}_{L,\mathfrak{p}}$-module of rank $n := [K : L]$. Let $e_1, \cdots, e_n$ be an $\mathcal{O}_{L,\mathfrak{p}}$-basis of $\mathcal{O}_{K,\mathfrak{p}}$. Then, $\mathcal{O}^{\vee}_{K,\mathfrak{p}}$ is a free $\mathcal{O}_{L,\mathfrak{p}}$-module with basis $e_1^*, \cdots, e_n^*$, where $e_j^* \in K$ is such that $\mathrm{Tr}_{K/L}(e_i e_j^*) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$. If we write $e_i = \sum_{j=1}^n a_{ij} e_j^*$, $a_{ij} \in \mathcal{O}_{L,\mathfrak{p}}$, then

$$\mathrm{Tr}_{K/L}(e_i e_j) = a_{ij},$$

which implies that $M = (a_{ij})_{1 \le i,j \le n}$, a change-of-basis matrix from $(e_1^*, \cdots, e_n^*)$ to $(e_1, \cdots, e_n)$, has determinant which generates the discriminant ideal $\mathrm{disc}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}})$. Namely, $M : \mathcal{O}^{\vee}_{K,\mathfrak{p}} \to \mathcal{O}^{\vee}_{K,\mathfrak{p}}$ is an injective $\mathcal{O}_{L,\mathfrak{p}}$-module homomorphism whose image is $\mathcal{O}_{K,\mathfrak{p}} \subset \mathcal{O}^{\vee}_{K,\mathfrak{p}}$. Now the Smith normal form over PID (see the link in the main webpage) says that $(\det M) = \mathrm{disc}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}})$ is the ideal generated by $d_1 \cdots d_r$, where $\mathcal{O}^{\vee}_{K,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_{L,\mathfrak{p}}/(d_1) \oplus \cdots \oplus \mathcal{O}_{L,\mathfrak{p}}/(d_r)$ (using the structure theorem of modules over a PID). Note that as $\mathcal{O}_{K,\mathfrak{p}}$ is also a principal ideal domain (Dedekind domain with finitely many principal ideals), $\mathcal{O}^{\vee}_{K,\mathfrak{p}} = (\alpha)$ for some $\alpha \in K$, which implies that $\mathrm{diff}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}}) = (\alpha^{-1})$, whence $\mathcal{O}^{\vee}_{K,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_{K,\mathfrak{p}}/\mathrm{diff}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}})$. If $\mathrm{diff}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}}) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, by the Chinese Remainder Theorem, $\mathcal{O}_{K,\mathfrak{p}}/\mathrm{diff}(\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}}) \cong \prod_{i=1}^g \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}_i^{e_i}$. Thus, the statement we want to prove reduces to the following statement.

Claim. If $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}_i^e \cong \mathcal{O}_{L,\mathfrak{p}}/(m_1) \oplus \cdots \oplus \mathcal{O}_{L,\mathfrak{p}}/(m_k)$ as $\mathcal{O}_{L,\mathfrak{p}}$-modules, then $N_{\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}}}(\mathfrak{p}_i^e) = (m_1 \cdots m_k)$.

In general, for a finitely generated torsion $\mathcal{O}_{L,\mathfrak{p}}$-module M, which must be isomorphic to $\mathcal{O}_{L,\mathfrak{p}}/(m_1) \oplus \cdots \oplus \mathcal{O}_{L,\mathfrak{p}}/(m_r)$ for some $m_1, \cdots, m_r \in \mathcal{O}_{L,\mathfrak{p}}$, let $d(M) := (m_1 \cdots m_r)$. Then, note that the right side is multiplicative in the sense that, if M is a finitely generated torsion $\mathcal{O}_{L,\mathfrak{p}}$-module with a submodule N, then $d(M) = d(N)d(M/N)$. Therefore, if we consider $\mathfrak{p}_i/\mathfrak{p}_i^e \subset \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}_i^e$, then as $\mathcal{O}_{K,\mathfrak{p}}$ is a PID, $\mathfrak{p}_i/\mathfrak{p}_i^e \cong \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}_i^{e-1}$, so that we can use induction on e. Thus, the proof of **Claim**

is reduced to the case of $e = 1$, where $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}_i$ is a finite field, $\mathbb{F}_{p^{f(\mathfrak{p}_i|p)}}$, where $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$. Since $f(\mathfrak{p}_i|p) = f(\mathfrak{p}_i|\mathfrak{p})f(\mathfrak{p}|p)$, it follows that

$$\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}_i \cong \mathbb{F}_{p^{f(\mathfrak{p}_i|p)}} \cong \mathbb{F}_{p^{f(\mathfrak{p}|p)}}^{\oplus f(\mathfrak{p}_i|\mathfrak{p})},$$

as $\mathcal{O}_{L,\mathfrak{p}}$-modules (here $\mathbb{F}_{p^{f(\mathfrak{p}|p)}}$ is an $\mathcal{O}_{L,\mathfrak{p}}$-module as $\mathbb{F}_{p^{f(\mathfrak{p}|p)}} \cong \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}$). Thus,

$$d(\mathbb{F}_{p^{f(\mathfrak{p}|p)}}^{\oplus f(\mathfrak{p}_i|\mathfrak{p})}) = (\pi^{f(\pi_i|\mathfrak{p})}) = \mathfrak{p}^{f(\mathfrak{p}_i|\mathfrak{p})} = N_{\mathcal{O}_{K,\mathfrak{p}}/\mathcal{O}_{L,\mathfrak{p}}}(\mathfrak{p}_i),$$

as desired, where π is a uniformizer of $\mathcal{O}_{L,\mathfrak{p}}$. □

– –

Exercise 12.1. Let $p \neq q$ be two different rational primes such that $p, q \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, and $L = \mathbb{Q}(\sqrt{pq})$, so that $L \subset K$. Show that **every prime ideal of** $\mathcal{O}_L$ is unramified in K.

Exercise 12.2.

(1) Let $f(X) \in \mathbb{Z}[X]$ be any nonconstant polynomial. Show that $f(X)$ has a root mod p for infinitely many rational primes p.

Hint. If all prime factors of $f(n)$ are less than N, then show that, for large enough M, $\frac{f(M!f(0))}{f(0)}$ must have a prime factor bigger than N.

(2) Let K be a number field. Show that there are infinitely many prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that the residue degree of $\mathfrak{p}$ is 1.

(3) Let K/L be an extension of number fields. Show that there are infinitely many prime ideals of L that split completely in K.

Hint. Apply (2) to the Galois closure of K over $\mathbb{Q}$.

13. Lectures 16 and 17. Ramification and local fields

Summary. Relative splitting of primes in the Galois case; valuations and absolute values; completion; complete discretely valued fields and complete discrete valuation rings; local fields; Hensel's lemma; Newton polygon; ramification groups; tame and wild ramification.

Content. We now discuss the relative splitting of prime ideals in the presence of Galois action, namely when K/L is a Galois extension of number fields. Let $\mathfrak{p} \subset \mathcal{O}_L$ be a maximal ideal, and let $\mathfrak{p}_1, \cdots, \mathfrak{p}_g \subset \mathcal{O}_K$ be the prime ideals lying over $\mathfrak{p}$ (i.e. $\mathfrak{p}_i \cap \mathcal{O}_L = \mathfrak{p}$). There is an action of $\mathrm{Gal}(K/L)$ on the prime ideals lying over $\mathfrak{p}$,

$$\mathrm{Gal}(K/L) \times \{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\} \to \{\mathfrak{p}_1, \cdots, \mathfrak{p}_g\}, \quad (\sigma, \mathfrak{p}_i) \mapsto \sigma(\mathfrak{p}_i).$$

The proof of Theorem 8.1 did not use anything specific about the base field, so it generalizes immediately:

Theorem 13.1. *The action of $\mathrm{Gal}(K/L)$ on the set of prime ideals of $\mathcal{O}_K$ dividing $\mathfrak{p}$ is transitive, i.e. for any $1 \le i, j \le g$, there is $\sigma \in \mathrm{Gal}(K/L)$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$. Consequently, the ramification indices $e(\mathfrak{p}_i|\mathfrak{p})$ are all equal, and the residue degrees $f(\mathfrak{p}_i|\mathfrak{p})$ are all equal.*

Again, we then have the relation $efg = [K : L]$, where e is the shared ramification index and f is the shared residue degree.

Definition 13.2 (Decomposition/inertia groups)**.** Let K/L be Galois, and let $\mathfrak{p} \subset \mathcal{O}_K$ lie over $\mathfrak{q} \subset \mathcal{O}_L$ (i.e. $\mathfrak{p} \cap \mathcal{O}_L = \mathfrak{q}$). Then, the **decomposition group** at $\mathfrak{p}$ over $\mathfrak{q}$ is

$$D(\mathfrak{p}|\mathfrak{q}) := \{\sigma \in \mathrm{Gal}(K/L) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

The **inertia group** at $\mathfrak{p}$ over $\mathfrak{q}$ is

$$I(\mathfrak{p}|\mathfrak{q}) := \{\sigma \in D(\mathfrak{p}|\mathfrak{q}) \mid \sigma(x) - x \in \mathfrak{p} \text{ for all } x \in \mathcal{O}_K\}.$$

The following is again immediate.

Proposition 13.3. *Let K/L be Galois, and let $\mathfrak{p} \subset \mathcal{O}_K$ lie over $\mathfrak{q} \subset \mathcal{O}_L$. Then, for each $\sigma \in \mathrm{Gal}(K/L)$,*

$$D(\sigma(\mathfrak{p})|\mathfrak{q}) = \sigma D(\mathfrak{p}|\mathfrak{q})\sigma^{-1}, \quad I(\sigma(\mathfrak{p})|\mathfrak{q}) = \sigma I(\mathfrak{p}|\mathfrak{q})\sigma^{-1}.$$

In particular, if $\mathrm{Gal}(K/L)$ is abelian, $D(\mathfrak{p}|\mathfrak{q})$ and $I(\mathfrak{p}|\mathfrak{q})$ do not depend on $\mathfrak{p}$ and only depend on $\mathfrak{q}$.

For $\mathfrak{p} \subset \mathcal{O}_K$ lying over $\mathfrak{q} \subset \mathcal{O}_L$, let $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ and $k_\mathfrak{q} = \mathcal{O}_L/\mathfrak{q}$ be the residue fields of $\mathfrak{p}$ and $\mathfrak{q}$, respectively. Then, there is a natural map

$$D(\mathfrak{p}|\mathfrak{q}) \to \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q}), \quad \sigma \mapsto \sigma \pmod{\mathfrak{q}}.$$

Theorem 8.4 can be proved in the similar way.

Theorem 13.4. *Let K/L be Galois, with $\mathfrak{p} \subset \mathcal{O}_K$ lying over $\mathfrak{q} \subset \mathcal{O}_L$, with residue fields $k_\mathfrak{p}$, $k_\mathfrak{q}$, respectively. Then, the natural group homomorphism $D(\mathfrak{p}|\mathfrak{q}) \to \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})$ is surjective, with the kernel equal to $I(\mathfrak{p}|\mathfrak{q})$.*

Proof. The proof of Theorem 8.4 works exactly in the same way, with the only difference being that we use a $\mathcal{O}_{L,\mathfrak{q}}$-basis of $\mathcal{O}_{K,\mathfrak{q}}$, which is a free $\mathcal{O}_{L,\mathfrak{q}}$-module as $\mathcal{O}_{L,\mathfrak{q}}$ is a PID and $\mathcal{O}_{K,\mathfrak{q}}$ is a torsion-free $\mathcal{O}_{L,\mathfrak{q}}$-module. The rest is exactly the same. □

Theorem 13.5. *Let K/L be Galois, with $\mathfrak{p} \subset \mathcal{O}_K$ lying over $\mathfrak{q} \subset \mathcal{O}_L$. If $\mathfrak{q}$ is unramified in K, then $I(\mathfrak{p}|\mathfrak{q}) = 1$. Therefore, if $\mathfrak{q}$ is unramified in K, then there is a natural isomorphism $D(\mathfrak{p}|\mathfrak{q}) \cong \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})$.*

Proof. We have $|\mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})| = f(\mathfrak{p}|\mathfrak{q}) = f$, and $|D(\mathfrak{p}|\mathfrak{q})| = \frac{[K:L]}{g} = ef$, so the natural surjective map is an isomorphism if and only if $e = 1$, or $\mathfrak{q}$ is unramified, and this is if and only if the kernel, the inertia group, is trivial. □

Thus, if $\mathfrak{q} \subset \mathcal{O}_L$ is unramified in Galois K/L, then $D(\mathfrak{p}|\mathfrak{q})$ is a cyclic group of order $f = f(\mathfrak{p}|\mathfrak{q})$, for a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ lying over $\mathfrak{q}$. Furthermore, it has a natural generator, the Frobenius, corresponding to the Frobenius automorphism in $\mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})$,

$$\mathrm{Fr}_{N(\mathfrak{q})} \in \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q}), \quad \mathrm{Fr}_{k_\mathfrak{q}}(x) = x^{N(\mathfrak{q})}.$$

Definition 13.6 (Frobenius element/Artin symbol)**.** Let K/L be Galois with $\mathfrak{q} \subset \mathcal{O}_L$ unramified in K. Let $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q}) \in D(\mathfrak{p}|\mathfrak{q})$ be the element corresponding to $\mathrm{Fr}_{N(\mathfrak{q})} \in \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})$ under the natural isomorphism $D(\mathfrak{p}|\mathfrak{q}) \cong \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})$. In other words, $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q}) \in D(\mathfrak{p}|\mathfrak{q})$ is the unique element such that

$$\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})(x) \equiv x^{N(\mathfrak{q})} \pmod{\mathfrak{p}},$$

for all $x \in \mathcal{O}_K$. Another notation for the Frobenius element is

$$\left(\frac{K/L}{\mathfrak{p}}\right) := \mathrm{Fr}(\mathfrak{p}|\mathfrak{q}),$$

called the **Artin symbol**.

It's called the Artin symbol because it is the main ingredient of the **Artin reciprocity law** which will come very soon. Everything we had abut the Frobenius in §8 holds the same as the proof was Galois-theoretic and did not use anything about the base field.

Theorem 13.7. *Let K/L be Galois with $\mathfrak{q} \subset \mathcal{O}_L$ unramified in K. Let $\mathfrak{p} \subset \mathcal{O}_K$ lie over $\mathfrak{q}$.*

*(1) For $\sigma \in \mathrm{Gal}(K/L)$, $\sigma \,\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})\sigma^{-1} = \mathrm{Fr}(\sigma(\mathfrak{p})|\mathfrak{q})$. Therefore, $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})$ lies in a single conjugacy class in $\mathrm{Gal}(K/L)$ regardless of what $\mathfrak{p}$ is. The conjugacy class is often denoted as $\mathrm{Fr}_\mathfrak{q} \subset \mathrm{Gal}(K/L)$ and called the **Frobenius conjugacy class**. In particular, if $\mathrm{Gal}(K/L)$ is abelian, $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})$ does not depend on $\mathfrak{p}$ and only depends on $\mathfrak{q}$.*

(2) We have $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q}) = 1$ if and only if $\mathfrak{q}$ splits completely in K.

(3) Let $G = \mathrm{Gal}(K/L)$ and $H \leq G$ be a subgroup, and let $M = K^H$ be the fixed field of H. Then, the splitting of $\mathfrak{q}$ in $\mathcal{O}_M$ can be described as follows.

- *The Frobenius* $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q}) \in G$ *acts on the right on the set of right cosets* $H\backslash G$ *by* $H\sigma \mapsto H\sigma \,\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})$.
- *The set* $H\backslash G$ *splits into the orbits under the action of* $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})$ *as*

$$H\backslash G = \{H\sigma_1, \cdots, H\sigma_1 \,\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})^{m_1-1}\} \amalg \cdots \amalg \{H\sigma_r, \cdots, H\sigma_r \,\mathrm{Fr}(\mathfrak{p}|\mathfrak{q})^{m_r-1}\}.$$

- *Then, the prime ideal factorization of* $\mathfrak{q}\mathcal{O}_M \subset \mathcal{O}_M$ *is*

$$\mathfrak{q}\mathcal{O}_M = \mathfrak{q}_1 \cdots \mathfrak{q}_r,$$

where $\mathfrak{q}_i = \sigma_i\mathfrak{p} \cap \mathcal{O}_M$. *Moreover,* $f(\mathfrak{q}_i|\mathfrak{q}) = m_i$.

We have thus generalized all the concepts we had to the relative setting. The main tool for this was clearly the notion of localization and the discrete valuation rings, exploiting the fact that Dedekind domains with finitely many prime ideals are PIDs.

There is an even more conceptual approach to this. One of the main annoying factor of the localization approach is that, given a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, $\mathcal{O}_{K,\mathfrak{p}}$ is something that ultimately depends on K – for example, $\mathrm{Frac}(\mathcal{O}_{K,\mathfrak{p}}) = K$. It turns out that there is a world of "local fields" where you obtain something that does not depend on K but rather depend on the "prime ideal" $\mathfrak{p}$ in some sense, if you localize in a clever way!

The idea comes from the topology as used in real analysis. Recall that the field of real numbers $\mathbb{R}$ is obtained by taking the completion of rational numbers by giving some notion of the distance between two numbers. One can mimic this construction for the prime ideals and number fields, as follows.

Definition 13.8 (Absolute value, valued field, open/closed disk, topology)**.** On a field F, an **absolute value** is a map $|\cdot| : F \to \mathbb{R}_{\geq 0}$ that satisfies the following conditions:

- $|xy| = |x||y|$;
- $|x| = 0$ if and only if $x = 0$;
- $|x + y| \leq |x| + |y|$.

If the third condition, the **triangle inequality**, can be rather strengthened to be the **strong triangle inequality**,

$$|x + y| \leq \max(|x|, |y|),$$

then we say that $|\cdot|$ is a **non-archimedean absolute value**. Otherwise, we say that $|\cdot|$ is an **archimedean absolute value**. A non-archimedean absolute value is **discrete** if there exists $0 < \alpha < 1$ such that the image of $|\cdot|$ is equal to $\alpha^{\mathbb{Z}} \cup \{0\}$. In that case, the map $v : F \to \mathbb{Z} \cup \{\infty\}$ given by $v(x) = \log_\alpha |x|$ (with $v(0) = \infty$) defines a normalized valuation on F, and the valuation ring

$$\mathcal{O}_F := \{x \in F \mid v(x) \geq 0\} = \{x \in F \mid |x| \leq 1\},$$

is a discrete valuation ring. Conversely, by taking $0 < \alpha < 1$ and doing the construction in reverse, a discrete valuation on F defines a discrete non-archimedean absolute value on F. As the two notions are equivalent, we can talk about a uniformizer in a discretely valued field.

If a field F is equipped with an absolute value, we call F a **valued field** (and a **discretely valued field** if the absolute value is discrete). On a valued field F, we define the **open disk** (**closed disk**, respectively) of radius $r > 0$ at $a \in F$ as

$$D(a,r) := \{x \in F \mid |x-a| < r\} \quad (\overline{D}(a,r) := \{x \in F \mid |x-a| \leq r\}, \text{ respectively}).$$

In this case, F is naturally equipped with the topology generated by the open disks. A valued field F is **complete** if every Cauchy sequence converges.

The two absolute values $|\cdot|_1, |\cdot|_2$ on a field F are **equivalent** if there is $\alpha \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^\alpha$ for all $x \in F$. The equivalent absolute values induce the same topology on F.

Proposition 13.9. *Let F be a field with two non-archimedean absolute values $|\cdot|_1, |\cdot|_2$. If they induce the same topology on F, the two absolute values are equivalent.*

Proof. Suppose that $|\cdot|_1, |\cdot|_2$ induce the same topology but are not equivalent. Let $D(a,r)_1, D(a,r)_2$ be the open disks on F defined using $|\cdot|_1, |\cdot|_2$, respectively. As the two topologies agree, it follows that, for any $x \in D(a,r)_1$, there exists $r' > 0$ such that $D(x,r')_2 \subset D(a,r)_1$, and vice versa. Let $x \neq a$, and $s = |x-a|_1$, and choose $r' < s$ so that $a \notin D(x,r')_2$.

As $|\cdot|_1, |\cdot|_2$ are inequivalent, $\frac{\log|\cdot|_1}{\log|\cdot|_2}$ is a nonconstant function on F. Let $\alpha, \beta \in F^\times$ be such that $\frac{\log|\alpha|_1}{\log|\alpha|_2} \neq \frac{\log|\beta|_1}{\log|\beta|_2}$. Without loss of generality, assume that $\frac{\log|\alpha|_1}{\log|\alpha|_2} > \frac{\log|\beta|_1}{\log|\beta|_2}$. Also, by replacing $|\cdot|_1$ with an equivalent absolute value, we can assume that $|\beta|_1 = |\beta|_2$, and $|\alpha|_1 > |\alpha|_2$. Let $C = |\beta|_1 = |\beta|_2$, and maybe by possibly replacing β by β^{-1}, we can assume that $C > 1$. Then $\log_C |\alpha|_1 > \log_C |\alpha|_2$. Therefore, there is $N \in \mathbb{N}$ big enough so that $N(\log_C |\alpha|_1 - \log_C |\alpha|_2) > 1$, which implies that there is some integer $M \in \mathbb{Z}$ such that $N \log_C |\alpha|_1 > M > N \log_C |\alpha|_2$. This is equivalent to $|\alpha|_1^N > C^M > |\alpha|_2^N$. If we let $\gamma = \alpha^N/\beta^M$, then $|\gamma|_1 > 1$ and $|\gamma|_2 < 1$. Let $\gamma' \in F$ be similarly defined so that $|\gamma'|_1 < 1$ and $|\gamma'|_2 > 1$.

Now, for $n \in \mathbb{N}$, let

$$x_n := x\frac{\gamma'^n}{1+\gamma'^n} + a\frac{\gamma^n}{1+\gamma^n}.$$

This has the property that $\lim_{n\to\infty} |x_n|_1 = x$ and $\lim_{n\to\infty} |x_n|_2 = a$. As the two absolute values induce the same topology, it follows that any open set containing x also contains a and vice versa, which is definitely impossible if $x \neq a$, so a contradiction. □

Example 13.10.

(1) For any field F, the map $|\cdot| : F \to \mathbb{R}_{\geq 0}$ defined by

$$|x| = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0, \end{cases}$$

is an absolute value, called the **trivial absolute value**. Any absolute value that is not trivial is called **nontrivial**.

(2) On $\mathbb{Q}$, for each rational prime p, we can define a discrete non-archimedean absolute value, called the p-**adic absolute value**,

$$|x|_p := p^{-v_p(x)} \quad (|0|_p = 0).$$

(3) On $\mathbb{Q}$, we can define an archimedean absolute value, called the ∞-**adic absolute value** (or just called the archimedean absolute value),

$$|x|_\infty := |x| \quad \text{(the usual absolute value of real numbers)}.$$

The following is not really crucial in the development of the theory but certainly nice to have. The proof can be found in the handout linked in the webpage.

Theorem 13.11 (Ostrowski's theorem)**.** *The absolute values $|\cdot|_p$ for $p \leq \infty$ on $\mathbb{Q}$ are mutually not equivalent to each other. Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some $p \leq \infty$.*

The crucial idea is that **complete valued fields are "local"**, i.e. something that "only depends on the prime ideal, not a number field."

Definition 13.12 (Completion)**.** Let K be equipped with an absolute value $|\cdot|$. Let $\widehat{K}$ be the **completion** of K with respect to the induced topology; namely, $\widehat{K}$ is the colletion of equivalence classes of Cauchy sequences, equipped with natural addition, multiplication, topology, etc. Furthermore, the absolute value on K naturally extends to an absolute value on $\widehat{K}$ as $|(x_1, x_2, \cdots)| := \lim_{n\to\infty} |x_n|$. The completion $\widehat{K}$ together with the natural absolute value defines a **complete valued field**. If K is a discretely valued field, $\widehat{K}$ is a **complete discretely valued field**.

Given a discrete valuation ring A with a uniformizer π, its **completion** $\widehat{A}$ is defined as[20][21]

$$\widehat{A} := \{(a_1, a_2, \cdots) \mid a_n \in A/\pi^n A,\ a_{n+1} \pmod{\pi^n} = a_n\},$$

which can be endowed a natural ring structure via entrywise addition and multiplication. Furthermore, $\widehat{A}$ is a discrete valuation ring as $\widehat{A}$ is equipped with a discrete valuation $v(a_1, a_2, \cdots) = \min(n \mid a_n \neq 0 \pmod{\pi^n})$ (with $v(0, 0, \cdots) = \infty$).

The completion admits a natural injective ring homomorphism, $A \hookrightarrow \widehat{A}$, $n \mapsto (n, n, \cdots)$. A discrete valuation ring A is **complete** if the natural homomorphism $A \hookrightarrow \widehat{A}$ is an isomorphism, i.e. when $A \cong \widehat{A}$.

The two notions (complete discretely valued fields and complete discrete valuation rings) are very much compatible with each other.

Proposition 13.13.

(1) Let K be a complete discretely valued field. Then, $\mathcal{O}_K$ is a complete discrete valuation ring. Furthermore, $\mathcal{O}_K$ is complete as a topological space (with respect to the subspace topology).

(2) Let A be a complete discrete valuation ring. Then, $\mathrm{Frac}(A)$ is a complete discretely valued field. Furthermore, $A = \mathcal{O}_{\mathrm{Frac}(A)}$.

[20]The ring of p-adic integers is defined in the same way in Exercise 11.3. This construction, i.e. taking the ring of compatible sequences, is called the **inverse limit**.

[21]The construction of $\widehat{A}$ is independent of the choice of a uniformizer as $\pi^n A = \mathfrak{m}_A^n$.

Proof. (1) That $\mathcal{O}_K$ is complete as a topological space is immediate as $\mathcal{O}_K \subset K$ is a closed subspace (cut out by an inequality involving $\leq$), and a closed subspace of a complete topological space is complete. To show that $\mathcal{O}_K$ is a complete discrete valuation ring, we need to show that $\mathcal{O}_K \hookrightarrow \widehat{\mathcal{O}_K}$ is surjective. Let $(a_1, a_2, \cdots)$ be a compatible sequence, $a_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$ for a uniformizer π. As $\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/\pi^n\mathcal{O}_K$ is surjective for any n, we can choose $\overline{a}_n \in \mathcal{O}_K$ whose mod π^n congruence class is $a_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$. Then, $(\overline{a}_1, \overline{a}_2, \cdots)$ is a Cauchy sequence in $\mathcal{O}_K$, which must converge to $a \in \mathcal{O}_K$. As $a \pmod{\pi^n} = \overline{a}_n \pmod{\pi^n} = a_n$, $(a_1, a_2, \cdots) \in \widehat{\mathcal{O}_K}$ is in the image of the natural map $\mathcal{O}_K \hookrightarrow \widehat{\mathcal{O}_K}$, so it is surjective, as desired.

(2) That $A = \mathcal{O}_{\mathrm{Frac}(A)}$ is a general feature of a discrete valuation ring. Let $(b_1, b_2, \cdots)$ be a Cauchy sequence in $\mathrm{Frac}(A)$. As the limit $\lim_{n\to\infty} v(b_n)$ must exist, it follows that $\lim_{n\to\infty} v(b_n) = N$ for some $N \in \mathbb{Z}$, and by the discreteness of the valuation, for this limit to exist, it must be true that there exists $N_0 > 0$ such that $v(b_n) = N$ for every $n \geq N_0$. We can truncate the Cauchy sequence to start from $n = N_0$, and multiply the whole sequence by π^{-N_0} for a chosen uniformizer π, so that we can assume that $v(b_n) = 0$ for all n (equivalently, $|b_n| = 1$). In particular, $b_n \in A$ for all n.

Note that, for any $n \geq 1$, the fact that $(b_1, b_2, \cdots)$ is a Cauchy sequence implies that $(b_1 \pmod{\pi^n}, b_2 \pmod{\pi^n}, \cdots)$ must stabilize in $A/\pi^n A$ (i.e. there exists $M_n > 0$ and $\overline{b}_n \in A/\pi^n A$ such that, for all $m \geq M_n$, $b_m \pmod{\pi^n} = \overline{b}_n$). Then, $(\overline{b}_1, \overline{b}_2, \cdots)$ is a compatible sequence, which must come from $b \in A$ as A is a complete discrete valuation ring. It can be easily seen that b indeed can be served as the limit of the Cauchy sequence $(b_1, b_2, \cdots)$. Therefore, A is a complete discretely valued field.

□

Proposition 13.14. *Let A be a discrete valuation ring with a uniformizer $\pi \in A$. Then, the image of π under the natural map $A \hookrightarrow \widehat{A}$ is also a uniformizer of $\widehat{A}$, which we will also denote π. For any $n \geq 1$, the natural map induces an isomorphism*

$$A/\pi^n A \xrightarrow{\sim} \widehat{A}/\pi^n \widehat{A}.$$

In particular, the residue fields of A and $\widehat{A}$ are isomorphism, $k_A \xrightarrow{\sim} k_{\widehat{A}}$.

Proof. That the image of π is a uniformizer is immediate as the normalized valuation stays the same. The natural map $A \hookrightarrow \widehat{A}$ induces a natural map $A \to \widehat{A}/\pi^n\widehat{A}$. By considering the corresponding normalized discrete valuation, we see that an element $a \in A$ is in the kernel of this map if and only if $v(a) \leq n$, or if $a \in \pi^n A$. Therefore, we get an injective map $A/\pi^n \hookrightarrow \widehat{A}/\pi^n\widehat{A}$. If $(a_1, a_2, \cdots) \in \widehat{A}$ is a compatible sequence, choose an element $a \in A$ whose mod π^n reduction is a_n. Then, $a - (a_1, a_2, \cdots) = (0, 0, \cdots, 0, b_{n+1}, b_{n+2}, \cdots)$ where $b_{n+k} \in A/\pi^{n+k}A$ is divisible by π^n. Therefore, $a - (a_1, a_2, \cdots) \in \pi^n\widehat{A}$, which implies that the natural map $A/\pi^n \hookrightarrow \widehat{A}/\pi^n\widehat{A}$ is surjective, as desired. □

Definition 13.15 (Local fields)**.** A **local field** is a complete discretely valued field whose residue field is a finite field. A local field is p-**adic** if its residue field is of characteristic p.

Example 13.16.

(1) The field of p-adic numbers, $\mathbb{Q}_p$ (cf. Exercise 11.3), is a p-adic local field. More generally, for a number field K and a maximal ideal $\mathfrak{p} \subset \mathcal{O}_K$, the **$\mathfrak{p}$-adic localization of** K, denoted $K_\mathfrak{p}$, is the local field obtained by

$$K_\mathfrak{p} = \mathrm{Frac}(\widehat{\mathcal{O}_{K,\mathfrak{p}}}).$$

Alternatively, it can be obtained as the completion of K using a discrete valuation on K coming from the discrete valuation of $\mathcal{O}_{K,\mathfrak{p}}$. It is p-adic for $p \in \mathbb{Z}$ such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

(2) The field of formal Laurent series with $\mathbb{F}_p$-coefficients,

$$\mathbb{F}_p((X)) := \left\{ \sum_{n=-N}^{\infty} a_n X^n \mid a_n \in \mathbb{F}_p \right\},$$

is a p-adic local field, with the discrete valuation given by $v\left(\sum a_n X^n\right) = \min(n \mid a_n \neq 0)$. The main difference of this example from the prior examples is that $\mathbb{F}_p((X))$ is itself a **field of characteristic** p, unlike $\mathbb{Q}_p$ which is a field of characteristic 0. In this course, we will be only concerned about local fields of characteristic 0.[22]

A really nice feature about local fields is that, as you take the completion, you also pick a single prime ideal "upstairs". This comes from what's known as **Hensel's lemma**.

Theorem 13.17 (Hensel's lemma)**.** *Let A be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$ and residue field k. Let $f(X) \in A[X]$ be a polynomial, and let $\overline{f}(X) \in k[X]$ be its mod $\mathfrak{m}$ reduction. Let $\overline{f}(X) = \overline{g}(X)\overline{h}(X)$, where $\overline{g}(X), \overline{h}(X) \in k[X]$ are coprime to each other. Then, there exist $g(X), h(X) \in A[X]$ whose mod $\mathfrak{m}$ reductions are $\overline{g}(X), \overline{h}(X)$, respectively, and such that $\deg g = \deg \overline{g}$.*

Proof. Let π be a uniformizer of A. Let $g_0(X), h_0(X) \in A[X]$ be such that the mod π reduction of $g_0(X)$ is $\overline{g}(X)$, the mod π reduction of $h_0(X)$ is $\overline{h}(X)$, and $\deg \overline{g}(X) = \deg g_0(X)$, $\deg \overline{h}(X) = \deg h_0(X)$. Then, the polynomials $g_0(X), h_0(X)$ have the properties that

$$f(X) \equiv g_0(X)h_0(X) \pmod{\pi}, \quad \deg g_0(X) = \deg \overline{g}(X), \quad \deg h_0(X) \leq \deg f(X) - \deg \overline{g}(X).$$

We would like to show that, by induction, there are polynomials $p_i(X), q_i(X) \in A[X]$, such that $\deg p_i(X) < \deg \overline{g}(X)$, $\deg q_i(X) \leq \deg f(X) - \deg \overline{g}(X)$, and if we define

$$g_n(X) := g_0(X) + \pi p_1(X) + \pi^2 p_2(X) + \cdots + \pi^n p_n(X),$$

$$h_n(X) := h_0(X) + \pi q_1(X) + \pi^2 q_2(X) + \cdots + \pi^n q_n(X),$$

[22] It is interesting that $\mathbb{Q}_p$, despite being a characteristic 0 field, is something that arose as patching characteristic p pieces. In general, a p-adic local field can be either of characteristic 0 or of characteristic p. If it is of characteristic 0, we call it a **mixed characteristic local field**, and if it is of characteristic p, we call it a **equi-characteristic local field**.

then $f(X) \equiv g_n(X)h_n(X) \pmod{\pi^{n+1}}$, for every $n \geq 0$. If we indeed prove this, then we can let $g(X) := \lim_{n\to\infty} g_n(X)$, $h(X) := \lim_{n\to\infty} h_n(X)$ (well-defined as A is complete!), and $\deg g(X) = \deg g_0(X) = \deg \overline{g}(X)$, with $f(X) = g(X)h(X)$. Note that the induction hypothesis guarantess that $\deg g_n(X) = \deg \overline{g}(X)$ and $\deg h_n(X) \leq \deg f(X) - \deg \overline{g}(X)$.

The base case is already given. Suppose that we have the congruence $f(X) \equiv g_n(X)h_n(X) \pmod{\pi^{n+1}}$ for some n. Let $d_n(X) = \frac{f(X)-g_n(X)h_n(X)}{\pi^{n+1}}$. For the induction hypothesis to hold for $n+1$, we want

$$\pi^{n+2} | \left(f(X) - (g_n(X) + \pi^{n+1}p_{n+1}(X))(h_n(X) + \pi^{n+1}q_{n+1}(X))\right),$$

or

$$f(X) - g_n(X)h_n(X) \equiv \pi^{n+1}(p_{n+1}(X)h_n(X) + q_{n+1}(X)g_n(X)) \pmod{\pi^{n+2}}.$$

Note that both sides are divisible by π^{n+1} by the induction hypothesis. Thus, we want

$$d_n(X) \equiv p_{n+1}(X)h_n(X) + q_{n+1}(X)g_n(X) \equiv p_{n+1}(X)h_0(X) + q_{n+1}(X)g_0(X) \pmod{\pi},$$

as $h_n(X) \equiv h_0(X) \pmod{\pi}$ and $g_n(X) \equiv g_0(X) \pmod{\pi}$, respectively.

Since $k[X]$ is a Euclidean domain, there are $\overline{a}(X), \overline{b}(X) \in k[X]$ such that $\overline{a}(X)\overline{g}(X) + \overline{b}(X)\overline{h}(X) \equiv 1 \pmod{\pi}$. Pick the lifts $a(X), b(X) \in A[X]$ of $\overline{a}(X), \overline{b}(X) \in k[X]$. Then, if we let $r_{n+1}(X) = d_n(X)b(X)$ and $s_{n+1}(X) = d_n(X)a(X)$, then

$$r_{n+1}(X)h_0(X) + q_{n+1}(X)g_0(X) \equiv d_n(X) \pmod{\pi}.$$

This is not enough, as the polynomials $r_{n+1}(X), s_{n+1}(X)$ will probably have too large degrees, whereas we want $\deg p_{n+1}(X) < \deg \overline{g}(X)$ and $\deg q_{n+1}(X) \leq \deg f(X) - \deg \overline{g}(X)$. We first use the division algorithm in $k[X]$[23], so that

$$\overline{d}_n(X)\overline{b}(X) = \overline{\alpha}(X)\overline{g}(X) + \overline{\beta}(X), \quad \overline{\alpha}(X), \overline{\beta}(X) \in k[X],\ \deg \overline{\beta}(X) < \deg \overline{g}(X).$$

Take a lift $\alpha(X), \beta(X) \in A[X]$ of $\overline{\alpha}(X), \overline{\beta}(X) \in k[X]$ preserving their degrees. Then, $r_{n+1}(X) = d_n(X)b(X) \equiv \alpha(X)g_0(X) + \beta(X) \pmod{\pi}$, so we have

$$\beta(X)h_0(X) + (\alpha(X)h_0(X) + q_{n+1}(X))g_0(X) \equiv d_n(X) \pmod{\pi}.$$

Since $\deg \beta(X) = \deg \overline{\beta}(X) < \deg \overline{g}(X)$, we can safely take $p_{n+1}(X) = \beta(X)$. We also take $q_{n+1}(X)$ be the lift of mod π reduction of $\alpha(X)h_0(X) + q_{n+1}(X)$ where $\deg q_{n+1}(X)$ is the same as the degree of its mod π reduction. We would then like to show that $\deg q_{n+1}(X) \leq \deg f(X) - \deg \overline{g}(X)$. Let $\overline{\gamma}(X)$ be the mod π reduction of $q_{n+1}(X)$. Then, it is equivalent to showing that $\deg \overline{\gamma}(X) \leq \deg f(X) - \deg \overline{g}(X)$. Note that we have

$$\overline{\beta}(X)\overline{h}(X) + \overline{\gamma}(X)\overline{g}(X) = \overline{d_n}(X),$$

in $k[X]$, where $\overline{d_n}(X)$ is the mod π reduction of $d_n(X)$. Note that $\deg \overline{d_n}(X) \leq \deg f(X)$, as

$$\deg \overline{d_n}(X) \leq \deg d_n(X) = \deg\left(f(X) - g_n(X)h_n(X)\right) \leq \max(\deg f(X), \deg g_n(X) + \deg h_n(X)) = \deg f(X).$$

[23] You can't do this on $A[X]$ as we don't know whether $A[X]$ is a Euclidean domain or not.

Thus, $\overline{\gamma}(X)\overline{g}(X) = \overline{d_n}(X) - \overline{\beta}(X)\overline{h}(X)$ implies that

$$\deg \overline{\gamma}(X) \le \max(\deg \overline{d_n}(X), \deg \overline{\beta}(X) + \deg \overline{h}(X)) - \deg \overline{g}(X)$$

$$\le \max(\deg f(X), \deg \overline{g}(X) + \deg \overline{h}(X)) - \deg \overline{g}(X) = \deg f(X) - \deg \overline{g}(X),$$

as desired. □

Here comes the real usefulness of local fields: they behave extremely well with respect to the extensions.

Theorem 13.18 (Complete absolute value extends automatically)**.** *Let L be a complete discretely valued field of characteristic 0 with an absolute value $|\cdot|$. Let K/L be a field extension of degree n.*

(1) An element $x \in K$ is integral over $\mathcal{O}_L$ if and only if $N_{K/L}(x) \in \mathcal{O}_L$.

(2) The absolute value $|\cdot|_K$ on K, defined as

$$|x|_K := |N_{K/L}(x)|^{1/n}, \quad x \in K,$$

is the unique absolute value on K that extends $|\cdot|$; namely, $|y| = |y|_K$ for $y \in L$.

(3) Under the absolute value $|\cdot|_K$, K becomes a complete discretely valued field.

(4) The valuation ring $\mathcal{O}_K$ is the integral closure of $\mathcal{O}_L$ in K.

(5) Let $\mathfrak{p} \subset \mathcal{O}_L$, $\mathfrak{q} \subset \mathcal{O}_K$ be the maximal ideals, and let $v_\mathfrak{p}, v_\mathfrak{q}$ be the normalized discrete valuations on $\mathcal{O}_L$, $\mathcal{O}_K$, so that $|y| = \alpha^{v_\mathfrak{p}(y)}$ for $y \in L$. Then,

$$|x|_K = \alpha^{\frac{1}{e(\mathfrak{q}|\mathfrak{p})} v_\mathfrak{q}(x)}, \quad x \in K.$$

(6) We have $v_\mathfrak{q}(x) = \frac{1}{f(\mathfrak{q}|\mathfrak{p})} v_\mathfrak{p}(N_{K/L}(x))$ for $x \in K$.

Proof. Let π be a uniformizer of L.

(1) It is obvious that if $x \in K$ is integral over $\mathcal{O}_L$, $N_{K/L}(x) \in \mathcal{O}_L$. Conversely, suppose that $N_{K/L}(x) \in \mathcal{O}_L$. Then, the minimal polynomial of x over L, say $f(X) \in L[X]$, is monic and has the constant coefficient in $\mathcal{O}_L$. We would like to show that $f(X) \in \mathcal{O}_L[X]$. If not, then there is a positive power π^m such that $\pi^m f(X) \in \mathcal{O}_L[X]$ whose mod π reduction, which we denote $\overline{\alpha}(X)$, is not zero. As $\overline{\alpha}(X)$ has constant term 0, we have the factorization $\overline{\alpha}(X) = \overline{\beta}(X)X^d$ where $d \ge 1$ and $\overline{\beta}(X) \in k[X]$ is not divisible by X. By Hensel's lemma, there is a factorization $\pi^m f(X) = g(X)h(X)$, $g(X), h(X) \in \mathcal{O}_L[X]$, where $g(X) \equiv X^d \pmod{\pi}$, $h(X) \equiv \overline{\beta}(X) \pmod{\pi}$, and $\deg g(X) = d$. Note that $1 \le g \le \deg \overline{\alpha}(X) < \deg f(X)$, as the coefficient of the highest power term of $\pi^m f(X)$ is divisible by π. On the other hand, $L[X]$ is a UFD, so any polynomial in $L[X]$ dividing $\pi^m f(X)$ must be either a unit or the polynomial itself times a unit. As all units are of degree 0 in $L[X]$, $0 < \deg g(X) < \deg f(X)$ gives a contradiction.

(2) It is obvious that $|\cdot|_K$ extends $|\cdot|$, and that $|\cdot|_K$ is multiplicative. Also, $|x|_K = 0$ if and only if $N_{K/L}(x) = 0$ if and only if $x = 0$. To show the strong triangle inequality, assume that $x, y \in K$ such that $x, y \neq 0$ and $|x|_K \leq |y|_K$, and we want to show that $|x + y|_K \leq |y|_K$. Let $x = yz$, so that $|z|_K \leq 1$. Then, this means that $|N_{K/L}(z)| \leq 1$, which implies that $N_{K/L}(z) \in \mathcal{O}_L$, which by (1) implies that z is in the integral closure of $\mathcal{O}_L$ in K. As the integral closure is a ring, $z+1$ is integral over $\mathcal{O}_L$, which implies that $N_{K/L}(z+1) \leq 1$, or $|z + 1|_K \leq 1$. Thus, $|x + y|_K \leq |x|_K$, which is the strong triangle inequality we wanted.

(3) We only need to show that K is complete with respect to $|\cdot|_K$. Let $e_1, \cdots, e_n$ be an L-basis of K. Then, by the triangle inequality, a sequence $x_i = a_{i,1}e_1 + \cdots + a_{i,n}e_n$ of $x_i \in K$ is a Cauchy sequence if and only if the sequences $\underline{a}_j = \{a_{1,j}, a_{2,j}, \cdots\}$ is a Cauchy sequence for $j = 1, 2, \cdots, n$. Since L is complete, if $x_1, \cdots$ is a Cauchy sequence, then $\underline{a}_j$ converges to $a_j \in L$, and therefore $x_1, \cdots$ converges to $a_1e_1 + \cdots + a_ne_n$.

(4) This follows from (1).

(5) Note that, as $\mathcal{O}_K$ is a discrete valuation ring, $\mathfrak{p}\mathcal{O}_K$ factorizes into a power of $\mathfrak{q}$, and the exponent is precisely $e(\mathfrak{q}|\mathfrak{p})$. Namely,

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}.$$

To deduce the formula, we only need to show that $\frac{1}{e(\mathfrak{q}|\mathfrak{p})}v_\mathfrak{q}(x) = v_\mathfrak{p}(x)$ for $x \in L$, or that $v_\mathfrak{q}(\pi) = e(\mathfrak{q}|\mathfrak{p})$. This however follows from the above factorization as $\pi\mathcal{O}_K = \mathfrak{p}\mathcal{O}_K = \mathfrak{q}^{e(\mathfrak{q}|\mathfrak{p})}$.

(6) This follows from (5) and (2), as $n = e(\mathfrak{q}|\mathfrak{p})f(\mathfrak{q}|\mathfrak{p})$.

□

Therefore, as soon as you move on to the world of complete fields, we basically only need to deal with one prime ideal at a time, and everything is a discretely valued field/discrete value ring! This is extremely useful especially when you want to know how ramified a prime ideal upstairs is (out of e, f, g, you removed g from the discussion, and knowing e is pretty much the same as knowing f).

Definition 13.19 (Unramified/ramified/totally ramified extensions of local fields)**.** Let K/L be an extension of local fields of degree n. Let $e_{K/L}$, $f_{K/L}$ be the ramification index and the residue degree of the unique maximal ideal of $\mathcal{O}_K$ over the unique maximal ideal of $\mathcal{O}_L$, respectively. We say K/L and $\mathcal{O}_K/\mathcal{O}_L$ are **unramified extensions** if $e_{K/L} = 1$, and **ramified** if $e_{K/L} > 1$. We say K/L and $\mathcal{O}_K/\mathcal{O}_L$ are **totally ramified extensions** if $f_{K/L} = 1$.

The following is immediate.

Proposition 13.20. *If $K/L/M$ is a tower of local fields, one has*

$$e_{K/M} = e_{K/L}e_{L/M}, \quad f_{K/M} = f_{K/L}f_{L/M}.$$

Proof. The multiplicativity of f follows from the residue field considerations, and from this the multiplicativity of e follows. □

Unramified extensions and totally ramified extensions of local fields are very easy to understand. For unramified extensions we have:

Theorem 13.21 (Unramified extensions of local fields)**.** *Let L be a p-adic local field of characteristic 0. Let $\mathfrak{p}$ be the unique maximal ideal of $\mathcal{O}_L$, and let $k_L = \mathcal{O}_L/\mathfrak{p}$ be the residue field of $\mathcal{O}_L$, which is a finite field. Also, let $\pi \in \mathcal{O}_L$ be a uniformizer of L.*

(1) For every K/L field extension of degree n, which is again a p-adic local field thanks to Theorem 13.18, there exists $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O}_L[\alpha]$.

(2) For a finite field l that is an extension of the finite field k_L, there exists an unramified extension K/L whose residue field extension k_K/k_L is precisely l/k_L.

(3) Let $K_1, K_2/L$ be two local field extensions, where K_1/L is unramified. Then, there is a natural bijection between the set of L-algebra homomorphisms from K_1 to K_2 and the set of k_L-algebra homomorphisms from k_{K_1} to k_{K_2},

$$\mathrm{Hom}_L(K_1, K_2) \xrightarrow{\sim} \mathrm{Hom}_{k_L}(k_{K_1}, k_{K_2}),$$

defined as follows. Given $f : K_1 \to K_2$, define $\overline{f} : k_{K_1} \to k_{K_2}$ as, for $x \in \mathcal{O}_{K_1}$, $\overline{f}(\overline{x}) = \overline{f(x)}$, where $\overline{x}$ and $\overline{f(x)}$ are the images of $x \in \mathcal{O}_{K_1}$, $f(x) \in \mathcal{O}_{K_2}$ in their residue fields, respectively.

(4) For each l/k_L, the unramified extension constructed in (2) is unique up to isomorphism (i.e. given l, any two unramified extensions of (2) are isomorphic to each other). Furthermore, unramified extensions are Galois.

*(5) Given a local field extension K/L of degree n, there is a unique intermediate field K_0/L that contains every unramified extensions of L in K (**maximal unramified extension** of L in K). The degree is $[K_0 : L] = f_{K/L}$, and K/K_0 is totally ramified of degree $[K : K_0] = e_{K/L}$.*

Proof. (1) By primitive element theorem, the residue field of K, k_K, is of the form $k_L(\alpha_0)$ for some $\alpha_0 \in k_K$, where k_L is the residue field of L. Let $g(X) \in \mathcal{O}_L[X]$ be a monic lift of the minimal polynomial of α over k_L, which must be of degree $f = [k_K : k_L]$. Let $\alpha_0 \in \mathcal{O}_K$ be any lift of $\alpha_0 \in k_K$. Then, $g(\alpha_0) \in \mathcal{O}_K$ is divisible by π_K, a uniformizer of K. Note that, if $g(\alpha_0)$ is divisible by π_K^2, then

$$g(\alpha_0 + \pi_K) \equiv g(\alpha_0) + \pi_K g'(\alpha_0) \pmod{\pi_K^2},$$

is not divisible by π_K^2, as $g'(\alpha_0)$ is not divisible by π_K, which is just the manifestation of the fact that k_K/k_L is a separable extension. Thus, either $v_K(g(\alpha_0)) = 1$ or $v_K(g(\alpha_0+\pi_K)) = 1$, where v_K is the normalized discrete valuation on K. Let $\alpha = \alpha_0$ or $\alpha_0 + \pi_K$ so that $v_K(g(\alpha)) = 1$, or that $g(\alpha) \in \mathcal{O}_K$ is a uniformizer in K.

Our claim is now that $\mathcal{O}_K = \mathcal{O}_L[\alpha]$. Let $n = [K : L]$. It is sufficient to prove that $\mathcal{O}_K$ is generated by $1, \alpha, \cdots, \alpha^{n-1}$ as an $\mathcal{O}_L$-module. Let $M \subset \mathcal{O}_K$ be the $\mathcal{O}_L$-submodule

generated by $1, \alpha, \cdots, \alpha^{n-1}$. Then, by Nakayama's lemma (Lemma 11.14), $M = \mathcal{O}_K$ (as an $\mathcal{O}_L$-module) if and only if $M/\mathfrak{p}M = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, where $\mathfrak{p} \subset \mathcal{O}_L$ is the unique maximal ideal. Note that $\mathfrak{p}\mathcal{O}_K = \mathfrak{q}^e$, where $\mathfrak{q} \subset \mathcal{O}_K$ is the unique maximal ideal, and $\mathfrak{q} = (g(\alpha))$. Thus, $\mathfrak{p}\mathcal{O}_K = (g(\alpha)^e)$. Therefore, $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is represented by elements $b_0 + b_1 g(\alpha) + \cdots + b_{e-1} g(\alpha)^{e-1}$, where $b_0, b_1, \cdots, b_{e-1} \in \mathcal{O}_K$, and they are insensitive to differences by elements in $g(\alpha)\mathcal{O}_K = \mathfrak{q}$. Note that $\mathcal{O}_K/\mathfrak{q}$ is represented by elements of the form $a_0 + a_1\alpha + \cdots + a_{f-1}\alpha^{f-1}$, $a_0, \cdots, a_{f-1} \in \mathcal{O}_L$, and they are insensitive to differences by elements in $\mathfrak{p}$. Thus, every element in $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is generated by $\alpha^i g(\alpha)^j$, $0 \leq i \leq f-1$, $0 \leq j \leq e-1$. Since $g(\alpha)$ is a degree f polynomial in α, so $\alpha^i g(\alpha)^j$ is expressed as a polynomial in α with degree $\leq (f-1) + f(e-1) = ef - 1 = n - 1$, which implies that $M/\mathfrak{p}M = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$, as desired.

(2) By primitive element theorem, we can write $l = k_L(\overline{\alpha})$ for some $\overline{\alpha} \in l$, with minimal polynomial $\overline{g}(X) \in k_L[X]$ of degree $[l : k_L]$. Let $g(X) \in \mathcal{O}_L[X]$ be any monic lift of $\overline{g}(X)$. This is irreducible, as $\overline{g}(X)$ is irreducible. Let $B = \mathcal{O}_L[X]/(g(X))$. Since $\overline{g}(X)$ is irreducible, by Chinese Remainder Theorem, if we let $\mathfrak{p} \subset \mathcal{O}_L$ be the maximal ideal, then

$$B/\mathfrak{p}B = \mathcal{O}_L[X]/(\mathfrak{p}, g(X)) = k_L[X]/(\overline{g}(X)) = l,$$

which implies that $\mathfrak{p}B$ is a maximal ideal. Since $\mathfrak{p} \subset \mathcal{O}_L$ is the unique maximal ideal, $\mathfrak{p}B \subset B$ is the unique maximal ideal. Let $K = \mathrm{Frac}(B)$. Since $B \subset \mathcal{O}_K$, we have a ring homomorphism

$$l = B/\mathfrak{p}B \to \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K.$$

This map is nonzero, as 1 is sent to 1, which is nonzero. Thus, the kernel of this map is a proper ideal of l, which is a field, so a zero ideal. Thus, this homomorphism is in fact injective. Let e, f be the ramification index and the residue degree of K/L, respectively. On the other hand,

$$\#\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = (\#\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K)^e = (\#k_L)^{fe} = (\#k_L)^{[l:k_L]} = \#l,$$

so the homomorphism $B/\mathfrak{p}B \hookrightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is actually an isomorphism. By Nakayama's lemma (Lemma 11.14, applied to $\mathcal{O}_L$-modules), this implies that $B = \mathcal{O}_K$. Thus, the residue field extension of K/L is precisely l/k_L.

(3) We first need to see that the map is well-defined, which is the same as saying, given $f : K_1 \to K_2$ and $x \in \mathfrak{m}_{K_1}$ is in the maximal ideal of $\mathcal{O}_{K_1}$, $f(x) \in \mathfrak{m}_{K_2}$, the maximal ideal of $\mathcal{O}_{K_2}$. Since K_1 is unramified over L, if π is a uniformizer of L, then $\mathfrak{m}_{K_1} = \pi\mathcal{O}_{K_1}$. Since $\pi \in \mathfrak{m}_{K_2}$, so this is implied by showing that $f(x) \in \mathcal{O}_{K_2}$ if $x \in \mathcal{O}_{K_1}$. This is true because if x is integral over $\mathcal{O}_L$ then $f(x)$ is integral over $\mathcal{O}_L$. Thus, the map is well-defined. From this investigation, we know that restriction to $\mathcal{O}_{K_1}$ gives rise to

$$\mathrm{Hom}_L(K_1, K_2) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_L}(\mathcal{O}_{K_1}, \mathcal{O}_{K_2}).$$

By (1), $\mathcal{O}_{K_1} = \mathcal{O}_L[\alpha]$ for some $\alpha \in \mathcal{O}_{K_1}$ whose reduction mod π generates the residue field, i.e. $k_{K_1} = k_L[\alpha]$. Let $g(X) \in \mathcal{O}_L[X]$ be the minimal polynomial of α over L, and

let $\overline{g}(X) \in k_L[X]$ be its mod π reduction. Then, $\mathrm{Hom}_{\mathcal{O}_L}(\mathcal{O}_{K_1}, \mathcal{O}_{K_2})$ is in one-to-one correspondence with the roots of $g(X)$ in $\mathcal{O}_{K_2}$, and $\mathrm{Hom}_{k_L}(k_{K_1}, k_{K_2})$ is in one-to-one correspondence with the roots of $\overline{g}(X)$ in k_{K_2}. By Hensel's lemma, any root of $\overline{g}(X)$ in k_{K_2} lifts to a root in $\mathcal{O}_{K_2}$, so $\mathrm{Hom}_{\mathcal{O}_L}(\mathcal{O}_{K_1}, \mathcal{O}_{K_2}) \to \mathrm{Hom}_{k_L}(k_{K_1}, k_{K_2})$ is surjective. Also, since $\overline{g}(X)$ is separable, it is injective.

(4) This is an immediate consequence of (3).

(5) Let K_0/L be a field extension constructed by (2) applied to k_K/k_L. Then, (3) implies that the identity map from k_K to itself give rise to a homomorphism from K_0 to K, which must be an injection as K_0 is a field. The other properties of K_0 are clear.

□

From the above discussion, we can define the Frobenius in unramified extensions.

Definition 13.22 (Frobenius)**.** An unramified local field extension K/L is Galois by Theorem 13.21(4), and $\mathrm{Gal}(K/L)$ has a specific element called the **Frobenius**,

$$\mathrm{Fr}_{K/L} \in \mathrm{Gal}(K/L),$$

given by the element corresponding to the map $\mathrm{Fr} \in \mathrm{Gal}(k_K/k_L)$, where $\mathrm{Fr}(x) = x^{\#k_L}$.

For totally ramified extensions, we have:

Theorem 13.23 (Totally ramified extensions of local fields)**.** *A local field extension K/L is totally ramified if and only if $\mathcal{O}_K = \mathcal{O}_L[\alpha]$ for an $\alpha \in \mathcal{O}_K$ whose minimal polynomial $p_\alpha(X) \in \mathcal{O}_L[X]$ over L is Eisenstein at π.*

Here, the terminology **Eisenstein** is identical to the Eisenstein irreducibility criterion we proved for integer coefficient polynomials. Before we formally define the notion of Eisenstein polynomials in the local fields context and prove this theorem, we discuss a very general tool that is very useful in studying the factorization of polynomials in local fields, called the **Newton polygon**.

Definition 13.24 (Newton polygon)**.** Let K be a complete discretely valued field with a normalized discrete valuation v (i.e. $v(\pi) = 1$ for a uniformizer π). Given a polynomial

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in K[X],$$

with $a_n \neq 0$, the **Newton polygon** of $f(X)$, $\mathrm{NP}(f(x))$, is the lower convex hull in $\mathbb{R}^2$ of the points $(0, v(a_0)), (1, v(a_1)), \cdots, (n, v(a_n))$ (if any $a_i = 0$, then we may ignore the corresponding point). If $(a_0, b_0) = (0, v(a_0)), (a_1, b_1), \cdots, (a_r, b_r) = (n, v(a_n))$ are the breaking points of the Newton polygon, the **slopes** of the Newton polygons are the negative of the slopes of the line segments,

$$s_j = \frac{b_{j-1} - b_j}{a_j - a_{j-1}}, \quad j = 1, \cdots, r.$$

As the Newton polygon is convex, $s_1 > s_2 > \cdots > s_r$. We call $m_j := a_j - a_{j-1}$ the **multiplicity** of the slope s_j.

Example 13.25. Consider the polynomial

$$f(X) = \frac{X^6}{6} + \frac{X^5}{5} + \frac{X^4}{4} + \frac{X^3}{3} + \frac{X^2}{2} + X + 1 \in \mathbb{Q}_2[X].$$

The Newton polygon of $f(X)$ is as follows.

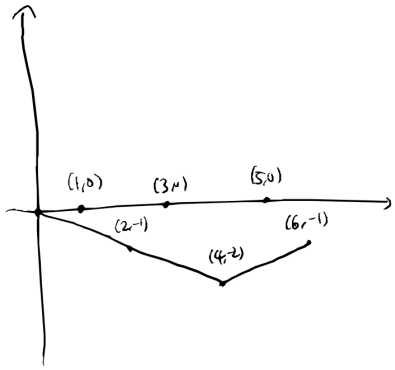


Figure 4. The Newton polygon of $f(X)$.

The breaking points are $(0,0)$, $(4,-2)$, and $(6,-1)$, and the slopes are $\frac{1}{2}$ (with multiplicity 4) and $-\frac{1}{2}$ (with multiplicity 2).

Definition 13.26. Let K be a complete discretely valued field. A polynomial $f(X) \in \mathcal{O}_K[X]$ of degree n is an **Eisenstein** polynomial if $\mathrm{NP}(f(X))$ has a unique slope $\frac{1}{n}$ with multiplicity n.

It is clear that this is directly analogous to the known definition of Eisenstein polynomials. The Eisenstein's irreducibility criterion has the following vast generalization in the local fields case.

Theorem 13.27. *Let K be a complete discretely valued field with a normalized valuation v, and $f(X) \in K[X]$ be a polynomial with the slopes $s_1 > s_2 > \cdots > s_r$ with multiplicities $m_1, m_2, \cdots, m_r$, respectively.*

(1) In the normal closure of $f(X)$ (which admits a unique extension of the valuation v), $f(X)$ has exactly m_j roots with valuation s_j.

(2) If $g(X) \in K[X]$ is another polynomial, then $\mathrm{NP}(f(X)g(X))$ is obtained from $\mathrm{NP}(f(X))$ and $\mathrm{NP}(g(X))$ by dividing $\mathrm{NP}(f(X))$ and $\mathrm{NP}(g(X))$ into striaght line segments, arranging the line segments in the order of increasing slopes, and concatenating the line segments in that order.

(3) We have $f(X) = \prod_{i=1}^{r} f_i(X)$ where $f_i(X) \in K[X]$ has only one slope, s_i, with $\deg f_i = m_i$.

(4) If $f(X)$ is irreducible, then $r = 1$ (i.e. it has only one slope). Conversely, if $r = 1$, then $s_1 = \frac{a}{\deg f(X)}$ for some $a \in \mathbb{Z}$, and if $(a, \deg f(X)) = 1$, $f(X)$ is irreducible.

Proof. (1) The slopes of the Newton polygon do not change if we multiply the whole polynomial by a nonzero number, so we may assume that $a_0 = 1$. Let L be the normal closure of K, and let $f(X)$ factorize as

$$f(X) = (1 - \alpha_1 X) \cdots (1 - \alpha_n X).$$

Arrange the roots so that

$$\begin{aligned} \rho_1 = v(\alpha_1) = v(\alpha_2) = \cdots = v(\alpha_{\mu_1}) \\ < \rho_2 = v(\alpha_{\mu_1+1}) = \cdots = v(\alpha_{\mu_1+\mu_2}) \\ < \cdots < \rho_s = v(\alpha_{\mu_1+\cdots+\mu_{s-1}+1}) = \cdots = v(\alpha_{\mu_1+\cdots+\mu_s}). \end{aligned}$$

Here, $\mu_1 + \cdots + \mu_s = n$. Then,

$$a_i = (-1)^i \sum_{1 \le j_1 < \cdots < j_i \le n} \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_i}.$$

From the valuation of the roots, for any $1 \le i \le s$,

$$v(a_{\mu_1+\cdots+\mu_i}) = v(\alpha_1 \alpha_2 \cdots \alpha_{\mu_1+\cdots+\mu_s}) = \sum_{j=1}^{i} \mu_j \rho_j.$$

This is because the sum expression for $a_{\mu_1+\cdots+\mu_i}$ has various terms, but any term other than $\alpha_1 \cdots \alpha_{\mu_1+\cdots+\mu_i}$ has strictly larger valuation. On the other hand, for any k that lies between $\mu_1 + \cdots + \mu_{i-1}$ and $\mu_1 + \cdots + \mu_i$, then there are more than one term in the sum expression for a_k that have valuation equal to

$$v(\alpha_1 \alpha_2 \cdots \alpha_k) = \left(\sum_{j=1}^{i-1} \mu_j \rho_j \right) + (k - (\mu_1 + \cdots + \mu_{i-1}))\rho_i,$$

but we know that all terms in the sum expression for a_k have valuation greater than equal to the above quantity, so we know

$$v(a_k) \ge \left(\sum_{j=1}^{i-1} \mu_j \rho_j \right) + (k - (\mu_1 + \cdots + \mu_{i-1}))\rho_i.$$

This implies that the point $(k, v(a_k))$ lies above the line connecting $(\mu_1 + \cdots + \mu_{i-1}, v(a_{\mu_1+\cdots+\mu_{i-1}}))$ and $(\mu_1 + \cdots + \mu_i, v(a_{\mu_1+\cdots+\mu_i}))$, which has a slope (in the usual sense)

$$\frac{v(a_{\mu_1+\cdots+\mu_i}) - v(a_{\mu_1+\cdots+\mu_{i-1}})}{(\mu_1 + \cdots + \mu_i) - (\mu_1 + \cdots + \mu_{i-1})} = \frac{\mu_i \rho_i}{\mu_i} = \rho_i.$$

Thus, the polygon connecting $(0, 0)$, $(\mu_1, v(a_{\mu_1}))$, $\cdots$, $(n, v(a_n))$, is a polygon consisted of line segments of increasing slopes (in the usual sense), so is convex. Thus, this must coincide with $\mathrm{NP}(f(X))$, which implies that $s_j = -\rho_j$ and $m_j = \mu_j$. Since the roots of $f(X)$ are $\alpha_1^{-1}, \cdots, \alpha_n^{-1}$, this is what we want.

(2) This immediately follows from (1).

(3) It is immediate that conjugates have the same valuation, as they have the same absolute value (as the extension of an absolute value is calculated using the norm). We retain the notation of the proof of (1), then

$$f_i(X) := (1 - \alpha_{\mu_1+\cdots+\mu_{i-1}+1}X)\cdots(1 - \alpha_{\mu_1+\cdots+\mu_i}X),$$

is stable under $\mathrm{Gal}(L/K)$, so $f_i(X) \in K[X]$.

(4) If $f(X)$ is irreducible, then $r = 1$ by (3). If $r = 1$ and $s_1 = \frac{a}{\deg f(X)}$ with $(a, \deg f(X)) = 1$, then the Newton polygon has no integer point other than the breaking points, so it cannot possibly be a concatenation of two Newton polygons that are not points. By (2), this implies that $f(X)$ cannot possibly be a product of two nontrivial polynomials.

□

Example 13.28. We can use the Newton polygon to determine the irreducibility of a polynomial in $\mathbb{Q}[X]$. Consider the polynomial

$$f(X) = \frac{X^6}{6} + \frac{X^5}{5} + \frac{X^4}{4} + \frac{X^3}{3} + \frac{X^2}{2} + X + 1 \in \mathbb{Q}[X].$$

We want to argue that $f(X)$ is irreducible in $\mathbb{Q}[X]$. From the previous example, we see that $f(X)$, seen as a polynomial in $\mathbb{Q}_2[X]$, has a 2-adic Newton polygon whose slopes are $\frac{1}{2}$ with multiplicity 4 and $-\frac{1}{2}$ with multiplicity 2. Note furthermore that the line segment corresponding to slope $\frac{1}{2}$ has one other integer point in the middle, so $f(X)$ factorizes in $\mathbb{Q}_2[X]$ as either a polynomial in degree 2 times a polynomial in degree 4 or a product of three polynomials of degree 2.

On the other hand, $f(X)$, seen as a polynomial in $\mathbb{Q}_5[X]$, has a 5-adic Newton polygon whose slopes are $\frac{1}{5}$ with multiplicity 5 and -1 with multiplicity 1, and there are no integer points on the Newton polygon other than the breaking points. Thus, $f(X)$ factorizes in $\mathbb{Q}_5[X]$ as a product of a polynomial in degree 5 and a polynomial in degree 1. This implies that if $f(X)$ were not irreducible in $\mathbb{Q}[X]$, it must be a product of a polynomial in degree 5 times a polynomial in degree 1 (by 5-adic considerations), but this factorization is impossible 2-adically, so a contradiction.

Now we can prove the characterization of totally ramified extensions of local fields.

Proof of Theorem 13.23. Assume $\alpha \in \mathcal{O}_K$ is such that its minimal polynomial $p_\alpha(X) \in \mathcal{O}_L[X]$ is Eisenstein, and that $\mathcal{O}_K = \mathcal{O}_L[\alpha]$. Let $p_\alpha(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Let $\mathfrak{p} \subset \mathcal{O}_L$ be the unique maximal ideal. Then, by Chinese Remainder Theorem, $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_L[X]/(\mathfrak{p}, p_\alpha(X)) = k_L[X]/(X^n)$, where k_L is the residue field of $\mathcal{O}_L$. Thus, the unique maximal ideal of $\mathcal{O}_K$ is $(\mathfrak{p}, \alpha)$, with ramification index n, so totally ramified.

Conversely, suppose K/L is totally ramified. Let $\pi_K \in \mathcal{O}_K$ be a uniformizer. Let $g(X) \in \mathcal{O}_L[X]$ be the minimal polynomial of π_K. If we let v be the normalized discrete valuation on L, then $v(\pi_K) = \frac{1}{n}$, as $v((\pi_K)^n) = 1$. Thus, $\mathrm{NP}(g(X))$ has a slope $\frac{1}{n}$, which implies that $\mathrm{NP}(g(X))$ must be a single line of slope $\frac{1}{n}$, or Eisenstein. □

We finally remark the connection between the ramification of local fields with the Galois theory of local fields.

Definition 13.29 (Ramification groups)**.** Let K/L be a finite extension of local fields, and let $\pi_K \in K$ be a uniformizer. For $i \geq -1$ an integer, define the i-**th ramification group** $G_i \leq \mathrm{Gal}(K/L)$ as

$$G_i := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\alpha \equiv \alpha \pmod{\pi_K^{i+1}} \text{ for all } \alpha \in \mathcal{O}_K\}.$$

We call G_0 the **inertia subgroup**[24] and G_1 the **wild inertia subgroup**.

The following is a basic relationship between the ramification groups and the unramified extensions.

Proposition 13.30. *Let K/L be a finite extension of local fields, and let $G = \mathrm{Gal}(K/L)$. Let v_K be the normalized discrete valuation on K, so that $v_K(\pi_K) = 1$ for a uniformizer π_K.*

(1) We have $G_{-1} = G$, i.e. any Galois element preserves $\mathcal{O}_K$. Moreover, any Galois element preserves v_K.

(2) The maximal unramified extension of L in K, $K/K_0/L$, is obtained by $K_0 = K^{G_0}$.

(3) If $i \geq 0$ and $\sigma \in \mathrm{Gal}(K/L)$ satisfies $\sigma\pi_K \equiv \pi_K \pmod{\pi_K^{i+1}}$, then $\sigma \in G_i$.

(4) For i big enough, $G_i = \{1\}$.

(5) For each $i \geq 0$, G_i is a normal subgroup of G_{i-1}, and G_{i-1}/G_i is abelian. Therefore, $G = \mathrm{Gal}(K/L)$ is solvable.

Proof. (1) Note that v_K is the unique extension of $v_L := v_K|_L$. On the other hand, for any $\sigma \in G$, $v_K^\sigma(x) := v_K(\sigma x)$ is also an extension of v_L, so it must be true that $v_K^\sigma(x) = v_K(x)$.

(2) By the same proof as Theorem 8.4, we see that $\mathrm{Gal}(K/L) \to \mathrm{Gal}(k_K/k_L)$ is surjective with the kernel equal to G_0, the inertia group, where k_K and k_L are residue fields of K and L, respectively. Thus, $|G_0| = e_{K/L} = [K : K_0] = |\mathrm{Gal}(K/K_0)|$. Moreover, as K/K_0 is totally ramified with $k_{K_0} = k_K$, it follows that the composition $\mathrm{Gal}(K/K_0) \to \mathrm{Gal}(K/L) \to \mathrm{Gal}(k_K/k_L)$ is a zero morphism. Thus, $\mathrm{Gal}(K/K_0) \leq G_0$, which must be equality as the two groups have the same cardinalities.

(3) By Theorem 13.23, we know that $\mathcal{O}_K = \mathcal{O}_{K_0}[\pi_K']$ for some uniformizer π_K' of $\mathcal{O}_K$. On the other hand, as π_K' is a unit times π_K, $\mathcal{O}_K = \mathcal{O}_{K_0}[\pi_K]$. Therefore, if $\sigma\pi_K \equiv \pi_K \pmod{\pi_K^{i+1}}$, then firstly $\sigma \in G_0 = \mathrm{Gal}(K/K_0)$, and therefore $\sigma\alpha \equiv \alpha \pmod{\pi_K^{i+1}}$ for any $\alpha \in \mathcal{O}_{K_0}[\pi_K] = \mathcal{O}_K$, as desired.

(4) If K/L is unramified, then $G_0 = 1$. If not, then any uniformizer π_K of K can never be an element of L, so the statement follows from (3).

[24] The convention is a bit weird, but it is because we want G_0 be the inertia subgroup.

(5) The statement for $i = 0$ follows from the analogue of Theorem 8.4 where G_0 is the kernel of the surjective map $\mathrm{Gal}(K/L) \to \mathrm{Gal}(k_K/k_L)$, as any Galois group of finite fields is a finite cyclic group. For $i \geq 1$, let π_K be a uniformizer of K and, for $\sigma \in G_{i-1}$, consider $\frac{\sigma(\pi_K)}{\pi_K}$. By definition, it satisfies

$$\frac{\sigma(\pi_K)}{\pi_K} \equiv 1 \,(\mathrm{mod}\, \pi_K^{i-1}).$$

Thus, if we let $1 + \pi_K^{i-1}\mathcal{O}_K$ as the multiplicative group of elements in $\mathcal{O}_K$ which are $\equiv 1 \,(\mathrm{mod}\, \pi_K^{i-1})$, then the natural map $G_{i-1} \to 1 + \pi_K^{i-1}\mathcal{O}_K \twoheadrightarrow \frac{1+\pi_K^{i-1}\mathcal{O}_K}{1+\pi_K^{i}\mathcal{O}_K}$ has a kernel equal to, by (3), G_i. Thus, G_i is a normal subgroup of G_{i-1}, and $G_{i-1}/G_i \hookrightarrow \frac{1+\pi_K^{i-1}\mathcal{O}_K}{1+\pi_K^{i}\mathcal{O}_K}$. Since G_{i-1}/G_i is a subgroup of an abelian group, it is abelian.

□

Furthermore, the **wild inertia group** G_1 also has a special meaning, corresponding to the **wild ramification**.

Definition 13.31 (Tamely ramified/wildly ramified extensions)**.** Let K/L be a finite extension of p-adic local fields. Such an extension is called **tamely ramified** if $(p, e_{K/L}) = 1$, and is called **wildly ramified** if p divides $e_{K/L}$.

Theorem 13.32. *Let K/L be a finite extension of p-adic local fields.*

*(1) If K/L is Galois, the **tame quotient** G_0/G_1 is a cyclic group of order prime to p.*

(2) If K/L is Galois, the wild inertia group G_1 is a p-group.

*(3) If K/L is Galois, there is a unique intermediate field $K/K_1/L$ that contains every tamely ramified extensions of L in K (**maximal tamely ramified extension** of L in K), given by $K_1 = K^{G_1}$. If $e_{K/L} = p^a b$ with $(p, b) = 1$, then $[K : K_1] = p^a$, and K/K_1 is totally wildly ramified.*

*(4) For any K/L a finite extension of local fields, the **maximal tamely ramified extension** $K/K_1/L$ exists. If $e_{K/L} = p^a b$ with $(p, b) = 1$, then $[K : K_1] = p^a$, and K/K_1 is totally wildly ramified.*

Proof. (1) Note that the proof of Proposition 13.30(5) implies that G_0/G_1 is a subgroup of $\frac{\mathcal{O}_K^\times}{1+\pi_K\mathcal{O}_K} \cong k_K^\times$, where π_K is a uniformizer of K. Since $k_K^\times$ is a cyclic group of order prime to p, the result follows.

(2) Similarly, the proof of Proposition 13.30(5) implies that, for $n \geq 1$, G_n/G_{n+1} is a subgroup of $\frac{1+\pi_K^n\mathcal{O}_K}{1+\pi_K^{n+1}\mathcal{O}_K}$. The latter group is easily seen to be isomorphic to $\mathcal{O}_K/\pi_K\mathcal{O}_K \cong k_K$, which is as an additive group of p-power order, so G_n/G_{n+1} is also a p-group. Thus, G_1 is a p-group.

(3) Note that, as K/K_1 is totally ramified, this follows from $K_0 = K^{G_0}$, G_0/G_1 is of order prime to p, and G_1 is of a p-power order.

(4) Let $\widetilde{K}/L$ be the Galois closure of K/L, and let $\widetilde{K}/\widetilde{K}_1/L$ be the maximal tamely ramified extension using (3). Let $K_1 = \widetilde{K}_1 \cap K$. Note that K_1/L is tamely ramified, as any subextension of a tamely ramified extension is tamely ramified by the multiplicativity of e. Furthermore, for any tamely ramified extension $K/M/L$, $M \subset \widetilde{K}_1$, so $M \subset K_1$. Thus, K_1 is the maximal tamely ramified extension. As $K_1 \supset K_0$, K/K_1 is totally ramified, and must be wildly ramified. As $e_{K_1/L} = [K_1 : K_0]$, the numerology follows.

□

– –

Exercise 13.1. Let K be a valued field with a non-archimedean absolute value $|\cdot|$.

(1) Let $D(a, r)$ be the open disk of radius $r > 0$ centered at $a \in K$. For any $b \in D(a, r)$, show that $D(a, r) = D(b, r)$ (i.e. any point in an open disk is its center).

(2) Show that $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is continuous.

(3) If $|\cdot|$ is discrete, show that any open disk is closed.

(4) If K is furthermore complete, show that the infinite sum $\sum_{n=1}^{\infty} a_n$ converges if and only if $\lim_{n\to\infty} a_n = 0$.

Exercise 13.2. Let $p > 2$ be a rational prime, and let v_p be the normalized discrete valuation on $\mathbb{Q}_p$ (i.e. $v_p(p) = 1$; cf. Exercise 11.1).

(1) Show that, for $n \geq 1$,
$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{n}{p-1}.$$

(2) Let K be a finite extension of $\mathbb{Q}_p$, equipped with the extension of v_p. Let π be a uniformizer, and let $e = e_{K/\mathbb{Q}_p}$, so that $v_p(\pi) = \frac{1}{e}$. Show that, for $x \in \pi^r \mathcal{O}_K$ with $r > \frac{e}{p-1}$, the infinite sum
$$e^x := \sum_{n=0}^{\infty} \frac{x^n}{n!},$$
converges to an element in $1 + \pi^r \mathcal{O}_K$.

(3) Under the same setup as (2), show that the infinite sum
$$\log(1 + x) := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n},$$
converges to an element in $\pi^r \mathcal{O}_K$.

(4) Using (2) and (3), show that the multiplicative group $(1+\pi^r\mathcal{O}_K, \times)$ and the additive group $(\pi^r\mathcal{O}_K, +)$ are isomorphic to each other.

Exercise 13.3. Let K/L be an extension of p-adic local fields of degree n. We say that K/L is **tamely ramified** if $(p, e_{K/L}) = 1$. Otherwise, i.e. if $p|e_{K/L}$, we say that K/L is **wildly ramified**. In this question, we want to show that totally ramified extensions that are tamely ramified (**totally tamely ramified** in short) has a simpler description.[25]

(1) Suppose $(n, p) = 1$, and let π_L be a uniformizer of L. Show that $K := L(\pi_L^{1/n})$ is a totally tamely ramified extension of L.

(2) Suppose that K/L is totally tamely ramified (so that $(n, p) = 1$). Let π_K be a uniformizer of K. Show that any element $x \in 1 + \pi_K\mathcal{O}_K$ has an n-th root in K.

Hint. Use Hensel's lemma; $x \pmod{\pi_K} = 1$ has an obvious n-th root.

(3) In the setup of (2), show that there exists a unit $u \in \mathcal{O}_K^\times$ such that $\left(\frac{\pi_K}{u}\right)^n \in L$. Deduce that $K = L(\pi_K'^{1/n})$ for some uniformizer π_K' of K.

Hint. A priori, $\pi_K^n = u'\pi_L$ for a uniformizer π_L of L and a unit $u' \in \mathcal{O}_K^\times$. Show that one can choose a different uniformizer of L so that $u' \equiv 1 \pmod{\pi_K}$. Then, use (2).

Exercise 13.4.

(1) Let p be an odd rational prime. Show that an element $x = p^n u \in \mathbb{Q}_p$, $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$, is a square in $\mathbb{Q}_p$, if and only if n is even and u is a square mod p.

(2) Show that an element $x = 2^n u \in \mathbb{Q}_2$, $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_2^\times$, is a square in $\mathbb{Q}_2$, if and only if n is even and $u \equiv 1 \pmod 8$.

(3) Show that there are in total 7 isomorphism classes of quadratic extensions of $\mathbb{Q}_2$ and 3 isomorphism classes of quadratic extensions of $\mathbb{Q}_p$ for p odd. How many are ramified?

Hint. For any field K of characteristic $\neq 2$, isomorphism classes of quadratic extensions of K are in bijection with non-trivial elements of $K^\times/(K^\times)^2$.

[25] This question tells us that the Eisenstein polynomial can be taken to be $X^n - \pi_L$ for a uniformizer π_L. A field extension obtained by adjoining an n-th root of an element downstairs is called a **Kummer extension**.

14. Lecture 18. Local fields and number fields

Summary. Local Galois groups and decomposition groups; tensor product of fields; ramification in towers and compositums.

Content. Now we connect the theory of local fields to the number fields. Recall that, for a maximal ideal $\mathfrak{p}$ of a number field K, $K_{\mathfrak{p}}$ is a p-adic local field, for $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. What this tells us are:

- $K \hookrightarrow K_{\mathfrak{p}}$ is a subfield (of infinite degree by the cardinality reason, Exercise 11.3);
- the normalized discrete valuation/absolute value induces a discrete valuation/absolute value on K.

As the relative theory of local fields is very nice, we would like to connect this to number fields. This can be done by the notion of tensor product of fields.

Definition 14.1 (Tensor product)**.** Let $K, M/L$ be two field extensions (not necessarily of finite degree). Let $K \otimes_L M$ be the commutative M-algebra defined as follows. Let $\{v_i\}_{i\in I}$ be an L-basis of K, with $v_i v_j = \sum_{k\in I} a_{ijk} v_k$, $a_{ijk} \in L$ (for each i, j, there are finitely many $k \in I$ such that $a_{ijk} \neq 0$, by the definition of basis). Then, $K \otimes_L M$ is, as an M-module, the M-vector space with basis vector $\{v_i\}_{i\in I}$, with the multiplication defined by $v_i v_j = \sum_{k\in I} a_{ijk} v_k$.

Remark 14.2. The above construction verbatim works for any two L-algebras. Even more generally, for any commutative ring A and two A-algebras B_1, B_2, there is the notion of tensor product $B_1 \otimes_A B_2$, which is both a B_1-algebra and a B_2-algebra. The challenge for this more general notion of tensor product is that one has to also consider the relations.

By definition, the following are immediate (check yourself).

Proposition 14.3. *Let L be a field, and let K_1, K_2 be two L-algebras. Then, there is a natural surjective L-linear map $K_1 \times K_2 \to K_1 \otimes_L K_2$. The image of (x, y) is denoted as $x \otimes y$. The tensor product notation satisfies the following relations.*

(1) If $x_1, x_2 \in K_1$ and $y \in K_2$, $(x_1 + x_2) \otimes y = (x_1 \otimes y) + (x_2 \otimes y)$.

(2) If $x \in K_1$ and $y_1, y_2 \in K_2$, $x \otimes (y_1 + y_2) = (x \otimes y_1) + (x \otimes y_2)$.

(3) If $x \in K_1$, $y \in K_2$ and $t \in L$, $x \otimes (ty) = (tx) \otimes y = t(x \otimes y)$.

Proposition 14.4. *Let $K = L[X]/(f(X))$ with a polynomial $f(X) \in L[X]$. Then, $K \otimes_L M \cong M[X]/(f(X))$ as M-algebras.*

Proposition 14.5. *The commutative M-algebra $K \otimes_L M$ is also naturally a K-algebra.*

Now the relative prime splitting of a number field connects with local fields as follows.

Theorem 14.6. *Let K/L be a finite extension of number fields. Let $\mathfrak{p} \subset \mathcal{O}_L$ be a maximal ideal. Then, as $L_{\mathfrak{p}}$-algebras,*

$$K \otimes_L L_{\mathfrak{p}} \cong \prod_{\mathfrak{q} \text{ a prime ideal of } \mathcal{O}_K \text{ lying over } \mathfrak{p}} K_{\mathfrak{q}}.$$

Proof. By the Primitive Element Theorem, $K = L(\alpha)$ for some $\alpha \in K$. Let $f(X)$ be the minimal polynomial of α over L. Thus, $K \otimes_L L_\mathfrak{p} \cong L_\mathfrak{p}[X]/(f(X))$. Let $f(X)$ factorize into

$$f(X) = f_1(X) \cdots f_g(X),$$

in $L_\mathfrak{p}[X]$, where $f_1(X), \cdots, f_g(X)$ are distinct monic irreducible polynomials. It suffices to show that $\{L_\mathfrak{p}[X]/(f_i(X))\}_{1 \le i \le g}$ runs through $\{K_\mathfrak{q}\}_{\mathfrak{q}|\mathfrak{p}}$. Note that, given $f_i(X)$, $L_\mathfrak{p}[X]/(f_i(X))$ is a finite extension of $L_\mathfrak{p}$, so it is a local field. Furthermore, the natural map $K = L[X]/(g(X)) \to L_\mathfrak{p}[X]/(f_i(X))$ is injective, as it is a nonzero field homomorphism. Therefore, the unique absolute value of $L_\mathfrak{p}[X]/(f_i(X))$ extending that of $L_\mathfrak{p}$ gives an absolute value $|\cdot|_i$ on K, thus giving rise to a prime ideal $\mathfrak{q} = \{x \in K \mid |x|_i < 1\}$ lying over $\mathfrak{p}$.

Conversely, given a prime ideal $\mathfrak{q} \subset \mathcal{O}_K$ lying over $\mathfrak{p}$, consider $K_\mathfrak{q}$ which contains $L_\mathfrak{p}(\alpha)$, as $K_\mathfrak{q} \supset L_\mathfrak{p}$ and $\alpha \in K_\mathfrak{q}$. On the other hand, as $K \subset L_\mathfrak{p}(\alpha)$, there is a natural injective homomorphism $K_\mathfrak{q} \to L_\mathfrak{p}(\alpha)$. Therefore, $K_\mathfrak{q} = L_\mathfrak{p}(\alpha)$. The minimal polynomial of $\alpha \in K_\mathfrak{q}$ over $L_\mathfrak{p}$ must be equal to some $f_i(X)$. These two operations are clearly inverses to each other, so we are done. □

The above Theorem is the key to convert a problem about a prime in a number field into a problem about local fields. Some of the immedate corollaries are:

Corollary 14.7. *Let $\mathfrak{p} \subset L$ be a prime ideal and K/L be an extension of number fields. Then, for $x \in K$, we have*

$$\mathrm{Tr}_{K/L}(x) = \sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{Tr}_{K_\mathfrak{q}/L_\mathfrak{p}}(x), \quad N_{K/L}(x) = \prod_{\mathfrak{q}|\mathfrak{p}} N_{K_\mathfrak{q}/L_\mathfrak{p}}(x).$$

Proof. By definition, the multiplication-by-x matrix is the same for both K/L and $K \otimes_L L_\mathfrak{p}/L_\mathfrak{p}$. The statement then follows from Theorem 14.6. □

Corollary 14.8. *Let K/L be a finite Galois extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$ and $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Then, the local field extension $K_\mathfrak{q}/L_\mathfrak{p}$ is Galois. Furthermore, $\mathrm{Gal}(K_\mathfrak{q}/L_\mathfrak{p})$ is naturally identified with the decomposition group $D(\mathfrak{q}|\mathfrak{p}) \le \mathrm{Gal}(K/L)$ as follows.*

- *Given $\sigma \in D(\mathfrak{q}|\mathfrak{p})$, $\sigma\mathfrak{q} = \mathfrak{q}$, which implies that the normalized discrte valuation $v_\mathfrak{q}$ on K is stabilized by σ, which means that $\sigma : K \to K$ extends to the completion $\sigma : K_\mathfrak{q} \to K_\mathfrak{q}$. As it fixes $L_\mathfrak{p}$, this gives rise to an element in $\mathrm{Gal}(K_\mathfrak{q}/L_\mathfrak{p})$.*
- *The identity $L_\mathfrak{p} \cap K = L$ gives rise to a natural map $\mathrm{Gal}(K_\mathfrak{q}/L_\mathfrak{p}) \to \mathrm{Gal}(K/L)$, which is injective and its image is precisely the decomposition group $D(\mathfrak{q}|\mathfrak{p})$.*

Under the identification, the inertia group of the local Galois group is the same as the inertia group of the prime ideals in the number fields.

Proof. From the first description, one obtains at least $|D(\mathfrak{q}|\mathfrak{p})|$ many distinct elements of $\mathrm{Hom}_{L_\mathfrak{p}}(K_\mathfrak{q}, K_\mathfrak{q})$. As $|D(\mathfrak{q}|\mathfrak{p})| = e(\mathfrak{q}|\mathfrak{p})f(\mathfrak{q}|\mathfrak{p}) = [K_\mathfrak{q} : L_\mathfrak{p}]$, this implies that $K_\mathfrak{q}/L_\mathfrak{p}$ is Galois, and the homomorphism $D(\mathfrak{q}|\mathfrak{p}) \to \mathrm{Gal}(K_\mathfrak{q}/L_\mathfrak{p})$ is an isomorphism. It is straightforward to check that the second description gives the inverse. □

Using the local methods, we can study how the prime ideals interact in various settings, e.g. taking subfields, taking compositums, given a tower of fields.

Definition 14.9. Let K/L be a field extension of number fields, and let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal. We say that $\mathfrak{p}$ is **tamely ramified** in K if, for every $\mathfrak{q} \subset \mathcal{O}_K$ lying over $\mathfrak{p}$, $(p, e(\mathfrak{q}|\mathfrak{p})) = 1$, where $\mathfrak{p}$ lies over a rational prime $p \in \mathbb{Z}$.

Theorem 14.10 (Unramified/tamely ramified primes in compositums, subfields and towers)**.** *Let L be a number field, and let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal.*

(1) If $J/K/L$ is a tower of number fields, and if $\mathfrak{p}$ is unramified (tamely ramified, respectively) in J, then $\mathfrak{p}$ is unramified (tamely ramified, respectively) in K.

(2) Let $J/K/L$ be a tower of number fields, and suppose that $\mathfrak{p}$ is unramified (tamely ramified, respectively) in K. Suppose also that, for every prime ideal $\mathfrak{q} \subset \mathcal{O}_K$ lying over $\mathfrak{p}$, $\mathfrak{q}$ is unramified (tamely ramified, respectively) in J. Then, $\mathfrak{p}$ is unramified (tamely ramified, respectively) in J.

(3) If $K_1, K_2/L$ are two field extensions of number fields such that $\mathfrak{p}$ is unramified (tamely ramified, respectively) in both K_1, K_2, then $\mathfrak{p}$ is unramified (tamely ramified, respectively) in the compositum K_1K_2.

Proof. Let $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

(1) Let $\mathfrak{q} \subset \mathcal{O}_K$ be a prime ideal lying over $\mathfrak{p}$. Pick a prime ideal $\mathfrak{r} \subset \mathcal{O}_J$ lying over $\mathfrak{q}$. Then, $e(\mathfrak{r}|\mathfrak{p}) = 1$ ($(p, e(\mathfrak{r}|\mathfrak{p})) = 1$, respectively). This is the same as $e_{J_\mathfrak{r}/L_\mathfrak{p}} = 1$ ($(p, e_{J_\mathfrak{r}/L_\mathfrak{p}}) = 1$, respectively). As $e_{K_\mathfrak{q}/L_\mathfrak{p}}$ divides $e_{J_\mathfrak{r}/L_\mathfrak{p}}$, $e_{K_\mathfrak{q}/L_\mathfrak{p}} = 1$ ($(p, e_{K_\mathfrak{q}/L_\mathfrak{p}}) = 1$, respectively), or $e(\mathfrak{q}|\mathfrak{p}) = 1$ ($(p, e(\mathfrak{q}|\mathfrak{p})) = 1$, respectively). As this holds for any $\mathfrak{q}$ lying over $\mathfrak{p}$, $\mathfrak{p}$ is unramified (tamely ramified, respectively) in K.

(2) Let $\mathfrak{r} \subset \mathcal{O}_J$ be a prime ideal lying over $\mathfrak{p}$. We want to prove that $e(\mathfrak{r}|\mathfrak{p}) = 1$ ($(p, e(\mathfrak{r}|\mathfrak{p})) = 1$, respectively), or $e_{J_\mathfrak{r}/L_\mathfrak{p}} = 1$ ($(p, e_{J_\mathfrak{r}/L_\mathfrak{p}}) = 1$, respectively). Note that $e_{J_\mathfrak{r}/L_\mathfrak{p}} = e_{J_\mathfrak{r}/K_\mathfrak{q}} e_{K_\mathfrak{q}/L_\mathfrak{p}}$, where $\mathfrak{q} = \mathfrak{r} \cap \mathcal{O}_K$, and we have $e_{J_\mathfrak{r}/K_\mathfrak{q}} = 1$ and $e_{K_\mathfrak{q}/L_\mathfrak{p}} = 1$ ($(p, e_{J_\mathfrak{r}/K_\mathfrak{q}}) = 1$ and $(p, e_{K_\mathfrak{q}/L_\mathfrak{p}}) = 1$, respectively), so we get the desired statement.

(3) Consider the natural map

$$K_1 \otimes_L K_2 \to K_1K_2, \quad x \otimes y \mapsto xy.$$

The map is clearly surjective. From this, the natural map

$$(K_1 \otimes_L L_\mathfrak{p}) \otimes_{L_\mathfrak{p}} (K_2 \otimes_L L_\mathfrak{p}) \to K_1K_2 \otimes_L L_\mathfrak{p}, \quad (x \otimes y) \otimes (x' \otimes y') \mapsto (xx') \otimes (yy'),$$

is surjective. Using the natural map, we know that the natural map

$$(*) \qquad (K_1 \otimes_L L_\mathfrak{p}) \times (K_2 \otimes_L L_\mathfrak{p}) \to K_1K_2 \otimes_L L_\mathfrak{p}, \quad (x \otimes y, x' \otimes y') \mapsto (xx') \otimes (yy'),$$

is surjective. We would like to show that, for every $\mathfrak{q} \subset \mathcal{O}_{K_1K_2}$ lying over $\mathfrak{p}$, $(K_1K_2)_\mathfrak{q}$ is an unramified extension of $L_\mathfrak{p}$. Note that, by assumption, the left hand side of $(*)$ is a product of unramified (tamely ramified) extensions of $L_\mathfrak{p}$, so the product of such extensions surjects onto $(K_1K_2)_\mathfrak{q}$,

$$\prod_{i=1}^{n} F_i \twoheadrightarrow (K_1K_2)_\mathfrak{q},$$

where $F_i/L_\mathfrak{p}$ is unramified (tamely ramified, respectively). On the other hand, for each F_i, the homomorphism

$$F_i \to (K_1K_2)_\mathfrak{q},$$

is either zero or injective, and in either case, it factors through $F' \subset (K_1K_2)_\mathfrak{q}$, the maximal unramified (tamely ramified, respectively) extension of $L_\mathfrak{p}$ in $(K_1K_2)_\mathfrak{q}$. Therefore, $\prod_{i=1}^n F_i \to (K_1K_2)_\mathfrak{q}$ factors through F', which must be $(K_1K_2)_\mathfrak{q}$, as desired.

□

Theorem 14.11 (Ramification index/residue degree in towers)**.** *Let $K/L/M$ be a tower of number fields, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal with $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_L$ and $\mathfrak{r} = \mathfrak{p} \cap \mathcal{O}_M$. Then,*

$$e(\mathfrak{p}|\mathfrak{r}) = e(\mathfrak{p}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{r}), \quad f(\mathfrak{p}|\mathfrak{r}) = f(\mathfrak{p}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{r}).$$

Proof. This follows immediately from the multiplicativity of e, f for local fields. □

Theorem 14.12 (Splitting completely in compositums, subfields and towers)**.** *Let L be a number field, and let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal.*

(1) If $J/K/L$ is a tower of number fields, and if $\mathfrak{p}$ splits completely in J, then $\mathfrak{p}$ splits completely in K.

(2) Let $J/K/L$ be a tower of number fields, and suppose that $\mathfrak{p}$ splits completely in K. Suppose also that, for every prime ideal $\mathfrak{q} \subset \mathcal{O}_K$ lying over $\mathfrak{p}$, $\mathfrak{q}$ splits completely in J. Then, $\mathfrak{p}$ splits completely in J.

(3) If $K_1, K_2/L$ are two field extensions of number fields such that $\mathfrak{p}$ splits completely in both K_1, K_2, then $\mathfrak{p}$ splits completely in the compositum K_1K_2.

Proof. (1) This follows from the multiplicativity of e, f.

(2) This follows from the multiplicativity of e, f.

(3) As above, there is a natural surjective map

$$(K_1 \otimes_L L_\mathfrak{p}) \otimes_{L_\mathfrak{p}} (K_2 \otimes_L L_\mathfrak{p}) \twoheadrightarrow K_1K_2 \otimes_L L_\mathfrak{p}.$$

As the left hand side is a product of $L_\mathfrak{p}$, we see that any local field appearing in the right hand side is $L_\mathfrak{p}$, which means that $\mathfrak{p}$ splits completely in K_1K_2.

□

Theorem 14.13 (Decomposition group, inertia group, Frobenius in towers)**.** *Let $K/L/M$ be a tower of number fields, with $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{q} \subset \mathcal{O}_L$, $\mathfrak{r} \subset \mathcal{O}_M$ prime ideals lying over each other.*

(1) Suppose that K/M is Galois. Then,

$$D(\mathfrak{p}|\mathfrak{q}) = D(\mathfrak{p}|\mathfrak{r}) \cap \mathrm{Gal}(K/L), \quad I(\mathfrak{p}|\mathfrak{q}) = I(\mathfrak{p}|\mathfrak{r}) \cap \mathrm{Gal}(K/L).$$

If $I(\mathfrak{p}|\mathfrak{r}) = \{1\}$, we have $\mathrm{Fr}(\mathfrak{p}|\mathfrak{q}) = \mathrm{Fr}(\mathfrak{p}|\mathfrak{r})^{f(\mathfrak{q}|\mathfrak{r})}$.

(2) Suppose that $K/L/M$ are all Galois. Then,

$$D(\mathfrak{q}|\mathfrak{r}) = D(\mathfrak{p}|\mathfrak{r})/D(\mathfrak{p}|\mathfrak{q}), \quad I(\mathfrak{q}|\mathfrak{r}) = I(\mathfrak{p}|\mathfrak{r})/I(\mathfrak{p}|\mathfrak{q}).$$

If $I(\mathfrak{p}|\mathfrak{r}) = \{1\}$, $\mathrm{Fr}(\mathfrak{q}|\mathfrak{r})$ is identified with the image of $\mathrm{Fr}(\mathfrak{p}|\mathfrak{r})$.

Proof. (1) The first two assertions are literally just by the definition. If the inertia is trivial, the subgroup $D(\mathfrak{p}|\mathfrak{q}) \leq D(\mathfrak{p}|\mathfrak{r})$ is identified with $\mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q}) \leq \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{r})$, where $k_\mathfrak{p}, k_\mathfrak{q}, k_\mathfrak{r}$ are residue fields of $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$, respectively, and the statement about the Frobenius readily follows.

(2) As $K_\mathfrak{p}/L_\mathfrak{q}/M_\mathfrak{r}$ are Galois, $D(\mathfrak{q}|\mathfrak{r}) = D(\mathfrak{p}|\mathfrak{r})/D(\mathfrak{p}|\mathfrak{q})$ follows from

$$\mathrm{Gal}(L_\mathfrak{q}/M_\mathfrak{r}) = \mathrm{Gal}(K_\mathfrak{p}/M_\mathfrak{r})/\mathrm{Gal}(K_\mathfrak{p}/L_\mathfrak{q}).$$

As $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{r}) = \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{r})/\mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q})$, it follows that the inertia group also satisfies $I(\mathfrak{q}|\mathfrak{r}) = I(\mathfrak{p}|\mathfrak{r})/I(\mathfrak{p}|\mathfrak{q})$. This is a standard argument in commutative algebra, where I replicate. We want to show that there is a natural map $I(\mathfrak{p}|\mathfrak{r}) \to I(\mathfrak{q}|\mathfrak{r})$ which is surjective and has kernel equal to $I(\mathfrak{p}|\mathfrak{q})$. The obvious candidate is the restriction of the natural map $D(\mathfrak{p}|\mathfrak{r}) \twoheadrightarrow D(\mathfrak{q}|\mathfrak{r})$ to $I(\mathfrak{p}|\mathfrak{r})$. Since anything in $I(\mathfrak{p}|\mathfrak{r})$ is sent to $0 \in \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{r})$, it follows that the image of $I(\mathfrak{p}|\mathfrak{r})$ under this natural map will be sent to the image of 0 in $\mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{r})$, which is again 0, so the image of $I(\mathfrak{p}|\mathfrak{r})$ is contained in $\ker(D(\mathfrak{q}|\mathfrak{r}) \to \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{r})) = I(\mathfrak{q}|\mathfrak{r})$. To show that this natural map is surjective, we want to show that any element $x \in I(\mathfrak{q}|\mathfrak{r})$ is the image of some element $x' \in I(\mathfrak{p}|\mathfrak{r})$. Note that $D(\mathfrak{p}|\mathfrak{r}) \twoheadrightarrow D(\mathfrak{q}|\mathfrak{r})$ is surjective, there is $x'' \in D(\mathfrak{p}|\mathfrak{r})$ that is sent to $x \in I(\mathfrak{q}|\mathfrak{r}) \leq D(\mathfrak{q}|\mathfrak{r})$. This x'' may not be contained in the inertia. However, what we know is that its image $[x''] \in \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{r})$ is sent to $0 \in \mathrm{Gal}(k_\mathfrak{q}/k_\mathfrak{r})$, so $[x''] \in \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{q}) \leq \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{r})$. Take $x''' \in D(\mathfrak{p}|\mathfrak{q})$ whose image is $[x'']$. Then, $x''' \in D(\mathfrak{p}|\mathfrak{q}) \leq D(\mathfrak{p}|\mathfrak{r})$, and $x''(x''')^{-1} \in D(\mathfrak{p}|\mathfrak{r})$ is now contained in $I(\mathfrak{p}|\mathfrak{r})$, as it is sent to $0 \in \mathrm{Gal}(k_\mathfrak{p}/k_\mathfrak{r})$. Note also that this is still sent to $x \in I(\mathfrak{q}|\mathfrak{r}) \leq D(\mathfrak{q}|\mathfrak{r})$, so this is what we wanted.

To show that the natural map has $I(\mathfrak{p}|\mathfrak{q})$ as its kernel, we need to go through a similar argument as above.

The statement about Frobenius is obvious.

□

– –

Exercise 14.1. Let L be a field, and let K_1, K_2 be two commutative L-algebras. We aim to provide several ways to think about the tensor product $K_1 \otimes_L K_2$.

(1) Note that $K_1 \otimes_L K_2$ has natural L-algebra homomorphisms

$$\iota_1 : K_1 \xrightarrow{x \mapsto x \otimes 1} K_1 \otimes_L K_2, \quad \iota_2 : K_2 \xrightarrow{x \mapsto 1 \otimes x} K_1 \otimes_L K_2.$$

Show that $K_1 \otimes_L K_2$ satisfies the **universal property of tensor products of commutative algebras**, as follows. If R is a commutative L-algebra, and if $f_1 : K_1 \to R$, $f_2 : K_2 \to R$ are L-algebra homomorphisms, then there exists a unique L-algebra homomorphism $f : K_1 \otimes_L K_2 \to R$ such that

$$f_1 = f \circ \iota_1, \quad f_2 = f \circ \iota_2.$$

(2) Show that the above universal property uniquely characterizes $K_1 \otimes_L K_2$ as an L-algebra. Namely, show that if a commutative L-algebra S with L-algebra homomorphisms $j_1 : K_1 \to S$ and $j_2 : K_2 \to S$ satisfies the above universal property (i.e. given any two maps $f_1 : K_1 \to R$, $f_2 : K_2 \to R$, there is a unique map $f : S \to R$ such that $f_1 = f \circ j_1$, $f_2 = f \circ j_2$), then $S \cong K_1 \otimes_L K_2$.

(3) Let X be the L-vector space spanned by the basis vectors $v \otimes w$ for any pair of $v \in K_1, w \in K_2$, and endow the L-algebra structure by defining the multiplication to be $(v_1 \otimes w_1)(v_2 \otimes w_2) = (v_1 v_2) \otimes (w_1 w_2)$. Let $I \subset X$ be the L-vector subspace spanned by the following elements:

$$I = \langle \{(v_1 + v_2) \otimes w - v_1 \otimes w - v_2 \otimes w \ : \ v_1, v_2 \in K_1, w \in K_2\},$$
$$\{v \otimes (w_1 + w_2) - v \otimes w_1 - v \otimes w_2 \ : \ v \in K_1, w_1, w_2 \in K_2\},$$
$$\{t(v \otimes w) - (tv) \otimes w \ : \ t \in L, v \in K_1, w \in K_2\},$$
$$\{t(v \otimes w) - v \otimes (tw) \ : \ t \in L, v \in K_1, w \in K_2\}\rangle.$$

Show that $I \subset X$ is an ideal.

(4) Show that the L-algebra X/I, together with the natural maps

$$j_1 : K_1 \xrightarrow{x \mapsto x \otimes 1} X/I, \quad j_2 : K_2 \xrightarrow{x \mapsto 1 \otimes x} X/I,$$

satisfies the universal property of (1). This gives another construction of $K_1 \otimes_L K_2$.

Exercise 14.2. Let L be a p-adic local field of characteristic 0.

(1) Using Hensel's lemma, show that a finite field extension K/L is unramified if and only if $K = L(\zeta_n)$ for some $(n, p) = 1$.

(2) If K/L is an unramified extension, and if M is a p-adic local field of characteristic 0, show that KM/LM is unramified.

Exercise 14.3. Let $K = \mathbb{Q}(\alpha, i)$, where $\alpha^4 = 2$ and $i^2 = -1$. Note that $K/\mathbb{Q}$ is Galois with $G := \mathrm{Gal}(K/\mathbb{Q}) \cong D_4$, a dihedral group, generated by $s, t \in G$ where

$$s(\alpha) = i\alpha, \quad s(i) = i, \quad t(\alpha) = \alpha, \quad t(i) = -i,$$

so that $s^4 = t^2 = 1$ and $tst^{-1} = s^{-1}$. Note that K contains two particular subfields, $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(i)$.

(1) Show that 2 is totally ramified in both $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(i)$.

(2) Show that $\mathbb{Q}_2(\alpha) \cap \mathbb{Q}_2(i) = \mathbb{Q}_2$.

Hint. Otherwise, $\mathbb{Q}_2(\alpha) \supset \mathbb{Q}_2(i)$, and therefore $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2(i)$, which is a quadratic extension, is automatically Galois. Show that the nontrivial element $\sigma \in \mathrm{Gal}(\mathbb{Q}_2(\alpha)/\mathbb{Q}_2(i))$ must send $\sigma(\alpha) = -\alpha$. This implies that $\mathbb{Q}_2(\sqrt{2}) = \mathbb{Q}_2(i)$. Deduce a contradiction using Exercise 13.4.

(3) Show that $K_2 := K \otimes_{\mathbb{Q}} \mathbb{Q}_2$ is a field.

(4) Show that $K_2/\mathbb{Q}_2$ is totally ramified. Deduce that 2 is totally ramified in K.

Hint. Suppose not. As $\mathbb{Q}_2(\alpha)/\mathbb{Q}_2$ is totally ramified, it should be the case that $e_{K_2/\mathbb{Q}_2} = 4$ and $f_{K_2/\mathbb{Q}_2} = 2$. Therefore, the maximal unramified extension of $\mathbb{Q}_2$ in K_2 is a quadratic extension of $\mathbb{Q}_2$. Using that $\mathrm{Gal}(K_2/\mathbb{Q}_2) \cong D_4$, enumerate all quadratic subfields of K_2, and show that they are all ramified over $\mathbb{Q}_2$ (use Exercise 13.4), yielding a contradiction.

(5) Show that any rational prime $p \neq 2$ is unramified in K.

15. Lecture 19. Local class field theory

Summary. Local Kronecker–Weber theorem; infinite Galois theory; statements of local class field theory (local Artin reciprocity, local existence theorem); local conductor.

Content. This and the following section together form the major milestone in modern number theory called the **class field theory**. In short, it gives a very precise description of **abelian extensions** of local and number fields. Recall that a field extension is **abelian** if it is Galois and its Galois group is abelian. By basic Galois theory, a compositum of abelian extensions is again abelian, so in particular one can form the **maximal abelian extension** K^{ab} of any field K inside its algebraic closure. The local class field theory is heuristically quite easy to formulate.

Slogan. For a local field K, $K^\times$ and $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ are "almost isomorphic."

Let's try to see what kind of statement this is. By Galois theory, this should mean that finite index subgroups of $K^\times$ are in one-to-one correspondence with finite abelian extensions of K. On the other hand, we are working with local fields, so it is natural to incorporate topology in our setup. We arrive at a statement that is actually precise.

Open finite index subgroups of $K^\times \leftrightarrow$ finite abelian extensions of K.

This statement is a part of the local class field theory called the **local existence theorem**.

Let's see why the local existence theorem is believable, by relating it to a slightly more believable statement.

Example 15.1 (The case of $\mathbb{Q}_p$)**.** As mentioned before in class briefly, the **Kronecker–Weber theorem** asserts that

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n>1} \mathbb{Q}(\zeta_n).$$

Well, there is a local analogue, called the **local Kronecker–Weber theorem**.

Theorem 15.2 (Local Kronecker–Weber theorem)**.** *We have*

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_{n>1} \mathbb{Q}_p(\zeta_n).$$

We won't prove this.[26] Rather, we will take this and see why this gives some explanation of the local existence theorem.

In the case of $\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. However, this is no longer true for $\mathbb{Q}_p$, because the proof that relied on the irreducibility of cyclotomic polynomial no longer holds for powers of primes different from p. However, it is still valid when $n = p^a$; $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^a})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times$,

[26] However, unlike the latter statements without proofs, whose proofs would require advanced machinery like group cohomology, this theorem can be proved by only using elementary methods (mainly the **Hasse–Arf theorem**; the formulation requires a different numbering of ramification groups which is quite a headache).

and $\mathbb{Q}_p(\zeta_{p^a})/\mathbb{Q}_p$ is totally ramified. In fact, the maximal unramified extension of $\mathbb{Q}_p$ in $\mathbb{Q}_p^{\mathrm{ab}}$ (often called the **maximal unramified abelian extension** of $\mathbb{Q}_p$), denoted $\mathbb{Q}_p^{\mathrm{ur}}$, is

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

Let us also denote $\mathbb{Q}_p(\zeta_{p^\infty}) := \bigcup_{n\geq 1} \mathbb{Q}_p(\zeta_{p^n})$. Then, the local Kronecker–Weber theorem becomes

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{ur}}\mathbb{Q}_p(\zeta_{p^\infty}),$$

where the $\mathbb{Q}_p^{\mathrm{ur}}$-part corresponds to the unramified extensions, and the $\mathbb{Q}_p(\zeta_p^\infty)$-part corresponds to the totally ramified extensions.

On the $\mathbb{Q}_p^\times$ side, we have a similar decomposition,

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

I claim that, under the local existence theorem, the $p^{\mathbb{Z}}$-part corresponds to the unramified extensions, and the $\mathbb{Z}_p^\times$-part corresponds to the totally ramified extensions.

Firstly, the finite unramified extensions of $\mathbb{Q}_p$ are the same as the finite extensions of its residue field, $\mathbb{F}_p$, and such extensions are determined by the degree $f \geq 1$. Indeed, the finite index subgroups of $p^{\mathbb{Z}}$ are precisely $p^{f\mathbb{Z}}$ for some $f \geq 1$.

Moreover, the totally ramified extensions of $\mathbb{Q}_p$, by the local Kronecker–Weber theorem, are finite intermediate extensions of $\mathbb{Q}_p(\zeta_p^\infty)/\mathbb{Q}_p$. On the other hand, we see that $\mathbb{Q}_p(\zeta_{p^n})$'s are related via

$$\begin{array}{ccccccccc}
\cdots & \twoheadrightarrow & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) & \twoheadrightarrow & \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n-1}})/\mathbb{Q}_p) & \twoheadrightarrow \cdots \twoheadrightarrow & \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p), \\
\cdots & \twoheadrightarrow & (\mathbb{Z}/p^n\mathbb{Z})^\times & \twoheadrightarrow & (\mathbb{Z}/p^{n-1}\mathbb{Z})^\times & \twoheadrightarrow \cdots \twoheadrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times.
\end{array}$$

Therefore, an element of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ is a compatible sequence of elements in $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ for each n, and this is the same as a compatible sequence of elements in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for each n, and this is precisely $\mathbb{Z}_p^\times$!

To precisely formulate the local class field theory, we need to know something about topology of Galois group of infinite Galois extensions. This theory is often called the **infinite Galois theory**. There is nothing to worry about; the upshot is that the fundamental theorem of Galois theory works with only one difference that we have to take the topology into account. Namely, in the infinite Galois theory, the Galois group are **topological groups**.

Definition 15.3 (Topological groups)**.** A **topological group** is a group G which is also a topological space, such that the multiplication map $G \times G \xrightarrow{(x,y)\mapsto xy} G$ and the inverses map $G \xrightarrow{x\mapsto x^{-1}} G$ are continuous with respect to the topology.

Example 15.4. (1) Given any group G, you may endow it the **discrete topology** and make it a topological group. Recall that the discrete topology means that any subset is an open subset, so there is nothing to check for the continuity properties.

(2) The real numbers $\mathbb{R}$ with its additive group structure and the usual topology form a topological group. Also, the multiplicative group of nonzero real numbers $\mathbb{R}^\times$ with the induced subspace topology forms a topological group.

(3) Complete discrete valuation rings and complete discretely valued fields are, additively, topological groups. In fact, they are respectively **topological rings** (both addition and multiplication are continuous) and **topological fields** (additionally, the multiplicative inverse map is continuous on nonzero elements). This for example means that, for a complete discrete valuation ring A, the multiplicative group of units $A^\times$ is a topological ring (with the subspace topology), and similarly for a complete discretely valued field.

We can now define the Galois group as a topological group.

Definition 15.5 (Galois extensions)**.** Let K/L be an algebraic extension of fields (maybe infinite). We say that K/L is **separable** if, for every $\alpha \in K$, the minimal polynomial $p_\alpha(X) \in L[X]$ over L is separable. We say that K/L is **normal** if $p_\alpha(X)$ splits in K for every $\alpha \in K$. We say that K/L is **Galois** if it is both separable and normal. In that case, we write $\mathrm{Gal}(K/L)$ as the group of L-automorphisms (=bijective homomorphisms of L-algebras) $K \to K$.

Again, whenever either L is of characteristic zero or a finite field, separability is automatically satisfied.

Definition 15.6 (Krull topology on the Galois group)**.** For K/L a Galois extension, we define the **Krull topology** as the topology generated by the basis

$$\{\mathrm{Gal}(K/M) \subset \mathrm{Gal}(K/L) \ : \ K/M/L \text{ with } M/L \text{ finite}\}.$$

In other words, a subset $U \subset \mathrm{Gal}(K/L)$ is open if, for every $x \in U$, there exists a finite subextension M/L of K/L such that $\sigma\,\mathrm{Gal}(K/M) \subset U$.

The Galois group with the Krull topology has the following topological properties.

Proposition 15.7. *Let K/L be a Galois extension.*

(1) The Galois group $\mathrm{Gal}(K/L)$ with the Krull topology is a topological group.

(2) If K/L is a finite extension, the Krull topology on $\mathrm{Gal}(K/L)$ is the discrete topology.

(3) The Krull topology on $\mathrm{Gal}(K/L)$ is alternatively constructed as follows. Let I be the set

$$I = \{F/L \text{ finite Galois subextensions of } K/L\}.$$

Then, $\mathrm{Gal}(K/L)$ is identified with the subset

$$\mathrm{Gal}(K/L) \cong \left\{ (x_F) \in \prod_{F \in I} \mathrm{Gal}(F/L) \ : \ \begin{array}{c} \text{whenever } F_2 \text{ is a subextension of } F_1,\ x_{F_1} \text{ is} \\ \text{sent to } x_{F_2} \text{ via the natural map} \\ \mathrm{Gal}(F_1/L) \to \mathrm{Gal}(F_2/L) \end{array} \right\} \subset \prod_{F \in I} \mathrm{Gal}(F/L).$$

For each $F \in I$, let $\mathrm{Gal}(F/L)$ be the finite set with discrete topology, and let $\prod_{F\in I} \mathrm{Gal}(F/L)$ be endowed with the product topology[27]. Then, the Krull topology on $\mathrm{Gal}(K/L)$ is the subspace topology. In this perspective, the natural quotient map $\mathrm{Gal}(K/L) \to \mathrm{Gal}(F/L)$ for any $F \in I$ is continuous (when the target $\mathrm{Gal}(F/L)$ is regarded as a discrete topological space).

(4) The Krull topology on $\mathrm{Gal}(K/L)$ is compact, Hausdorff, and totally disconnected (the only connected sets are singletons).

Proof. See Theorems 4.6, 5.1 and 5.4 of the handout on infinite Galois theory by Keith Conrad. The proofs are elementary, but also irrelevant for our purpose. □

The following is the fundamental theorem of infinite Galois theory, namely the Galois correspondence in the context of infinite Galois extensions; **closed subgroups correspond to subextensions**.

Theorem 15.8 (Fundamental theorem of infinite Galois theory; Galois correspondence)**.** *Let K/L be a Galois extension. Then, there is an inclusion-reversing one-to-one correspondence,*

$$\{\textbf{\textit{Closed}} \textit{ subgroups of } \mathrm{Gal}(K/L)\} \leftrightarrow \{\textit{Subextensions of } K/L\},$$

where the maps in both directions are given by

$$H \mapsto K^H,$$

$$\mathrm{Gal}(K/M) \hookleftarrow M/L.$$

The above correspondence restricts to various inclusion-reversing one-to-one correspondences,

$$\{\textbf{\textit{Closed normal}} \textit{ subgroups of } \mathrm{Gal}(K/L)\} \leftrightarrow \{\textbf{\textit{Galois}} \textit{ subextensions of } K/L\},$$

$$\{\textbf{\textit{Open}} \textit{ subgroups of } \mathrm{Gal}(K/L)\} \leftrightarrow \{\textbf{\textit{Finite}} \textit{ subextensions of } K/L\},$$

$$\{\textbf{\textit{Open normal}} \textit{ subgroups of } \mathrm{Gal}(K/L)\} \leftrightarrow \{\textbf{\textit{Finite Galois}} \textit{ subextensions of } K/L\}.$$

Furthermore, if M/L is a Galois subextension of K/L, then there is a natural isomorphism

$$\frac{\mathrm{Gal}(K/L)}{\mathrm{Gal}(K/M)} \xrightarrow{\sim} \mathrm{Gal}(M/L).$$

Proof. See Theorem 4.7 and Theorem 4.10 of Ketih Conrad's notes. □

Remark 15.9. What is included in the above Galois correspondence are that every open subgroup is of the form $\mathrm{Gal}(K/F)$ for a finite subextension F/L (that this is open is obvious by definition), and that such open subgroups are furthermore **closed**. This is reminiscent of $\mathbb{Z}_p$, where the open disks are also also closed.

[27] Be aware that the product topology of an infinite product of discrete topological spaces is not discrete!

Under the infinite Galois theory, the **Slogan** we had seen in the beginning should look like:

Slogan. For a local field K, $K^\times$ and $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ are "almost isomorphic" as topological groups.

Now we can formulate the package of statements called the **local class field theory**. The proofs of the statements of local class field theory are beyond the scope of the course.

Theorem 15.10 (Local Artin reciprocity)**.** *Let L be a local field. Then, there is a **unique** continuous homomorphism, called the **local Artin map***

$$\mathrm{Art}_L : L^\times \to \mathrm{Gal}(L^{\mathrm{ab}}/L),$$

satisfying the following properties.

(1) For any finite abelian subextension K/L of L^{ab}/L, the local Artin map composed with the natural map $\mathrm{Gal}(L^{\mathrm{ab}}/L) \to \mathrm{Gal}(K/L)$ defines a continuous homomorphism

$$\mathrm{Art}_{K/L} : L^\times \to \mathrm{Gal}(K/L),$$

which is surjective with kernel $N_{K/L}(K^\times)$. In particular, there is an isomorphism

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

(2) If K/L is unramified, for any uniformizer $\pi_L \in L^\times$,

$$\mathrm{Art}_{K/L}(\pi_L) = \mathrm{Fr}_{K/L}\,.$$

(3) If K/L is a finite extension of local fields, the following diagram commutes, where the right vertical arrow is the restriction to L^{ab}.

$$\begin{array}{ccc} K^\times & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ {\scriptstyle N_{K/L}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ L^\times & \xrightarrow[\mathrm{Art}_L]{} & \mathrm{Gal}(L^{\mathrm{ab}}/L) \end{array}$$

Theorem 15.11 (Local existence theorem)**.** *Let L be a local field. Then, there exists an inclusion-reversing one-to-one correspondence,*

$$\left\{\textit{Open finite index subgroups of } L^\times\right\} \leftrightarrow \left\{\textit{Finite abelian extensions of } L\right\},$$

where the maps in both directions are given by

$$H \mapsto (L^{\mathrm{ab}})^{\mathrm{Art}_L(H)},$$

$$N_{K/L}(K^\times) \hookleftarrow K/L.$$

Remark 15.12. If L is a local field of characteristic 0, then any finite index subgroup of $L^\times$ is automatically open.

This is extremely nice in various ways, but it may seem baffling at the first sight. Let's see what the local Artin map should be in the case of $\mathbb{Q}_p$, continuing the discussion we had before.

Example 15.13 (The case of $\mathbb{Q}_p$, redux)**.** Recall that the local Kronecker–Weber theorem asserts that

$$\mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p^{\mathrm{ur}}\mathbb{Q}_p(\zeta_{p^\infty}).$$

Thus,

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p),$$

and we have seen that literally

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times.$$

So what is $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$? Note that if $K/\mathbb{Q}_p$ is an unramified extension, we have the natural isomorphism

$$\mathrm{Gal}(K/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(k_K/\mathbb{F}_p),$$

by Theorem 13.21, where k_K is the residue field of K. Since this map is compatible with changing unramified extensions K, by Proposition 15.7(3), we see that

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}\Big(\bigcup_{K/\mathbb{Q}_p \text{ unramified}} k_K/\mathbb{F}_p\Big).$$

So what is $\bigcup_{K/\mathbb{Q}_p} k_K$? Again, by Theorem 13.21, finite unramified extensions of $\mathbb{Q}_p$ are in one-to-one correspondence with finite extensions of $\mathbb{F}_p$. Thus, $\bigcup_{K/\mathbb{Q}_p} k_K$ is just the union of all finite extensions of $\mathbb{F}_p$, so it is the algebraic closure $\overline{\mathbb{F}_p}$.

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p).$$

Note that the finite extensions of finite field $\mathbb{F}_p$ are precisely $\mathbb{F}_{p^n}$ for $n \geq 1$, and that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, with $\mathrm{Fr} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ (the p-power map) identified with $1 \in \mathbb{Z}/n\mathbb{Z}$. Thus, Proposition 15.7(3) gives a description of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ as follows.

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \left\{ (x_n) \in \prod_{n\geq 1} (\mathbb{Z}/n\mathbb{Z}) \ : \ \text{if } n|m, \text{ then } x_m \pmod n = x_n \right\} \subset \prod_{n\geq 1} (\mathbb{Z}/n\mathbb{Z}).$$

The ring on the right hand side,

$$\left\{ (x_n) \in \prod_{n\geq 1} (\mathbb{Z}/n\mathbb{Z}) \ : \ \text{if } n|m, \text{ then } x_m \pmod n = x_n \right\},$$

is usually denoted as $\widehat{\mathbb{Z}}$, called the ring of **profinite integers**, which obviously admits a natural injective map $\mathbb{Z} \to \widehat{\mathbb{Z}}$. Thus,

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

We now have a full description of $\mathrm{Art}_{\mathbb{Q}_p} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$: it is the map

$$\mathbb{Q}_p^\times \cong p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \xrightarrow{\iota} \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p),$$

where the middle map ι is the identity map on $\mathbb{Z}_p^\times$, and is the natural map $\mathbb{Z} \to \widehat{\mathbb{Z}}$ on $p^{\mathbb{Z}} \cong \mathbb{Z}$. This matches with the desiderata of the local Artin map, as a uniformizer $p \in \mathbb{Q}_p$ is sent to $1 \in \widehat{\mathbb{Z}}$, which corresponds to the Frobenius whenever you restrict to finite unramified extensions.

The example of $\mathbb{Q}_p$ tells a lot. Firstly, by arguing in the same way, we get the following results.

Theorem 15.14. *Let L be a local field of characteristic 0. Then, there is the **maximal unramified extension** L^{ur}, which is the union of all unramified extensions of L in its algebraic closure $\overline{L}$. It is abelian over L, so that $L^{\mathrm{ur}} \subset L^{\mathrm{ab}}$. Its Galois group is naturally identified with*

$$\mathrm{Gal}(L^{\mathrm{ur}}/L) \xrightarrow{\sim} \mathrm{Gal}(\overline{k_L}/k_L) \cong \widehat{\mathbb{Z}},$$

where k_L is the residue field of L. Here, the second isomorphism $\mathrm{Gal}(\overline{k_L}/k_L) \cong \widehat{\mathbb{Z}}$ is given by $\mathrm{Fr} \mapsto 1$, where Fr is the $\#k_L$-power map.

Proof. Argue exactly as in the case of $\mathbb{Q}_p$ in Example 15.13. □

What happens for Art_L in general is the following.

- Choose a uniformizer $\pi_L \in L$. Upon the choice of the uniformizer π_L, just as $\mathbb{Q}_p$, L^{ab} is split into two parts,
$$L^{\mathrm{ab}} = L^{\mathrm{ur}} L_{\pi_L,\infty},$$
where L^{ur}/L is the maximal unramified extension, and $L_{\pi_L,\infty}/L$ is totally ramified.
- The Galois group $\mathrm{Gal}(L_{\pi_L,\infty}/L)$ is identified with $\mathcal{O}_L^\times$ (even as topological groups).
- The local Artin map is then defined as

$$\mathrm{Art}_L : L^\times \cong \pi_L^{\mathbb{Z}} \times \mathcal{O}_L^\times \to \widehat{\mathbb{Z}} \times \mathrm{Gal}(L_{\pi_L,\infty}/L) \cong \mathrm{Gal}(L^{\mathrm{ur}}/L) \times \mathrm{Gal}(L_{\pi_L,\infty}/L) \cong \mathrm{Gal}(L^{\mathrm{ab}}/L).$$

- There are two parts in the above procedure (i.e. the field $L_{\pi_L,\infty}$ and the splitting $L^\times \cong \pi_L^{\mathbb{Z}} \times \mathcal{O}_L^\times$) that depend on the choice of a uniformizer π_L, but their effects **cancel out each other**, so that the local Artin map $\mathrm{Art}_L : L^\times \to \mathrm{Gal}(L^{\mathrm{ab}}/L)$ does not depend on π_L.

The following is a nice byproduct of the local class field theory.

Corollary 15.15. *Let K/L be a finite abelian extension of local fields. Then,*

$$e_{K/L} = [\mathcal{O}_L^\times : N_{K/L}(\mathcal{O}_K^\times)].$$

In particular, K/L is unramified if and only if $\mathcal{O}_L^\times = N_{K/L}(\mathcal{O}_K^\times)$.

Proof. By the local Artin reciprocity, Theorem 15.10, we know that $L^\times/N_{K/L}(K^\times) \cong \mathrm{Gal}(K/L)$. Let v_K, v_L be the normalized discrete valuations on K, L, respectively. Then, $v_K(x) = e_{K/L}v_L(x)$ for $x \in L$. Also, by Theorem 13.18, when translated into the language of discrete valuations, we see that $\frac{1}{e_{K/L}}v_K(x) = \frac{1}{[K:L]}v_L(N_{K/L}(x))$ for $x \in K$, or

$$v_L(N_{K/L}(x)) = f_{K/L}v_K(x).$$

Thus, by taking v_L on $L^\times/N_{K/L}(K^\times)$, we get a surjection

$$v_L : L^\times/N_{K/L}(K^\times) \twoheadrightarrow \mathbb{Z}/f_{K/L}\mathbb{Z}.$$

The kernel of this map is simply

$$\frac{N_{K/L}(\pi_K)^{\mathbb{Z}} \times \mathcal{O}_L^\times}{N_{K/L}(K^\times)} = \frac{\mathcal{O}_L^\times N_{K/L}(K^\times)}{N_{K/L}(K^\times)} = \frac{\mathcal{O}_L^\times}{\mathcal{O}_L^\times \cap N_{K/L}(K^\times)},$$

where π_K is a uniformizer of K. It is clear that $\mathcal{O}_L^\times \cap N_{K/L}(K^\times) = N_{K/L}(\mathcal{O}_K^\times)$ as this is the subset of $N_{K/L}(K^\times)$ on which $v_L = 0$. As $[K : L] = e_{K/L}f_{K/L}$, the result follows. □

Definition 15.16 (Local conductor)**.** Let K/L be a finite abelian extension of local fields. Let $\mathfrak{p} \subset \mathcal{O}_L$ be the maximal ideal. Then, the **(local) conductor** of K/L, denoted $\mathfrak{f}_{K/L}$, is defined as

$$\mathfrak{f}_{K/L} := \begin{cases} 0 & \text{if } \mathcal{O}_L^\times = N_{K/L}(\mathcal{O}_K^\times) \\ \min\{n \geq 1 \ : \ 1 + \mathfrak{p}^n \subset N_{K/L}(\mathcal{O}_K^\times)\} & \text{otherwise.} \end{cases}$$

Of course, by Corollary 15.15, an abelian extension of local fields is unramified if and only if the local conductor is 0.

Remark 15.17 (Two ways to rectify the **Slogan**)**.** We now see that where Art_L fails to become an isomorphism: it is precisely about the difference between $\mathbb{Z}$ and $\widehat{\mathbb{Z}}$. Indeed, there is an injective map $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$, but this is not an isomorphism. One may see this abstractly by using topology: as asserted in Proposition 15.7, $\widehat{\mathbb{Z}}$ is compact. On the other hand, $\mathbb{Z}$ is a discrete group, and a discrete topological space with infinitely many elements is not compact.

There are two ways to upgrade Art_L into an isomorphism.

- One way is to upgrade $\mathbb{Z}$ into $\widehat{\mathbb{Z}}$. The topological group $\widehat{\mathbb{Z}}$ is a **profinite group**; a profinite group is a topological group that is constructed as a collection of elements in a family of finite discrete groups that are compatible in every sense, just like how $\widehat{\mathbb{Z}}$ is constructed. More generally, any (infinite) Galois group with Krull topology is a profinite group by Proposition 15.7.

  In general, given any discrete group G, there is a procedure called the **profinite completion** that yields a profinite group $\widehat{G}$ which also admits a natural map $G \to \widehat{G}$. It turns out that the profinite completion of $\mathbb{Z}$ is precisely $\widehat{\mathbb{Z}}$. Taking the profinite completion of $L^\times$, we get an isomorphism

$$\mathrm{Art}_L : \widehat{L^\times} \xrightarrow{\sim} \mathrm{Gal}(L^{\mathrm{ab}}/L).$$

- Another way, which is the mainstream way in modern number theory, is to downgrade $\widehat{\mathbb{Z}}$ into $\mathbb{Z}$. This is done by replacing the Galois group $\mathrm{Gal}(L^{\mathrm{ab}}/L)$ into a subgroup called the **Weil group** $W(L^{\mathrm{ab}}/L)$, which has the effect of changing $\widehat{\mathbb{Z}}$ of unramified part of the Galois group into $\mathbb{Z}$. This yields an isomorphism

$$\mathrm{Art}_L : L^\times \xrightarrow{\sim} W(L^{\mathrm{ab}}/L).$$

  The definition of the Weil group is subtle, as the topology of $W(L^{\mathrm{ab}}/L)$ is not just the subspace topology taken from $\mathrm{Gal}(L^{\mathrm{ab}}/L)$. This is because we want the discrete topology for $\mathbb{Z}$, but the subspace topology of $\mathbb{Z}$ taken from $\widehat{\mathbb{Z}}$ is **not the discrete topology**; for example, $0 \in \widehat{\mathbb{Z}}$ is a limit point of the set $\{n! \,:\, n \in \mathbb{N}\} \subset \widehat{\mathbb{Z}}$.

– –

Exercise 15.1. What we have learned so far suggests that **absolute values correspond to primes** – from this perspective, the archimedean absolute values should be primes! In this analogy, we regard $\mathbb{R}$ and $\mathbb{C}$ as local fields as well, and they are called either **∞-adic local fields** or **archimedean local fields**. Given a number field K, an embedding $i : K \hookrightarrow \mathbb{C}$ defines an **archimedean prime** of K, where a real embedding defines a **real prime**, and a pair of complex embeddings defines a **complex prime**. The extension $\mathbb{C}/\mathbb{R}$ is considered **ramified**.

We will see that many aspects of theory of primes and the local class field theory translate well into the case of archimedean primes and local fields.

(1) Let K/L be an extension of number fields. Using the above perspective, define what it means for an archimedean prime of K to lie over an archimedean prime of L.

(2) Retaining the setup of (1), define what it means for an archimedean prime of L to be unramified in K.

(3) The local Artin map for $\mathbb{R}$ can be defined as

$$\mathrm{Art}_{\mathbb{R}} : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \{\pm 1\}, \quad x \mapsto \frac{x}{|x|}.$$

  Show that Part (1) of local Artin reciprocity (Theorem 15.10(1) of the notes) holds.

(4) State and prove the local existence theorem for $L = \mathbb{R}$.

16. Lectures 20 and 21. Global class field theory; Hilbert class fields

Summary. More on archimedean primes; Artin map; conductor; statement of global class field theory (Artin reciprocity, existence theorem); Hilbert class field; primes of the form $x^2 + ny^2$; principal ideal theorem; Hilbert symbols; Hilbert reciprocity law; power reciprocity law.

Content. There is an analogous statement for number fields, called the **global class field theory**. There is a version of the statements of global class field theory that is more directly analogous to the local class field theory, using the language of **adeles and ideles**. In that setup, the statement is something like, for a number field K, $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ is isomorphic to something (as topological groups). However, it is also a bit pedantic; as in the local class field theory case, the main issue is mainly topology, i.e. how to build a group with the correct topology, whereas the actual information carried by the statement is unrelated to the matter of topology. This viewpoint will be introduced only in the last lecture where we discuss how the class field theory is the starting point of the Langlands program.

In this lecture, we will formulate a more tangible and classical version of the global class field theory. As introduced in Exercise 15.1, we have to adopt a viewpoint where archimedean absolute values are also regarded as primes, **archimedean primes**. To summarize: given a number field K,

- a real embedding $K \hookrightarrow \mathbb{R}$ gives a **real prime**;
- a pair of complex embeddings $K \hookrightarrow \mathbb{C}$ gives a **complex prime**;
- an archimedean prime of an extension L/K lies over an archimedean prime of K if the corresponding embeddings restrict to one another;
- a complex prime lying over a real prime is considered **ramified**.

In particular, there is no inert case for archimedean primes (i.e. residue degrees are always 1).

Definition 16.1 (Archimedean completion)**.** Let K be a number field, and let v be an archimedean prime of K. Let K_v, the **completion of K at** v, be $\mathbb{R}$ if v is a real prime and $\mathbb{C}$ if v is a complex prime, endowed with its usual topology, and regarded as an archimedean local field. The completion K_v admits a natural map $K \hookrightarrow K_v$ (if v is complex, either complex embedding is fine; both are "topologically the same").

We have the analogues of the relation between number fields and local fields for archimedean primes, which are easy to verify.

Theorem 16.2. *Let K/L be an extension of number fields, and let v be an archimedean prime of L. Then,*

$$K \otimes_L L_v \cong \prod_{w \text{ primes of } K \text{ lying over } v} K_w.$$

Proof. If $L_v = \mathbb{C}$, there is nothing to prove. If $L_v = \mathbb{R}$ and $K = L(\alpha)$, then the number of real primes of K above v are precisely the number of real roots of the minimal polynomial $f(X) \in L[X] \subset L_v[X]$ of α over L, which implies the statement. □

Theorem 16.3 (Unramified archimedean primes in compositums, subfields and towers)**.** *Let L be a number field, and let v be an archimedean prime of L.*

(1) If $J/K/L$ is a tower of number fields, and if v is unramified in J, then v is unramified in K.

(2) Let $J/K/L$ be a tower of number fields, and suppose that v is unramified in K. Suppose also that, for every archimedean prime w of K lying over v, w is unramified in J. Then, v is unramified in J.

(3) If $K_1, K_2/L$ are two field extensions of number fields, such that v is unramified in both K_1 and K_2, then v is unramified in the compositum K_1K_2.

Proof. Completely analogous to the proof of Theorem 14.10 (much easier). □

Now we define the **Artin map** in the number fields context.

Definition 16.4 (Modulus)**.** Let K be a number field. A **finite modulus** is a nonzero ideal $\mathfrak{m}_f \subset \mathcal{O}_K$, regarded as a prime ideal factorization $\mathfrak{m}_f = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$. An **infinite modulus** $\mathfrak{m}_\infty$ is a (possibly empty) set of **real** primes of K; if a real prime v belongs to an infinite modulus $\mathfrak{m}_\infty$, we use the notation $v|\mathfrak{m}_\infty$. A **modulus** $\mathfrak{m}$ for K is a pair of a finite modulus $\mathfrak{m}_f$ (the **finite part** of the modulus) and an infinite modulus $\mathfrak{m}_\infty$ (the **infinite part** of the modulus), denoted as a product $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$.

Definition 16.5 ($J_K^{\mathfrak{m}}$)**.** Let K be a number field, and $\mathfrak{m}$ be a modulus for K. We define $J_K^{\mathfrak{m}}$ to be the group of fractional ideals whose prime factorizations do not contain any prime ideals dividing the finite part $\mathfrak{m}_f$ of the modulus $\mathfrak{m}$. Namely, $\mathfrak{a} \subset J_K^{\mathfrak{m}}$ if it is expressed as a fraction $\mathfrak{a} = \frac{\mathfrak{b}}{\mathfrak{c}}$ for integral ideals $\mathfrak{b}, \mathfrak{c} \subset \mathcal{O}_K$ such that both $\mathfrak{b}$ and $\mathfrak{c}$ are coprime to $\mathfrak{m}_f$.

Note that the definition of $J_K^{\mathfrak{m}}$ does not depend on the infinite part $\mathfrak{m}_\infty$ of the modulus $\mathfrak{m}$, and also does not depend on the exponents of the prime ideals in the finite part $\mathfrak{m}_f$.

Definition 16.6 (Artin map)**.** Let K/L be an abelian extension of number fields, and let $\mathfrak{m}$ be a modulus for L such that its finite part $\mathfrak{m}_f$ is divisible by every prime ideal of L that ramifies in K. We define the **Artin map** $\mathrm{Art}_{K/L}^{\mathfrak{m}} : J_L^{\mathfrak{m}} \to \mathrm{Gal}(K/L)$ as (cf. Definition 13.6)

$$\mathrm{Art}_{K/L}^{\mathfrak{m}}\left(\prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \mathfrak{p}^{n_\mathfrak{p}}\right) := \prod_{\mathfrak{p} \nmid \mathfrak{m}_f} \left(\frac{K/L}{\mathfrak{p}}\right)^{n_\mathfrak{p}}.$$

Remark 16.7. The definition of the Artin symbol (=Frobenius) $\left(\frac{K/L}{\mathfrak{p}}\right)$ can be extended to the case when K/L is an infinite algebraic extension. For a number field L, an algebraic extension K/L is **unramified** at a prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ if $\mathfrak{p}$ is unramified in every finite subextension F/L. For such K/L, for each finite subextension F/L, there is $\left(\frac{F/L}{\mathfrak{p}}\right) \in \mathrm{Gal}(F/L)$. As the collection of these elements are compatible with each other (Theorem 14.13), it defines an element $\left(\frac{K/L}{\mathfrak{p}}\right) \in \mathrm{Gal}(K/L)$ by Proposition 15.7.

The following is true.

Theorem 16.8. *Let K/L be an abelian extension of number fields, and let $\mathfrak{m}$ be a modulus for L such that its finite part $\mathfrak{m}_f$ is divisible by every prime ideal of L that ramifies in K. Then, the Artin map $\mathrm{Art}_{K/L}^{\mathfrak{m}} : J_L^{\mathfrak{m}} \to \mathrm{Gal}(K/L)$ is surjective.*

Proof. Let H be the image of $\mathrm{Art}_{K/L}^{\mathfrak{m}}$, and let $F = K^H$. Then, by definition, for every prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ that is coprime to $\mathfrak{m}_f$, $\left(\frac{F/L}{\mathfrak{p}}\right)$ is the image of $\left(\frac{K/L}{\mathfrak{p}}\right)$ in $\mathrm{Gal}(F/L) = \mathrm{Gal}(K/L)/H$, which is trivial. This implies that all but finitely many prime ideals of L split completely in F. This implies that, in F/L, the set of prime ideals

$$S = \{\mathfrak{p} \subset \mathcal{O}_L \ : \ \mathrm{Fr}_{\mathfrak{p}} = 1\},$$

has density 1. By the Chebotarev density theorem, Theorem 16.10, this implies that $F = L$, as desired. □

The above proof used the Chebotarev density theorem (which we will not prove) and the notion of density. This line of information is "analytic."

Definition 16.9 (Density)**.** Let K be a number field, and let S be a certain set of prime ideals of K. For a positive integer M, let

$$P_M := \{\mathfrak{p} \subset \mathcal{O}_K \text{ prime } : \ N(\mathfrak{p}) \leq M\}.$$

The **density** of S is the quantity, if exists,

$$\delta(S) := \lim_{M \to \infty} \frac{|S \cap P_M|}{|P_M|}.$$

Theorem 16.10 (Chebotarev density theorem)**.** *Let K/L be a finite Galois extension of number fields, and let $C \subset G := \mathrm{Gal}(K/L)$ be a subset that is stable under conjugation in G. Let*

$$S_C := \{\mathfrak{p} \subset \mathcal{O}_L \textit{ prime } : \ \mathfrak{p} \textit{ unramified in } K, \mathrm{Fr}_{\mathfrak{p}} \subset C\}.$$

Then, the density of S_C exists, and is equal to $\frac{|C|}{|G|}$.

For each modulus $\mathfrak{m}$, there is the notion of a "class group with modulus $\mathfrak{m}$":

Definition 16.11 (Ray class group)**.** Let K be a number field, and let $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$ be a modulus for K, where

$$\mathfrak{m}_f = \prod_{i=1}^{n} \mathfrak{p}_i^{r_i}.$$

Define $P_K^{\mathfrak{m}} \leq J_K^{\mathfrak{m}}$ to be the subgroup of the following kinds of principal ideals:

$$P_K^{\mathfrak{m}} := \left\{ \begin{array}{c} (\alpha) \text{ for } \alpha \in K^\times \text{ such that the following conditions hold.} \\ 1.\ \alpha = \frac{\beta}{\gamma} \text{ for } \beta, \gamma \in \mathcal{O}_K \text{ such that } ((\beta), \mathfrak{m}_f) = ((\gamma), \mathfrak{m}_f) = 1 \text{ (i.e. } (\alpha) \in J_K^{\mathfrak{m}}). \\ 2.\ \text{For each } 1 \leq i \leq n, \text{ if we let } v_{\mathfrak{p}} \text{ be the normalized discrete valuation of } K \text{ induced} \\ \text{by the normalized discrete valuation of } K_{\mathfrak{p}}, \text{ then } v_{\mathfrak{p}}(\alpha - 1) \geq r_i. \\ 3.\ \text{For each } v | \mathfrak{m}_\infty, v(\alpha) > 0, \text{ where } v : K \hookrightarrow \mathbb{R} \text{ is regarded as a real embedding.} \end{array} \right\}.$$

The **ray class group of K with modulus $\mathfrak{m}$** is defined as

$$\mathrm{Cl}_K^{\mathfrak{m}} := J_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}.$$

Example 16.12. If $\mathfrak{m}$ is a modulus where $\mathfrak{m}_f = (1)$ and $\mathfrak{m}_\infty$ is empty (we call such $\mathfrak{m}$ the **empty modulus**), then $\mathrm{Cl}_K^{\mathfrak{m}} = \mathrm{Cl}(K)$. The empty modulus is often just denoted as 1.

Proposition 16.13 (Finiteness of ray class group)**.** *Let K be a number field, and let $\mathfrak{m}$ be a modulus for K. Then, the ray class group $\mathrm{Cl}_K^{\mathfrak{m}}$ is finite.*

Proof. Note that the natural map $J_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$ is surjective. This is because this is equivalent to the statement that, given any fractional ideal I of K, there is $\alpha \in K^\times$ such that αI has no prime factors dividing $\mathfrak{m}_f$. If $\mathfrak{m}_f = \prod_{i=1}^n \mathfrak{p}_i^{k_i}$ and $I = (\prod_{i=1}^n \mathfrak{p}_i^{e_i}) \times \left(\prod_{j=1}^m \mathfrak{q}_i^{f_i}\right)$, where $\mathfrak{q}_1, \cdots, \mathfrak{q}_m$ are coprime to $\mathfrak{m}_f$, then by the weak approximation theorem, one can find $\alpha \in K^\times$ such that the power of $\mathfrak{p}_i$ in (α) is precisely $\mathfrak{p}_i^{-e_i}$. Then, αI will have no prime factor dividing $\mathfrak{m}_f$ involved in its prime factorization.

The above paragraph implies that $\mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$ is surjective, and its kernel is $(J_K^{\mathfrak{m}} \cap P_K)/P_K^{\mathfrak{m}}$. Thus, by the finiteness of class number, it suffices to prove that this kernel is finite. Let $K^{\mathfrak{m}} \subset K^\times$ be the subgroup of elements $\alpha \in K^\times$ such that $(\alpha) \in J_K^{\mathfrak{m}}$, and let $K^{\mathfrak{m},1} \subset K^\times$ be the subgroup of elements $\alpha \in K^{\mathfrak{m}}$ such that $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_f)$ for all $\mathfrak{p} | \mathfrak{m}_f$ and $v(\alpha) > 0$ for all $v | \mathfrak{m}_\infty$. Consider the composition of natural surjective maps

$$K^{\mathfrak{m}} \twoheadrightarrow J_K^{\mathfrak{m}} \cap P_K \twoheadrightarrow \frac{J_K^{\mathfrak{m}} \cap P_K}{P_K^{\mathfrak{m}}},$$

where $K^{\mathfrak{m},1}$ is obviously contained its kernel, so that we get a natural surjective map

$$\frac{K^{\mathfrak{m}}}{K^{\mathfrak{m},1}} \twoheadrightarrow \frac{J_K^{\mathfrak{m}} \cap P_K}{P_K^{\mathfrak{m}}}.$$

Therefore, it is sufficient to prove that $K^{\mathfrak{m}}/K^{\mathfrak{m},1}$ is finite. Consider the natural map

$$K^{\mathfrak{m}} \to \left(\prod_{v | \mathfrak{m}_\infty} \{\pm 1\}\right) \times (\mathcal{O}_K/\mathfrak{m}_f)^\times,$$

$$\alpha \mapsto ((\mathrm{sgn}(v(\alpha)))\,, \alpha).$$

It is obvious that the kernel is $K^{\mathfrak{m},1}$. Therefore, $|K^{\mathfrak{m}}/K^{\mathfrak{m},1}| \leq 2^{\#\{v \,:\, v | \mathfrak{m}_\infty\}}(N(\mathfrak{m}_f) - 1)$, which implies that $K^{\mathfrak{m}}/K^{\mathfrak{m},1}$ is finite, as desired. □

The main upshot of global class field theory is that **we know precisely when the Artin map $\mathrm{Art}_{K/L}^{\mathfrak{m}}$ factors through the ray class group, i.e. when $\ker \mathrm{Art}_{K/L}^{\mathfrak{m}} \supset P_L^{\mathfrak{m}}$.**

Theorem 16.14 (Artin reciprocity)**.** *Let K/L be a finite abelian extension of number fields. Then, there exists a modulus for L, the **conductor** of K/L, denoted $\mathfrak{f}_{K/L}$, such that whenever a modulus*

$\mathfrak{m}$ *for* L *is divisible by the conductor* $\mathfrak{f}_{K/L}$*, the kernel of the Artin map* $\mathrm{Art}^{\mathfrak{m}}_{K/L} : J^{\mathfrak{m}}_L \twoheadrightarrow \mathrm{Gal}(K/L)$ *is equal to*

$$\ker \mathrm{Art}^{\mathfrak{m}}_{K/L} = P^{\mathfrak{m}}_L N_{K/L}(J^{\mathfrak{m}}_K).$$

Furthermore, the kernel contains $P^{\mathfrak{m}}_L$*, yielding a surjective map*

$$\mathrm{Art}^{\mathfrak{m}}_{K/L} : \mathrm{Cl}^{\mathfrak{m}}_L \twoheadrightarrow \mathrm{Gal}(K/L).$$

The Artin map satisfies the commutative diagram: if K'/L' *is an abelian extension, and* L/L' *is an extension of number fields, such that* $K = LK'$ *is abelian over* L*, for* $\mathfrak{m}_L$ *and* $\mathfrak{m}_{L'}$ *moduli of* L, L'*, respectively, such that, for every* $\mathfrak{p}|(\mathfrak{m}_L)_f$*,* $(\mathfrak{p} \cap \mathcal{O}_{L'})|(\mathfrak{m}_{L'})_f$*,*

$$\begin{array}{ccc} J^{\mathfrak{m}_L}_L & \xrightarrow{\mathrm{Art}^{\mathfrak{m}_L}_{K/L}} & \mathrm{Gal}(K/L) \\ {\scriptstyle N_{L/L'}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ J^{\mathfrak{m}_{L'}}_{L'} & \xrightarrow[\mathrm{Art}^{\mathfrak{m}_{L'}}_{K'/L'}]{} & \mathrm{Gal}(K'/L') \end{array}$$

Theorem 16.15 (Existence theorem)**.** *Let* K *be a number field. For each modulus* $\mathfrak{m}$ *for* K*, there exists a unique abelian extension of* K*, called the* ***ray class field*** *of* K *for modulus* $\mathfrak{m}$*, denoted* $K(\mathfrak{m})$*, such that* $\mathfrak{f}_{K(\mathfrak{m})/K}|\mathfrak{m}$*, and the Artin map for modulus* $\mathfrak{m}$ *induces an isomorphism*

$$\mathrm{Art}^{\mathfrak{m}}_{K(\mathfrak{m})/K} : \mathrm{Cl}^{\mathfrak{m}}_K \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{m})/K).$$

Therefore, there is an one-to-one inclusion-reversing correspondence,

$$\{\textit{Finite subgroups of } \mathrm{Cl}^{\mathfrak{m}}_K\} \leftrightarrow \left\{\textit{Finite abelian extensions } J/K \textit{ with } \mathfrak{f}_{J/K}|\mathfrak{m}\right\},$$

$$H \mapsto K(\mathfrak{m})^H,$$

$$\mathrm{Gal}(K(\mathfrak{m})/J) \hookleftarrow J.$$

Remark 16.16. There is a more modern formulation of the Artin map where the reciprocity establishes a literal isomorphism with $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ for a number field K, just like the case of the local class field theory. This involves packaging $\mathrm{Cl}^{\mathfrak{m}}_K$ for varying $\mathfrak{m}$ appropriately as a single topological group, and this is often done using the language of **ideles**. On the other hand, as in the case of local class field theory, the formulation is pretty much irrelevant and the essential content of the theorem does not change.

The global and local class field theories must be compatible in some way. In that regard, the following is quite natural.

Definition 16.17 (Local conductor of an abelian extension of number fields)**.** Let L/K be a finite abelian extension of number fields, and let $\mathfrak{p}$ be a prime of K (including the case of archimedean primes). The **local conductor** of L/K at $\mathfrak{p}$, denoted $\mathfrak{f}_{L/K,\mathfrak{p}}$, is defined as follows. If $\mathfrak{p} \subset \mathcal{O}_K$ is a maximal ideal, then $\mathfrak{f}_{L/K,\mathfrak{p}} := \mathfrak{f}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$, where $\mathfrak{q}$ is a prime of L lying over $\mathfrak{p}$ (the local conductor $\mathfrak{f}_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}$ is independent of the choice of $\mathfrak{q}$). If $\mathfrak{p}$ is an archimedean prime, then $\mathfrak{f}_{L/K,\mathfrak{p}} = 1$ if $\mathfrak{p}$ is a real prime and a prime of L lying over $\mathfrak{p}$ is a complex prime (again, it is either all primes over $\mathfrak{p}$ are real or all primes over $\mathfrak{p}$ are complex), and 0 otherwise.

Theorem 16.18 (Computing the conductor)**.** *Let L/K be a finite abelian extension of number fields. Then, the conductor $\mathfrak{f}_{L/K}$ is equal to*

$$\mathfrak{f}_{L/K} = (\mathfrak{f}_{L/K})_f (\mathfrak{f}_{L/K})_\infty, \quad (\mathfrak{f}_{L/K})_f := \prod_{\mathfrak{p} \subset \mathcal{O}_K \text{ maximal}} \mathfrak{p}^{\mathfrak{f}_{L/K,\mathfrak{p}}}, \quad (\mathfrak{f}_{L/K})_\infty := \prod_{\mathfrak{p} \text{ archimedean prime of } K,\, \mathfrak{f}_{L/K,\mathfrak{p}} = 1} \mathfrak{p}.$$

More concisely, one can write as

$$\mathfrak{f}_{L/K} = \prod_{\mathfrak{p} \text{ prime of } K} \mathfrak{p}^{\mathfrak{f}_{L/K,\mathfrak{p}}}.$$

The case of empty modulus is of particular importance.

Definition 16.19 (Hilbert class field)**.** Let K be a number field. The ray class field $K(1)$ of K for the empty modulus is called the **Hilbert class field**, also denoted H_K. By definition, this is the maximal abelian unramified (including all archimedean primes) extension of K.

By Theorem 14.10 and Theorem 16.3, it is easy to see without the global class field theory that the Hilbert class field exists (it is the compositum of all finite abelian unramified extensions), but it is already unclear whether the Hilbert class field is a finite extension over K. The global class field theory implies the following

Corollary 16.20. *Let K be a number field.*

(1) The Hilbert class field H_K is a finite extension over K, and $\mathrm{Gal}(H_K/K) \cong \mathrm{Cl}(K)$.

(2) Let $\mathfrak{p} \subset \mathcal{O}_K$ be a maximal ideal, and let m be the order of the element $[\mathfrak{p}] \in \mathrm{Cl}(K)$. For any prime ideal $\mathfrak{q} \subset \mathcal{O}_{H_K}$ lying over $\mathfrak{p}$, $f(\mathfrak{q}|\mathfrak{p}) = m$.

Proof. (1) Immediate from the definition of ray class field.

(2) As the isomorphism $\mathrm{Cl}(K) \cong \mathrm{Gal}(H_K/K)$ comes from the Artin map $\mathrm{Art}^1_{H_K/K} : J_K \to \mathrm{Gal}(H_K/K)$, the order of $[\mathfrak{p}] \in \mathrm{Cl}(K)$ is equal to the order of $\left(\frac{H_K/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(H_K/K)$, which is the same as the residue degree $f(\mathfrak{q}|\mathfrak{p})$.

□

Remark 16.21. It is a theorem of Golod–Shafarevich that there exists a number field with infinite degree unramified Galois extension, necessarily with nonabelian Galois group.

There is a surprising turn: this gives a complete characterization of when a prime is of the form $x^2 + ny^2$ for many n's!

Corollary 16.22. *Let $n \in \mathbb{N}$ be a squarefree integer such that $n \not\equiv 3 \pmod 4$. Then, for an odd prime p not dividing n,*

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow p \text{ splits completely in } H_{\mathbb{Q}(\sqrt{-n})}.$$

Similarly, for $n \in \mathbb{N}$ a squarefree integer with $n \equiv 3 \pmod 4$, then, for an odd prime p not dividing n,

$$p = x^2 + xy + \frac{n+1}{4} y^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow p \text{ splits completely in } H_{\mathbb{Q}(\sqrt{-n})}.$$

Proof. Let $K = \mathbb{Q}(\sqrt{-n})$. Note that $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$ in the case of $n \not\equiv 3 \pmod 4$ and $p = x^2 + xy + \frac{n+1}{4}y^2$ for some $x, y \in \mathbb{Z}$ in the case of $n \equiv 3 \pmod 4$, if and only if $p = N_{K/\mathbb{Q}}(\alpha)$ for some $\alpha = x + y\sqrt{-n} \in \mathbb{Z}[\sqrt{-n}] = \mathcal{O}_K$. As p is unramified in K, this is equivalent to saying that p splits completely in K, $(p) = \mathfrak{p}\overline{\mathfrak{p}}$, and that $\mathfrak{p}$ is a principal ideal. By Corollary 16.20, $\mathfrak{p}$ being a principal ideal is equivalent to $\mathfrak{p}$ splitting completely in H_K, which finishes the proof. □

The latter condition has a rather concrete description.

Theorem 16.23. *Let $n \in \mathbb{N}$ be a squarefree integer, and let $K = \mathbb{Q}(\sqrt{-n})$.*

(1) The Hilbert class field H_K is Galois over $\mathbb{Q}$.

(2) Choose an embedding $\iota : H_K \hookrightarrow \mathbb{C}$. There exists a real algebraic integer $\alpha \in \mathcal{O}_{H_K} \cap \mathbb{R}$ such that $H_K = K(\alpha)$.

(3) Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Let $p \in \mathbb{Z}$ be an odd rational prime that does not divide n and also not divide the discriminant of the polynomial $f(X)$. Then,

$$\left\{\begin{matrix} p = x^2 + ny^2 & n \not\equiv 3 \pmod 4 \\ p = x^2 + xy + \frac{n+1}{4}y^2 & n \equiv 3 \pmod 4 \end{matrix}\right\} \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow \left(\frac{-n}{p}\right) = 1 \text{ and } f(X) \equiv 0 \pmod p \text{ has a solution in } \mathbb{F}_p.$$

Proof. (1) Let $\iota : H_K \hookrightarrow \mathbb{C}$ be an embedding, and let $\sigma : \mathbb{C} \to \mathbb{C}$ be the complex conjugation. Then $\sigma(H_K)$ is the maximal abelian unramified extension of $\sigma(K) = K$, so $\sigma(H_K) = H_K$. This implies that $\mathrm{Aut}_{\mathbb{Q}}(H_K) = \mathrm{Gal}(H_K/K) \coprod \sigma\,\mathrm{Gal}(H_K/K)$, so that $H_K/\mathbb{Q}$ is Galois.

(2) Note that $H_K \cap \mathbb{R} = H_K^{\tau=1}$, which, by Galois theory, is a subfield with $[H_K : H_K \cap \mathbb{R}] = 2$. Take $\alpha \in H_K \cap \mathbb{R}$ such that $H_K \cap \mathbb{R} = \mathbb{Q}(\alpha)$: then, $H_K \supset K(\alpha) \supset\neq \mathbb{Q}(\alpha)$, which implies that $K(\alpha) = H_K$. We can multiply α by a large enough integer so that α is an algebraic integer.

(3) By Corollary 16.22, we know that the left hand side holds if and only if p splits completely in H_K. By the knowledge of prime splitting in quadratic fields, we know that p splits completely in K if and only if $\left(\frac{-n}{p}\right) = 1$. Let $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K. We would like to use Dedekind's criterion for $\mathfrak{p}$, which requires $(p, [\mathcal{O}_{H_K} : \mathcal{O}_K[\alpha]]) = 1$. Note that $[\mathcal{O}_{H_K} : \mathcal{O}_K[\alpha]]$ divides $\mathrm{disc}(\mathcal{O}_K[\alpha])$. Let $\beta \in \mathcal{O}_K$ be such that $\mathcal{O}_K = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \beta$. Then, $\mathcal{O}_K[\alpha]$ is a free $\mathbb{Z}$-module with basis $1, \alpha, \cdots, \alpha^{[H_K:K]-1}, \beta, \beta\alpha, \cdots, \beta\alpha^{[H_K:K]-1}$, which implies that $\mathrm{disc}(\mathcal{O}_K[\alpha]) = \mathrm{disc}(\mathbb{Z}[\alpha])^2 \,\mathrm{disc}(\mathcal{O}_K)^{[H_K:K]}$, which is not divisible by p by assumption. Therefore, we can use the Dedekind's criterion, that $\mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha] \cong \mathcal{O}_{H_K}/\mathfrak{p}\mathcal{O}_{H_K}$. As $f(X)$ has a solution in $\mathbb{F}_p = \mathcal{O}_K/\mathfrak{p}$, there is a prime $\mathfrak{q} \subset \mathcal{O}_{H_K}$ lying over $\mathfrak{p}$ such that $f(\mathfrak{q}|\mathfrak{p}) = 1$. Since H_K/K is Galois, this means that $e = f = 1$, so $\mathfrak{p}$ splits completely in H_K. It is clear that this is an equivalence.

□

Example 16.24 (The case of $x^2 + 5y^2$, redux)**.** Recall that in Example 10.26 we showed that $K = \mathbb{Q}(\sqrt{-5})$ has class number 2 and showed that, for $p \neq 2, 5$,

$$\text{either } p \text{ or } 2p \text{ is } x^2 + 5y^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow \left(\frac{-5}{p}\right) = 1.$$

We want to use Theorem 16.23, which means we need to compute the Hilbert class field H_K, which is an unramified degree 2 extension of K. We claim that H_K is the field $J = K(\sqrt{5}) = K(\sqrt{-1})$. As all archimedean primes of K are already complex, any archimedean prime of K is unramified in J. Thus, we need to prove that $\operatorname{disc}(J/K)$ is the unit ideal. Using the K-basis $\{1, \sqrt{-1}\}$ of J, we see that

$$-4 = \det \begin{pmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{pmatrix}^2 \in \operatorname{disc}(J/K).$$

Using the K-basis $\{1, \frac{1+\sqrt{5}}{2}\}$ of J, we see that

$$5 \in \det \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 \in \operatorname{disc}(J/K).$$

Thus, $1 = 5 - 4 \in \operatorname{disc}(J/K)$, which implies that $\operatorname{disc}(J/K)$ is a unit ideal, as desired. Thus, this implies that $J = H_K$. Thus, using Theorem 16.23 with $\alpha = \sqrt{5}$, $f(X) = X^2 - 5$, we see that, for $p \neq 2, 5$,

$$p = x^2 + 5y^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow \left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) = 1.$$

The Hilbert class field has another nice property.

Theorem 16.25 (Principal ideal theorem)**.** *Let K be a number field. For every maximal ideal $\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{p}\mathcal{O}_{H_K}$ is a principal ideal in $\mathcal{O}_{H_K}$.*

Proof. We want to prove that the natural map $\operatorname{Cl}(K) \to \operatorname{Cl}(H_K)$, $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{H_K}$, sends everything to zero. As we have the isomorphisms coming from the Artin reciprocity law,

$$\operatorname{Art}^1_{H_K/K} : \operatorname{Cl}(K) \xrightarrow{\sim} \operatorname{Gal}(H_K/K),$$

$$\operatorname{Art}^1_{H_{H_K}/H_K} : \operatorname{Cl}(H_K) \xrightarrow{\sim} \operatorname{Gal}(H_{H_K}/H_K),$$

we wonder if the natural map $\operatorname{Cl}(K) \to \operatorname{Cl}(H_K)$ has another description in terms of $\operatorname{Gal}(H_K/K) \to \operatorname{Gal}(H_{H_K}/H_K)$. Note that H_{H_K}/K is Galois, as any element in $\operatorname{Gal}(\overline{K}/K)$ sends H_{H_K} to the maximal unramified abelian extension of the maximal unramified abelian extension of K, which is just H_{H_K} again. Thus, $\operatorname{Gal}(H_{H_K}/K)$ is solvable, with an abelian normal subgroup $\operatorname{Gal}(H_{H_K}/H_K)$ and an abelian quotient $\operatorname{Gal}(H_K/K)$, or that $\operatorname{Gal}(H_K/K) = \operatorname{Gal}(H_{H_K}/K)^{\mathrm{ab}}$.

Let $\mathfrak{p} \subset \mathcal{O}_K$ be a maximal ideal. Let $\mathfrak{q}_1, \cdots, \mathfrak{q}_g \subset \mathcal{O}_{H_K}$ be the prime ideals lying over $\mathfrak{p}$, so that

$$\mathfrak{p}\mathcal{O}_{H_K} = \mathfrak{q}_1 \cdots \mathfrak{q}_g.$$

Then,

$$\mathrm{Art}^1_{H_{H_K}/H_K}(\mathfrak{p}\mathcal{O}_{H_K}) = \prod_{i=1}^{g} \left(\frac{H_{H_K}/H_K}{\mathfrak{q}_i} \right).$$

Let $\mathfrak{r}_i \subset \mathcal{O}_{H_{H_K}}$ be a prime ideal lying over $\mathfrak{q}_i$. Then,

$$\left(\frac{H_{H_K}/H_K}{\mathfrak{q}_i} \right) = \mathrm{Fr}(\mathfrak{r}_i|\mathfrak{p})^{f(\mathfrak{q}_i|\mathfrak{p})}.$$

Therefore, if we enumerate the representatives of $\mathrm{Gal}(H_{H_K}/K)/\mathrm{Gal}(H_{H_K}/H_K)$ as $g_1, \cdots, g_{h_K}$, then we have

$$\mathrm{Art}^1_{H_{H_K}/H_K}(\mathfrak{p}\mathcal{O}_{H_K}) = \prod_{i=1}^{h_K} g_{f(i)}^{-1} \mathrm{Fr}(\mathfrak{r}|\mathfrak{p}) g_i \in \mathrm{Gal}(H_{H_K}/K)^{\mathrm{ab}},$$

for any prime $\mathfrak{r} \subset \mathcal{O}_{H_{H_K}}$ lying over $\mathfrak{p}$, where $g_{f(i)}$ is such that $\mathrm{Fr}(\mathfrak{r}|\mathfrak{p})g_i \in g_{f(i)}\,\mathrm{Gal}(H_{H_K}/H_K)$. As $\mathrm{Fr}(\mathfrak{r}|\mathfrak{p}) = \left(\frac{H_K/K}{\mathfrak{p}}\right)$, the map $\mathrm{Cl}(K) \to \mathrm{Cl}(H_K)$ has the following group-theoretic description, with $H = \mathrm{Gal}(H_{H_K}/H_K) \leq G = \mathrm{Gal}(H_{H_K}/K)$: if we denote the representatives of G/H as $g_1, \cdots, g_h$, then we have a map

$$G^{\mathrm{ab}} \to H^{\mathrm{ab}}, \quad x \mapsto \prod_{i=1}^{h} g_{f(i)}^{-1} x g_i,$$

where again $g_{f(i)}$ is such that $xg_i \in g_{f(i)}H$. This follows from the following tricky group-theory lemma whose proof we will not provide as it is irrelevant. □

Lemma 16.26. *Let G be a finite group, and let $H = [G, G]$. Let $g_1, \cdots, g_n$ be the representatives of G/H, and define*

$$V : G^{\mathrm{ab}} \to H^{\mathrm{ab}}, \quad x \mapsto \prod_{i=1}^{n} g_{f(i)}^{-1} x g_i,$$

where $g_{f(i)}$ is such that $xg_i \in g_{f(i)}H$. Then, $V = 0$.

We record the relative relationship of various quantities.

Proposition 16.27.

(1) Let K/L be an extension of number fields. Suppose that $H_L \cap K = L$. Then, $h_L | h_K$.

(2) Let K/L be an extension of number fields, such that there exists a prime $\mathfrak{p}$ of L (maybe archimedean) that is totally ramified in K. Then, $h_L | h_K$. For example, if K/L is a quadratic extension where a complex prime of K restricts to a real prime of L, then $h_L | h_K$.

(3) Let $J/K/L$ be a tower of either local or number fields. Then, $\mathfrak{f}_{K/L} | \mathfrak{f}_{J/L}$.

Proof.

(1) Note that H_LK/K is abelian, as $\mathrm{Gal}(H_L/L) = \mathrm{Gal}(H_L/K \cap H_L) = \mathrm{Gal}(H_LK/K)$. Also, by the same reason, H_LK/K is unramified. Thus, $H_LK \leq H_K$, so $h_L | h_K$.

(2) As $H_L \cap K = L$, its follows from (1).

(3) It follows from the transitivity of norms.

□

Remark 16.28. In general, if K/L is an extension of number fields, h_K and h_L have no relationship.

As another Diophantine application of global class field theory, we understand the algebraic proof of quadratic reciprocity law in a more general context in relation to global class field theory.

Definition 16.29 (μ_n)**.** Let $n > 1$ be a positive integer. We define μ_n to be the group of n-th roots of unity. It is abstractly isomorphic as a group to $\mathbb{Z}/n\mathbb{Z}$.

Definition 16.30 (Hilbert symbols)**.** Let $n > 1$ be a positive integer, and let K be a local field of characteristic 0 that contains μ_n. Then, for $a, b \in K^\times$, the n-**th Hilbert symbol** $(a, b) \in \mu_n$ is such that

$$(a, b) = \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}},$$

where $\sigma \in \mathrm{Gal}(K(\sqrt[n]{b})/K)$ is the natural image of $\mathrm{Art}_K(a) \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ under the natural quotient map $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(K(\sqrt[n]{b})/K)$.

If K is a number field that contains μ_n, and $\mathfrak{p}$ is a prime of K (maybe archimedean), then for $a, b \in K^\times$, we define $(a, b)_\mathfrak{p} := (a, b)$ defined using $a, b \in K_\mathfrak{p}^\times$.

Proposition 16.31. *The local Hilbert symbols satisfy the following properties.*

(1) $(a_1, b)(a_2, b) = (a_1a_2, b)$ *and* $(a, b_1)(a, b_2) = (a, b_1b_2)$.

(2) $(a, b) = (b, a)^{-1}$.

Proof. (1) Clear from the definition.

(2) Let $x \in K$ be such that $x^n - b \neq 0$. Then,

$$x^n - b = \prod_{i=0}^{n-1} (x - \zeta_n^i \sqrt[n]{b}),$$

which implies that $x^n - b \in N_{K(\sqrt[n]{b})/K}(K(\sqrt[n]{b})^\times)$[28]. Thus, $(x^n - b, b) = 1$. Therefore, in particular, $(-b, b) = 1$. We have

$$(a, b) = (a, -a)(a, b) = (a, -ab), \quad (b, a) = (b, a)(b, -b) = (b, -ab),$$

[28]To be very precise, we have to take into account the cases when some m-th root of b exists in K, but the general case is not much different from this case.

so

$$(a,b)(b,a) = (a,-ab)(b,-ab) = (ab,-ab) = 1,$$

as desired.

□

When $(n,p) = 1$, the n-th Hilbert symbol for a p-adic local field becomes more concrete, and is often also called the **tame Hilbert symbol**.

Theorem 16.32 (Tame Hilbert symbols)**.** *Let $(n,p) = 1$, and let K be a p-adic local field which contains μ_n. Let $\mathfrak{p} \subset \mathcal{O}_K$ be the maximal ideal, v_K be the normalized discrete valuation, and q be the order of the residue field of K.*

(1) The prime-to-p-power roots of unity of K form a group μ_{q-1}. In particular, $n|(q-1)$.

(2) For every $x \in \mathcal{O}_K^\times$, there exists a unique $\omega(x) \in \mu_{q-1}$ such that $x \equiv \omega(x) \pmod{\mathfrak{p}}$.

(3) For $x \in \mathcal{O}_K^\times$, the extension $K(\sqrt[n]{x})/K$ is unramified.

(4) For $a, b \in K^\times$, we have

$$(a,b) = \omega\left((-1)^{v_K(a)v_K(b)}\frac{b^{v_K(a)}}{a^{v_K(b)}}\right)^{\frac{q-1}{n}}.$$

In particular, $(a,b) = 1$ if $a, b \in \mathcal{O}_K^\times$, and $(\pi_K, b) = \omega(b)^{\frac{q-1}{n}} \equiv b^{\frac{q-1}{n}} \pmod{\mathfrak{p}}$ for a uniformizer $\pi_K \in K$ and $b \in \mathcal{O}_K^\times$.

Proof. (1) By Hensel's lemma, μ_{q-1} in the residue field $\mathbb{F}_q$ lifts to $\mu_{q-1} \subset \mathcal{O}_K^\times$. On the other hand, if $\mu_n \subset \mathcal{O}_K^\times$, then as $X^n - 1$ is separable mod $\mathfrak{p}$, it must have $\mu_n \subset \mathbb{F}_q^\times$, implying that $n|(q-1)$.

(2) This is immediate from (1).

(3) As $\mathbb{F}_q(\sqrt[n]{x})/\mathbb{F}_q$ is of degree n, $f_{K(\sqrt[n]{x})/K} \geq n$, which implies that $f = n$ and $e = 1$, so the extension is unramified.

(4) The general formula follows from the special cases when $b \in \mathcal{O}_K^\times$ and a is either π_K or in $\mathcal{O}_K^\times$, because of the multiplicativity. By (3), $K(\sqrt[n]{b})/K$ is unramified, so in particular $\mathrm{Art}_K(a) \in \mathrm{Gal}(K(\sqrt[n]{b})/K)$ is 1 if $a \in \mathcal{O}_K^\times$ and Fr if $a = \pi_K$, hence the formula.

□

Theorem 16.33 (Hilbert reciprocity law)**.** *Let K be a number field containing μ_n, and let $a, b \in K^\times$. Then,*

$$\prod_{\mathfrak{p} \text{ prime of } K} (a,b)_{\mathfrak{p}} = 1.$$

This is some form of the compatibility between the local Artin map and the (global) Artin map; it is called the **local-global compatibility**. As the proof requires an idelic version of global class field theory, we will not prove here. Rather, we deduce a vast generalization of quadratic reciprocity law, called the **power reciprocity law**.

Definition 16.34 (Power residue symbols)**.** Let $n > 1$ be a positive integer, and let K be a number field containing μ_n. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a maximal ideal lying over p, where $(p, n) = 1$. For any uniformizer $\pi_{K_\mathfrak{p}}$ of $K_\mathfrak{p}$ and $a \in K^\times \cap \mathcal{O}_{K_\mathfrak{p}}^\times$, let the n-**th power residue symbol** $\left(\frac{a}{\mathfrak{p}}\right) \in \mu_n$ be defined as

$$\left(\frac{a}{\mathfrak{p}}\right) := (\pi_{K_\mathfrak{p}}, a)_\mathfrak{p},$$

which is independent of the choice of $\pi_{K_\mathfrak{p}}$ by Theorem 16.32. We define, for $\mathfrak{a} \subset \mathcal{O}_K$ an ideal, with $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{k_i}$,

$$\left(\frac{a}{\mathfrak{a}}\right) := \prod_{i=1}^n \left(\frac{a}{\mathfrak{p}_i}\right)^{k_i},$$

whenever the right hand side makes sense. If $\mathfrak{a}$ is a principal ideal, we also write its generator in the denominator.

Theorem 16.35 (Power reciprocity law)**.** *Let $n > 1$ be a positive integer. Let K be a number field containing μ_n, and let $a, b \in K^\times$ be coprime to each other, and to n. Then,*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|n\infty} (a, b)_\mathfrak{p}.$$

Proof. If $\mathfrak{p}$ is prime to $bn\infty$, then, if we let $v_\mathfrak{p}$ be the normalized discrete valuation on $K_\mathfrak{p}$,

$$\left(\frac{b}{\mathfrak{p}}\right)^{v_\mathfrak{p}(a)} = (\pi_{K_\mathfrak{p}}, b)_\mathfrak{p}^{v_\mathfrak{p}(a)} = (a, b)_\mathfrak{p}(u, b)_\mathfrak{p} = (a, b)_\mathfrak{p},$$

by Theorem 16.32, where $\pi_{K_\mathfrak{p}} \in K_\mathfrak{p}$ is a uniformizer and $u \in \mathcal{O}_{K_\mathfrak{p}}^\times$ is a unit with $a = \pi_{K_\mathfrak{p}}^{v_\mathfrak{p}(a)} u$. Thus

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|(b)} \left(\frac{a}{\mathfrak{p}}\right)^{v_\mathfrak{p}(b)} \prod_{\mathfrak{p}|(a)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_\mathfrak{p}(a)} = \prod_{\mathfrak{p}|(b)} (b, a)_\mathfrak{p} \prod_{\mathfrak{p}|(a)} (a, b)_\mathfrak{p}^{-1} = \prod_{\mathfrak{p}|(ab)} (b, a)_\mathfrak{p}.$$

Here, the subscript $\mathfrak{p}|(a)$ for example means that $v_\mathfrak{p}(a) \neq 0$. Since $(b, a)_\mathfrak{p} = 1$ for $\mathfrak{p}$ prime to $abn\infty$, by Hilbert Reciprocity Law, Theorem 16.33,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}|(ab)} (b, a)_\mathfrak{p} = \prod_{\mathfrak{p} \not| n\infty} (b, a)_\mathfrak{p} = \prod_{\mathfrak{p}|n\infty} (b, a)_\mathfrak{p}^{-1} = \prod_{\mathfrak{p}|n\infty} (a, b)_\mathfrak{p}.$$

□

The power reciprocity law is a massive generalization of quadratic reciprocity law. As a sanity check, we see how the quadratic reciprocity law follows from the power reciprocity law.

Example 16.36 (Quadratic reciprocity from power reciprocity)**.** We apply the power reciprocity law, Theorem 16.35, for $K = \mathbb{Q}$ and $n = 2$ (possible since $\mu_2 = \{\pm 1\} \subset \mathbb{Q}$). Then, for $a, b \in \mathbb{Z}$ odd and coprime integeres,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (a,b)_2(a,b)_\infty.$$

Note that the power residue symbol $\left(\frac{a}{b}\right)$ really is the (multiplicatively extended) Legendre symbol, because if p, q are odd distinct primes, $\left(\frac{p}{q}\right) \in \{\pm 1\}$ and is congruent to $p^{\frac{q-1}{2}} \bmod q$. So what are $(a,b)_2$ and $(a,b)_\infty$?

- By the local Artin reciprocity, Theorem 15.10, $(a,b)_2 = 1$ if and only if a is a norm from $\mathbb{Q}_2(\sqrt{b})/\mathbb{Q}_2$. This extension is unramified if and only if $b \equiv 1 \pmod 4$ (cf. Exercise 13.4), so $a \in \mathcal{O}_{\mathbb{Q}_2}^\times$ is in the norm if $b \equiv 1 \pmod 4$. If not, we consider if $x^2 - by^2 = a$ has solutions in $x, y \in \mathbb{Q}_2$. Suppose $a \equiv 1 \pmod 4$. Then, as $b \equiv 3 \pmod 4$, either a or $a-4$ is congruent to $-b$ mod 8, so either $\frac{a}{-b}$ or $\frac{a-4}{-b}$ is $\equiv 1 \pmod 8$. By Exercise 13.4, this has a square root in $\mathbb{Z}_2$, which means that $x^2 - by^2 = a$ has solutions (with either $x = 0$ or $x = 2$). On the other hand, if $a \equiv 3 \pmod 4$, then $x^2 - by^2 \equiv x^2 + y^2 \pmod 4$ can never by equal to $3 \pmod 4$, so $x^2 - by^2 = a$ has no solutions in $\mathbb{Z}_2$. If $x^2 - by^2 = a$ has solutions in $\mathbb{Q}_2$, then $x = \frac{w}{2^n}$, $y = \frac{z}{2^n}$ for some $n > 0$. Let n be minimal such, so that either w or z is odd. Then, from $w^2 - bz^2 = 4^n a$, we have $w^2 \equiv bz^2 \pmod 4$, so $b \equiv 1 \pmod 4$, a contradiction. Thus, $x^2 - by^2 = a$ has no solutions in $\mathbb{Q}_2$. Thus,

$$(a,b)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = \begin{cases} 1 & \text{if either } a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4 \\ -1 & \text{otherwise.} \end{cases}$$

- By definition, $(a,b)_\infty = 1$ if and only if $\mathrm{Art}_{\mathbb{R}}(a)$ fixes $\sqrt{b}$. Note that $\mathrm{Art}_{\mathbb{R}}(a)$ is the identity if $a > 0$ and the complex conjugation if $a < 0$, so the only way that $\mathrm{Art}_{\mathbb{R}}(a)$ can send $\sqrt{b}$ to a different number is when $a < 0$ and $\sqrt{b}$ is a complex number, i.e. when $b < 0$. Thus,

$$(a,b)_\infty = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}\frac{\mathrm{sgn}(b)-1}{2}} = \begin{cases} 1 & \text{if either } a > 0 \text{ or } b > 0 \\ -1 & \text{otherwise.} \end{cases}$$

Thus,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2} + \frac{\mathrm{sgn}(a)-1}{2}\frac{\mathrm{sgn}(b)-1}{2}}.$$

This in particular contains the case of $\left(\frac{-1}{p}\right)$. One can also compute $\left(\frac{2}{p}\right)$ for an odd prime $p \in \mathbb{Z}$ by hand, namely

$$\left(\frac{2}{p}\right) = (p,2)_p,$$

and since $(p,2)_q = 1$ for any $q \neq 2, p, \infty$, by the Hilbert reciprocity law,

$$(p,2)_p = (2,p)_2 (2,p)_\infty.$$

Since $2, p > 0$, $(2,p)_\infty = 1$, so $(p,2)_p = (2,p)_2$. Now the question is whether 2 is the norm from $\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2$, i.e. if $x^2 - py^2 = 2$ has solutions in $x, y \in \mathbb{Q}_2$, or if $x^2 - py^2 = 2^{2n+1}$ has solutions in $x, y \in \mathbb{Z}_2$, $n \geq 0$ such that if $n > 1$, either x or y is odd. Obviously if both x and y are even, then $x^2 - py^2$ is divisible by 4, so the condition is just always x or y odd. If only one of them is odd, then $x^2 - py^2$ is simply odd, so we want both x, y odd. This implies that $2^{2n+1} = x^2 - py^2 \equiv 1 - p \pmod 8$, so $1 - p$ is congruent to either 0 or 2 mod 8, or p is congruent to either 1 or 7 mod 8. Conversely, if $p \equiv 1 \pmod 8$, then $1 - py^2 = 8$ has a solution $y \in \mathbb{Z}_2$, and if $p \equiv 7 \pmod 8$, then $1 - py^2 = 2$ has a solution in $\mathbb{Z}_2$ (cf. Exercise 13.4), so $(2,p)_2 = 1$. Thus,

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

Using the prototype as above, we may try to prove more general reciprocity laws in elementary terms.

Example 16.37 (Cubic reciprocity)**.** We now want to do the similar thing for $n = 3$. For that, we want to use the number field $K = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. Note that $\mathcal{O}_K = \mathbb{Z}[\zeta_3] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a PID, so a UFD. Note that a rational prime $p \in \mathbb{Z}$ is inert in K if $p \equiv 2 \pmod 3$ and splits completely in K if $p \equiv 1 \pmod 3$. Also, 3 is totally ramified, with $(3) = \mathfrak{p}_3^2$ where $\mathfrak{p}_3 = (1 - \zeta_3)$. As K has no real prime, the power reciprocity law says that, if $a, b \in K^\times$ are coprime to each other and to 3, then

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = (a,b)_{\mathfrak{p}_3}.$$

Note that K has quite a few units, $\{\pm 1\} \times \mu_3$, so an ideal-theoretic statement does not translate verbatim into a number-theoretic statement (i.e. there is always the unit worth of ambiguity in the process of taking a generator of an ideal). To have a clean statement, people often use the concept of **primary numbers**.

Definition 16.38 (Primary numbers)**.** A number $\alpha \in \mathbb{Z}[\zeta_3]$ is **primary** if $(\alpha, 3) = 1$ and

$$\alpha \equiv 2 \pmod{(1 - \zeta_3)^2}.$$

Note that $(1 - \zeta_3)^2 = \zeta_3^2 - 2\zeta_3 + 1 = -3\zeta_3$, so a number $a + b\zeta_3 \in \mathbb{Z}[\zeta_3]$, $a, b \in \mathbb{Z}$, is primary if and only if $3|b$ and $a \equiv 2 \pmod 3$.

Starting from a rational prime $p \in \mathbb{Z}$, it is as itself a primary number if $p \equiv 2 \pmod 3$. What about a prime ideal $\mathfrak{p} \subset \mathbb{Z}[\zeta_3]$, $N(\mathfrak{p}) \equiv 1 \pmod 3$?

Lemma 16.39. *Given a maximal ideal $\mathfrak{p} \subset \mathbb{Z}[\zeta_3]$, $N(\mathfrak{p}) \equiv 1 \pmod 3$, there is exactly one generator $\pi \in \mathfrak{p}$ that is a primary number.*

Proof. Take a generator $x = a + b\zeta_3$, $a, b \in \mathbb{Z}$, of $\mathfrak{p}$. Then, the possible generators of $\mathfrak{p}$ are $\pm x$, $\pm\zeta_3 x$, $\pm\zeta_3^2 x$, or

$$a + b\zeta_3, \quad -a - b\zeta_3, \quad -b + (a-b)\zeta_3, \quad b - (a-b)\zeta_3, \quad (b-a) - a\zeta_3, \quad -(b-a) + a\zeta_3.$$

Note that $a^2 - ab + b^2$ is a rational prime $\equiv 1 \pmod 3$, so either a or b is not a multiple of 3. If $3|a$, then exactly one of $(b-a) - a\zeta_3$ or $-(b-a) + a\zeta_3$ is primary. If $3|b$, then exactly one of $a + b\zeta_3$ or $-a - b\zeta_3$ is primary. If neither of these happen, then $a^2 - ab + b^2 \equiv 2 - ab \equiv 1 (\mathrm{mod}\, 3)$, which implies that $ab \equiv 1 \pmod 3$ or $a \equiv b \pmod 3$. Thus, exactly one of $-b + (a-b)\zeta_3$ or $b - (a-b)\zeta_3$ is primary. □

Now let α, β be primary primes of K. Then, by definition,

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{(\beta)}\right) = (\pi_{K_\beta}, \alpha)_{(\beta)},$$

which, by tame Hilbert symbol, Theorem 16.32, is equal to the power of ζ_3 that is congruent to $\alpha^{\frac{N(\beta)-1}{3}}$ mod β. Note that this is 1 if and only if $\alpha \pmod \beta$ is a cubic residue.

Now we can state the cubic reciprocity law.

Theorem 16.40 (Cubic reciprocity law)**.** *Let $K = \mathbb{Q}(\zeta_3)$, and let $\pi_1, \pi_2 \in \mathcal{O}_K$ be primary primes. Then,*

$$\left(\frac{\pi_1}{\pi_2}\right) = \left(\frac{\pi_2}{\pi_1}\right).$$

Proof. By the earlier observation, it suffices to prove that $(\pi_1, \pi_2)_{\mathfrak{p}_3} = 1$. This only depends on the classes that π_1, π_2 belong to in $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^3$, so let's first identify what this is. Since $\zeta_3 - 1 \in \mathcal{O}_L$ is a uniformizer which is Eisenstein (cf. Exercise **??**), we see that $\mathcal{O}_L = \mathbb{Z}_3[\zeta_3 - 1] = \mathbb{Z}_3[\zeta_3]$. Note that $e_{L/\mathbb{Q}_3} = 3$, so by Exercise 13.2 (because $r = 2 > \frac{e}{p-1} = \frac{3}{2}$),

$$(1 + (\zeta_3 - 1)^2\mathcal{O}_L, \times) \cong ((\zeta_3 - 1)^2\mathcal{O}_L, +) = (3\mathcal{O}_L, +),$$

by the exponential and the logarithm. Thus, under this correspondence, $(1 + (\zeta_3 - 1)^2\mathcal{O}_L)^3 \cong 3(\zeta_3 - 1)^2\mathcal{O}_L = (\zeta_3 - 1)^4\mathcal{O}_L$, so in the multiplicative world we have

$$(1 + (\zeta_3 - 1)^2\mathcal{O}_L)^3 = 1 + (\zeta_3 - 1)^4\mathcal{O}_L.$$

Thus, $(\mathcal{O}_L^\times)^3 \supset 1 + (\zeta_3 - 1)^4\mathcal{O}_L$. Thus, we only need to check the classes of primary primes in $\mathcal{O}_L^\times/(1 + (\zeta_3 - 1)^4\mathcal{O}_L)$. As $(\zeta_3 - 1)^2 = -3\zeta_3$, this is just the congruence classes modulo 9. If $x = a + b\zeta_3$ is a primary prime, $a, b \in \mathbb{Z}$, then $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$. Thus, x modulo 9 must be congruent to $a(1 + b\zeta_3)$ for $a = 2, 5, 8$, $b = 0, 3, -3$. Note that $(x, x)_{\mathfrak{p}_3} = (x, x)_{\mathfrak{p}_3}^{-1}$, so $(x, x)_{\mathfrak{p}_3}^2 = 1$, which is only possible when $(x, x)_{\mathfrak{p}_3} = 1$. Also, 8 is a cube, and we can replace 5 by -4. So, we have to show

$$(2, -4)_{\mathfrak{p}_3} = 1, \quad (1 + 3\zeta_3, 1 - 3\zeta_3)_{\mathfrak{p}_3} = 1,$$

$$(a, 1 + b\zeta_3)_{\mathfrak{p}_3} = 1, \quad a = 2, -4, \quad b = \pm 3.$$

Note that $(2,2)_{\mathfrak{p}_3} = (2,-2)_{\mathfrak{p}_3} = 1$ so the first identity follows. Also,

$$(-4, 1+b\zeta_3)_{\mathfrak{p}_3} = (2, 1+b\zeta_3)^2_{\mathfrak{p}_3}(-1, 1+b\zeta_3)_{\mathfrak{p}_3} = (2, 1+b\zeta_3)^2_{\mathfrak{p}_3},$$

as -1 is a cube. Finally, as $(1+3\zeta_3)^{-1} \equiv 1-3\zeta_3 \pmod 9$, so $(1+3\zeta_3, 1-3\zeta_3)_{\mathfrak{p}_3} = (1+3\zeta_3, (1+3\zeta_3)^{-1})_{\mathfrak{p}_3} = (1+3\zeta_3, 1+3\zeta_3)^{-1}_{\mathfrak{p}_3} = 1$, and $(2, 1-3\zeta_3)_{\mathfrak{p}_3} = (2, (1+3\zeta_3)^{-1})_{\mathfrak{p}_3} = (2, 1+3\zeta_3)^{-1}_{\mathfrak{p}_3}$. Thus, we only need to prove that

$$(2, 1+3\zeta_3)_{\mathfrak{p}_3} = 1.$$

Note that $N_{K/\mathbb{Q}}(1+3\zeta_3) = 7$, and 7 splits completely in K as

$$(7) = (1+3\zeta_3)\overline{(1+3\zeta_3)} = (1+3\zeta_3)(2+3\zeta_3).$$

On the other hand, 2 is inert in K. Thus, by the Hilbert reciprocity law,

$$(2, 1+3\zeta_3)_{\mathfrak{p}_3} = (1+3\zeta_3, 2)_2(1+3\zeta_3, 2)_{1+3\zeta_3} = (2, 1+3\zeta_3)_2^{-1}(1+3\zeta_3, 2)_{1+3\zeta_3}.$$

We can compute the symbols on the right hand side as the tame Hilbert symbols. Note that $K_2 = \mathbb{Q}_2(\zeta_3)$ is the degree 2 unramified extension of $\mathbb{Q}_2$, so

$$(2, 1+3\zeta_3)_2 = \omega(1+3\zeta_3)^{\frac{4-1}{3}} = \omega(1+3\zeta_3).$$

Note that

$$1+3\zeta_3 = 2\zeta_3 - \zeta_3^2 \equiv \zeta_3^2 \pmod 2,$$

so $(2, 1+3\zeta_3)_2 = \zeta_3^2$. On the other hand, $K_{(1+3\zeta_3)} = \mathbb{Q}_7$, so

$$(1+3\zeta_3, 2)_{1+3\zeta_3} = \omega(2)^{\frac{7-1}{3}} = \omega(2)^2.$$

We want to show that $\omega(2) = \zeta_3$, which means that $2 \equiv \zeta_3 \pmod{1+3\zeta_3}$. This is indeed true, as $(1+3\zeta_3)\zeta_3^2 = \zeta_3^2 + 3 = 2 - \zeta_3$. Therefore, $(2, 1+3\zeta_3)_{\mathfrak{p}_3} = 1$ as desired. □

What does Theorem 16.40 mean in concrete terms? We want to answer whether, given integers m, n, m is a cubic residue mod n in a systematic way.

Definition 16.41 (Rational cubic residue symbol)**.** Let $m, n \in \mathbb{Z}$ be coprime integers. The **rational cubic residue symbol** is defined as

$$\left[\frac{m}{n}\right]_3 := \begin{cases} 1 & \text{if } m \text{ is a cubic residue mod } n \\ -1 & \text{otherwise.} \end{cases}$$

For a prime $p \neq 3$, if $p \equiv 2 \pmod 3$, then every congruence class mod 3 is a cubic residue, as $(3, p-1) = 1$. Thus, it is interesting only if $p \equiv 1 \pmod 3$. As p splits completely in K, this means there is $\alpha := a + b\zeta_3 \in \mathbb{Z}[\zeta_3]$, $a, b \in \mathbb{Z}$, such that $a^2 - ab + b^2 = p$. As seen above, there is a unique $a, b \in \mathbb{Z}$ satisfying $a^2 - ab + b^2 = p$, $3|b$, $a \equiv 2 \pmod 3$. As $\mathcal{O}_K/\alpha\mathcal{O}_K \cong \mathbb{F}_p$, we can compute $\left[\frac{m}{p}\right]_3$ in terms of $\left(\frac{m}{\alpha}\right)$. For example:

Proposition 16.42 (Euler). *Let $p \equiv 1 \pmod 3$ be a rational prime, so that $p = a^2 - ab + b^2$, $a, b \in \mathbb{Z}$, with $3|b$ and $a \equiv 2 \pmod 3$.*[29]

(1) We have $\left[\frac{2}{p}\right]_3 = 1$ if and only if $2|b$.

(2) We have $\left[\frac{5}{p}\right]_3 = 1$ if and only if either $5|b$ or $5|(2a-b)$.

(3) If $p \neq 7$, we have $\left[\frac{7}{p}\right]_3 = 1$ if and only if $7|b$ or $7|(2a-b)$.

Proof. Let $\alpha = a + b\zeta_3 \in \mathbb{Z}[\zeta_3]$. Let $K = \mathbb{Q}(\zeta_3)$.

(1) Note that, by cubic reciprocity, $\left[\frac{2}{p}\right]_3 = 1$ if and only if $\left(\frac{\alpha}{2}\right) = 1$. As 2 is inert in K, we see that $\left(\frac{\alpha}{2}\right) = 1$ if and only if $\alpha \in \mathcal{O}_K/2\mathcal{O}_K$ is a cube. Note that $\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_4$ with representatives $\{0, 1, \zeta_3, 1+\zeta_3\}$, and 1 is the only nonzero cubic residue here. Thus, $\left(\frac{\alpha}{2}\right) = 1$ if and only if $2|b$ and a is odd. Since $2|b$ implies automatically that a is odd (as p is odd), we get the result.

(2) Note that, by cubic reciprocity, $\left[\frac{5}{p}\right]_3 = 1$ if and only if $\left(\frac{\alpha}{5}\right) = 1$. As 5 is inert in K, we see that $\left(\frac{\alpha}{5}\right) = 1$ if and only if $\alpha \in \mathcal{O}_K/5\mathcal{O}_K$ is a cube. Note that $\mathcal{O}_K/5\mathcal{O}_K \cong \mathbb{F}_{25}$ with representatives $\{a + b\zeta_3 \mid 0 \leq a, b \leq 4\}$. There are 8 nonzero cubic residues here, and we know that $1, 2, 3, 4$ are cubic residues. Furthermore,

$$(\zeta_3 - 1)^3 = \zeta_3^3 - 3\zeta_3^2 + 3\zeta_3 - 1 = 6\zeta_3 + 3 \equiv \zeta_3 + 3 \pmod 5,$$

is a cubic residue, so $x(\zeta_3 + 3)$, $x = 1, 2, 3, 4$, are. These subsume all the 8 nonzero cubic residues in $\mathcal{O}_K/5\mathcal{O}_K$. Thus, $\alpha \in \mathcal{O}_K/5\mathcal{O}_K$ is a cube if and only if either $5|b$ or $a \equiv 3b \pmod 5$ (the latter condition is the same as $(2a-b)$ being divisible by 5).

(3) Note that, by cubic reciprocity, $\left[\frac{7}{p}\right]_3 = 1$ if and only if $\left(\frac{\alpha}{7}\right) = 1$. Note that 7 splits completely in K, as

$$(7) = (\beta)(\overline{\beta}), \quad \beta = 1 + 3\zeta_3,$$

where $\bar{\cdot}$ is the conjugation. Thus, $\left(\frac{\alpha}{7}\right) = \left(\frac{\alpha}{\beta}\right)\left(\frac{\alpha}{\overline{\beta}}\right)$. Both symbols can be computed as the tame Hilbert symbol. Note that

$$\left(\frac{\alpha}{\beta}\right) = \omega_\beta(\alpha)^{\frac{7-1}{3}} = \omega_\beta(\alpha)^2,$$

where $\omega_\beta(\alpha) \in \{1, \zeta_3, \zeta_3^2\}$ is such that $\omega_\beta(\alpha) \equiv \alpha \pmod \beta$. This implies that $\beta|(\alpha - \omega_\beta(\alpha))$, so $\overline{\beta}|(\overline{\alpha} - \overline{\omega_\beta(\alpha)})$. This implies that

$$\omega_{\overline{\beta}}(\overline{\alpha}) = \overline{\omega_\beta(\alpha)} = \omega_\beta(\alpha)^{-1}.$$

[29] Note that $4p = 4a^2 - 4ab + 4b^2 = (2a-b)^2 + 3b^2$, so, with $3|b$, one can write as $p = \frac{1}{4}(L^2 + 27M^2)$ for some $L, M \in \mathbb{Z}$, and this representation is unique up to the sign changes of L and M. Then, (1) is the same as $2|M$ (which implies $2|L$), (2) is the same as $5|LM$, and (3) is the same as $7|LM$.

Thus,

$$\left(\frac{\alpha}{7}\right) = \omega_\beta(\alpha)^2\omega_{\overline{\beta}}(\alpha)^2 = \omega_\beta(\alpha)^2\omega_\beta(\overline{\alpha})^{-2}.$$

So we are looking for when $\omega_\beta(\alpha) = \omega_\beta(\overline{\alpha})$. Note that $\mathcal{O}_K/\beta\mathcal{O}_K \cong \mathbb{F}_7$, so there are 2 nonzero cubic residues, ± 1. Thus, $\omega_\beta(\alpha) = \omega_\beta(\overline{\alpha})$ if and only if $\frac{\alpha}{\overline{\alpha}} \equiv \pm 1 \pmod{\beta}$, or $\alpha \pm \overline{\alpha} \equiv 0 \pmod{\beta}$. Note that $\alpha + \overline{\alpha} = 2a + b\zeta_3 + b\zeta_3^2 = 2a - b$, and $\alpha - \overline{\alpha} = b\zeta_3 - b\zeta_3^2 = b\zeta_3(1-\zeta_3)$. As $2a-b \in \mathbb{Z}$, $2a-b$ is divisible by β if and only if $2a-b$ is in $\beta\mathcal{O}_K \cap \mathbb{Z} = 7\mathbb{Z}$, or if $2a \equiv b \pmod{7}$. On the other hand, $b\zeta_3(1-\zeta_3)$ is b times a unit times an element of norm 3, so $b\zeta_3(1-\zeta_3)$ is divisible by β if and only if b is divisible by β, which, again by the same logic, is equivalent to $7|b$.

□

– –

Exercise 16.1. Let $L = \mathbb{Q}(\sqrt{3})$.

(1) Show that $h_L = 1$, so that the Hilbert class field of L is $H_L = L$.

(2) Let $K = L(\sqrt{-1})$. Show that every prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ is unramified in K.

(3) Why are (1) and (2) consistent with the global class field theory?

Hint. Compute the conductor $\mathfrak{f}_{K/L}$.

Exercise 16.2. In this question, we determine the ray class fields of $\mathbb{Q}$. Let ∞ denote the unique archimedean prime of $\mathbb{Q}$.

(1) Let $m > 1$ is such that $v_2(m) \neq 1$. Show that the kernel of the Artin map

$$\mathrm{Art}^m_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} : J^m_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}),$$

is equal to $P^{m\infty}_{\mathbb{Q}}$. Deduce that $\mathbb{Q}(\zeta_m)$ is the ray class field of $\mathbb{Q}$ for modulus $m\infty$. Deduce that $\mathfrak{f}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} = n\infty$ with $n|m$.

(2) Retaining the same notation as (1), show that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$. Deduce that $n = m$.

(3) For $m \geq 1$ odd, show that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$. Deduce that, for $n \geq 1$,

$$\mathfrak{f}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = \begin{cases} 1 & \text{if } n = 1 \\ \frac{n}{2}\infty & \text{if } n \text{ is even, } \frac{n}{2} \text{ is odd} \\ n\infty & \text{otherwise.} \end{cases}$$

(4) For a finite extension $K/\mathbb{Q}_2$, show that the local conductor $\mathfrak{f}_{K/\mathbb{Q}_2}$ cannot be equal to 1.

(5) Using (3) and (4), deduce that the ray class field of $\mathbb{Q}$ for modulus $\mathfrak{m}$ is

$$\mathbb{Q}(\mathfrak{m}) = \begin{cases} \mathbb{Q}(\zeta_n) & \text{if } \mathfrak{m} = n\infty \\ \mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1}) & \text{if } \mathfrak{m} = n. \end{cases}$$

Exercise 16.3. In this question, we revisit Exercise 10.3 on the primes $p \neq 2, 7$ of the form $p = x^2 + 14y^2$ for some integers $x, y \in \mathbb{Z}$. We have already seen that $\mathrm{Cl}(\mathbb{Q}(\sqrt{-14})) \cong \mathbb{Z}/4\mathbb{Z}$.

(1) Let $K = \mathbb{Q}(\sqrt{-14})$ and $K' = K(\sqrt{2})$. Show that K'/K is an unramified extension (including the archimedean primes).

Hint. Use that $K' = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ and that 2 splits completely in $\mathbb{Q}(\sqrt{-7})$.

(2) Let $K'' = K'(\sqrt{2\sqrt{2} - 1})$. Using that $(2\sqrt{2} - 1)(-2\sqrt{2} - 1) = -7$, show that $K'' = K'(\sqrt{-2\sqrt{2} - 1})$. Using the discriminant, show that K''/K' is unramified at every prime coprime to 2 (including the archimedean primes).

(3) Note that $2\sqrt{2} - 1 = (1 + \sqrt{2})^2 - 4$, so that $K'' = K'(\alpha)$, where

$$\alpha = \frac{1 + \sqrt{2} + \sqrt{2\sqrt{2} - 1}}{2}, \quad \alpha^2 - (1 + \sqrt{2})\alpha + 1 = 0.$$

Using the discriminant, show that K''/K' is unramified at every prime.

(4) Show that K''/K is an abelian extension. Deduce that $K'' = H_K$.

(5) Show that, for $p \neq 2, 7$ a rational prime,

$$p = x^2 + 14y^2 \text{ for some } x, y \in \mathbb{Z} \Leftrightarrow \left(\frac{-14}{p}\right) = 1 \text{ and } X^4 + 2X^2 - 7 \equiv 0 \pmod{p} \text{ has an integer solution.}$$

Exercise 16.4. Let $n > 1$ be an odd integer, and let K be a local field of characteristic 0 that contains μ_n. For $a, b \in K^\times$ with $a \neq -b$, show that

$$(a, b) = (a, a + b)(a + b, b).$$

Hint. Let $a + b = c$. Then, we have

$$1 = (1 - ac^{-1}, ac^{-1}) = (bc^{-1}, ac^{-1}).$$

Use that -1 is an n-th power.

Exercise 16.5. Let p be an odd rational prime, and let $K = \mathbb{Q}(\zeta_p)$. Let $\pi = 1 - \zeta_p$, which generates the unique prime ideal $\mathfrak{p} = (\pi)$ lying over p (more precisely, $p = \mathfrak{p}^{p-1}$), and define $e_i = 1 - \pi^i$ for $i \geq 1$.

(1) Using Exercise 13.2, show that, in $K_{\mathfrak{p}}$, $(1+\pi^2\mathcal{O}_{K_{\mathfrak{p}}},\times) \cong (\pi^2\mathcal{O}_{K_{\mathfrak{p}}},+)$. Deduce that $(\mathcal{O}_{K_{\mathfrak{p}}}^{\times})^p \supset 1+\pi^{p+1}\mathcal{O}_{K_{\mathfrak{p}}}$.

(2) For $i,j \geq 1$ with $i+j \geq p+1$, use $e_i + \pi^i e_j = e_{i+j}$ and Question 4 to show that $(e_i, e_j)_{\mathfrak{p}} = 1$.

Hint. Using (1), show that e_{i+j} is a p-th power in $K_{\mathfrak{p}}$. Apply Question 4 to $(e_i, \pi^i e_j)$.

(3) Show that, if $x \in 1+\pi^i\mathcal{O}_{K_{\mathfrak{p}}}$, x can be expressed as an infinite product

$$x = e_i^{m_i} e_{i+1}^{m_{i+1}} \cdots, \qquad \text{for some } m_i, m_{i+1}, \cdots \in \mathbb{Z}.$$

Here, the above expression means that the sequence $x_i, x_{i+1}, \cdots \in \mathcal{O}_{K_{\mathfrak{p}}}$ defined by

$$x_j := e_i^{m_i} e_{i+1}^{m_{i+1}} \cdots e_j^{m_j}, \quad j \geq i,$$

converges to x.

Hint. Note that $\mathcal{O}_{K_{\mathfrak{p}}}/\pi\mathcal{O}_{K_{\mathfrak{p}}} \cong \mathbb{F}_p$ with representatives $\{0,1,\cdots,p-1\}$. Deduce that, if $x \equiv 1 + r\pi^i \pmod{\pi^{i+1}}$, $0 \leq n \leq p-1$, then $\frac{x}{e_i^{-r}} \equiv 1 \pmod{\pi^{i+1}}$.

(4) Show that for $a, b \in K^{\times}$ coprime to each other and to p, such that $a, b \equiv 1 \pmod{\pi^{\frac{p+1}{2}}}$, the p-th power residue symbols satisfy

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

17. Lecture 22. Dirichlet's unit theorem

Summary. Dirichlet's unit theorem; Pell's equations; continued fractions; fundamental units of real quadratic fields.

Content. We now move on to the "analytic" aspect of algebraic number theory. It is an oxymoron that there is an analytic aspect in algebraic number theory, but this provides crucial tools that are otherwise not easily accessed by just using pure algebra. There is a general theme of L-**functions** (e.g. the Riemann zeta function) and **periods** (e.g. π, $\log 2$, etc.) that appear in algebraic number theory that are a priori analytic but essentially encoding algebraic and geometric information, and they involve things like special functions (e.g. logarithm and exponential) or integrals of those with all numbers written in the formulae are algebraic numbers. For example, we have already seen the usefulness of logarithms and exponentials in the study of p-adic local fields (really, local fields are made to do analysis over them).

As we saw earlier, the algebraic approach gives a very clean statement in terms of the ideals, but an ideal-theoretic statement does not translate well into a number-theoretic statement because an ideal can have many choices for its generators. This ambiguity comes mostly from the **units**. Dirichlet's unit theorem gives a precise structure of the group of units, $\mathcal{O}_K^\times$, for a number field K.

Theorem 17.1 (Dirichlet's unit theorem)**.** *Let K be a number field with r real embeddings and s pairs of complex embeddings. Then,*

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1},$$

where μ_K is the group of roots of unity in K, which is a finite cyclic group.

Proof. Let $\sigma_1, \cdots, \sigma_r : K \to \mathbb{R}$ be the different real embeddings of K, and let $\sigma_{r+1}, \cdots, \sigma_{r+s} : K \to \mathbb{C}$ be the s complex embeddings, one from each pair of complex conjugates. Recall that we know that $x \in \mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(x) = \pm 1$; thus, it is natural to consider the logarithmic version of what we used for the proof of finiteness of class number,

$$L : K^\times \to \mathbb{R}^{r+s}, \quad x \mapsto (\log|\sigma_1(x)|, \cdots, \log|\sigma_r(x)|, 2\log|\sigma_{r+1}(x)|, \cdots, 2\log|\sigma_{r+s}(x)|).$$

Note that, for $x \in \mathcal{O}_K^\times$, $N_{K/\mathbb{Q}}(x) = \pm 1$ implies that

$$\sigma_1(x)\cdots\sigma_r(x)|\sigma_{r+1}(x)|^2\cdots|\sigma_{r+s}(x)|^2 = \pm 1.$$

Therefore, $L(\mathcal{O}_K^\times) \subset V$, where $V \subset \mathbb{R}^{r+s}$ is an $r+s-1$-dimensional Euclidean space defined by

$$V := \{(t_1, t_2, \cdots, t_{r+s}) \in \mathbb{R}^{r+s} \mid t_1 + t_2 + \cdots + t_{r+s} = 0\}.$$

The image $L(\mathcal{O}_K^\times)$ is an additive subgroup of V. A crucial fact is that $L(\mathcal{O}_K^\times)$ is a **discrete subgroup** of V. This can be proved as follows.

Definition 17.2 (Height)**.** Let $\alpha \in \overline{\mathbb{Q}}$ be an **algebraic integer**. The **height** of α, denoted $H(\alpha)$, is defined as

$$H(\alpha) := \max\{|\alpha'| \ : \ \alpha' \text{ is a conjugate of } \alpha\}.$$

More generally, for an **algebraic number** $\alpha \in \overline{\mathbb{Q}}$, the height of α, $H(\alpha)$, is defined as

$$H(\alpha) := d(\alpha) \max\{1 \ , \ \max\{|\alpha'| \ : \ \alpha' \text{ is a conjugate of } \alpha\}\},$$

where $d(\alpha) \in \mathbb{N}$ is the minimal integer such that $d(\alpha)\alpha$ is an algebraic integer.

The notion of height measures the complexity of an algebraic number: a height of an algebraic number is large if "either the numerator or the denominator is large."

Lemma 17.3 (Northcott property)**.** *Let $n \in \mathbb{N}$ and $M > 0$. Then, there are finitely many algebraic numbers α whose degree (i.e. the degree of the minimal polynomial over $\mathbb{Q}$) is $\leq n$ and whose height is $< M$.*

Proof. As $H(\alpha) \geq d(\alpha)$, there are finitely many choices of $d(\alpha)$. Thus, it is sufficient to prove this for algebraic integers. Let $\alpha_1, \cdots, \alpha_m$ be the conjugates of α, and let $p(X) = X^m + a_1 X^{m-1} + \cdots + a_m \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Then, a_i is, up to sign, the sum of the products of all possible i-tuples from $\alpha_1, \cdots, \alpha_m$. Therefore,

$$|a_i| \leq \binom{m}{i} H(\alpha)^i,$$

so that if we assert $H(\alpha) < M$, then $|a_i| < \binom{m}{i} M^i$. As $a_i \in \mathbb{Z}$, there are finitely many choices for the polynomial. Thus, there are finitely many choices for $p(X)$ (note that we also assert $m \leq n$). As each polynomial has at most n roots, we get the desired result. □

Thus, the notion of heights gives a way to enumerate the countable set $\overline{\mathbb{Q}}$ (in the order of increasing degree and height).

Now, suppose we choose an open ball $D(0, R)$ of some radius $R > 0$ around $0 \in \mathbb{R}^{r+s}$, i.e.

$$D(0, R) = \{(t_1, \cdots, t_{r+s}) \in \mathbb{R}^{r+s} \mid t_1^2 + \cdots + t_{r+s}^2 < R^2\}.$$

To show that $L(\mathcal{O}_K^\times)$ is discrete, it suffices to prove that $L(\mathcal{O}_K^\times) \cap D(0, R)$ is a finite set. On the other hand, if $\alpha \in \mathcal{O}_K^\times$ has $L(\alpha) \in D(0, R)$, then this implies that $\log |\sigma_i(\alpha)| < R$ for every i. Thus, $H(\alpha) < e^R$, and α has degree $\leq [K : \mathbb{Q}]$, so by the Northcott property, Theorem 17.3, there are only finitely many α's in the intersection, as desired.

The above paragraph not only proves that $L(\mathcal{O}_K^\times)$ is a discrete subgroup but also proves that $\ker L$ is finite! Note that $\alpha \in \mathcal{O}_K^\times \cap \ker L$ means that $|\alpha'| = 1$ for every conjugate α' of α. As any integer power of α has the same property, we see that $\{1, \alpha, \alpha^2, \cdots\} \subset \ker L \cap \mathcal{O}_K^\times$. As $\ker L \cap \mathcal{O}_K^\times$ is finite, it follows that $\{1, \alpha, \alpha^2, \cdots\}$ is a finite set, i.e. $\alpha^m = 1$ for some $m > 0$! Therefore, it follows that $\ker L \cap \mathcal{O}_K^\times$ is precisely consisted of the roots of unity in K, which is usually denoted as μ_K. We already know that μ_K is a finite abelian group, and it is actually a cyclic group: if we let m be the lcm of the orders of all roots of unity in μ_K, then $\mu_K \cong \mathbb{Z}/m\mathbb{Z}$

(i.e. there is a primitive m-th root of unity in μ_K). This is because if $m = \prod_{i=1}^k p_i^{e_i}$ is the prime factorization, then by definition there is $\zeta_i \in \mu_K$ whose order is divisible by $p_i^{e_i}$, so by taking an appropriate power of ζ_i, we have $\zeta_i' \in \mu_K$ which is a primitive $p_i^{e_i}$-th root of unity, then $\zeta_1' \cdots \zeta_k'$ is a primitive m-th root of unity (check!).

Anyway, we have

$$\mathcal{O}_K^\times/\mu_K \cong L(\mathcal{O}_K^\times).$$

Since $L(\mathcal{O}_K^\times)$ is an additive subgroup of V, it is torsion-free. Furthermore, as $L(\mathcal{O}_K^\times) \subset V$ is a discrete subgroup, $L(\mathcal{O}_K^\times)$ is a free $\mathbb{Z}$-module of rank $\leq \dim_{\mathbb{R}} V$. This is because of the following lemma.

Lemma 17.4. *Let $M \subset \mathbb{R}^n$ be a discrete subgroup. Then, M is a free $\mathbb{Z}$-module of rank $r \leq n$.*

Proof. We use an induction on n. If $n = 1$, then we want to show that M is free of rank ≤ 1. Otherwise, M has $\mathbb{Z}$-linearly independent elements $v_1, v_2 \in M \subset \mathbb{R}$. By scaling, we can let $v_1 = 1$. Then, v_2 is not a rational number by assumption. Then, for any $N > 0$, there is a big enough $N' \in \mathbb{N}$ such that $N'v_2$ has fractional part in between $-\frac{1}{N}$ and $\frac{1}{N}$, which is a simple pigeonhole principle. This contradicts the discreteness of M.

Now for general $n > 1$, if the $\mathbb{R}$-span of M is strictly smaller than $\mathbb{R}^n$, then we can use induction hypothesis of smaller dimension. Thus, we can assume that the $\mathbb{R}$-span of M is $\mathbb{R}^n$. Suppose also that M is not of rank $\leq n$. Then, there are $\mathbb{Z}$-linearly independent elements $v_1, \cdots, v_{n+1} \in M$, and by the dimension reason, they are necessarily $\mathbb{R}$-linearly dependent. We can choose $v_1, \cdots, v_{n+1}$ so that the $\mathbb{R}$-span is $\mathbb{R}^n$. Then, there is, up to scaling, only one $\mathbb{R}$-linear relation, $a_1v_1 + \cdots + a_{n+1}v_{n+1} = 0$. Since $v_1, \cdots, v_{n+1}$ has no $\mathbb{Q}$-linear relation, it follows that the $\mathbb{Q}$-vector space spanned by $a_1, \cdots, a_{n+1}$ in $\mathbb{R}$ is of dimension > 1. As $n + 1 \geq 3$, one can choose one a_i such that the rest of a's still span a $\mathbb{Q}$-vector space of dimension ≥ 2 (otherwise this means that the ratio between every pair of a's is a rational number, which cannot hold). After reshuffling the index, we can assume that the $\mathbb{Q}$-span of $a_1, \cdots, a_n$ in $\mathbb{R}$ is of dimension > 1. Then, it follows that any $\mathbb{Z}$-linear combination of $v_1, \cdots, v_n$ is not a scalar multiple of v_{n+1}. Thus, if we take the orthogonal projection along v_{n+1} of $M \subset \mathbb{R}^n$ to $\mathbb{R}^{n-1}$, then the images of $v_1, \cdots, v_n$ in $\mathbb{R}^{n-1}$ are still $\mathbb{Z}$-linearly independent, which by induction cannot happen, a contradiction. □

This implies first that $\mathcal{O}_K^\times$ is a finitely generated abelian group, and the torsion part of $\mathcal{O}_K^\times$ is precisely μ_K, and, by the fundamental theorem of finitely generated abelian groups, we have the decomposition

$$\mathcal{O}_K^\times \cong \mu_K \times L(\mathcal{O}_K^\times).$$

We now only need to compute the rank of $L(\mathcal{O}_K^\times)$, i.e. show that it is of full rank. We make use of the embedding we used in the proof of finiteness of class number:

$$\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s, \quad x \mapsto (\sigma_1(x), \cdots, \sigma_r(x), \sigma_{r+1}(x), \cdots, \sigma_{r+s}(x)).$$

Take $R > 0$ big enough such that the radius R ball centered at the origin, $D(0, R) \subset \mathbb{R}^r \times \mathbb{C}^s$, satisfies $\mathrm{vol}(D(0, R)) > 2^{r+2s} \mathrm{vol}(D_{\sigma(\mathcal{O}_K)})$, where $\mathrm{vol}(D_{\sigma(\mathcal{O}_K)})$ is the volume of a fundamental parallelopiped of $\sigma(\mathcal{O}_K) \subset \mathbb{R}^r \times \mathbb{C}^s$. By Minkowski's theorem, there is a nonzero element $\sigma(x) \in$

$\sigma(\mathcal{O}_K) \cap D(0,R)$, $x \in \mathcal{O}_K \backslash \{0\}$. Note that, by definition, $|N_{K/\mathbb{Q}}(x)| < R^{r+2s}$, and as $N_{K/\mathbb{Q}}(x)$ is a nonzero integer, there are finitely many possibilities for $N_{K/\mathbb{Q}}(x)$.

Now consider $W \subset \mathbb{R}^r \times \mathbb{C}^s$,

$$W = \{(x_1, \cdots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \ : \ |x_1 \cdots x_r x_{r+1}^2 \cdots x_{r+s}^2| = 1\}.$$

Then consider, for $\alpha = (\alpha_1, \cdots, \alpha_{r+s}) \in W$, the region

$$\alpha D(0,R) = \{(\alpha_1 x_1, \cdots, \alpha_{r+s} x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \ : \ (x_1, \cdots, x_{r+s}) \in D(0,R) \subset \mathbb{R}^r \times \mathbb{C}^s\}.$$

As multiplying by α gives an $\mathbb{R}$-linear isomorphism $\mathbb{R}^r \times \mathbb{C}^s \to \mathbb{R}^r \times \mathbb{C}^s$ that preserves the volume (which is the same as $|\alpha_1 \cdots \alpha_r \alpha_{r+1}^2 \cdots \alpha_{r+s}^2| = 1$), we see that $\alpha D(0,R)$ is a compact, symmetric, convex region of $\mathbb{R}^r \times \mathbb{C}^s$ of the same volume as $D(0,R)$. Thus, again by Minkowski's theorem, there is a nonzero element $\sigma(x) \in \sigma(\mathcal{O}_K) \cap \alpha D(0,R)$, for $x \in \mathcal{O}_K \backslash \{0\}$. Again, by the same logic, $|N_{K/\mathbb{Q}}(x)| < R^{r+2s}$. This implies that $(x) \subset \mathcal{O}_K$ is of norm $< R^{r+2s}$, and there are finitely many ideals that satisfy this. As taking a generator out of an ideal is precisely ambiguous up to a factor of $\mathcal{O}_K^\times$, this implies that there are finitely many elements $y_1, \cdots, y_b \in \mathcal{O}_K$ such that $x = y_i u$ for some $1 \le i \le b$ and $u \in \mathcal{O}_K^\times$.

Then, there is a natural group homomorphism (from multiplicative to additive) $L : W \to V$,

$$L(x_1, \cdots, x_{r+s}) = (\log|x_1|, \cdots, \log|x_r|, 2\log|x_{r+1}|, \cdots, 2\log|x_{r+s}|) \in V.$$

Furthermore, the following diagram obviously commutes:

$$\begin{array}{ccc} \mathcal{O}_K^\times & \xrightarrow{\sigma} & W \\ {\scriptstyle L}\downarrow & & \downarrow{\scriptstyle L} \\ L(\mathcal{O}_K^\times) & \hookrightarrow & V \end{array}$$

Our observation in the previous paragraph was that, for any $\alpha \in W$, $\alpha D(0,R) \cap \sigma(y_i)\sigma(\mathcal{O}_K^\times) \neq \emptyset$ for some $1 \le i \le b$, or if we denote $C = \sigma(y_1)^{-1} D(0,R) \cup \cdots \cup \sigma(y_b)^{-1} D(0,R)$, then $\alpha C \cap \sigma(\mathcal{O}_K^\times) \neq \emptyset$. If we let $C' = L(C \cap W)$, then this implies that, for any $\beta \in V$, $(\beta + C') \cap L(\mathcal{O}_K^\times) \neq \emptyset$, or $C' \cap (-\beta + L(\mathcal{O}_K^\times)) \neq \emptyset$. This implies that the $L(\mathcal{O}_K^\times)$-traslates of C' covers the whole V. As C' is a compact subset of V, this is possible only if $L(\mathcal{O}_K^\times)$ is of full rank! More precisely, $C' \to V/L(\mathcal{O}_K^\times)$ is continuous and surjective, so $V/L(\mathcal{O}_K^\times)$ is compact, which is only possible if the rank of $L(\mathcal{O}_K^\times)$ is equal to $\dim_{\mathbb{R}} V$ (in general, it is topologically isomorphic to $(S^1)^{\mathrm{rank}_{\mathbb{Z}} L(\mathcal{O}_K^\times)} \times \mathbb{R}^{\dim_{\mathbb{R}} V - \mathrm{rank}_{\mathbb{Z}} L(\mathcal{O}_K^\times)}$). Thus we are done. □

Therefore, this implies that there exist multiplicatively independent units $u_1, \cdots, u_{r+s-1} \in \mathcal{O}_K^\times$ such that every unit $u \in \mathcal{O}_K^\times$ can be uniquely written as

$$u = \zeta u_1^{m_1} \cdots u_{r+s-1}^{m_{r+s-1}}, \quad \zeta \in \mu_K, m_1, \cdots, m_{r+s-1} \in \mathbb{Z}.$$

We call $u_1, \cdots, u_{r+s-1}$ a **fundamental system of units**. In general, computing a fundamental system of units is a very challenging task.

Example 17.5. (1) We see that $\mathcal{O}_K^\times$ is finite if $r+s-1=0$, i.e. if either $r=1, s=0$ (which is just $r+2s=1$, i.e. $K=\mathbb{Q}$), or $r=0, s=1$ (which means $r+2s=2$, i.e. K is an imaginary quadratic field). Namely, if K is an imaginary quadratic field, $\mathcal{O}_K^\times = \mu_K$. This is something that we kind of expected.

(2) We see that $\mathcal{O}_K^\times$ is of rank 1 if K is a real quadratic field. Then, a fundamental system of units is just consisted of one unit. As $\mu_K = \{\pm 1\}$ (because $\mu_{\mathbb{R}} = \{\pm 1\}$), this implies that, there is a unit ϵ of K such that all units of K are of the form $\pm\epsilon^n$, $n \in \mathbb{Z}$. There are four choices for the generator of the free part: $\epsilon, -\epsilon, \epsilon^{-1}, -\epsilon^{-1}$. After choosing a real embedding $K \hookrightarrow \mathbb{R}$, there is only one out of the four units above that is bigger than 1. This specific generating unit is often called as the **fundamental unit** of a real quadratic field.

If $d = \operatorname{disc} K$, then finding the units of K is the same as finding the integer solutions to the equation

$$x^2 - dy^2 = \pm 1 \quad (\text{if } d \not\equiv 1 \pmod 4), \qquad x^2 - dy^2 = \pm 4 \quad (\text{if } d \equiv 1 \pmod 4).$$

The above equation is called the **Pell's equation**.

Although a fundamental system of units is difficult to compute in general, for real quadratic fields there is a nice way of computing the fundamental unit (and thus the complete solution to the Pell's equation) using **continued fractions**, which we explain in the rest of the lecture.

Definition 17.6 (Continued fractions)**.** Let $r \in \mathbb{R}$ be a real number. Then, a **continued fraction** of r is the expression

$$r = (a_0; a_1, a_2, \cdots) := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}},$$

where $a_0, a_1, \cdots \in \mathbb{Z}$ are defined inductively as follows.

- We let $t_0 = r$ and $a_0 = \lfloor t_0 \rfloor$.
- For each $i \geq 1$, we let $t_i = \frac{1}{t_{i-1} - a_{i-1}}$ and $a_i = \lfloor t_i \rfloor$. If t_i is an integer (i.e. $t_i = a_i$), we terminate the sequence.

By definition, $a_1, a_2, \cdots > 0$. A continued fraction is **finite** if the sequence $a_0, a_1, \cdots$ terminates at some point, and is **infinite** otherwise. A continued fraction is **periodic** if it is infinite and if there is a positive integer $\ell > 0$ and $N > 0$ such that $a_{n+\ell} = a_n$ for any $n > N$. The minimal such ℓ is called the **period** of the continued fraction.

The following is a fundamental result on continued fractions.

Theorem 17.7. *For $r \in \mathbb{R}$, its continued fraction is finite if and only if $r \in \mathbb{Q}$, and its continued fraction is periodic if and only if $\mathbb{Q}(r)$ is a real qudaratic field.*

Proof. That a finite continued fraction gives rise to a rational number and a periodic continued fraction gives rise to a (necessarily real) quadratic number is clear. Also, a rational number must

have a finite continued fraction as the process is just the Euclidean algorithm which must stop at a finite stage. Thus, it remains to prove that any real irrational number r has a periodic continued fraction. As the continued fraction after a_0 stays the same even if we add an integer to r, without loss of generality, we may assume that $r > 0$.

Note that we have

$$a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_n + \frac{1}{x}}}} = \frac{P_n x + P_{n-1}}{Q_n x + Q_{n-1}},$$

where $(P_{-1}, P_0, P_1, \cdots)$ and $(Q_{-1}, Q_0, Q_1, \cdots)$ are the sequences of integers defined recursively by

$$P_{-1} = 1,\ P_0 = a_0,\ P_n = a_n P_{n-1} + P_{n-2} \text{ for } n \geq 1,$$

$$Q_{-1} = 0,\ Q_0 = 1,\ Q_n = a_n Q_{n-1} + Q_{n-2} \text{ for } n \geq 1.$$

The proof of this is a simple induction; the $n = 0$ case is

$$a_0 + \frac{1}{x} = \frac{a_0 x + 1}{x},$$

and

$$a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_n + \frac{1}{x}}}} = a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_{n-1} + \frac{1}{a_n + \frac{1}{x}}}}}} = \frac{P_{n-1}\left(a_n + \frac{1}{x}\right) + P_{n-2}}{Q_{n-1}\left(a_n + \frac{1}{x}\right) + Q_{n-2}}$$

$$= \frac{(P_{n-1}a_n + P_{n-2})x + P_{n-1}}{(Q_{n-1}a_n + Q_{n-2})x + Q_{n-1}} = \frac{P_n x + P_{n-1}}{Q_n x + Q_{n-1}}.$$

The sequences (P_n) and (Q_n) have the following properties.

- The sequence (Q_n) is consisted of positive integers and is strictly increasing. This is because $a_n > 0$ for $n \geq 1$.

- For any $n \geq 1$,

$$\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_{n+1}Q_n}, \quad \frac{P_{n+2}}{Q_{n+2}} - \frac{P_n}{Q_n} = \frac{(-1)^n a_{n+2}}{Q_{n+2}Q_n}.$$

  This is because

$$P_{n+1}Q_n - Q_{n+1}P_n = (a_{n+1}P_n + P_{n-1})Q_n - (a_{n+1}Q_n + Q_{n-1})P_n = P_{n-1}Q_n - Q_{n-1}P_n$$

$$= \cdots = (-1)^{n+1}(P_0 Q_{-1} - Q_0 P_{-1}) = (-1)^n,$$

  and

$$P_{n+2}Q_n - Q_{n+2}P_n = (a_{n+2}P_{n+1} + P_n)Q_n - (a_{n+2}Q_{n+1} + Q_n)P_n = a_{n+2}(P_{n+1}Q_n - Q_{n+1}P_n) = (-1)^n a_{n+2}.$$

Given the continued fraction $(a_0; a_1, \cdots)$, we define the n-**th convergent** as $(a_0; a_1, \cdots, a_n)$. Then, by the above formula, $(a_0; a_1, \cdots, a_n) = \frac{P_n}{Q_n}$. Note that, by the above observation, we see that

$$r = \lim_{n\to\infty} \frac{P_n}{Q_n}.$$

Rigorously, we see that $r = \frac{P_n(a_{n+1}; a_{n+2}, \cdots) + P_{n-1}}{Q_n(a_{n+1}; a_{n+2}, \cdots) + Q_{n-1}}$, which implies that r is a real number between $\frac{P_n}{Q_n}$ and $\frac{P_{n-1}}{Q_{n-1}}$, but the sequence $\left(\frac{P_n}{Q_n}\right)_n$ is a Cauchy sequence. Furthermore, the sequence of convergents alternates, i.e.

$$\frac{P_n}{Q_n} = a_0 + \sum_{i=0}^{n-1} (-1)^i \frac{1}{Q_i Q_{i+1}}.$$

Thus, as an alternating sum,

$$\left| r - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n Q_{n+1}}.$$

Now suppose that r is a root of $aX^2 + bX + c = 0$, $a, b, c \in \mathbb{Z}$. Then, using the above calculation, $r_n := (a_n; a_{n+1}, \cdots)$ is a root of

$$a(P_{n-1}X + P_{n-2})^2 + b(P_{n-1}X + P_{n-2})(Q_{n-1}X + Q_{n-2}) + c(Q_{n-1}X + Q_{n-2})^2 = 0,$$

or $A_nX^2 + B_nX + C_n = 0$, where

$$A_n = aP_{n-1}^2 + bP_{n-1}Q_{n-1} + cQ_{n-1}^2,$$

$$B_n = 2aP_{n-1}P_{n-2} + b(P_{n-1}Q_{n-2} + Q_{n-1}P_{n-2}) + 2cQ_{n-1}Q_{n-2},$$

$$C_n = aP_{n-2}^2 + bP_{n-2}Q_{n-2} + cQ_{n-2}^2.$$

Note that this is a change-of-basis of the quadratic form with a matrix $\begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix}$ which has determinant ± 1 as observed above, we see that the discriminant is preserved, i.e. $b^2 - 4ac = B_n^2 - 4A_nC_n$. Note that $\left| r - \frac{P_n}{Q_n} \right| < \frac{1}{Q_nQ_{n+1}}$ implies that

$$\frac{A_n}{Q_{n-1}^2} = a\left(r + \frac{\epsilon}{Q_nQ_{n+1}}\right)^2 + b\left(r + \frac{\epsilon}{Q_nQ_{n+1}}\right) + c = \frac{\epsilon(2ar + b)Q_nQ_{n+1} + a\epsilon^2}{Q_n^2Q_{n+1}^2},$$

for some $|\epsilon| < 1$. Thus,

$$|A_n| \leq \frac{Q_{n-1}^2}{Q_n^2Q_{n+1}^2}\left((2ar + b)Q_nQ_{n+1} + a\right) < 3ar + b,$$

which means that there are only finitely many possibilities for $A_n \in \mathbb{Z}$. Note also that $C_n = A_{n-1}$, so there are also finitely many possibilities for $C_n \in \mathbb{Z}$. From $b^2 - 4ac = B_n^2 - 4A_nC_n$, it follows that there are only finitely many possibilities for (A_n, B_n, C_n). Thus, there are only finitely many possibilities for r_n. Thus, $r_n = r_{n+h}$ for some $n > 0$, $h > 0$, which implies that the continued fraction for r is periodic. $\square$

Using the continued fractions, we can now find the fundamental unit of a real quadratic field!

Theorem 17.8. *Let $d > 0$ be a squarefree integer $\not\equiv 1 \pmod 4$, and let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ (sending $\sqrt{d}$ to $\sqrt{d}$). Let $\sqrt{d} = (a_0; a_1, a_2, \cdots)$ be the continued fraction of $\sqrt{d}$, which is periodic with period ℓ. Let $(P_{-1}, P_0, P_1, \cdots)$ and $(Q_{-1}, Q_0, Q_1, \cdots)$ be the sequences of integers defined recursively as in the proof of Theorem 17.7. Then, the fundamental unit of K is*

$$\epsilon = P_{\ell-1} + Q_{\ell-1}\sqrt{d}.$$

Proof. The key idea is that the convergents $\frac{P_n}{Q_n}$ are the rational numbers that approximate the irrational number $\sqrt{d}$ in the best possible way. First, note that the fundamental unit $\epsilon = x + y\sqrt{d}$ is the solution to $x^2 - dy^2 = \pm 1$ such that $x, y > 0$ and $|y|$ is as small as possible. This is because:

- for any $\alpha = z + w\sqrt{d} \in K$, $z, w \in \mathbb{Q}^\times$, exactly two of the four numbers, $z+w\sqrt{d}$, $z-w\sqrt{d}$, $-z+w\sqrt{d}$, $-z-w\sqrt{d}$, are positive, and the product of the two positive numbers is $|N(\alpha)|$;
- so, if $z, w > 0$, then $z + w\sqrt{d}$, being the largest number out of the four numbers $\pm z \pm w\sqrt{d}$, is larger than $\sqrt{|N(\alpha)|}$, and conversely, there is exactly one number out of the four numbers $\pm z \pm w\sqrt{d}$ that is larger than $\sqrt{|N(\alpha)|}$;
- thus, the units $s + t\sqrt{d} \in \mathcal{O}_K^\times$ that are larger than 1 are exactly those that $s, t \in \mathbb{N}$;
- if two units $x_1 + y_1\sqrt{d}$, $x_2 + y_2\sqrt{d}$, with $x_1, y_1, x_2, y_2 > 0$, satisfy $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$, then $\frac{x_2+y_2\sqrt{d}}{x_1+y_1\sqrt{d}} > 1$ is a unit, so $\frac{x_2+y_2\sqrt{d}}{x_1+y_1\sqrt{d}} = x_3 + y_3\sqrt{d}$, $x_3, y_3 > 0$, which means

  $$x_2 = x_1x_3 + dy_1y_3, \quad y_2 = y_1x_3 + x_1y_3,$$

  so in particular $x_2 > x_1$ and $y_2 > y_1$, which implies that the fundamental unit has $x, y > 0$ and has the smallest $|y|$.

Now, as $x^2 - dy^2 = \pm 1$, we have

$$\left|\sqrt{d} - \frac{x}{y}\right| = \frac{1}{y(x + \sqrt{d}y)} \le \frac{1}{(\sqrt{d} + \sqrt{d-1})y^2} < \frac{1}{2y^2},$$

using the crude approximation that $x^2 \ge dy^2 - 1 \ge (d-1)y^2$. This shows that $\frac{x}{y}$ is a very good rational approximation of $\sqrt{d}$.

Claim. If $\frac{p}{q} \in \mathbb{Q}$ satisfies $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ is a convergent to the continued fraction of $\sqrt{d}$.

Let's assume this and finish the proof of the Theorem first. The Claim implies that $\frac{x}{y}$ is a convergent to the continued fraction of $\sqrt{d}$, so $(x, y) = (P_n, Q_n)$ for some n. As $A_{n+1} = P_n^2 - dQ_n^2$, and as (P_n) is positive and increasing in this case ($a_0 = \lfloor\sqrt{d}\rfloor \ge 0$), we see that the fundamental unit is $P_n + Q_n\sqrt{d}$ such that $n \ge 0$ is the minimal integer that satisfies $A_{n+1} = \pm 1$ (note

that $(A_0, B_0, C_0) = (1, 0, -d)$, but $A_0 = 1$ doesn't appear as A_{n+1} in the range $n \geq 0$). Note that as $A_{n+1} = Q_n^2(\left(\frac{P_n}{Q_n}\right)^2 - d)$, and as the sequence $\left(\frac{P_n}{Q_n}\right)$ converges to $\sqrt{d}$ as an alternating sum with difference < 1, it follows that the signs of $A_1, A_2, A_3, \cdots$ alternate, $-, +, -, \cdots$. Thus, we are looking for when $A_{n+1} = (-1)^{n+1}$. Alternatively, we define $D_n = (-1)^n A_n$, $E_n = (-1)^n \frac{B_n}{2}$, $F_n = (-1)^n C_n$ (here B_n is always even as $b = 0$; look at the formula for B_n), so that $r_n = (a_n; a_{n+1}, \cdots)$ is a root of $D_n X^2 + 2E_n X + F_n = 0$, and we have $D_n > 0$ and $F_n < 0$, $E_n^2 - D_n F_n = d$, $F_n = -D_{n-1}$. Note that the roots of $D_n X^2 + 2E_n X + F_n = 0$ are $\frac{-E_n \pm \sqrt{d}}{D_n}$, and we know that precisely one is positive, which must be $\frac{-E_n + \sqrt{d}}{D_n}$.

So what happens when $D_n = 1$? This means that $a_n = -E_n + \lfloor \sqrt{d} \rfloor$, and $a_{n+1} = a_1$, etc. Thus, this means that $\sqrt{d}$ should have a continued fraction that is periodic in the stronger sense: namely, the whole continued fraction repeats maybe except a_0. More precisely, there exists $m \in \mathbb{Z}$ such that $m + \sqrt{d}$ has a **purely periodic continued fraction**, which means that there exists $\ell > 0$ such that $a_n = a_{n+\ell}$ **for all** $n \geq 0$. If this is the case, then the fundamental unit is indeed $P_{\ell-1} + Q_{\ell-1}\sqrt{d}$, as desired. Thus, the Theorem follows from the additional

Claim 2. $\lfloor \sqrt{d} \rfloor + \sqrt{d}$ has a purely periodic continued fraction.

The two claims will follow from the two lemmas, Lemmas 17.9 and 17.10, after the proof. □

Lemma 17.9. *Let $r \in \mathbb{R}$ has a continued fraction $r = (a_0; a_1, \cdots)$. If $\frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, $q > 0$, satisfies*

$$\left| r - \frac{p}{q} \right| < \frac{1}{2q^2},$$

then $\frac{p}{q}$ is a convergent to the continued fraction of r.

Proof. The bound requires more if p, q are not coprime, so we may assume that p, q are coprime. Suppose that $\frac{p}{q}$ is not a convergent. If $q = Q_n$ for some n, then p must be P_n, as otherwise $\left| r - \frac{p}{Q_n} \right| \geq \frac{1}{Q_n}$ which violates the bound. Thus, we see that there exists n such that $Q_n < q < Q_{n+1}$ (recall that (Q_n) is a strictly increasing sequence). If $|p - qr| \geq |P_n - Q_n r|$, then $|P_n - Q_n r| < \frac{1}{2q}$, so

$$\frac{|pQ_n - qP_n|}{qQ_n} = \left| \frac{p}{q} - \frac{P_n}{Q_n} \right| \leq \left| \frac{p}{q} - r \right| + \left| r - \frac{P_n}{Q_n} \right| < \frac{1}{2q^2} + \frac{1}{2Q_n q} < \frac{1}{Q_n q},$$

which implies that $pQ_n - qP_n = 0$, which again contradicts with the assumption that $\frac{p}{q}$ is not a convergent. Thus, $|p - qr| < |P_n - Q_n r|$. As the inverse of the matrix $\begin{pmatrix} P_n & P_{n+1} \\ Q_n & Q_{n+1} \end{pmatrix}$ is also integer-entried, it follows that there exist $u, v \in \mathbb{Z}$ such that

$$p = uP_n + vP_{n+1}, \quad q = uQ_n + vQ_{n+1}.$$

Then,

$$|p - qr| = |u(P_n - Q_n r) + v(P_{n+1} - Q_{n+1} r)|.$$

Note that $q = uQ_n + vQ_{n+1}$ and $0 < Q_n < q < Q_{n+1}$ implies that u, v cannot have the same sign. As $P_n - Q_n r$ and $P_{n+1} - Q_{n+1} r$ have different signs, it follows that $u(P_n - Q_n r)$ and $v(P_{n+1} - Q_{n+1} r)$ have the same signs (0 is assumed to have both $+$ and $-$ sign), so that

$$|p - qr| = |u(P_n - Q_n r) + v(P_{n+1} - Q_{n+1} r)| = |u||(P_n - Q_n r)| + |v||(P_{n+1} - Q_{n+1} r)|.$$

For this to be less than $|P_n - Q_n r|$, we need $u = 0$. Then, $q = vQ_{n+1}$, so $v > 0$, but as $q < Q_{n+1}$, $v < 1$, which is a contradiction. □

Lemma 17.10. *Let $r \in \mathbb{R}$ be a quadratic irrational number. Then, r has a purely periodic continued fraction if $r > 1$ and $-1 < \overline{r} < 0$, where $\overline{r}$ is the conjugate of r.*

Proof. Let $r_n = (a_n; a_{n+1}, \cdots)$. Then, $r_n = a_n + \frac{1}{r_{n+1}}$, which implies that $\overline{r_n} = a_n + \frac{1}{\overline{r_{n+1}}}$. We claim that for every n, $-1 < \overline{r_n} < 0$. We prove this by induction on n, where $n = 0$ is the base case as given. Now, assume $-1 < \overline{r_n} < 0$. Then, $a_n \geq 1$, as $a_n \geq 1$ automatically for any $n \geq 1$ with infinite continued fraction and $a_0 \geq 1$ by assumption that $r > 1$. Thus, $\overline{r_n} - a_n < -1$, which means that $0 > \overline{r_{n+1}} > -1$. This also implies that $a_n = \left\lfloor -\frac{1}{\overline{r_{n+1}}} \right\rfloor$.

As the continued fraction of r is periodic, we have $r_i = r_j$ for some $0 < i < j$. Then, by the above formula, $a_{i-1} = a_{j-1}$, so $r_{i-1} = r_{j-1}$. Thus, we can subtract indices to obtain $r_0 = r = r_\ell$ for some $\ell > 0$. This implies that the continued fraction of r is purely periodic. □

Example 17.11. Consider the case of $K = \mathbb{Q}(\sqrt{7})$. Then, we consider the continued fraction of $r = \sqrt{7} \sim 2.64$.

$$a_0 = \lfloor \sqrt{7} \rfloor = 2, \quad r_1 = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3} \sim 1.55, \quad a_1 = \lfloor r_1 \rfloor = 1,$$

$$r_2 = \frac{1}{r_1 - 1} = \frac{3}{\sqrt{7} - 1} = \frac{\sqrt{7} + 1}{2} \sim 1.82, \quad a_2 = \lfloor r_2 \rfloor = 1, \quad r_3 = \frac{1}{r_2 - 1} = \frac{2}{\sqrt{7} - 1} = \frac{\sqrt{7} + 1}{3} \sim 1.22,$$

$$a_3 = \lfloor r_3 \rfloor = 1, \quad r_4 = \frac{1}{r_3 - 1} = \frac{3}{\sqrt{7} - 2} = \sqrt{7} + 2 \sim 4.64, \quad a_4 = \lfloor r_4 \rfloor = 4, \quad r_5 = \frac{1}{r_4 - 4} = \frac{1}{\sqrt{7} - 2} = r_1.$$

Therefore, $\ell = 4$, and the fundamental unit is $\epsilon = P_3 + Q_3\sqrt{7}$, where

$$P_{-1} = 1, P_0 = 2, P_1 = 3, P_2 = 5, P_3 = 8,$$

$$Q_{-1} = 0, Q_0 = 1, Q_1 = 1, Q_2 = 2, Q_3 = 3,$$

which means that the fundamental unit is $\epsilon = 8 + 3\sqrt{7}$. Indeed, $8^2 - 7 \cdot 3^2 = 64 - 63 = 1$, which means $(8, 3)$ gives rise to a solution to the Pell's equation $x^2 - 7y^2 = \pm 1$, and all solutions to the Pell's equations satisfy $x + y\sqrt{7} = \pm\epsilon^n$ for some $n \in \mathbb{Z}$ (or equivalently either $\pm\epsilon^n$ or $\pm\overline{\epsilon}^n$ for $n \geq 0$).

– –

Exercise 17.1. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $d > 1$ is a square-free integer with $d \equiv 1 \pmod 4$, i.e. $\mathrm{disc}(K) = d$, and $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{d}+1}{2}]$.

(1) Show that the continued fraction of

$$\left\lfloor \frac{\sqrt{d}+1}{2} \right\rfloor + \frac{\sqrt{d}-1}{2},$$

is purely periodic.

(2) Let $(a_0; a_1, \cdots)$ be the continued fraction of $\frac{\sqrt{d}-1}{2}$, whose period is ℓ. Show that the fundamental unit of K is $\epsilon = P_{\ell-1} + Q_{\ell-1}\frac{\sqrt{d}+1}{2}$.

Exercise 17.2. Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ be a real quadratic field, with $d > 1$ a square-free integer. The **sign** of K is $N(K) := N_{K/\mathbb{Q}}(\epsilon)$, where ϵ is the fundamental unit of K (i.e. the smallest unit > 1).

(1) Show that $N(K) = -1$ if and only there is a unit whose norm is -1. Deduce that $N(K) = -1$ if and only if the equation $x^2 - \mathrm{disc}(K)y^2 = -4$ has integer solutions $x, y \in \mathbb{Z}$.

(2) If d has a prime factor that is $\equiv 3 \pmod 4$, show that $N(K) = 1$.

(3) Let $\mathfrak{m}$ be the modulus of K such that $\mathfrak{m}_f = 1$ and $\mathfrak{m}_\infty$ is the product of the two real embeddings of K. Show that the natural surjective map $\mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$ is an isomorphism if and only if there exists a unit of norm -1.

(4) Using (2) and (3), deduce that if d has a prime factor that is $\equiv 3 \pmod 4$, then there is an abelian extension L/K that is strictly bigger than H_K and is unramified at every prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ (cf. Exercise 16.1).

18. Lectures 23 and 24. Dirichlet L-functions

Summary. Dirichlet characters; Dirichlet L-functions; Euler product; analytic continuation; Gauss sums and Jacobi sums; functional equation; analytic proof of quadratic reciprocity; analytic proof of Fermat's $p = x^2 + y^2$; analytic proof of cubic reciprocity; Bernoulli numbers.

Content. We will eventually see that the periods can tell some nontrivial information about the class number and the units. To compute the periods, we need the notion of L-functions. The most basic L-function is that of **Dirichlet characters**.

Definition 18.1 (Dirichlet characters)**.** A **Dirichlet character** χ of **modulus** m (or mod m in short) is a multiplicative homomorphism

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times.$$

By multiplicativity, any Dirichlet character χ satisfies $\chi(-1)^2 = 1$. The Dirichlet character χ is **even** if $\chi(-1) = 1$, and **odd** if $\chi(-1) = -1$.

If $m|n$, then a Dirichlet character χ mod m can be regarded as a Dirichlet character mod n by using the natural map

$$(\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times.$$

Any Dirichlet character mod n arising from a Dirichlet character mod m for $m|n$, $m < n$, is called **imprimitive**. If not, we call it **primitive**. Every Dirichlet character χ arises from a unique primitive Dirichlet character whose modulus is called the **conductor** f_χ of χ.

In general, given a finite abelian group G, a **character** of G is a homomorphism $\chi : G \to \mathbb{C}^\times$. The set of characters of G forms an obvious abelian group by entrywise multiplication, and this group is denoted as $\widehat{G}$. The identity element in $\widehat{G}$ is called the **principal character**, defined as $\mathbf{1}(g) = 1$, and the inverse of $\chi \in \widehat{G}$ is $\overline{\chi}$. The principal Dirichlet character of modulus m is often denoted as $\mathbf{1}_m$.

Theorem 18.2. *Let G be a finite abelian group. Then, $G \cong \widehat{G}$; in particular, $\widehat{G}$ is a finite abelian group.*

Proof. By the fundamental theorem of finitely generated abelian groups, $G = (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})$. Then, a character $\chi : G \to \mathbb{C}^\times$ is determined by a tuple $(\zeta_1, \cdots, \zeta_k)$ where $\zeta_1^{m_1} = \cdots = \zeta_k^{m_k} = 1$. Thus, $\widehat{G} \cong \mu_{m_1} \times \cdots \times \mu_{m_k}$, where $\mu_n \subset \mathbb{C}^\times$ is a multiplicative group of n-th roots of unity. As $\mu_n \cong (\mathbb{Z}/n\mathbb{Z})$ as abelian groups, we are done. □

The following is typical in the representation theory of finite groups.

Theorem 18.3. *Let G be a finite abelian group.*

(1) Let $\chi, \psi \in \widehat{G}$. Then,

$$\sum_{g \in G} \chi(g)\overline{\psi(g)} = \begin{cases} |G| & \text{if } \chi = \psi \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $\sum_{g \in G} \chi(g) = 0$ for $\chi \neq \mathbf{1}$.

(2) *Let $f : G \to \mathbb{C}$ be any function. Then, f is a linear combination of the characters of G. More precisely, $f = \sum_{\chi \in \widehat{G}} a_\chi \chi$, where*

$$a_\chi = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)}.$$

(3) *The characters are linearly independent over $\mathbb{C}$. More precisely, if there exist $a_\chi \in \mathbb{C}$ for each $\chi \in \widehat{G}$ such that $\sum_{\chi \in \widehat{G}} a_\chi \chi$ is zero, namely if*

$$\sum_{\chi \in G} a_\chi \chi(g) = 0, \quad g \in G,$$

then $a_\chi = 0$ for all $\chi \in \widehat{G}$.

(4) *Let $g, h \in G$. Then,*

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |G| & \text{if } g = h \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (1) Let $\varphi = \chi\psi^{-1} \in \widehat{G}$. Then, we would like to show that $\sum_{g \in G} \varphi(g) = 0$ for $\varphi \neq \mathbf{1}$. For $\varphi \neq \mathbf{1}$, there exists $h \in G$ such that $\varphi(h) \neq 1$. Then,

$$\varphi(h) \sum_{g \in G} \varphi(g) = \sum_{g \in G} \varphi(gh) = \sum_{g \in G} \varphi(g),$$

so $\sum_{g \in G} \varphi(g) = 0$.

(2) Note that, for $g \in G$, $g \neq 1$, $\sum_{\chi \in \widehat{G}} \chi(g) = 0$; as there is $\psi \in \widehat{G}$ such that $\psi(g) \neq 1$,

$$\psi(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \psi(g)\chi(g) = \sum_{\chi \in \widehat{G}} \chi(g).$$

Now, the statement we want to prove is true as

$$\sum_{\chi \in \widehat{G}} a_\chi \chi(g) = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \sum_{h \in G} f(h)\overline{\chi(h)}\chi(g) = \frac{1}{|G|} \sum_{h \in G} f(h) \sum_{\chi \in \widehat{G}} \chi(gh^{-1}) = f(g).$$

(3) Since (2) implies that a $|G|$-dimensional $\mathbb{C}$-vector space, the vector space of functions $f : G \to \mathbb{C}$, is spanned by the characters in $\widehat{G}$, which is of order $|G|$, they are linearly independent.

(4) As $\chi(g)\overline{\chi(h)} = \chi(gh^{-1})$, we may assume that h is the identity. By induction, it is sufficient to prove when G is a cyclic group, say $G \cong (\mathbb{Z}/m\mathbb{Z})$. Then, for $g = n \in (\mathbb{Z}/m\mathbb{Z})$,

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{j=1}^{m} e^{\frac{2\pi i j n}{m}},$$

and this is easily seen to be zero if $n \neq m$, and is m if $n = 0$.

□

Given a Dirichlet character χ of modulus m, we oftentimes regard it also as a map $\mathbb{Z} \to \mathbb{C}$ such that $\chi(n) = 0$ whenever $(n, m) \neq 1$.

Definition 18.4 (Dirichlet L-functions)**.** Let χ be a Dirichlet character, regarded as a map $\mathbb{Z} \to \mathbb{C}$. The **Dirichlet L-function** of χ is defined as

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

This expression defines a holomorphic function in s in the region $\mathrm{Re}(s) > 1$.

Example 18.5. Let χ be the trivial Dirichlet character of modulus 1. Then, $L(s, \chi) = \zeta(s)$ is the **Riemann zeta function**.

The Dirichlet L-function, like the Riemann zeta function, has an infinite product expression, called the **Euler product**.

Theorem 18.6. *Let χ be a Dirichlet character of modulus m. Then, for $\mathrm{Re}(s) > 1$, we have an expression*

$$L(s, \chi) = \prod_{p \text{ rational prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

In particular, if χ is induced from a primitive Dirichlet character $\widetilde{\chi}$, then

$$L(s, \chi) = L(s, \widetilde{\chi}) \prod_{p \mid m} \left(1 - \frac{\widetilde{\chi}(p)}{p^s}\right).$$

Proof. Formally both sides coincide, and the fact that they coincide as numbers follows from simple convergence argument. □

Here comes the crucial main analytic property of the Dirichlet L-functions.

Theorem 18.7. *Let χ be a Dirichlet character of modulus m.*

*(1) **(Analytic continuation)** The Dirichlet L-function $L(s, \chi)$, a priori only defined for $\mathrm{Re}(s) > 1$, has an analytic continuation as a meromorphic function on $\mathbb{C}$. The only possible pole can appear at $s = 1$, and the pole appears if and only if χ is a principal Dirichlet character, in which case $L(s, \chi)$ has a simple pole at $s = 1$. In other words, if χ is not principal, the analytic continuation of $L(s, \chi)$ to the whole $s \in \mathbb{C}$ is an entire function.*

(2) ***(Functional equation)*** *The Dirichlet L-function has a functional equation, relating $L(s,\chi)$ and $L(1-s,\overline{\chi})$. More precisely, if χ is a primitive Dirichlet character, then if we define*

$$\Lambda(s,\chi) := \left(\frac{m}{\pi}\right)^{\frac{s+a}{2}} \Gamma\left(\frac{s+a}{2}\right) L(s,\chi), \quad a = \begin{cases} 0 & \text{if } \chi \text{ is even} \\ 1 & \text{if } \chi \text{ is odd,} \end{cases}$$

then

$$\Lambda(s,\chi) = \varepsilon(\chi)\Lambda(1-s,\overline{\chi}), \quad \varepsilon(\chi) = \frac{G(\chi)}{i^a\sqrt{m}}, \quad G(\chi) = \sum_{n=1}^{m} \chi(n) e^{\frac{2\pi i n}{m}}.$$

*The quantity $G(\chi)$ is called the **Gauss sum**, and $|G(\chi)| = \sqrt{m}$, so that $|\varepsilon(\chi)| = 1$.*

Proof. By the relation between the Dirichlet L-function for imprimitive Dirichlet characters and primitive Dirichlet characters, we only need to prove both (1) and (2) for primitive Dirichlet characters. We will prove everything simultaneously, using the **theta series**, just as the functional equation to the Riemann zeta function is usually proved. Recall that the Gamma function $\Gamma(s)$ has an integral representation when $\mathrm{Re}(s) > 0$,

$$\Gamma(s) = \int_0^\infty y^s e^{-y} \frac{dy}{y}.$$

In particular, for any $r > 0$, the change of variables gives

$$\int_0^\infty y^s e^{-ry} \frac{dy}{y} = \frac{1}{r^s}\Gamma(s).$$

If we define the **theta series** to be

$$\theta_\chi(iy) = \sum_{n\in\mathbb{Z}} \chi(n) e^{-\pi n^2 y}, \quad y > 0,$$

then this is identically zero if χ is odd, and is $2\sum_{n\geq 1}\chi(n)e^{-\pi n^2 y}$ if χ is even, and is $1+2\sum_{n\geq 1} e^{-\pi n^2 y}$ if $\chi = \mathbf{1}$. Thus, when χ is even and nonprincipal and $\mathrm{Re}(s) > 1$,

$$\int_0^\infty y^{\frac{s}{2}} \frac{\theta_\chi(iy)}{2} \frac{dy}{y} = \sum_{n\geq 1} \chi(n) \int_0^\infty y^{\frac{s}{2}} e^{-\pi n^2 y} \frac{dy}{y} = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) L(s,\chi),$$

and for $\chi = \mathbf{1}$,

$$\int_0^\infty y^{\frac{s}{2}} \frac{\theta_{\mathbf{1}}(iy) - 1}{2} \frac{dy}{y} = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Note that, for χ even and non-principal, $\theta_\chi(iy)$ decays exponentially as $y \to +\infty$, so for any $\epsilon > 0$, the integral

$$\int_\epsilon^\infty y^{\frac{s}{2}} \frac{\theta_\chi(iy)}{2} \frac{dy}{y},$$

defines an entire function on $s \in \mathbb{C}$, and similarly $\int_\epsilon^\infty y^{\frac{s}{2}} \frac{\theta_1(iy)-1}{2} \frac{dy}{y}$. The behavior of the integral $\int_0^\epsilon$ and the functional equation comes from the functional equation for the theta series:

$$\theta_\chi(iy) = \frac{G(\chi)}{m\sqrt{y}} \theta_{\overline{\chi}} \left(\frac{i}{m^2 y} \right).$$

This is a standard application of the **Poisson summation formula**.

Definition 18.8 (Schwartz function)**.** A smooth (i.e. C^∞) function $f : \mathbb{R} \to \mathbb{C}$ is called to be a **rapidly decreasing function** if, for any $N > 0$, $\lim_{x \to \pm\infty} |x|^N f(x) = 0$. A smooth function $f : \mathbb{R} \to \mathbb{C}$ is called to be a **Schwartz function** if any n-th derivative of f, for all $n \geq 0$, is a rapidly decreasing function.

Example 18.9. A typical example of a Schwartz function is

$$f(x) = e^{p(x)}, \quad p(x) \text{ is an even degree polynomial in variable } x \text{ with the negative leading coefficient.}$$

For example, e^{-x^2} is a Schwartz function.

Theorem 18.10 (Poisson summation formula)**.** *Let $f : \mathbb{R} \to \mathbb{C}$ be a Schwartz function. Then,*

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n),$$

*where $\widehat{f} : \mathbb{R} \to \mathbb{C}$ is the **Fourier transform** of f,*

$$\widehat{f}(x) = \int_{\mathbb{R}} e^{-2\pi i x t} f(t) dt,$$

which is also a Schwartz function.

The proof of this can be found in any standard text in Fourier analysis, which uses the fact that the function

$$F(x) = \sum_{n \in \mathbb{Z}} f(x+n),$$

is a 1-periodic function, which has a Fourier series expansion, whose Fourier coefficients are actually given by $\widehat{f}(n)$.

Applying the Poisson summation formula to $f_{y,b}(x) := e^{-\pi(mx+b)^2 y}$, since

$$\widehat{f_{y,b}}(x) = \frac{e^{\frac{2\pi i x b}{m}}}{m\sqrt{y}} e^{-\frac{\pi x^2}{m^2 y}},$$

we have

$$\theta_\chi(iy) = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n \in \mathbb{Z}} e^{-\pi(mn+b)^2 y} = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n \in \mathbb{Z}} f_{y,b}(n) = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n \in \mathbb{Z}} \widehat{f_{y,b}}(n)$$

$$= \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n\in\mathbb{Z}} \frac{e^{\frac{2\pi inb}{m}}}{m\sqrt{y}} e^{-\frac{\pi n^2}{m^2 y}} = \frac{1}{m\sqrt{y}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{m^2 y}} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}}.$$

As

$$\frac{G(\chi)}{m\sqrt{y}} \theta_{\overline{\chi}}\left(\frac{i}{m^2 y}\right) = \frac{G(\chi)}{m\sqrt{y}} \sum_{n\in\mathbb{Z}} e^{-\frac{\pi n^2}{m^2 y}} \overline{\chi(n)},$$

the functional equation for the theta series will follow if

$$\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}} = G(\chi)\overline{\chi(n)},$$

for all $n \in \mathbb{Z}$. If n is invertible mod m, then $\{nb \ : \ b \in (\mathbb{Z}/m\mathbb{Z})^\times\}$ is a rearrangement of $(\mathbb{Z}/m\mathbb{Z})^\times$, so the identity holds as

$$\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}} = \overline{\chi(n)} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(nb) e^{\frac{2\pi inb}{m}} = \overline{\chi(n)} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi ib}{m}} = \overline{\chi(n)} G(\chi).$$

Thus, we are only left with showing that $\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}} = 0$ if n is not invertible mod m. Suppose that $(n, m) = \frac{m}{d} > 1$. Then, for any $x \in (\mathbb{Z}/m\mathbb{Z})^\times$ that $x \equiv 1 \pmod{d}$,

$$\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}} = \overline{\chi(x)} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(bx) e^{\frac{2\pi inb}{m}} = \overline{\chi(x)} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(bx) e^{\frac{2\pi inbx}{m}} = \overline{\chi(x)} \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}}.$$

If $\chi(x) = 1$ for any such x, then it means that χ is induced from a Dirichlet character of modulus $\frac{m}{d}$, which contradicts the primitivity of χ. Thus, this implies the desired statement.

From the functional equation of the theta series, for χ even and non-principal,

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) L(s, \chi) = \int_{\frac{1}{m}}^{\infty} y^{\frac{s}{2}} \frac{\theta_\chi(iy)}{2} \frac{dy}{y} + \frac{m^{1-s}}{G(\overline{\chi})} \int_{\frac{1}{m}}^{\infty} y^{\frac{1-s}{2}} \frac{\theta_{\overline{\chi}}(iy)}{2} \frac{dy}{y},$$

and both integrals now define entire functions in s. As the Gamma function has no zeros, $L(s, \chi)$ has an analytic continuation as an entire function. Massaging this equation also gives the functional equation. For the odd χ, one instead uses the theta series

$$\widetilde{\theta}_\chi(iy) = \sum_{n\in\mathbb{Z}} \chi(n) n\sqrt{y} e^{-\pi n^2 y},$$

and proceed similarly (see Exercise 18.1). Finally, for $\chi = \mathbf{1}$, we have

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_1^{\infty} y^{\frac{s}{2}} \frac{\theta_{\mathbf{1}}(iy) - 1}{2} \frac{dy}{y} + \int_1^{\infty} y^{\frac{s}{2}} \frac{\theta_{\mathbf{1}}(iy) - \frac{1}{\sqrt{y}}}{2} \frac{dy}{y}$$

$$= \int_1^{\infty} y^{\frac{s}{2}} (\theta_{\mathbf{1}}(iy) - 1) \frac{dy}{y} + \frac{1}{2} \int_1^{\infty} \left(y^{\frac{s}{2}-1} - y^{\frac{s-1}{2}-1}\right) dy = \int_1^{\infty} y^{\frac{s}{2}} (\theta_{\mathbf{1}}(iy) - 1) \frac{dy}{y} + \left(\frac{1}{s} - \frac{1}{s-1}\right),$$

which gives an analytic continuation of $\zeta(s)$. This implies that $\zeta(s)$ may have simple poles at $s=0$ and $s=1$, but as $\Gamma(s)$ has a pole at $s=0$, $\zeta(s)$ has a simple pole only at $s=1$.

Note that $\chi(-1)\overline{G(\chi)} = G(\overline{\chi})$, and

$$\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b)e^{\frac{2\pi inb}{m}} = G(\chi)\overline{\chi(n)},$$

for all $n\in\mathbb{Z}$. Therefore,

$$\varphi(m)|G(\chi)|^2 = \sum_{n=1}^{m}\sum_{a,b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\overline{\chi(b)}e^{\frac{2\pi in(a-b)}{m}} = \sum_{a,b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\overline{\chi(b)}\sum_{n=1}^{m} e^{\frac{2\pi in(a-b)}{m}}$$

$$= m\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)\overline{\chi(a)} = m\varphi(m),$$

which gives the desried result. □

The following is a famed result which we will see as a consequence of the analytic class number formula we will see in the next section.

Theorem 18.11. *Let χ be a nonprincipal Dirichlet character. Then, $L(1,\chi)\neq 0$.*

The Dirichlet L-functions are holomorphic functions that themselves have little to do with algebra, but the numbers appearing in various formulae regarding the Dirichlet L-functions (e.g. values at certain points, Gauss sum, residue at a pole) encode a surprising amount of arithmetic information.

Firstly, the Gauss sums can actually be used to prove quadratic reciprocity; this is the "analytic proof" (or "homological proof") of quadratic reciprocity.

Analytic proof of the quadratic reciprocity law. Let p,q be distinct odd rational primes. We want to show that

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

Consider the Dirichlet character $\chi_p(n) := \left(\frac{n}{p}\right)$ of modulus p, and similarly χ_q, a Dricihlet character of modulus q. The product $\chi_p\chi_q$ is a primitive Dirichlet character of modulus pq. Note that

$$G(\chi_p)G(\chi_q) = \sum_{n=1}^{p-1}\sum_{m=1}^{q-1}\left(\frac{n}{p}\right)\left(\frac{m}{q}\right)e^{\frac{2\pi in}{p}}e^{\frac{2\pi im}{q}} \sum_{n=1}^{p-1} = \sum_{m=1}^{q-1}\left(\frac{n}{p}\right)\left(\frac{m}{q}\right)e^{\frac{2\pi i(qn+pm)}{pq}}.$$

Since $qn+pm$ for $1\leq n\leq p-1$ and $1\leq m\leq q-1$ goes over all classes in $(\mathbb{Z}/pq\mathbb{Z})^\times$,

$$G(\chi_p\chi_q) = \sum_{n=1}^{p-1}\sum_{m=1}^{q-1}\left(\frac{qn+pm}{p}\right)\left(\frac{qn+pm}{q}\right)e^{\frac{2\pi i(qn+pm)}{pq}} = \sum_{n=1}^{p-1}\sum_{m=1}^{q-1}\left(\frac{qn}{p}\right)\left(\frac{pm}{q}\right)e^{\frac{2\pi i(qn+pm)}{pq}}.$$

Thus,

$$\frac{G(\chi_p\chi_q)}{G(\chi_p)G(\chi_q)} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Note that, for any prime p,

$$G(\chi_p) = \sum_{n=1}^{p}\left(\frac{n}{p}\right)e^{\frac{2\pi in}{p}} = \sum_{n=1}^{p}\left(\left(\frac{n}{p}\right)+1\right)e^{\frac{2\pi in}{p}} = \sum_{m=1}^{p} e^{\frac{2\pi im^2}{p}}.$$

Here, the last equality comes from the fact that, if m runs from 1 to p, $m^2 \pmod p$ hits nonzero quadratic residues twice and 0 once. Similarly, for any distinct primes p, q, we firstly have

$$\sum_{n=1}^{pq}\left(\frac{n}{p}\right)e^{\frac{2\pi in}{pq}} = \sum_{n=1}^{p}\left(\frac{n}{p}\right)e^{\frac{2\pi in}{pq}}\sum_{m=1}^{q} e^{\frac{2\pi ipm}{pq}} = 0,$$

so we have

$$G(\chi_p\chi_q) = \sum_{n=1}^{pq}\left(\frac{n}{p}\right)\left(\frac{n}{q}\right)e^{\frac{2\pi in}{pq}} = \sum_{n=1}^{pq}\left(\left(\frac{n}{p}\right)+1\right)\left(\left(\frac{n}{q}\right)+1\right)e^{\frac{2\pi in}{pq}} = \sum_{n=1}^{pq} e^{\frac{2\pi in^2}{pq}}.$$

Here, similarly, the last equality comes from the fact that, if m runs from 1 to pq, $m^2 \pmod{pq}$ hits quadratic residues coprime to pq four times, quadratic residues that are multiples of p or q twice, and 0 once. Thus, the quadratic reciprocity law is a consequence of the following

Claim. If, for a positive odd integer h, $S_h := \sum_{n=1}^{h} e^{\frac{2\pi in^2}{h}}$, then $S_h = \begin{cases}\sqrt{h} & \text{if } h \equiv 1 \pmod 4\\ i\sqrt{h} & \text{if } h \equiv 3 \pmod 4.\end{cases}$

There are various proofs to this; we present a complex-analytic proof. Consider the function

$$f_h(z) = \frac{e^{\frac{2\pi iz^2}{h}}}{e^{2\pi iz}-1},$$

which is a meromorphic function with simple poles precisely at the integers, and

$$\operatorname{Res}_{z=n} f_h(z) = \frac{e^{\frac{2\pi in^2}{h}}}{2\pi i},$$

so if we let C_N be the contour which is a parallelogram that has $\operatorname{Im}(z) = \pm N$ as the horizontal sides and $z = -\frac{1}{2}+(1+i)t$ and $z = h-\frac{1}{2}+(1+i)t$ as the vertical sides (expressed as parametric equations in variable t), by Cauchy's integral formula, we have

$$\int_{C_N} f_h(z)dz = S_h.$$

If $z = x+iy$, we have

$$|f_h(z)| \le \frac{e^{-\frac{4\pi xy}{h}}}{|e^{-2\pi y}-1|}.$$

Thus, the integral on the horizontal sides goes to zero as $N \to +\infty$. Thus, if we let L_1 and L_2 be the slope 1 lines (going upwards) passing through $-\frac{1}{2}$ and $h - \frac{1}{2}$, then

$$S_h = \int_{L_2} f_h(z)dz - \int_{L_1} f_h(z)dz.$$

Note also that

$$f_h(z+h) = e^{4\pi iz} f(z),$$

so

$$S_h = \int_{L_1} (e^{4\pi iz} - 1) f(z)dz = \int_{L_1} (e^{2\pi iz} + 1) e^{\frac{2\pi iz^2}{h}} dz = \int_{L_1} e^{2\pi iz} e^{\frac{2\pi iz^2}{h}} dz + \int_{L_1} e^{\frac{2\pi iz^2}{h}} dz$$

$$= \int_{L_1} e^{\frac{2\pi i(z^2+hz)}{h}} dz + \int_{L_1} e^{\frac{2\pi iz^2}{h}} dz = \int_{L_1 + \frac{h}{2}} e^{\frac{2\pi i\left(z^2 - \frac{h^2}{4}\right)}{h}} dz + \int_{L_1} e^{\frac{2\pi iz^2}{h}} dz,$$

where $L_1 + \frac{h}{2}$ is the contour L_1 shifted to the right by $\frac{h}{2}$. Since the integrand decays exponentially away from the imaginary axis fast as the imaginary part goes to infinity, by Cauchy's integral formula, we can shift the contour without changing the integral, yielding

$$S_h = \int_{L_1} e^{\frac{2\pi i\left(z^2 - \frac{h^2}{4}\right)}{h}} dz + \int_{L_1} e^{\frac{2\pi iz^2}{h}} dz = \left(e^{-\frac{\pi ih}{2}} + 1\right) \int_{L_1} e^{\frac{2\pi iz^2}{h}} dz = \left(e^{-\frac{\pi ih}{2}} + 1\right) \sqrt{h} \int_{\frac{L_1}{\sqrt{h}}} e^{2\pi iz^2} dz,$$

where again $\frac{L_1}{\sqrt{h}}$ is the contour L_1 scaled by $\frac{1}{\sqrt{h}}$. By the same reasoning, we can shift the contour $\frac{L_1}{\sqrt{h}}$ so that the contour passes through the origin. We claim that

$$\int_L e^{2\pi iz^2} dz = \frac{1+i}{2},$$

for any positive slope line L (going upward) passing through the origin. If the claim is true, then if $h \equiv 1 \pmod 4$, then $S_h = \frac{(1+i)(1-i)\sqrt{h}}{2} = \sqrt{h}$, and if $h \equiv 3 \pmod 4$, then $S_h = \frac{(1+i)^2\sqrt{h}}{2} = i\sqrt{h}$, which is what we want. By the same reasoning as above, it is easy to see that the integral does not depend on the slope, so let's assume that L is the slope 1 line. Then,

$$\int_L e^{2\pi iz^2} dz = \int_{-\infty}^{\infty} e^{2\pi i(t+ti)^2} (1+i) dt = (1+i) \int_{-\infty}^{\infty} e^{-4\pi t^2} dt = \frac{1+i}{2} \int_{-\infty}^{\infty} e^{-\pi t^2} dt = \frac{1+i}{2},$$

as desired. □

For two Dirichlet characters ψ, χ, the quantity

$$\frac{G(\psi\chi)}{G(\psi)G(\chi)},$$

is very interesting, as used in the above analytic proof of the quadratic reciprocity law. This is also useful when ψ, χ are of the same conductor, and even has a name to it.

Definition 18.12. Let p be a rational prime. For ψ, χ two Dirichlet characters of conductor p such that $\psi\chi \neq \mathbf{1}_p$, then the **Jacobi sum** is

$$J(\psi, \chi) := \frac{G(\chi)G(\psi)}{G(\chi\psi)}.$$

Lemma 18.13. *Let p be a rational prime, and let ψ, χ be Dirichlet characters of conductor p such that $\psi\chi$ is not principal. Then,*

$$J(\psi, \chi) = \sum_{a=1}^{p} \chi(a)\psi(1-a).$$

Proof. Note that

$$G(\chi)G(\psi) = \sum_{m,n=1}^{p} \chi(m)\psi(n)e^{\frac{2\pi i(m+n)}{p}} = \sum_{m=1}^{p} \chi(m)\psi(-m) + \sum_{a=1}^{p-1}\sum_{m=1}^{p} \chi(m)\psi(a-m)e^{\frac{2\pi ia}{p}}$$

$$= \psi(-1)\sum_{m=1}^{p} \chi(m)\psi(m) + \sum_{a=1}^{p-1}\sum_{m=1}^{p} \chi\left(\frac{m}{a}\right)\psi\left(1-\frac{m}{a}\right)\chi(a)\psi(a)e^{\frac{2\pi ia}{p}}$$

$$= \sum_{a=1}^{p-1}\sum_{n=1}^{p} \chi(n)\psi(1-n)\chi(a)\psi(a)e^{\frac{2\pi ia}{p}} = G(\chi\psi)\sum_{a=1}^{p} \chi(a)\psi(1-a),$$

as desired. □

Now we can give an "analytic proof" of Fermat's theorem that any prime $\equiv 1 \pmod 4$ is a sum of two squares.

Analytic proof that a prime $\equiv 1 \pmod 4$ is a sum of two squares. Let $p \equiv 1 \pmod 4$ be a rational prime. Then, as 4 divides $p-1$, there is a surjective group homomorphism $\chi : \mathbb{F}_p^\times \twoheadrightarrow \mathbb{Z}/4\mathbb{Z}$. By identifying $\mathbb{Z}/4\mathbb{Z}$ with $\mu_4 \subset \mathbb{C}$, we can see χ as a Dirichlet character of conductor p. Note that $|J(\chi,\chi)| = \sqrt{p}$ from the size of the Gauss sums, but also by Lemma 18.13, $J(\chi,\chi)$ is an integer linear combination of i and 1, so $J(\chi,\chi) \in \mathbb{Z}[i]$. Thus, $J(\chi,\chi) \in \mathbb{Z}[i]$ has norm p, so we actually explicitly constructed an element $\mathbb{Z}[i]$ whose norm is p. □

The Jacobi and Gauss sums can also give an "analytic proof" of the cubic reciprocity law!

Analytic proof of the cubic reciprocity law. Let $K = \mathbb{Q}(\zeta_3)$ and $\pi_1, \pi_2 \in \mathcal{O}_K$ be distinct primary primes, with $N(\pi_1) = p_1$, $N(\pi_2) = p_2$. Here, we will only prove the case $p_1 \equiv p_2 \equiv 1 \pmod 3$, which is the most difficult case. We can consider, for $j = 1, 2$, $\chi_j(n) := \left(\frac{n}{\pi_j}\right)$ as a Dirichlet character mod p_j. Then, $J(\chi_1, \chi_1) \in \mathbb{Z}[\zeta_3]$, whose norm is p_1, thus a prime number. Note on the other hand that $\chi_1^2 = \overline{\chi_1}$, so

$$J(\chi_1,\chi_1) = \frac{G(\chi_1)^2}{G(\chi_1^2)} = \frac{G(\chi_1)^2}{G(\overline{\chi_1})} = \frac{G(\chi_1)^2}{\chi_1(-1)\overline{G(\chi_1)}} = \frac{G(\chi_1)^3}{p_1},$$

as $\chi_1(-1) = \chi_1(-1)^3 = 1$. Therefore,

$$J(\chi_1,\chi_1) \equiv G(\chi_1)^3 = \left(\sum_{a=1}^{p-1} \chi_1(a) e^{\frac{2\pi i a}{p}}\right)^3 \equiv \sum_{a=1}^{p-1} \chi_1(a)^3 e^{3\cdot\frac{2\pi i a}{p}} = \sum_{a=1}^{p-1} e^{3\cdot\frac{2\pi i a}{p}} = \frac{e^{3\cdot 2\pi i}-1}{e^{3\cdot\frac{2\pi i}{p}}-1} - 1 \equiv 2 \pmod 3.$$

Therefore, it follows that $J(\chi_1,\chi_1)$ is a **primary prime**, so $J(\chi_1,\chi_1) = \pi_1$. In particular, $G(\chi_1)^3 = p_1\pi_1$.

Note that, for $j = 1, 2$, $\overline{\pi_j}$, the complex conjugate of π_j, is also a primary prime. Let $\psi_j(n) := \left(\frac{n}{\overline{\pi_j}}\right)$. Then, $G(\psi_1)^3 = p_1\overline{\pi_1}$. Thus,

$$G(\psi_1)^{p_2-1} = (p_1\overline{\pi_1})^{\frac{p_2-1}{3}} \equiv \chi_2(p_1\overline{\pi_1}) \pmod{\pi_2},$$

or

$$G(\psi_1)^{p_2} \equiv G(\psi_1)\chi_2(p_1\overline{\pi_1}) \pmod{\pi_2}.$$

On the other hand,

$$G(\psi_1)^{p_2} = \left(\sum_{a=1}^{p_1-1} \psi_1(a) e^{\frac{2\pi i a}{p_1}}\right)^{p_2} \equiv \sum_{a=1}^{p_1-1} \psi_1(a)^{p_2} e^{p_2\cdot\frac{2\pi i a}{p_1}} = \sum_{a=1}^{p_1-1} \psi_1(a) e^{p_2\cdot\frac{2\pi i a}{p_1}}$$

$$= \psi_1(p_2)^{-1} \sum_{a=1}^{p_1-1} \psi_1(p_2 a) e^{p_2\cdot\frac{2\pi i a}{p_1}} = \psi_1(p_2)^2 G(\psi_1) \pmod{\pi_2},$$

so we have

$$\psi_1(p_2)^2 \equiv \chi_2(p_1\overline{\pi_1}) \pmod{\pi_2}.$$

Since both are in $\mu_3 \subset K$, them being congruent mod π_2 is the same as them being equal;

$$\psi_1(p_2)^2 = \chi_2(p_1\overline{\pi_1}).$$

Note also that $\psi_1(p_2) \equiv p_2^{\frac{p_1-1}{3}} \pmod{\overline{\pi_1}}$, which implies that $\overline{\psi_1(p_2)} \equiv p_2^{\frac{p_1-1}{3}} \pmod{\pi_1}$, or $\overline{\psi_1(p_2)} = \chi_1(p_2)$. Since $\overline{\psi_1(p_2)} = \psi_1(p_2)^2$, we have

$$\chi_1(p_2) = \chi_2(p_1\overline{\pi_1}).$$

We can switch the roles to obtain various equalities:

$$\chi_1(p_2)^2 = \chi_2(p_1\pi_1), \quad \psi_2(p_1)^2 = \chi_1(p_2\overline{\pi_2}), \quad \chi_2(p_1)^2 = \chi_1(p_2\pi_2), \quad \cdots$$

Thus we have

$$\chi_1(\pi_2) = \frac{\chi_1(\pi_2)\chi_2(p_1\overline{\pi_1})}{\chi_2(p_1\overline{\pi_1})} = \frac{\chi_1(p_2\pi_2)}{\chi_2(p_1\overline{\pi_1})} = \frac{\chi_2(p_1)^2}{\chi_2(p_1\overline{\pi_1})} = \chi_2(\pi_1),$$

or

$$\left(\frac{\pi_2}{\pi_1}\right) = \left(\frac{\pi_1}{\pi_2}\right).$$

□

Another arithmetically interesting numbers coming out of the Dirichlet L-functions are the values of Dirichlet L-functions at certain numbers, in particular at the **integers**, which are expressed in terms of the **(generalized) Bernoulli numbers**.

Definition 18.14 (Bernoulli numbers)**.** The **Bernoulli numbers** $B_0, B_1, \cdots$ are a sequence of rational numbers defined as the coefficients of the power series as follows:

$$\frac{X}{e^X - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} X^n.$$

More generally, let χ be a Dirichlet character of modulus m. The **generalized Bernoulli numbers** $B_{0,\chi}, B_{1,\chi}, \cdots$ are a sequence of algebraic numbers defined as the coefficients of the power series as follows:

$$\sum_{a=1}^{m} \chi(a) \frac{X e^{aX}}{e^{mX} - 1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} X^n.$$

Note that $B_{n,\mathbf{1}} = B_n$ except $B_{1,\mathbf{1}}$, for which $B_1 = -\frac{1}{2}$ whereas $B_{1,\mathbf{1}} = \frac{1}{2}$; this disparity comes from the only appearance of pole in the Riemann zeta function and not in the other Dirichlet L-functions.

The generalized Bernoulli numbers can be computed using the **Bernoulli polynomials**,

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i},$$

from which, for a Dirichlet character of modulus m,

$$B_{n,\chi} = m^{n-1} \sum_{a=1}^{m} \chi(a) B_n(a/m).$$

In particular, $B_{n,\chi} \in \mathbb{Q}(\chi)$, where $\mathbb{Q}(\chi)$ is the **trace field** of χ, which is the smallest number field that contains $\chi(a)$ for all $a \in \mathbb{N}$.

Example 18.15. The first few Bernoulli numbers are:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \quad B_5 = 0, \quad B_6 = \frac{1}{42}.$$

There is an obvious pattern, which is in fact true in general:

Proposition 18.16.

(1) For an odd integer $n > 1$, $B_n = 0$.

(2) For a Dirichlet character χ of modulus $m > 1$, $B_{n,\chi} = 0$ if $(-1)^n \neq \chi(-1)$ (i.e. if n is odd and χ is even, or if n is even and χ is odd).

Proof. (1) This is an easy consequence of the fact that $\frac{X}{e^X-1}+\frac{X}{2}=\frac{X+Xe^X}{2(e^X-1)}$ is an even function in X, as

$$\frac{-X-Xe^{-X}}{2(e^{-X}-1)}=\frac{-Xe^X-X}{2(1-e^X)}=\frac{X+Xe^X}{2(e^X-1)}.$$

(2) Let $f(X)=\sum_{a=1}^{m-1}\chi(a)\frac{Xe^{aX}}{e^{mX}-1}$ (the sum can end at $a=m-1$ as $m>1$). Then,

$$f(-X)=\sum_{a=1}^{m-1}\chi(a)\frac{-Xe^{-aX}}{e^{-mX}-1}=\chi(-1)\sum_{a=1}^{m-1}\chi(-a)\frac{Xe^{(m-a)X}}{e^{mX}-1}=\chi(-1)f(X),$$

from which the statement follows.

□

We will see in a few lectures that these harmless-looking rational numbers have in fact a lot to do with the arithmetic of cyclotomic fields. In the meantime, we notice the relation between the generalized Bernoulli numbers and the values of the Dirichlet L-functions at the integers.

Theorem 18.17 (Values of the Dirichlet L-functions at the integers)**.** *Let χ be a primitive Dirichlet character of conductor m.*

(1) For a positive integer $n\geq 1$,

$$L(1-n,\chi)=-\frac{B_{n,\chi}}{n}.$$

*In particular, $L(1-n,\chi)\in\mathbb{Q}(\chi)$, and $L(1-n,\chi)=0$ if $(-1)^n\neq\chi(-1)$ (i.e. $L(s,\chi)$ vanishes at the negative odd integers when χ is odd, and at the nonpositive even integers when χ is even, with an exception $\zeta(0)=-\frac{1}{2}$). These zeros are called the **trivial zeros** of the Dirichlet L-functions.*

(2) Let χ be even. For a positive integer $n\geq 1$,

$$L(2n,\chi)=-G(\chi)\frac{\pi^{2n}}{2m^{2n}\binom{-1/2}{n}(n!)^2}\overline{B_{2n,\chi}}.$$

In particular, $\frac{L(2n,\chi)}{\pi^{2n}}\in\overline{\mathbb{Q}}$.

(3) Let χ be even. For a nonnegative integer $n\geq 0$,

$$L(2n+1,\chi)=(-1)^nG(\chi)\frac{2\pi^{2n}}{m^{2n+1}\binom{n-\frac{1}{2}}{n}(n!)^2}\lim_{s\to -2n}\frac{L(s,\overline{\chi})}{s+2n}.$$

(4) Let χ be odd. For a nonnegative integer $n\geq 0$,

$$L(2n+1,\chi)=iG(\chi)\frac{\pi^{2n+1}}{m^{2n+1}\binom{-1/2}{n}(n!)^2(2n+1)}\overline{B_{2n+1,\chi}}.$$

In particular, $\frac{L(2n+1,\chi)}{\pi^{2n+1}}\in\overline{\mathbb{Q}}$.

(5) Let χ be odd. For a positive integer $n \geq 1$,

$$L(2n,\chi) = (-1)^n iG(\chi)\frac{2\pi^{2n-1}}{m^{2n}\binom{n-\frac{1}{2}}{n}(n-1)!n!}\lim_{s\to 1-2n}\frac{L(s,\overline{\chi})}{s+2n-1}.$$

Proof. Note that (2), (3), (4), (5) are the consequences of (1) and the functional equation, with some facts such as $B_{n,\overline{\chi}} = \overline{B_{n,\chi}}$, $\Gamma(n) = (n-1)!$ for a positive integer n, $\operatorname{Res}_{z=-n}\Gamma(z) = \frac{(-1)^n}{n!}$ for a nonnegative integer n, and for a nonnegative integer n,

$$\Gamma\left(\frac{1}{2}+n\right) = \binom{n-\frac{1}{2}}{n}n!\sqrt{\pi}, \quad \Gamma\left(\frac{1}{2}-n\right) = \frac{\sqrt{\pi}}{\binom{-1/2}{n}n!}.$$

We now prove (1). We start from

$$\Gamma(s) = \int_0^\infty y^s e^{-y}\frac{dy}{y} = \int_0^\infty n^s y^s e^{-ny}\frac{dy}{y},$$

which holds for $\operatorname{Re}(s) > 1$. From this, we get, for $\operatorname{Re}(s) > 1$,

$$\Gamma(s)L(s,\chi) = \int_0^\infty \left(\sum_{n=1}^\infty \chi(n)e^{-ny}\right)y^s\frac{dy}{y}.$$

Let $P_\chi(X) = \sum_{n=1}^\infty \chi(n)X^n = \sum_{a=1}^m \chi(a)X^a\sum_{n=0}^\infty X^{mn} = \sum_{a=1}^m \chi(a)\frac{X^a}{1-X^m}$. Then, $\Gamma(s)L(s,\chi) = \int_0^\infty P_\chi(e^{-y})y^s\frac{dy}{y}$. We want to take this integral representation and perform the analytic continuation of the product $\Gamma(s)L(s,\chi)$ by doing integration by parts with $u = P_\chi(e^{-y})$ and $dv = y^{s-1}$, using that $\Gamma(s+1) = s\Gamma(s)$. The problem is that $P_\chi(e^{-y})$ diverges as $y \to 0^+$. Thus, we consider the modifed version, $L^*(s,\chi) = (1-2^{1-s})L(s,\chi)$. Then, we find that

$$\Gamma(s)L^*(s,\chi) = \int_0^\infty R_\chi(e^{-y})y^s\frac{dy}{y}, \quad R_\chi(X) = P_\chi(X) - 2P_\chi(X^2).$$

This has an advantage, that

$$R_\chi(X) = \sum_{a=1}^m \chi(a)\left(\frac{X^a}{1-X^m} - 2\frac{X^{2a}}{1-X^{2m}}\right) = \sum_{a=1}^m \chi(a)X^a\frac{X^a(X^{m-a-1}+\cdots+1)-(X^{a-1}+\cdots+1)}{X^{2m-1}+\cdots+1},$$

which now has the property that $\lim_{X\to 0^+}R_\chi(X) = \sum_{a=1}^m \chi(a)\frac{m-2a}{2m}$ is a finite number, and $\lim_{X\to+\infty}R_\chi(X) = 0$. Let $r_{\chi,k}(y) = \left(\frac{d^k}{dy^k}\right)R_\chi(e^{-y})$. Then, by integration by parts,

$$\Gamma(s)L^*(s,\chi) = r_{\chi,0}(y)\frac{y^s}{s}\Big|_{y=0}^{y=\infty} - \frac{1}{s}\int_0^\infty r_{\chi,1}(y)y^{s+1}\frac{dy}{y} = -\frac{1}{s}\int_0^\infty r_{\chi,1}(y)y^{s+1}\frac{dy}{y},$$

as $r_{\chi,0}(y)$ decays exponentially as $y \to +\infty$, so

$$\Gamma(s+1)L^*(s,\chi) = -\int_0^\infty r_{\chi,1}(y)y^{s+1}\frac{dy}{y}.$$

By a repeated application of integration by parts, we get, for any $k \geq 0$ nonnegative integer,

$$\Gamma(s+k)L^*(s,\chi) = (-1)^k \int_0^\infty r_{\chi,k}(y) y^{s+k} \frac{dy}{y}.$$

The integral on the right defines an entire function on $\mathrm{Re}(s) > -k$. Now applying this to $k = n$ and $s = 1-n$, we get

$$(1-2^n)L(1-n,\chi) = (-1)^n \int_0^\infty r_{\chi,n}(y)dy = (-1)^{n-1} r_{\chi,n-1}(0).$$

Note that

$$r_{\chi,0}(y) = P_\chi(e^{-y}) - 2P_\chi(e^{-2y}),$$
$$P_\chi(e^{-y}) = \sum_{a=1}^{m} \chi(a) \frac{e^{-ay}}{1-e^{-my}} = \sum_{k=0}^{\infty} (-1)^k \frac{B_{k,\chi}}{k!} y^{k-1},$$

so

$$r_{\chi,0}(y) = \sum_{k=0}^{\infty} (-1)^k (1-2^k) \frac{B_{k,\chi}}{k!} y^{k-1}.$$

Therefore,

$$(1-2^n)L(1-n,\chi) = (-1)^{n-1} \left(\frac{d^{n-1}}{dy^{n-1}} \right) r_{\chi,0}(y)\Big|_{y=0} = (-1)^{n-1}(-1)^n(1-2^n)\frac{B_{n,\chi}}{n},$$

or $L(1-n,\chi) = -B_{n,\chi}/n$, as desired. □

Example 18.18. For example, Theorem 18.17(2) applied to the Riemann zeta function implies that

$$\zeta(2n) = -\frac{\pi^{2n}}{2\binom{-1/2}{n}(n!)^2} B_{2n}.$$

This replicates the known values:

$$\zeta(2) = -\frac{\pi^2}{2\binom{-1/2}{1}} B_2 = \frac{\pi^2}{6}, \quad \zeta(2n) = -\frac{\pi^4}{8\binom{-1/2}{2}} B_4 = \frac{\pi^4}{30 \cdot 3} = \frac{\pi^4}{90}, \quad \cdots.$$

Note that Theorem 18.17 tells us that $L(s,\chi)$ evaluated at the nonpositive integers are algebraic numbers, and half of them are zeros. Furthermore, $L(s,\chi)$ evaluated at the positive integers with matching parity with χ is an algebraic number times a precise power of π. It is a well-known fact that π is a **transcendental number**, i.e. $\pi \notin \overline{\mathbb{Q}}$, so we know the transcendence of $L(s,\chi)$ at the positive integers with matching parity.

What about the values of $L(s,\chi)$ at the positive integers with **different parity** from χ, i.e. the cases of (3) and (5) in Theorem 18.17? Note that the limits appearing in the statement are the leading coefficients at the zeroes of Dirichlet L-functions; indeed, if χ is even, $L(s,\overline{\chi})$ has a zero at $s = -2n$, and $\lim_{s\to -2n} \frac{L(s,\overline{\chi})}{s+2n}$ is the leading coefficient of the Taylor series expansion of $L(s,\overline{\chi})$ at $s = -2n$, and similarly for χ odd case. These cases include the values of $\zeta(s)$ at the positive odd integers > 1. In fact, the following is expected.

Conjecture 18.19 (Folklore). *For a Dirichlet character χ and a positive integer $n > 1$, $L(n, \chi)$ is a transcendental number (i.e. $L(n, \chi) \notin \overline{\mathbb{Q}}$).*

Other than those covered by Theorem 18.17, the progress is minimal; the only progress so far is that $\zeta(3) \notin \mathbb{Q}$ (Apéry, 1978)[30]. Note that only the **irrationality** is known, not the transcendence!

Finally, we record the Generalized Riemann Hypothesis (GRH):

Conjecture 18.20 (Generalized Riemann Hypothesis). *Let χ be a Dirichlet character. If $s = z$ is a non-trivial zero of $L(s, \chi)$, then $\mathrm{Re}(z) = \frac{1}{2}$.*

– –

Exercise 18.1. Let χ be a primitive odd Dirichlet character of modulus m, and let

$$\widetilde{\theta}_\chi(iy) = \sum_{n \in \mathbb{Z}} \chi(n) n \sqrt{y} e^{-\pi n^2 y}, \quad y > 0.$$

(1) Show that, for $\mathrm{Re}(s) > 1$,

$$\pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right) L(s, \chi) = \int_0^\infty y^{\frac{s}{2}} \frac{\widetilde{\theta}_\chi(iy)}{2} \frac{dy}{y}.$$

(2) Using the Poisson summation formula, show that

$$\widetilde{\theta}_\chi(iy) = -\frac{iG(\chi)}{m\sqrt{y}} \widetilde{\theta}_{\overline{\chi}}\left(\frac{i}{m^2 y}\right).$$

Hint. The Fourier transform of $f(x) = xe^{-\pi x^2}$ is $\widehat{f}(x) = -ixe^{-\pi x^2}$.

Exercise 18.2. Let χ be a Dirichlet character. Note that the Euler product expansion of $L(s, \chi)$ implies that, for $\mathrm{Re}(s) > 1$,

$$\log L(s, \chi) = -\sum_{p \text{ prime}} \log(1 - \chi(p) p^{-s}).$$

(1) Show that, for $\mathrm{Re}(s) > 1$,

$$\log L(s, \chi) = \sum_{p \text{ prime}} \sum_{n=1}^{\infty} \frac{\chi(p)^n p^{-ns}}{n},$$

and the double infinite sum on the right hand side is absolutely convergent.

[30] In March 2024, Calegari–Dimitrov–Tang announced the proof of $L(2, \chi_3) \notin \mathbb{Q}$, where χ_3 is the unique non-principal Dirichlet character of modulus 3.

(2) Show that there exists a constant $C > 0$ such that for any χ and $\mathrm{Re}(s) > 1$,

$$\left| \log L(s,\chi) - \sum_{p \text{ prime}} \chi(p) p^{-s} \right| < C.$$

(3) Let $n > 1$, and let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Show that

$$\left| \frac{1}{\varphi(n)} \left(\sum_{\chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times}} \overline{\chi(a)} \log L(s,\chi) \right) - \left(\sum_{p \text{ prime}, \, p \equiv a \pmod n} p^{-s} \right) \right| < C.$$

Deduce that there are infinitely many primes that are $\equiv a \pmod n$.

Hint. Show that $\lim_{s \to 1^+} \sum_{p \text{ prime}, \, p \equiv a \pmod n} p^{-s}$ diverges.

Exercise 18.3. In the notes, we provided the "analytic" proof of the cubic reciprocity law between two primary primes lying over the rational primes $\equiv 1 \pmod 3$. In this exercise, we supplement this with the proof of the remaining cases of the cubic reciprocity law.

Recall that a primary prime in $\mathbb{Z}[\zeta_3]$ is either $\pi \in \mathbb{Z}[\omega]$ with $N(\pi)$ a rational prime $\equiv 1 \pmod 3$ or a rational prime $p \equiv 2 \pmod 3$. For primary primes $\pi_1, \pi_2 \in \mathbb{Z}[\zeta_3]$, $\left(\frac{\pi_1}{\pi_2}\right) \in \{1, \zeta_3, \zeta_3^2\}$ is such that

$$\left(\frac{\pi_1}{\pi_2}\right) \equiv \pi_1^{\frac{N(\pi_2)-1}{3}} \pmod{\pi_2}.$$

(1) If $\pi_1 = q$ is a rational prime $\equiv 2 \pmod 3$, show that any integer coprime to q is a cube mod q. Deduce the cubic reciprocity law in the case when both π_1, π_2 are rational primes $\equiv 2 \pmod 3$.

(2) Suppose that $\pi_1 = q$ is a rational prime $\equiv 2 \pmod 3$ and $\pi_2 = \pi$ is such that $N(\pi) = p$ is a rational prime $\equiv 1 \pmod 3$. Let $\chi(n) := \left(\frac{n}{\pi}\right)$ be a Dirichlet character mod p. From $G(\chi)^3 = p\pi$, show that

$$G(\chi)^{q^2} \equiv \left(\frac{\pi}{q}\right) G(\chi) \pmod q.$$

(3) Show that

$$G(\chi)^{q^2} \equiv \sum_{a=1}^{p-1} \chi(a) e^{\frac{2\pi i a q^2}{p}} \pmod q.$$

(4) Deduce that

$$\chi(q) = \left(\frac{q}{\pi}\right) = \left(\frac{\pi}{q}\right).$$

Exercise 18.4. Let n be an even positive integer.

(1) Show that, for any $m \geq 1$.

$$B_n = m^{n-1} \sum_{a=1}^{m} B_n(a/m).$$

(2) Show that the denominator of B_n is a square-free integer.

Hint. You need to show that $v_p(pB_n) \geq 0$ for any prime number p. Use (1) with $m = p$ to get

$$pB_n = \sum_{a=1}^{p} \sum_{i=0}^{n} \binom{n}{i} p^i B_i a^{n-i}.$$

Now, use induction on n.

(3) Show that, for any prime p,

$$pB_n \equiv \begin{cases} -1 & \text{if } (p-1)|n \\ 0 & \text{otherwise} \end{cases} \pmod{p}.$$

This implies that $B_n + \sum_{p \text{ primes such that } (p-1)|n} \frac{1}{p}$ is an integer.[31]

Hint. From the identity used in the Hint of (2), one has

$$pB_n \equiv \sum_{a=1}^{p} \left(a^n + npB_1 a^{n-1}\right) \pmod{p}.$$

Then, show that $v_p(npB_1) \geq 1$.

[31]This result is often called the **von Staudt–Clausen theorem**. This in particular implies that 6 always divides the denominator of B_n.

19. Lecture 25. The analytic class number formula

Summary. Dedekind zeta function; regulators; analytic class number formula; calculation of the class number; upper bound on the class number.

Content. We now study the information carried by an L-function associated with a number field, called the **Dedekind zeta function**.

Definition 19.1 (Dedekind zeta function)**.** Let K be a number field. The **Dedekind zeta function** $\zeta_K(s)$ is defined as

$$\zeta_K(s) := \sum_{\mathfrak{a}\subset\mathcal{O}_K \text{ nonzero ideals}} \frac{1}{N(\mathfrak{a})^s}, \quad \mathrm{Re}(s) > 1.$$

Example 19.2. The Dedekind zeta functions are generalizations of the Riemann zeta function, as $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.

Lemma 19.3. *For a number field K, the Dedekind zeta function $\zeta_K(s)$ has an Euler product expression*

$$\zeta_K(s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K \text{ maximal ideals}} \left(1 - N(\mathfrak{p})^{-s}\right)^{-1}, \quad \mathrm{Re}(s) > 1.$$

Proof. Easy. □

The Dedekind zeta function, just like Dirichlet L-functions or any other L-functions, has analytic continuation and functional equation. We will however focus more on the **poles** and the **residues** of $\zeta_K(s)$, which is encoded by the **analytic class number formula**. To state it, we need one more definition.

Definition 19.4 (Regulators)**.** Let K be a number field, with r real embeddings $\sigma_1, \cdots, \sigma_r$, and s pairs of complex embeddings, $\{\sigma_{r+1}, \overline{\sigma_{r+1}}\}, \cdots, \{\sigma_{r+s}, \overline{\sigma_{r+s}}\}$. The **regulator** of K, denoted R_K, is the volume of a fundamental parallelopiped of $\pi(L(\mathcal{O}_K^\times)) \subset \mathbb{R}^{r+s-1}$, where

$$L : \mathcal{O}_K^\times \to \mathbb{R}^{r+s}, \quad x \mapsto (\log|\sigma_1(x)|, \cdots, \log|\sigma_r(x)|, 2\log|\sigma_{r+1}(x)|, \cdots, 2\log|\sigma_{r+s}(x)|),$$

is the map considered in the proof of Dirichlet unit theorem, Theorem 17.1, and

$$\pi : \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}, \quad (t_1, \cdots, t_{r+s}) \mapsto (t_1, \cdots, t_{r+s-1}),$$

forgets the last coordinate.

In other words, if $u_1, \cdots, u_{r+s-1}$ is a fundamental system of units of K, then

$$R_K = \left| \det \begin{pmatrix} \log|\sigma_1(u_1)| & \log|\sigma_1(u_2)| & \cdots & \log|\sigma_1(u_{r+s-1})| \\ \cdots & \cdots & \cdots & \cdots \\ \log|\sigma_r(u_1)| & \log|\sigma_r(u_2)| & \cdots & \log|\sigma_r(u_{r+s-1})| \\ 2\log|\sigma_{r+1}(u_1)| & 2\log|\sigma_{r+1}(u_2)| & \cdots & 2\log|\sigma_{r+1}(u_{r+s-1})| \\ \cdots & \cdots & \cdots & \cdots \\ 2\log|\sigma_{r+s-1}(u_1)| & 2\log|\sigma_{r+s-1}(u_2)| & \cdots & 2\log|\sigma_{r+s-1}(u_{r+s-1})| \end{pmatrix} \right|.$$

Lemma 19.5. *For any $1 \leq i \leq r+s$, the regulator R_K can be computed by using $\pi_i : \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$ which forgets the i-th coordinate.*

Proof. This is because the $(r+s) \times (r+s-1)$ matrix

$$\begin{pmatrix} \log|\sigma_1(u_1)| & \log|\sigma_1(u_2)| & \cdots & \log|\sigma_1(u_{r+s-1})| \\ \cdots & \cdots & \cdots & \cdots \\ \log|\sigma_r(u_1)| & \log|\sigma_r(u_2)| & \cdots & \log|\sigma_r(u_{r+s-1})| \\ 2\log|\sigma_{r+1}(u_1)| & 2\log|\sigma_{r+1}(u_2)| & \cdots & 2\log|\sigma_{r+1}(u_{r+s-1})| \\ \cdots & \cdots & \cdots & \cdots \\ 2\log|\sigma_{r+s-1}(u_1)| & 2\log|\sigma_{r+s-1}(u_2)| & \cdots & 2\log|\sigma_{r+s-1}(u_{r+s-1})| \\ 2\log|\sigma_{r+s}(u_1)| & 2\log|\sigma_{r+s}(u_2)| & \cdots & 2\log|\sigma_{r+s}(u_{r+s-1})| \end{pmatrix},$$

has the property that each column sums up to zero. □

Example 19.6. Let K be a real quadratic field, regarded as a subfield of $\mathbb{R}$, and let ϵ_K be the fundamental unit. Then, $R_K = \log \epsilon_K$.

Now we can formulate the **analytic class number formula**.

Theorem 19.7 (Analytic class number formula)**.** *Let K be a number field of degree n, with r real embeddings and s pairs of complex embeddings. Then, the Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to a meromorphic function on the whole complex plane, with only one simple pole at $s = 1$, with residue*

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^r(2\pi)^s R_K h_K}{\#\mu_K \sqrt{|\operatorname{disc}(K)|}}.$$

It's very surprising that the residue of the Dedekind zeta function, an analytic quantity, is related to a bag of algebraic quantities we have defined so far! We will not try to prove the analytic class number formula in this class; the proof is elementary but time-consuming.[32] An application of the functional equation, which we also do not bother to state, gives an equivalent statement for the Dedekind zeta function at $s = 0$;

Theorem 19.8 (Analytic class number formula, alternative version)**.** *Let K be a number field of degree n, with r real embeddings and s pairs of complex embeddings. Then, the (analytically continued) Dedekind zeta function $\zeta_K(s)$ has a zero of order $r+s-1$ at $s = 0$, and*

$$\lim_{s \to 0} \frac{\zeta_K(s)}{s^{r+s-1}} = -\frac{h_K R_K}{\#\mu_K}.$$

The analytic class number formula is extremely useful both computationally and theoretically. Firstly, there is a relation between the Dedekind zeta function and the Dirichlet L-functions.

[32] The basic idea is to estimate the number of integral ideals of norms $\leq n$ and to use the so-called **Abelian/Tauberian theorems**. The class number appears as you can partition the integral ideals according to their ideal classes, and the regulator appears because you are counting something using geometry of numbers.

Lemma 19.9. *Let $K/\mathbb{Q}$ be an abelian extension, which is contained in $\mathbb{Q}(\zeta_n)$ by the Kronecker–Weber theorem, Theorem 9.9. Let X_K be the set of Dirichlet characters mod n that are trivial on $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Then,*

$$\zeta_K(s) = \prod_{\chi \in X_K} L(s, \chi_0),$$

where, for each $\chi \in X_K$, χ_0 is the primitive character inducing χ.

Proof. By the Euler product expansion, it suffices to show that

$$(*) \qquad \prod_{\mathfrak{p} \subset \mathcal{O}_K \text{ primes lying over } p} (1 - N(\mathfrak{p})^{-s}) = \prod_{\chi \in X_K} (1 - \chi_0(p) p^{-s}),$$

for all rational primes $p \in \mathbb{Z}$. As $K/\mathbb{Q}$ is Galois, the residue degrees are the same among the primes above p and the same applies for the ramification indices. Let e, f, g be the usual notation. Then, the left hand side of $(*)$ is $(1 - p^{-fs})^g$.

Note that if we take the smallest n such that K is contained in $\mathbb{Q}(\zeta_n)$, then any prime $p \in \mathbb{Z}$ that ramified in $\mathbb{Q}(\zeta_n)$ is also ramified in K; if not, if we let $n = p^a m$ for $a \geq 1$, $(p, m) = 1$, then any prime of $\mathbb{Q}(\zeta_m)$ lying over p is totally ramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m)$, so $K\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m)$, or $K \subset \mathbb{Q}(\zeta_m)$, a contradiction.

Suppose $e = 1$. Then, $p \in (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to $\mathrm{Fr}_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, and by the Frobenius in towers, Theorem 14.13, $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$ is the natural image of $p \in (\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, and f is the order of $p \in \mathrm{Gal}(\widehat{K/\mathbb{Q}})$. This implies that, for $\chi \in X_K$, $\chi(p)^f = 1$. Note that $\#X_K = [K : \mathbb{Q}] = fg$, as $X_K = \widehat{\mathrm{Gal}(K/\mathbb{Q})} \cong \mathrm{Gal}(K/\mathbb{Q})$. It is easy to see that there are precisely g characters in X_K that $\chi(p) = e^{2\pi i m/f}$ for each $m = 0, 1, \cdots, f-1$ (exercise!), so the right hand side of $(*)$ is $\prod_{j=1}^{f}(1 - e^{2\pi ij/f} p^{-s})^g$. Now the identity follows from the identity

$$(1 - X^f) = \prod_{j=1}^{f} (1 - e^{2\pi ij/f} X),$$

and plugging $X = p^{-s}$.

Suppose $e > 1$, so that $n = p^a m$ with $a \geq 1$, $(p, m) = 1$. Let $K/L/\mathbb{Q}$ be the maximal subextension on which p is unramified (this exists as p being unramified is preserved by the compositum of field). I first claim that $[K : L] = e$. This is because, if we take $\mathfrak{p} \subset \mathcal{O}_K$ lying over p, then $D(\mathfrak{p}|p) \subset \mathrm{Gal}(K/\mathbb{Q})$ is of order ef, and $D(\mathfrak{p}|p) \cong \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ for which $e_{K_\mathfrak{p}/\mathbb{Q}_p} = e$ and $f_{K_\mathfrak{p}/\mathbb{Q}_p} = f$, so the maximal unramified extension $K_\mathfrak{p}/M/\mathbb{Q}_p$ gives rise to a subgroup $\mathrm{Gal}(K_\mathfrak{p}/M) \subset \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ corresponding to a subgroup $G \subset D(\mathfrak{p}|p) \subset \mathrm{Gal}(K/\mathbb{Q})$, and this fixes a subfield L such that p is unramified in L and $[K : L] = e$. As this index cannot be smaller than e, we indeed have the claim.

Now I claim that the Dirichlet characters in X_K of conductor prime to p are precisely those induced from X_L. If this is true, the p-part of $(*)$ follows from the corresponding identity in L which we dealt in the above paragraph. As the Dirichlet characters in X_L have conductors prime to p, one containment is clear. Suppose conversely that a Dirichlet character $\chi \in X_K$ has

conductor prime to p. This implies that $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ comes from $\chi_0 : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$, or that χ is trivial on $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))$. Thus, χ is trivial on $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m))\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_m) \cap K)$. I claim that $L = \mathbb{Q}(\zeta_m) \cap K$, which will prove the claim. On one hand, L is the maximal subextension of $K/\mathbb{Q}$ on which p is unramified, and on the other hand, $\mathbb{Q}(\zeta_m)$ is the maximal subextension of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ on which p is unramified. Thus, $L \subset \mathbb{Q}(\zeta_m) \cap K$. On the other hand, certainly p is unramified in $\mathbb{Q}(\zeta_m) \cap K$, so $\mathbb{Q}(\zeta_m) \cap K \subset L$, yielding that $L = \mathbb{Q}(\zeta_m) \cap K$, as desired. □

Corollary 19.10. *Let $K/\mathbb{Q}$ be an abelian extension. Then, $\frac{\zeta_K(s)}{\zeta(s)}$ is an entire function.*

Combining Lemma 19.9 with the analytic class number formula, we get the following

Corollary 19.11. *Let $K/\mathbb{Q}$ be an abelian extension, and retain the notation of Lemma 19.9. Then,*

$$\frac{2^r(2\pi)^s R_K h_K}{\#\mu_K \sqrt{|\operatorname{disc}(K)|}} = \prod_{\chi \in X_K,\ \chi \text{ nonprincipal}} L(1, \chi_0).$$

Proof. This follows from the fact that the simple pole of $\zeta(s)$ at $s = 1$ has residue 1. □

We now can see why Theorem 18.11 is true.

Proof of Theorem 18.11. Let χ be a non-principal primitive Dirichlet character of modulus m. Then, by Theorem 18.7, the only way that $\zeta_{\mathbb{Q}(\zeta_m)}(s)$ has a simple pole at $s = 1$ (which is indeed the case by the analytic class number formula) is when $L(1, \psi) \neq 0$ for all nonprincipal $\psi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$, as $\zeta(s)$ has a simple pole at $s = 1$ and no other Dirichlet L-function has a pole at $s = 1$. □

The reason why this is computationally useful is that $L(1, \chi)$ has a closed formula!

Theorem 19.12. *Let χ be a primitive nonprincipal Dirichlet character of modulus m. Then,*

$$L(1,\chi) = \begin{cases} \frac{\pi i G(\chi)}{m^2} \sum_{a=1}^m \overline{\chi}(a) a & \text{if } \chi \text{ is odd} \\ -\frac{G(\chi)}{m} \sum_{a=1}^m \overline{\chi}(a) \log\left|1 - e^{\frac{2\pi i a}{m}}\right| & \text{if } \chi \text{ is even.} \end{cases}$$

Proof. The odd case is simply a reformulation of Theorem 18.17(4), which says $L(1,\chi) = \frac{\pi i G(\chi)}{m}\overline{B_{1,\chi}}$, combined with the identity $B_{1,\chi} = \frac{1}{m}\sum_{a=1}^m \chi(a)a$.

The basic idea for the even case comes from that

$$L(1,\chi) = \sum_{n=1}^\infty \frac{\chi(n)}{n} = \sum_{n=1}^\infty \frac{1}{nG(\overline{\chi})} \sum_{a=1}^m \overline{\chi}(a) e^{\frac{2\pi i a n}{m}} = \frac{1}{G(\overline{\chi})} \sum_{a=1}^m \overline{\chi}(a) \sum_{n=1}^\infty \frac{e^{\frac{2\pi i a n}{m}}}{n}$$

$$= -\frac{G(\chi)}{m} \sum_{a=1}^m \overline{\chi}(a) \log\left(1 - e^{\frac{2\pi i a}{m}}\right) = -\frac{G(\chi)}{m} \sum_{a=1}^m \overline{\chi}(a) \log\left|1 - e^{\frac{2\pi i a}{m}}\right|.$$

Here, the last identity comes from the fact that, as $\chi(-1) = 1$,

$$\overline{\chi}(a)\log\left(1 - e^{\frac{2\pi i a}{m}}\right) + \overline{\chi}(-a)\log\left(1 - e^{-\frac{2\pi i a}{m}}\right) = \overline{\chi}(a)\log\left|1 - e^{\frac{2\pi i a}{m}}\right| + \overline{\chi}(-a)\log\left|1 - e^{-\frac{2\pi i a}{m}}\right|.$$

However, this is not really a proof as the infinite series is only conditionally convergent, so we cannot freely change the order of summation. This can be justified as follows. We have, for $\mathrm{Re}(s) > 1$,

$$L(s,\chi) = \sum_{a=1}^{m} \chi(a) \sum_{n \equiv a \pmod m} \frac{1}{n^s} = \sum_{a=1}^{m} \frac{\chi(a)}{m} \sum_{n=1}^{\infty} \sum_{k=1}^{m} \frac{e^{\frac{2\pi i(a-n)k}{m}}}{n^s}$$

$$= \frac{1}{m} \sum_{k=1}^{m} \left(\sum_{a=1}^{m} \chi(a) e^{\frac{2\pi i a k}{m}} \right) \sum_{n=1}^{\infty} \frac{e^{-\frac{2\pi i n k}{m}}}{n^s} = \frac{1}{m} \sum_{k=1}^{m} G(\chi)\overline{\chi}(k) \sum_{n=1}^{\infty} \frac{e^{-\frac{2\pi i n k}{m}}}{n^s}.$$

We can now use the fact that, as $s \in \mathbb{R}_{>1}$ approaches 1 from the right on the real line, $\sum_{n=1}^{\infty} \frac{e^{-\frac{2\pi i n k}{m}}}{n^s}$ is sent to $-\log\left(1 - e^{-\frac{2\pi i k}{m}}\right)$. Switching k to $-k$, we get the desired result. □

Remark 19.13. Theorem 19.12 can be reformulated in terms of the leading coefficient of $L(s,\chi)$ at $s = 0$, i.e. $L(0,\chi)$ for χ odd, and $L'(0,\chi)$ for χ even. As seen in the analytic class number formula, the expressions for $L(s,\chi)$ at $s = 0$ are much nicer (in particular doesn't involve π or the Gauss sums). There is a generalized version of Lemma 19.9 that applies to any number field $K/\mathbb{Q}$, which factorizes $\zeta_K(s)$ into a product of **Artin L-functions** (non-abelian version of Dirichlet L-functions), and the analogue of Theorem 19.12 is called the **Stark conjecture**, which predicts the leading coefficient of the Artin L-functions at $s = 0$ in terms of a regulator matrix consisted of logarithms of units.

A surprising consequence of this is a closed-form formula of the class number of a quadratic field!

Definition 19.14. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d = \mathrm{disc}(K)$. The **quadratic Dirichlet character** (**quadratic character** in short) χ_d is a Dirichlet character of modulus $|d|$, defined as

$$\chi_d(n) = \begin{cases} 0 & \text{if } (n,d) > 1 \\ \left(\frac{d}{p_1}\right)^{e_1} \cdots \left(\frac{d}{p_k}\right)^{e_k} & \text{if } n > 0,\ n = p_1^{e_1} \cdots p_k^{e_k} \text{ and } (n,d) = 1 \\ \chi_d(-n)\chi_d(|d|-1) & \text{if } n < 0. \end{cases}$$

Lemma 19.15. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d = \mathrm{disc}(K)$.*

(1) The quadratic character χ_d is a primitive Dirichlet character of conductor $|d|$.

(2) The quadratic charcater χ_d is even if $d > 0$ and odd if $d < 0$.

Proof. (1) By quadratic reciprocity, it is easy to see that χ_d is indeed a Dirichlet character of modulus $|d|$.

We show that χ_d is a primitive Dirichlet character of conductor $|d|$. Then, $|d|$ can be a non-squarefree integer precisely because there might be a power of 2 dividing $|d|$, and it

can go up to $8|d$. On the other hand, $v_2(d)$ can only be 0, 2 or 3. If d is odd, thus square-free, the quadratic reciprocity law shows that indeed the conductor is divisible by every prime factor of d, thus equal to d.

Suppose that $v_2(d) = 3$. Let's take a prime $p \equiv \frac{d}{2} + 1 \pmod{d}$, which is possible due to the Dirichlet's theorem on primes in arithmetic progression (e.g. Exercise 18.2). Then,

$$\chi_d(p) = \left(\frac{d}{p}\right) = \left(\frac{d/4}{p}\right).$$

Now note that $d/4$ is a square-free integer, $d = \epsilon 2 q_1 \cdots q_r$, $\epsilon \in \{\pm 1\}$. Then,

$$\chi_d(p) = \left(\frac{\epsilon}{p}\right)\left(\frac{2}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i}{p}\right).$$

As $p \equiv 1 \pmod{4}$, by quadratic reciprocity, $\left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right) = \left(\frac{1}{q_i}\right) = 1$. Also, as $p \equiv 1 \pmod{4}$, regardless of whether ϵ is 1 or -1, $\left(\frac{\epsilon}{p}\right) = 1$. On the other hand, $\left(\frac{2}{p}\right) = -1$, as $p \equiv 5 \pmod{8}$. This implies that $\chi_d(p) = -1$. This implies that the conductor of χ_d does not divide $\frac{d}{2}$, which means that the conductor is precisely $|d|$, as desired.

Finally, suppose that $v_2(d) = 2$, so that $d = 4e$, $e \equiv 3 \pmod{4}$, $e = \pm q_1 \cdots q_r$ a squarefree integer. Let's take a prime $p \equiv \frac{d}{2} + 1 \pmod{d}$, which is possible due to the Dirichlet's theorem on primes in arithmetic progression. Then,

$$\chi_d(p) = \left(\frac{d}{p}\right) = \left(\frac{e}{p}\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i}{p}\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left((-1)^{\frac{q_i-1}{2}}\left(\frac{p}{q_i}\right)\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}(-1)^{\frac{q_i-1}{2}},$$

as $p \equiv 3 \pmod{4}$. If $e > 0$, then $\chi_d(p)$ is (-1) raised to the power of the number of q_i's that are $\equiv 3 \pmod{4}$, which is odd, so this is -1. On the other hand, if $e < 0$, then $\chi_d(p)$ is (-1) times (-1) raised to the power of the number of q_i's that are $\equiv 3 \pmod{4}$, which is even, so this is again -1. All in all, this implies that the conductor of χ_d does not divide $\frac{d}{2}$, which means that the conductor is precisely $|d|$, as desired.

(2) If d is odd, then $d = \pm q_1 \cdots q_r$ is a squarefree integer. Let $p \equiv 2q_1 \cdots q_r - 1 \pmod{4q_1 \cdots q_r}$ be a prime, whose existence is again guaranteed by the Dirichlet's theorem on primes in arithmetic progressions. Then,

$$\chi_d(-1) = \chi_d(p) = \left(\frac{d}{p}\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i}{p}\right) = \prod_{i=1}^{r}\left(\frac{p}{q_i}\right) = \prod_{i=1}^{r}\left(\frac{-1}{q_i}\right) = \prod_{i=1}^{r}(-1)^{\frac{q_i-1}{2}},$$

as $p \equiv 1 \pmod{4}$. Note that, if $d > 0$, then $q_1 \cdots q_r \equiv 1 \pmod{4}$, so that the number of q_i's that are $\equiv 3 \pmod{4}$ is even, so $\chi_d(-1) = 1$. On the other hand, if $d < 0$, then $q_1 \cdots q_r \equiv 3 \pmod{4}$, so that the number of q_i's that are $\equiv 3 \pmod{4}$ is odd, so $\chi_d(-1) = -1$.

If $v_2(d) = 8$, then $d = \pm 8q_1q_2 \cdots q_r, q_1, \cdots, q_r$ are distinct odd primes. Let $p \equiv -1 \pmod{|d|}$, whose existence is guaranteed by the Dirichlet's theorem on primes in arithmetic progressions. As $p \equiv 7 \pmod 8$,

$$\chi_d(-1) = \chi_d(p) = \left(\frac{d}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i}{p}\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left((-1)^{\frac{q_i-1}{2}}\left(\frac{p}{q_i}\right)\right)$$

$$= \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left((-1)^{\frac{q_i-1}{2}}\left(\frac{-1}{q_i}\right)\right) = \left(\frac{\pm 1}{p}\right).$$

Thus, $\chi_d(-1) = 1$ if $d > 0$ and $\chi_d(-1) = -1$ if $d < 0$.

Finally, if $v_2(d) = 4$, then $d = \pm 4q_1 \cdots q_r, q_1, \cdots, q_r$ are distinct odd primes, and $\pm q_1 \cdots q_r \equiv 3 \pmod 4$. Let $p \equiv -1 \pmod{|d|}$, whose existence is guaranteed by the Dirichlet's theorem on primes in arithmetic progressions. As $p \equiv 3 \pmod 4$,

$$\chi_d(-1) = \chi_d(p) = \left(\frac{d}{p}\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left(\frac{q_i}{p}\right) = \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left((-1)^{\frac{q_i-1}{2}}\left(\frac{p}{q_i}\right)\right)$$

$$= \left(\frac{\pm 1}{p}\right)\prod_{i=1}^{r}\left((-1)^{\frac{q_i-1}{2}}\left(\frac{-1}{q_i}\right)\right) = \left(\frac{\pm 1}{p}\right).$$

Thus, $\chi_d(-1) = 1$ if $d > 0$ and $\chi_d(-1) = -1$ if $d < 0$.

□

The factorization of Dedekind zeta function gives the following:

Corollary 19.16. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d = \operatorname{disc}(K)$. Then,*

$$\zeta_K(s) = \zeta(s)L(s, \chi_d).$$

Proof. This follows from Lemma 19.9 and Lemma 19.15(1). □

Theorem 19.17. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d = \operatorname{disc}(K)$.*

(1) If $d < 0$, then

$$h_K = \frac{\#\mu_K}{2|d|}\left|\sum_{a=1}^{|d|}\chi_d(a)a\right|.$$

(2) If $d > 0$, then

$$h_K = \frac{1}{\log|\epsilon_K|}\left|\sum_{a=1}^{\lfloor\frac{d}{2}\rfloor}\chi_d(a)\log\left(\sin\left(\frac{\pi a}{d}\right)\right)\right|,$$

where ϵ_K is the fundamental unit of K (with respect to the real embedding $K \subset \mathbb{R}$ sending $\sqrt{d} \mapsto \sqrt{d}$).

Proof. (1) As per the analytic class number formula and Lemma 19.15(2), we need to prove that

$$L(1,\chi_d)=\frac{\pi}{|d|^{3/2}}\left|\sum_{a=1}^{|d|}\chi_d(a)a\right|.$$

Note that χ_d is valued in ±1, so in particular $L(1,\chi_d)$ is a real number, and actually a positive real number, according to the analytic class number formula (alternatively you can use $L(1,\chi)=\sum_{n=1}^{\infty}\chi(n)/n$ and the alternating series test). By Theorem 19.12,

$$L(1,\chi_d)=|L(1,\chi_d)|=\frac{\pi\sqrt{|d|}}{|d|^2}\left|\sum_{a=1}^{|d|}\chi_d(a)a\right|=\frac{\pi}{|d|^{3/2}}\left|\sum_{a=1}^{|d|}\chi_d(a)a\right|.$$

(2) As per the analytic class number formula and Lemma 19.15(2), we need to prove that

$$L(1,\chi_d)=\frac{2}{\sqrt{d}}\left|\sum_{a=1}^{\lfloor\frac{d}{2}\rfloor}\chi_d(a)\log\left(\sin\left(\frac{\pi a}{d}\right)\right)\right|.$$

Again, by the same reasoning, $L(1,\chi_d)$ is a positive real number, so by Theorem 19.12,

$$L(1,\chi_d)=|L(1,\chi_d)|=\frac{1}{\sqrt{d}}\left|\sum_{a=1}^{d}\chi_d(a)\log\left|1-e^{\frac{2\pi ia}{d}}\right|\right|.$$

As χ_d is even,

$$\sum_{a=1}^{d}\chi_d(a)\log\left|1-e^{\frac{2\pi ia}{d}}\right|=2\sum_{a=1}^{\lfloor\frac{d}{2}\rfloor}\chi_d(a)\log\left|1-e^{\frac{2\pi ia}{d}}\right|,$$

noting that if d is even, $a=\frac{d}{2}$ will be still even, so that $\chi_d(a)=0$. Now the statement follows as

$$\left|1-e^{\frac{2\pi ia}{d}}\right|=\left|1-\cos\left(\frac{2\pi a}{d}\right)+i\sin\left(\frac{2\pi a}{d}\right)\right|=\sqrt{\left(1-\cos\left(\frac{2\pi a}{d}\right)\right)^2+\sin^2\left(\frac{2\pi a}{d}\right)}$$

$$=\sqrt{2-2\cos\left(\frac{2\pi a}{d}\right)}=\sqrt{2-2\left(1-2\sin^2\left(\frac{\pi a}{d}\right)\right)}=2\sin\left(\frac{\pi a}{d}\right),$$

as $0\leq\frac{\pi a}{d}\leq\frac{\pi}{2}$, and as $2\sum_{a=1}^{\lfloor\frac{d}{2}\rfloor}\chi_d(a)\log 2=\log 2\sum_{a=1}^{d}\chi_d(a)=0$.

□

Example 19.18. (1) Let $K = \mathbb{Q}(\sqrt{-5})$. Then, $d = \operatorname{disc}(K) = -20$, so

$$h_K = \frac{2}{2 \cdot 20} \left| 1 + \left(\frac{-5}{3}\right) 3 + \left(\frac{-5}{7}\right) 7 + \left(\frac{-5}{9}\right) 9 + \left(\frac{-5}{11}\right) 11 + \left(\frac{-5}{13}\right) 13 + \left(\frac{-5}{17}\right) 17 + \left(\frac{-5}{19}\right) 19 \right|$$

$$= \frac{\left|1 + 3 + 7 + 9 - \left(\frac{11}{5}\right) 11 + \left(\frac{13}{5}\right) 13 + \left(\frac{17}{5}\right) 17 - \left(\frac{19}{5}\right) 19\right|}{20} = \frac{|20 - 11 - 13 - 17 - 19|}{20} = \frac{40}{20} = 2,$$

which matches with our earlier discussion.

(2) We have found above that the fundamental unit of $K = \mathbb{Q}(\sqrt{7})$ is $8 + 3\sqrt{7}$. Then, $d = \operatorname{disc}(K) = 28$, so

$$h_K = \frac{\left|\log \sin \frac{\pi}{28} + \left(\frac{7}{3}\right) \log \sin \frac{3\pi}{28} + \left(\frac{7}{5}\right) \log \sin \frac{5\pi}{28} + \left(\frac{7}{9}\right) \log \sin \frac{9\pi}{28} + \left(\frac{7}{11}\right) \log \sin \frac{11\pi}{28} + \left(\frac{7}{13}\right) \log \sin \frac{13\pi}{28}\right|}{\log(8 + 3\sqrt{7})}$$

$$= \frac{\left|\log \sin \frac{\pi}{28} + \log \sin \frac{3\pi}{28} - \log \sin \frac{5\pi}{28} + \log \sin \frac{9\pi}{28} - \log \sin \frac{11\pi}{28} - \log \sin \frac{13\pi}{28}\right|}{\log(8 + 3\sqrt{7})}.$$

Now you can numerically compute the class number using calculator, as you are theoretically guaranteed to get an integer for this horrible expression! Indeed, both the numerator and the denominator are computed ~ 2.7686, so $h_K = 1$ (computation correct up to a certain error will actually rigorously pin down the class number as it is an integer). Alternatively, you may algebraically manipulate the fraction to show that it is 1, which I am sure is a fun exercise[33].

As you can see, the practicality of the formula comes from the ability to put this into computers, not from the simplicity of the formula – it's generally tedious to massage the closed-form formula into a number. Another virtue of the formula is that we can prove very general upper bounds on the class number. For example,

Theorem 19.19. *Let $K = \mathbb{Q}(\sqrt{-n})$ be an imaginary quadratic field with n squarefree integer > 1. Then, $h_K \leq \frac{n}{2}$.*

---

[33] Let's prove that $\frac{\sin \frac{13\pi}{28} \sin \frac{11\pi}{28} \sin \frac{5\pi}{28}}{\sin \frac{\pi}{28} \sin \frac{3\pi}{28} \sin \frac{9\pi}{28}} = 8 + 3\sqrt{7}$, which will prove the desired equality. Note that this is the same as $\frac{\tan \frac{5\pi}{28}}{\tan \frac{\pi}{28} \tan \frac{3\pi}{28}} = 8 + 3\sqrt{7}$. Let $a = \tan \frac{\pi}{28}$ for simplicity. Since $\tan \frac{5\pi}{28} = \frac{1 - \tan \frac{2\pi}{28}}{1 + \tan \frac{2\pi}{28}} = \frac{1 - 2a - a^2}{1 + 2a - a^2}$ and $\tan \frac{3\pi}{28} = \frac{3a - a^3}{1 - 3a^2}$, we want to show that $\frac{1 - 2a - a^2}{1 + 2a - a^2} = (8 + 3\sqrt{7}) \frac{3a^2 - a^4}{1 - 3a^2}$, or $\frac{(1 - 2a - a^2)(1 - 3a^2)}{(1 + 2a - a^2)(3a^2 - a^4)} = 8 + 3\sqrt{7}$. Note that as $\frac{\tan \frac{5\pi}{28}}{\tan \frac{\pi}{28} \tan \frac{3\pi}{28}} > 1$, it follows that the identity $\frac{(1 - 2a - a^2)(1 - 3a^2)}{(1 + 2a - a^2)(3a^2 - a^4)} = 8 + 3\sqrt{7}$ is equivalent to the identity $\left(\frac{(1 - 2a - a^2)(1 - 3a^2)}{(1 + 2a - a^2)(3a^2 - a^4)} - 8\right)^2 = 63$, or after clearing the denominators, $a^{12} - 4a^{11} - 52a^{10} + 28a^9 + 455a^8 - 24a^7 - 1032a^6 - 24a^5 + 455a^4 + 28a^3 - 52a^2 - 4a + 1 = 0$. Using the $\tan \frac{7\pi}{28} = 1$, we have $\frac{7a - 35a^3 + 21a^5 - a^7}{1 - 21a^2 + 35a^4 - 7a^6} = 1$, or $a^7 - 7a^6 - 21a^5 + 35a^4 + 35a^3 - 21a^2 - 7a + 1 = 0$. Note that this is $(a + 1)(a^6 - 8a^5 - 13a^4 + 48a^3 - 13a^2 - 8a + 1) = 0$, so as $a \neq -1$, we have $a^6 - 8a^5 - 13a^4 + 48a^3 - 13a^2 - 8a + 1 = 0$. As $(x^6 - 8x^5 - 13x^4 + 48x^3 - 13x^2 - 8x + 1)(x^6 + 4x^5 - 7x^4 - 24x^3 - 7x^2 + 4x + 1) = x^{12} - 4x^{11} - 52x^{10} + 28x^9 + 455x^8 - 24x^7 - 1032x^6 - 24x^5 + 455x^4 + 28x^3 - 52x^2 - 4x + 1$, we have shown the desired identity.

Proof. We know that $\#\mu_K = 2$ in this case, so $h_K = \frac{1}{|\operatorname{disc}(K)|}\left|\sum_{a=1}^{|\operatorname{disc}(K)|}\chi_{\operatorname{disc}(K)}(a)a\right|$. As $\chi_{\operatorname{disc}(K)}(-1) = -1$, we have

$$\begin{aligned} h_K &= \frac{1}{|\operatorname{disc}(K)|}\left|\sum_{a=1}^{\lfloor\frac{|\operatorname{disc}(K)|}{2}\rfloor}\left(\chi_{\operatorname{disc}(K)}(a)a - \chi_{\operatorname{disc}(K)}(a)(|\operatorname{disc}(K)| - a)\right)\right| \\ &= \frac{1}{|\operatorname{disc}(K)|}\left|\sum_{a=1}^{\lfloor\frac{|\operatorname{disc}(K)|}{2}\rfloor}\chi_{\operatorname{disc}(K)}(a)(|\operatorname{disc}(K)| - 2a)\right| \\ &\leq \frac{1}{|\operatorname{disc}(K)|}\sum_{1\leq a\leq\lfloor\frac{|\operatorname{disc}(K)|}{2}\rfloor,\ (a,\operatorname{disc}(K))=1}(|\operatorname{disc}(K)| - 2a). \end{aligned}$$

If $n \equiv 3 \pmod 4$, then $\operatorname{disc}(K) = -n$ is odd, so

$$h_K \leq \frac{1}{n}\sum_{a=1}^{\frac{n-1}{2}}(n-2a) = \frac{n-1}{2} - \frac{2}{n}\frac{\frac{n-1}{2}\frac{n+1}{2}}{2} < \frac{n}{2},$$

and if $n \equiv 1, 2 \pmod 4$, then $\operatorname{disc}(K) = -4n$, so

$$h_K \leq \frac{1}{4n}\sum_{a=1}^{n}(4n - 2(2a-1)) = \frac{(4n+2)n}{4n} - \frac{1}{n}\sum_{a=1}^{n}a = \frac{2n+1}{2} - \frac{n+1}{2} = \frac{n}{2}.$$

□

Remark 19.20. In general, when you are using the analytic class number formula, it is difficult to separate the terms h_K and R_K. Moreover, even in the case of K an imaginary quadratic field so that $R_K = 1$, giving a lower bound on h_K is the same as giving a lower bound on $L(1,\chi)$ for some χ, and this is generally much harder than giving an upper bound on $L(1,\chi)$ – giving a lower bound on $L(1,\chi)$ is related to the absence of zeros in a region around 1, and you may imagine that this is hard as the Generalized Riemann Hypothesis is also about the absence of zeros in a region.

– –

Exercise 19.1. Using the analytic class number formula, compute the class number $h_{\mathbb{Q}(\sqrt{-21})}$ of $\mathbb{Q}(\sqrt{-21})$.

Exercise 19.2. Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ be a real quadratic field, where d is a square-free integer > 1 satisfying $d \equiv 2, 3 \pmod 4$.

(1) Show that

$$\epsilon_K > \sqrt{d},$$

where ϵ_K is the fundamental unit.

(2) Using the analytic class number formula, show that

$$h_K < -\frac{1}{\log \sqrt{d}} d \log \left(\sin \left(\frac{\pi}{4d} \right) \right).$$

(3) Show that, for $0 < x < 1$, $\sin\left(\frac{\pi}{2}x\right) > x$. Deduce that $h_K < 4d$.

20. Lecture 26. Ideal class groups of the cyclotomic fields

Summary. Totally real/CM fields; conductor-discriminant formula; regular/irregular primes; Fermat's last theorem for regular primes; cyclotomic units; cyclotomic units and the plus part of the class number; Herbrand's theorem; Stickelberger's theorem; Stickelberger ideal and the minus part of the class number; Vandiver's conjecture.

Content. We apply the techniques we have learned so far to study the cyclotomic fields. The ideal class groups of cyclotomic fields are still actively researched in modern number theory.

Recall that the cyclotomic fields $\mathbb{Q}(\zeta_m)$, $m > 2$, have an index 2 subfield $\mathbb{Q}(\zeta_m)^+ := \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ whose archimedean primes are all real primes (see Exercise 9.1). This means that $\mathbb{Q}(\zeta_m)^+$ is **totally real**, and $\mathbb{Q}(\zeta_m)$ is a **CM field**:

Definition 20.1 (Totally real/totally imaginary/CM fields)**.** A number field is **totally real** (**totally complex**, respectively) if all archimedean primes are real primes (complex primes, respectively). A number field is a **CM field**[34] if it is totally complex and is a quadratic extension of a totally real subfield. Given a CM field K, we denote the totally real index 2 subfield as K^+, and call it **the totally real subfield**.

The notation is justified by the following.

Lemma 20.2. *In a CM field, there is a unique index* 2 *totally real subfield.*

Proof. Let K be a CM field and let $L, M \subset K$ be index 2 totally real subfields. Then, LM is totally real; if we take any embedding $LM \hookrightarrow \mathbb{C}$, then both L, M are contained in $\mathbb{R}$, so $LM \subset \mathbb{R}$. Thus either $[K : LM] = 2$ or $[K : LM] = 1$; the latter case is impossible as K is totally complex, so $[K : LM] = 2$, which means $L = LM = M$. □

CM fields have very close ties with their totally real subfields.

Theorem 20.3. *Let K be a CM field.*

1. *The norm map $N_{K/K^+} : \mathrm{Cl}(K) \to \mathrm{Cl}(K^+)$ is surjective. In particular, we have $h_{K^+} | h_K$. We call the quantity $h_K^- := \frac{h_K}{h_{K^+}}$ the **relative class number**.*
2. *Let $Q_K := [\mathcal{O}_K^\times : \mu_K \mathcal{O}_{K^+}^\times]$. Then, Q_K is either 1 or 2. If $K = \mathbb{Q}(\zeta_m)$, $m > 2$, then $Q = 1$ if and only if m is either a prime power or 2 times a prime power.*
3. *We have*
$$\frac{R_K}{R_{K^+}} = \frac{2^{[K^+:\mathbb{Q}]-1}}{Q_K}.$$
4. *If $K = \mathbb{Q}(\zeta_m)$, $m > 2$, then the natural map $\mathrm{Cl}(\mathbb{Q}(\zeta_m)^+) \to \mathrm{Cl}(\mathbb{Q}(\zeta_m))$, $I \mapsto I\mathcal{O}_{\mathbb{Q}(\zeta_m)}$, is an injection*[35].

[34] The word "CM" stands for "complex multiplication", as CM fields play a foundational role in the theory of complex multiplication of elliptic curves.

[35] From Theorem 20.3(1), one may think that Theorem 20.3(4) should be true for all CM fields, but this is actually false; for $K = \mathbb{Q}(\sqrt{10}, \sqrt{-2})$ with $K^+ = \mathbb{Q}(\sqrt{10})$, $(2, \sqrt{10})$ is non-principal in $\mathcal{O}_{K^+}$, but is principal in $\mathcal{O}_K$ (actually $(2, \sqrt{10}) = (\sqrt{-2})$ in $\mathcal{O}_K$).

Proof. (1) Let H_{K^+}, H_K be the Hilbert class fields of K^+, K, respectively. Then, the compatibility of the global Artin map with changing fields, Theorem 16.14, implies the commutativity of the diagram

$$\begin{array}{ccc} J_K & \xrightarrow{\mathrm{Art}^1_{H_K/K}} & \mathrm{Gal}(H_K/K) \\ {\scriptstyle N_{K/K^+}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ J_{K^+} & \xrightarrow[\mathrm{Art}^1_{H_{K^+}/K^+}]{} & \mathrm{Gal}(H_{K^+}/K^+) \end{array}$$

It gives another commutative diagram

$$\begin{array}{ccc} \mathrm{Cl}(K) & = & \mathrm{Gal}(H_K/K) \\ {\scriptstyle N_{K/K^+}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathrm{Cl}(K^+) & = & \mathrm{Gal}(H_{K^+}/K^+) \end{array}$$

so the surjectivity of the norm map will follow from the surjectivity of the restriction. Note that $K \supset H_{K^+} \cap K \supset K^+$. On the other hand, as an archimedean prime in K^+ ramifies in K, $H_{K^+} \cap K \neq K$. Thus, $H_{K^+} \cap K = K^+$. Since $H_{K^+}K/K$ is abelian and unramified everywhere (including the archimedean primes), $H_{K^+}K \subset H_K$. Now the restriction map can be regarded as $\mathrm{Gal}(H_K/K) \twoheadrightarrow \mathrm{Gal}(H_{K^+}K/K) \cong \mathrm{Gal}(H_{K^+}/K^+)$, which is surjective.

(2) Let $\psi : \mathcal{O}_K^\times \to \mu_K/\mu_K^2$ be the multiplicative group homomorphism defined as $\psi(x) = \frac{x}{\overline{x}}$, where $\bar{\cdot} : K \to K$ is the nontrivial Galois element in $\mathrm{Gal}(K/K^+)$. If $x \in \mu_K$, then $\psi(x) = \frac{x}{\overline{x}} = x^2 = 1 \in \mu_K/\mu_K^2$. Furthermore, if $x \in \mathcal{O}_{K^+}^\times$, then $\psi(x) = \frac{x}{\overline{x}} = \frac{x}{x} = 1$. Thus, $\ker\psi \supset \mu_K\mathcal{O}_{K^+}^\times$. Furthermore, if $x \in \mathcal{O}_K^\times$ is in $\ker\psi$, then $\frac{x}{\overline{x}} = u^2$ for $u \in \mu_K$, which means that

$$\frac{x}{\overline{x}} = u^2 = \frac{u}{\overline{u}},$$

so $y = \frac{x}{u}$ satisfies $\frac{y}{\overline{y}} = 1$, or $y = \overline{y}$, or $y \in K^+$. Thus, $y \in \mathcal{O}_K^\times$, which means that $x \in \mu_K\mathcal{O}_{K^+}^\times$. Thus, $\ker\psi = \mu_K\mathcal{O}_{K^+}^\times$. This implies that $Q_K \leq \#(\mu_K/\mu_K^2)$. Since μ_K is a finite cyclic group, $\#(\mu_K/\mu_K^2)$ is either 1 or 2, so Q_K is either 1 or 2.

Suppose that $K = \mathbb{Q}(\zeta_m)$, $m > 2$, such that m is a composite number. We may assume that $v_2(m) \neq 1$ as otherwise $K = \mathbb{Q}(\zeta_{m/2})$. Let $m = p_1^{e_1}\cdots p_r^{e_r}$, $r \geq 2$. Then, $\frac{X^m-1}{X-1}$ is divisible by $\frac{X^{\frac{m}{p_i^{e_i}}}-1}{X-1}$. As $\frac{X^{\frac{m}{p_i^{e_i}}}-1}{X-1}$'s are coprime to each other for $i = 1, \cdots, r$, it follows that $\frac{X^m-1}{X-1}$ is divisible by $\prod_{i=1}^r \frac{X^{\frac{m}{p_i^{e_i}}}-1}{X-1}$. Note that $X - \zeta_m$ divides $\dfrac{\frac{X^m-1}{X-1}}{\prod_{i=1}^r \frac{X^{\frac{m}{p_i^{e_i}}}-1}{X-1}}$, so by plugging $X = 1$, we get $1-\zeta_m$ divides $\frac{m}{\prod_{i=1}^r p_i^{e_i}} = 1$ in $\mathcal{O}_K$, so $1-\zeta_m$ is a unit. Note that $\phi(1-\zeta_m) = \frac{1-\zeta_m}{1-\zeta_m^{-1}} = -\zeta_m$. If m is odd, then $-\zeta_m = \zeta_{2m}^{m+2}$ is not a square, as otherwise $\zeta_{4m} \in K$. If m

is even, then $-\zeta_m = \zeta_m^{\frac{m}{2}+1}$. As $4|m$, $\zeta_m^{\frac{m}{2}+1}$ is not a square, as otherwise $\zeta_{2m} \in K$. Thus, if m is a composite number with $v_2(m) \neq 1$, $Q_K = 2$.

Suppose on the other hand that $m = p^a$ for some odd prime p. We want to show that $Q_K = 1$. Let $x \in \mathcal{O}_K^\times$. Then, $\frac{x}{\overline{x}} = \pm\zeta_{p^a}^i$. Since $x = b_0 + b_1\zeta_{p^a} + \cdots + b_{\phi(p^a)-1}\zeta_{p^a}^{\phi(p^a)-1}$, $b_0, \cdots, b_{\phi(p^a)-1} \in \mathbb{Z}$, we have

$$x \equiv b_0 + b_1 + \cdots + b_{\phi(p^a)-1} \pmod{1-\zeta_{p^a}}.$$

Similarly,

$$\overline{x} = b_0 + b_1\zeta_{p^a}^{-1} + \cdots + b_{\phi(p^a)-1}\zeta_{p^a}^{-\phi(p^a)+1} \equiv b_0 + b_1 + \cdots + b_{\phi(p^a)-1} \pmod{1-\zeta_{p^a}},$$

so $\frac{x}{\overline{x}} = \zeta_{p^a}^i$ (as $(1-\zeta_{p^a})$ is a maximal ideal in $\mathcal{O}_K$). As p^a is odd, $i \equiv 2j \pmod{p^a}$ for some $j \in \mathbb{Z}$, which implies that $x \in \ker\psi$, so $Q_K = 1$.

Suppose that $m = 2^a$ for some $a \geq 2$. We want to show that $Q_K = 1$, which will finish (2). Since μ_K is generated by ζ_{2^a}, we see that any element in $\mu_K \backslash \mu_K^2$ is a primitive 2^a-th root of unit. If $x \in \mathcal{O}_K^\times$ has $\psi(x) \neq 1$, then $\frac{x}{\overline{x}} = \zeta$ for a primitive 2^a-th root of unity ζ. Then, $\frac{N_{K/\mathbb{Q}(i)}(x)}{N_{K/\mathbb{Q}(i)}(\overline{x})} = N_{K/\mathbb{Q}(i)}(\zeta)$. Note that $N_{K/\mathbb{Q}(i)}(\overline{x}) = \overline{N_{K/\mathbb{Q}(i)}(x)}$, and $N_{K/\mathbb{Q}(i)}(x) \in \mathbb{Z}[i]^\times$. Furthermore, $N_{K/\mathbb{Q}(i)}(\zeta) = \zeta^{\sum_{1\leq b\leq 2^a,\ b\equiv 1 \pmod 4} b} = \zeta^{2^{a-2}+2^{a-1}(2^{a-2}-1)}$, whose exponent is divisible by 2^{a-2} but not divisible by 2^{a-1}, so $N_{K/\mathbb{Q}(i)}(\zeta) = \pm i$. Therefore, $Q_K = 1$ for $K = \mathbb{Q}(\zeta_{2^a})$ follows from $Q_K = 1$ for $K = \mathbb{Q}(i)$, which one can check manually (i.e. $\frac{i}{\overline{i}} = \frac{-i}{\overline{-i}} - 1 = i^2$ and $\frac{1}{\overline{1}} = \frac{-1}{\overline{-1}} = 1$).

(3) Let $r = [K^+ : \mathbb{Q}] - 1 = \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_{K^+}$, and let $\epsilon_1, \cdots, \epsilon_r$ be a fundamental system of units in K^+. Then, they form a finite index subgroup of $\mathcal{O}_K$, as $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K = \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_{K^+}$ by Dirichlet's unit theorem. Since all archimedean primes of K^+ are real and all archimedean primes of K are complex, the regulator determinant computed for K using $\epsilon_1, \cdots, \epsilon_r$ is 2^r times R_{K^+}. Note that by definition of Q_K, this determinant is $\frac{R_K}{Q_K}$, so $\frac{R_K}{Q_K} = 2^r R_{K^+}$, which is the desired equality.

(4) Suppose that $I \subset \mathcal{O}_{\mathbb{Q}(\zeta_m)^+}$ be such that $I\mathcal{O}_{\mathbb{Q}(\zeta_m)}$ is principal, generated by $\alpha \in \mathbb{Q}(\zeta_m)$. Then, $\frac{\overline{\alpha}}{\alpha}$ generates a unit ideal, which implies that $\frac{\overline{\alpha}}{\alpha}$ is a unit and thus a root of unity. If m is not a prime power and not twice a prime power, then $Q_K = 2$, so $\frac{\overline{\alpha}}{\alpha} = \frac{\overline{u}}{u}$ for some $u \in \mathcal{O}_K^\times$, which implies that $\alpha/u \in \mathcal{O}_{K^+}$ is another generator of $I\mathcal{O}_K$. This implies that α/u generates $I \subset \mathcal{O}_{K^+}$.

On the contrary, if m is a prime power (twice the prime power case is redundant), suppose $m = p^a$. Then, for $\pi = 1 - \zeta_{p^a}$, $\frac{\pi}{\overline{\pi}} = -\zeta_{p^a}$, which always generates μ_K (regardless of whether p is even or odd). Thus, $\frac{\overline{\alpha}}{\alpha} = \frac{\pi^b}{\overline{\pi}^b}$ for some $b \in \mathbb{Z}$, which implies that $\alpha\pi^b \in K^+$. Since α generates an ideal coming from K^+, if we denote v_π for the π-adic valuation on K, then $v_\pi(\alpha)$ is even, and so is $v_\pi(\alpha\pi^b)$. Thus, b is even. Thus, $\frac{\overline{\alpha}}{\alpha}$ is a square, which implies that $\frac{\overline{\alpha}}{\alpha} = \frac{\overline{u}}{u}$ for some $u \in \mathcal{O}_K^\times$. Arguing as above, we get that I is principal to begin with. □

The virtue of considering the relative class number is, as per Theorem 18.17, that the relative class number can be studied completely in the algebraic realm without invoking transcendental values.

Corollary 20.4. *Let $K = \mathbb{Q}(\zeta_m)$, $m > 2$. Then,*

$$h_K^- = Q_K \# \mu_K \prod_{\chi \text{ odd Dirichlet characters of modulus } m} \left(-\frac{1}{2} B_{1,\chi}\right).$$

Proof. The analytic class number formulae for K and K^+ are

$$\frac{(2\pi)^{[K:\mathbb{Q}]/2} R_K h_K}{\#\mu_K \sqrt{|\operatorname{disc}(K)|}} = \prod_{\chi \text{ Dirichlet characters of modulus } m,\ \chi \neq \mathbf{1}_m} L(1, \chi_0),$$

$$\frac{2^{[K^+:\mathbb{Q}]} R_{K^+} h_{K^+}}{\#\mu_{K^+} \sqrt{|\operatorname{disc}(K^+)|}} = \prod_{\chi \text{ even Dirichlet characters of modulus } m,\ \chi \neq \mathbf{1}_m} L(1, \chi_0).$$

Dividing, we get

$$\frac{\pi^{[K^+:\mathbb{Q}]} h_K^- 2^{[K^+:\mathbb{Q}]}}{Q_K \# \mu_K \sqrt{\left|\frac{\operatorname{disc}(K)}{\operatorname{disc}(K^+)}\right|}} = \prod_{\chi \text{ odd Dirichlet characters of modulus } m} L(1, \chi_0).$$

Let f_χ be the conductor of χ (=modulus of χ_0). Then, by Theorem 18.17(4), $L(1, \chi_0) = \frac{iG(\chi_0)\pi}{f_\chi} B_{1,\overline{\chi_0}}$. Note first that the formula says $B_{1,\overline{\chi_0}} = B_{1,\overline{\chi}}$. The desired formula follows from

$$\prod_{\chi \text{ odd Dirichlet characters of modulus } m} G(\chi_0) = i^{[K^+:\mathbb{Q}]} \sqrt{\left|\frac{\operatorname{disc}(K)}{\operatorname{disc}(K^+)}\right|},$$

which follows by comparing the functional equation for the Dedekind zeta function for K^+ and K and the Dirichlet L-functions, and

$$\prod_{\chi \text{ odd Dirichlet characters of modulus } m} f_\chi = \frac{|\operatorname{disc}(K)|}{|\operatorname{disc}(K^+)|},$$

which follows from the conductor-discriminant formula, which we will not prove in this notes.

Theorem 20.5 (Conductor-discriminant formula)**.** *Let $K \subset \mathbb{Q}(\zeta_m)$, and let $X \subset \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$ be the set of Dirichlet characters that are trivial on $\operatorname{Gal}(\mathbb{Q}(\zeta_m)/K) \subset \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Then,*

$$\operatorname{disc}(K) = (-1)^s \prod_{\chi \in X} f_\chi,$$

where s is the number of complex primes of K.

□

As per Corollary 20.4, things like whether a certain prime divides h_K^- or not can be studied by looking at the Bernoulli numbers $B_{1,\chi}$. One is interested in whether a prime divides a class number or not as such a result has an implication in Diophantine problems as we have seen above. For example, it has been of central interest for a long time whether p divides $h_{\mathbb{Q}(\zeta_p)}$, because of its relationship with Fermat's last theorem.

Theorem 20.6 (Fermat's Last Theorem; Taylor–Wiles)**.** *For an odd prime p, there is no solutions to $X^p + Y^p = Z^p$ with $X, Y, Z \in \mathbb{N}$.*

The reason why the condition $(p, h_{\mathbb{Q}(\zeta_p)}) = 1$ (if this is the case, we call p a **regular prime**) is relevant to Fermat's Last Theorem is as follows.

Theorem 20.7. *For a regular prime p, $X^p + Y^p = Z^p$ has no solutions with $X, Y, Z \in \mathbb{Z}$, $(XYZ, p) = 1$.*[36]

Proof. We can divide X, Y, Z by their greatest common divisor and suppose that $(X, Y, Z) = 1$. We have

$$\prod_{i=0}^{p-1}(X + \zeta_p^i Y) = Z^p.$$

As $(X + \zeta_p^i Y)$'s are coprime to each other, $(X + \zeta_p^i Y) = I_i^p$ for some ideal $I_i \subset \mathbb{Z}[\zeta_p]$. Since the class number is coprime to p, it follows that I_i is principal. Thus, $X + \zeta_p Y = ua^p$ for some $a \in \mathbb{Z}[\zeta_p]$ and $u \in \mathbb{Z}[\zeta_p]^\times$. Note that, by Theorem 20.3(2), $u = \pm\zeta_p^b u^+$ where $u^+ \in \mathcal{O}^\times_{\mathbb{Q}(\zeta_p)^+}$. Note also that $a^p \pmod p$ is congruent to an integer n. Thus, $X + \zeta_p Y \equiv \pm\zeta_p^b u^+ n \pmod p$, or $\zeta_p^{-b}(X + \zeta_p Y) \equiv \pm u^+ n \pmod p$. Since $\pm u^+ n$ is in $\mathbb{Q}(\zeta_p)^+$, it follows that

$$\zeta_p^{-b}(X + \zeta_p Y) \equiv \zeta_p^b(X + \zeta_p^{-1} Y) \pmod p.$$

As X, Y are not zero mod p, this implies that $X \equiv Y \pmod p$ with $\zeta_p^{-b} = \zeta_p^{b-1}$. On the other hand, the same logic applied to $X^p + (-Z)^p = (-Y)^p$ implies that $X \equiv -Z \pmod p$. This then implies that $2X^p \equiv -X^p \pmod p$, which is possible only if $p = 3$. If $p = 3$, then the only nonzero cubes mod 9 are ± 1, which implies the nonexistence of solutions. □

A central theme of the arithmetic of cyclotomic fields is that something about the field can be split into a product of something about the Dirichlet characters, just as in Corollary 20.4. What I mean is this: Corollary 20.4 is proved using the analytic class number formula, which is inherently analytic and has little to do with algebra. On the other hand, there is some precise sense that the ideal class group $\mathrm{Cl}(\mathbb{Q}(\zeta_m))$ factors as a direct sum over the Dirichlet characters,

$$\text{“}\mathrm{Cl}(\mathbb{Q}(\zeta_m)) = \bigoplus_{\chi \text{ Dirichlet characters of modulus } m} \mathrm{Cl}(\mathbb{Q}(\zeta_m))[\chi]\text{”},$$

[36] A more complicated argument (still elementary) shows the full Fermat's Last Theorem for regular primes (covering the case of some of X, Y, Z divisible by p), which we do not cover in this case.

where the double-quotation means this holds up to some caveat. The factorization of the class number then makes us wonder if there is a relation between $B_{1,\chi}$ and "$\mathrm{Cl}(\mathbb{Q}(\zeta_m))[\chi]$", for χ odd. This is given for example in the case of $m = p$ an odd prime by what's called the **Herbrand's theorem**. To formulate the algebraic decomposition of the class group, we need a bit of representation theory.

Definition 20.8 (Group ring)**.** Let A be a commutative ring, and let G be a finite abelian group. Then, the **group ring** $A[G]$ is an A-algebra defined as follows. As an A-module, $A[G] \cong A^{\oplus|G|}$, with a free basis given by the elements of G. The ring multiplication of $A[G]$ is given by the ring multiplication of A and the group structure on G.

Equivalently, an $A[G]$-module M is the same as an A-module M together with a representation of G on M, i.e. an A-module homomorphism $G \to \mathrm{End}_A(M)$.

Example 20.9.

(1) If $G = \mathbb{Z}/m\mathbb{Z}$ is a cyclic group, $A[G] = A[X]/(X^m - 1)$.

(2) A $\mathbb{Z}[G]$-module is an abelian group (=$\mathbb{Z}$-module) together with an action of G. A p-group with an action of G can be regarded as a $\mathbb{Z}_{(p)}[G]$-module, or even as a $\mathbb{Z}_p[G]$-module.

Proposition 20.10. *Let G be a finite abelian group. Let A be a commutative ring such that $|G|$ is invertible in A and $\mu_m \subset A$, where m is the exponent of G, so that the characters in $\widehat{G}$ can be regarded as taking values in A. For an $A[G]$-module M, there exists a decomposition*

$$M = \bigoplus_{\chi \in \widehat{G}} M[\chi],$$

as $A[G]$-modules, where any $g \in G$ acts on $M[\chi]$ as the scalar $\chi(g)$. In other words, this is the simultaneous eigenspace decomposition for commuting operators (one for each $g \in G$) where the eigenvalue of $g \in G$ on $M[\chi]$ is $\chi(g)$.

Proof. For $\chi \in \widehat{G}$, let

$$\varepsilon_\chi := \frac{1}{|G|} \sum_{g \in G} \chi(g) g^{-1} \in A[G].$$

It is easy to check that ε_χ's satisfy:

(1) $\varepsilon_\chi^2 = \varepsilon_\chi$;

(2) $\varepsilon_\chi \varepsilon_\psi = 0$ if $\chi \neq \psi$;

(3) $1 = \sum_{\chi \in \widehat{G}} \varepsilon_\chi$;

(4) and $\varepsilon_\chi g = \chi(g) \varepsilon_\chi$ for $g \in G$.

Let $M[\chi] := \varepsilon_\chi M \subset M$ be the image of the action of ε_χ on M. By (4), $M[\chi]$ is an $A[G]$-submodule of M. By (3), $M[\chi]$'s span M. By (1), (2), (3), (4), g acts on $M[\chi]$ as the scalar $\chi(g)$. This implies that the $M[\chi]$'s have no overlap, proving the statement. □

Now, for an odd prime p, consider the p-Sylow subgroup of $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$, denoted $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p$ ("the" because the class group is abelian), which is $\mathbb{Z}_p[G]$-module for $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. By Proposition 20.10, we have the decomposition

$$\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p = \bigoplus_{\chi \in \widehat{G}} \mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\chi].$$

Note that the $\mathbb{Z}_p$-valued characters of G have a very explicit shape: they are powers of the **Teichmüller character** ω.

Definition 20.11 (Teichmüller character)**.** The **Teichmüller character** $\omega : \mathbb{F}_p^\times \to \mu_{p-1} \subset \mathbb{Z}_p^\times$ is the inverse of the mod p reduction map $\mu_{p-1} \to \mathbb{F}_p^\times$, which is bijective by Hensel's lemma. Namely, $\omega(x)$ is the $(p-1)$-st root of unity in $\mathbb{Z}_p$ whose mod p reduction is x.

Therefore,

$$\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p = \bigoplus_{i=0}^{p-2} \mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i].$$

We would like to compare this with the analytic class number formula. First we need to relate this with the plus and minus part of the class number.

Lemma 20.12. *The subgroup $\mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)_p \subset \mathrm{Cl}(\mathbb{Q}(\zeta_p))_p$ is identified with*

$$\mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)_p = \bigoplus_{0 \le i \le p-2,\ i \text{ even}} \mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i].$$

Proof. It is clear that the right hand side contains the left hand side. The left hand side contains the right hand side as the norm map $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)^+} : \mathrm{Cl}(\mathbb{Q}(\zeta_p)) \to \mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)$ is surjective, because, for any element x in the right hand side, x^2 is in the left hand side, but 2 is invertible as p is odd. □

Thus, we have

$$(h^-_{\mathbb{Q}(\zeta_p)})_p = \prod_{0 \le i \le p-2,\ i \text{ odd}} \left|\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]\right|,$$

where for an integer n, $n_p = p^{v_p(n)}$ is the largest power of p dividing n. Comparing this formula with Corollary 20.4, we wonder:

Question. For odd i, is $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$ related to the generalized Bernoulli numbers?

This is the subject of Herbrand's theorem which we will state in a moment.

Remark 20.13 (On the even part of the class group)**.** It is known that the p-divisibility of $h_{\mathbb{Q}(\zeta_p)}$ can be detected by the p-divisibility of $h^-_{\mathbb{Q}(\zeta_p)}$; therefore, we may use Corollary 20.4 to see whether p is regular or not.

Theorem 20.14 (Kummer)**.** *Let p be an odd prime. If p is irregular (i.e. if $p | h_{\mathbb{Q}(\zeta_p)}$), then $p | h^-_{\mathbb{Q}(\zeta_p)}$. In other words, if $p | h_{\mathbb{Q}(\zeta_p)^+}$, then $p | h^-_{\mathbb{Q}(\zeta_p)}$.*

We will not prove this Theorem as it requires the so-called "p-adic class number formula".

On the other hand, studying the p-part of the even part of the class group $\mathrm{Cl}(\mathbb{Q}(\zeta_p)^+)_p$ is also inherently interesting. From the analytic class number formula, it is natural to expect that the even part of the class group should have something to do with the units of the cyclotomic field. We have seen in Exercise 3.4 that the cyclotomic fields have specific kinds of units, called the **cyclotomic units**.

Definition 20.15. Let $p \in \mathbb{Z}$ be a rational prime, and let $K = \mathbb{Q}(\zeta_{p^m})$, with $p^m > 2$. Then, the group of **cyclotomic units** is the group of units $C \subset \mathcal{O}_K^\times$ generated by ± 1, ζ_{p^m}, and, for $(k,p) = 1$, $\frac{1-\zeta_{p^m}^k}{1-\zeta_{p^m}}$. The group of **real cyclotomic units** is $C^+ := C \cap \mathcal{O}_{K^+}^\times$.

Then, in fact, the following holds!

Theorem 20.16. *Let $p \in \mathbb{Z}$ be a rational prime, and let $K = \mathbb{Q}(\zeta_{p^m})$, with $p^m > 2$.*

(1) The group of real cyclotomic units C^+ is generated by ± 1 and

$$\xi_a := \zeta_{p^m}^{\frac{1-a}{2}} \frac{1-\zeta_{p^m}^a}{1-\zeta_{p^m}}, \quad 1 < a < \frac{p^m}{2},\ (a,p) = 1.$$

(2) The group of real cyclotomic units C^+ is of finite index, and is exactly of index h_{K^+}: namely, $[\mathcal{O}_{K^+} : C^+] = h_{K^+}$.

Proof. (1) This amounts to checking that ξ_a is real.

(2) Note that $\mu_{K^+} = \{\pm 1\} \subset C^+$ and the number of $1 < a < \frac{p^m}{2}$, $(a,p) = 1$, is precisely the rank of $\mathcal{O}_{K^+}$ by Dirichlet's unit theorem. So, the statement will follow if the absolute value of the determinant of the regulator matrix formed by ξ_a is $R_{K^+} h_{K^+}$. This sounds a lot like something that appears in the analytic class number formula! Indeed, if you write out the determinant of the regulator, you obtain

$$R(\{\xi_a\}) = \left| \prod_{\chi \text{ even Dirichlet character of modulus } p^m} \frac{1}{2} \sum_{a=1}^{p^m} \chi(a) \log \left|1 - \zeta_{p^m}^a\right| \right| = h_{K^+} R_{K^+},$$

by the analytic class number formula. For more details, see [Was, Theorem 8.2].

□

Remark 20.17. If you look at the formula in Corollary 20.4, it seems like there is a factor of p in the right hand side, coming from $\#\mu_{\mathbb{Q}(\zeta_p)} = 2p$. However, it does not imply that $h^-_{\mathbb{Q}(\zeta_p)}$ is divisible by p, as $B_{1,\chi}$ may have denominators divisible by p. In fact,

$$B_{1,\omega^i} = \frac{1}{p} \sum_{a=1}^{p-1} \omega^i(a) a,$$

and as $\omega(a) \equiv a \pmod p$, so $pB_{1,\omega^i} \in \mathbb{Z}_p$, and $pB_{1,\omega^i} \in p\mathbb{Z}_p$ if $i \neq -1$. Thus, $B_{1,\omega^i} \in \mathbb{Z}_p$ for $i \neq p-2$, and $B_{1,\omega^{p-2}} - \frac{p-1}{p} \in \mathbb{Z}_p$, cancelling out with the p from $\#\mu_{\mathbb{Q}(\zeta_p)}$.

Now here comes the desired relation between $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$ and the Bernoulli numbers.

Theorem 20.18 (Herbrand's theorem). *Let p be an odd prime, and let $3 \leq i \leq p-2$ be an odd number. Then, $B_{1,\omega^{-i}} \in \mathbb{Z}_p$ annihilates $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$; in other words, the p-group $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$ has exponent dividing $p^{v_p(B_{1,\omega^{-i}})}$. In particular, if $p \nmid B_{1,\omega^{-i}}$, then $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i] = 0$.*

In fact, the converse is true, so that we can precisely tell when $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i] = 0$ by checking whether $B_{1,\omega^{-i}}$ is coprime to p.

Theorem 20.19 (Converse to Herbrand's theorem; Ribet). *Let p be an odd prime, and let $3 \leq i \leq p-2$ be an odd number. If $p | B_{1,\omega^{-i}}$, then $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i] \neq 0$.*

The proof of Ribet's Converse to Herbrand's theorem is beyond the scope of our course, as it uses the constructions in the Langlands program in the case of modular forms. We will prove Herbrand's theorem by using the Stickelberger's theorem.

Theorem 20.20 (Stickelberger's theorem). *Let $K = \mathbb{Q}(\zeta_p)$ for an odd prime p, and let $G = \mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$. Consider $\theta \in \mathbb{Q}[G]$ defined by*

$$\theta := \frac{1}{p} \sum_{a=1}^{p-1} a\sigma_a^{-1},$$

*where $\sigma_a \in G$ corresponds to $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, i.e. $\sigma_a(\zeta_p) = \zeta_p^a$. Let $I := \mathbb{Z}[G]\theta \cap \mathbb{Z}[G]$, which is an ideal of $\mathbb{Z}[G]$, called the **Stickelberger ideal**. Then, I annihilates $\mathrm{Cl}(K)$; namely, for any $x \in I$ and $c \in \mathrm{Cl}(K)$, $xc = 0$.*

Proof. What we will prove in the end is that, for $c \in \mathrm{Cl}(K)$, some specific multiple of θ annihilates c. This means that we exhibit some specific multiple of conjugates of c as a principal ideal with an explicit generator, which will in fact be given by a power of the Gauss sum!

Let ℓ be a prime $\ell \equiv 1 \pmod{p}$, and choose a primitive root s mod ℓ and define a Dirichlet character $\chi : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mathbb{Q}(\zeta_p)$ of modulus ℓ by $\chi(s) = \zeta_p$. Then, $\chi^p = 1$, and by the Jacobi sum identity, for any $m, n \not\equiv 0 \pmod{p}$ with $m + n \not\equiv 0 \pmod{p}$, $\frac{G(\chi^m)G(\chi^n)}{G(\chi^{m+n})} \in \mathbb{Q}(\zeta_p)$. This implies that $\frac{G(\chi)^{p-1}}{G(\chi^{p-1})} \in \mathbb{Q}(\zeta_p)$. Since $G(\chi^{p-1}) = G(\chi^{-1}) = \chi(-1)\overline{G(\chi)} = \frac{\ell\chi(-1)}{G(\chi)}$, it follows that $G(\chi)^p \in \mathbb{Q}(\zeta_p)$. As $\ell \equiv 1 \pmod{p}$, $G(\chi)^{\ell-1} \in \mathbb{Q}(\zeta_p)$.

We are eventually interested in the prime ideal factorization of the principal ideal $(G(\chi)^{\ell-1}) \subset \mathbb{Z}[\zeta_p]$. To compute this, it suffices to know the prime ideal factorization of the principal ideal $(G(\chi)) \subset \mathcal{O}_M$ of $M = K(\zeta_\ell)$, where $G(\chi)$ is understood as $G(\chi) = \sum_{a=1}^{\ell-1} \chi(a)\zeta_\ell^a \in \mathcal{O}_M$. Note that, as the norm of $G(\chi)$ is a power of ℓ, only the primes of M above ℓ can divide $G(\chi)$. Note that ℓ splits completely in K, and is totally ramified in $\mathbb{Q}(\zeta_\ell)$, so for each prime ideal $\mathfrak{l} | \ell$ of K lying over ℓ, there exists a unique prime ideal $\mathfrak{L}$ of M lying over $\mathfrak{l}$ such that $\mathfrak{l}\mathcal{O}_M = \mathfrak{L}^{\ell-1}$. Moreover, after you fix a prime ideal $\mathfrak{l}$ of K lying over ℓ, all prime ideals of K lying over ℓ are expressed as $\sigma_a^{-1}\mathfrak{l}$, and the same applies for all primes of M lying over ℓ. Therefore,

$$\mathcal{O}_M \supset (G(\chi)) = \prod_{a=1}^{p-1} \sigma_a^{-1}\mathfrak{L}^{r_a}, \quad r_a \geq 0.$$

Now we give an expression of what r_a is. Note that $\sigma_a^{-1}\mathfrak{L}$ for any a lies over the unique prime ideal of $\mathbb{Q}(\zeta_\ell)$ lying over ℓ, which is $(\zeta_\ell - 1) \subset \mathbb{Z}[\zeta_\ell]$. Thus, $\zeta_\ell - 1 \in \sigma_a^{-1}\mathfrak{L}$. In fact,

$$(\zeta_\ell - 1) = \prod_{a=1}^{p-1} \sigma_a^{-1}\mathfrak{L},$$

in $\mathcal{O}_M$. Therefore, $\frac{G(\chi)}{(\zeta_\ell - 1)^{r_a}}$ has no factor of $\sigma_a^{-1}\mathfrak{L}$ in its prime ideal factorization, i.e. $\frac{G(\chi)}{(\zeta_\ell - 1)^{r_a}}$ is invertible mod $\sigma_a^{-1}\mathfrak{L}$. Note that as $f(\mathfrak{L}|\ell) = 1$, we have $\mathcal{O}_M/\sigma_a^{-1}\mathfrak{L} = \mathcal{O}_K/\sigma_a^{-1}\mathfrak{l} = \mathbb{F}_\ell$.

Let $\tau \in \mathrm{Gal}(M/K)$ be such that $\tau(\zeta_\ell) = \zeta_\ell^s$. Since it fixes K, $\tau(\sigma_a^{-1}\mathfrak{L}) = \sigma_a^{-1}\mathfrak{L}$. Therefore, for any $x \in \mathcal{O}_M$, $\tau(x) \equiv x \pmod{\sigma_a^{-1}\mathfrak{L}}$. Applying this to $x = \frac{G(\chi)}{(\zeta_\ell - 1)^{r_a}}$, we get

$$\frac{G(\chi)}{(\zeta_\ell - 1)^{r_a}} \equiv \frac{\tau(G(\chi))}{(\zeta_\ell^s - 1)^{r_a}} = \frac{\sum_{a=1}^{\ell-1} \chi(a)\zeta_\ell^{sa}}{(\zeta_\ell^s - 1)^{r_a}} = \frac{G(\chi)\chi(s)^{-1}}{(\zeta_\ell^s - 1)^{r_a}} \pmod{\sigma_a^{-1}\mathfrak{L}}.$$

Thus, as we can divide by $\frac{G(\chi)}{(\zeta_\ell - 1)^{r_a}}$, we get

$$\zeta_p^{-1} = \chi(s)^{-1} \equiv \left(\frac{\zeta_\ell^s - 1}{\zeta_\ell - 1}\right)^{r_a} = (\zeta_\ell^{s-1} + \cdots + 1)^{r_a} \equiv s^{r_a} \pmod{\sigma_a^{-1}\mathfrak{L}}.$$

Note that both ζ_p^{-1} and s^{r_a} are in K, so this congruence is really

$$\zeta_p^{-1} \equiv s^{r_a} \pmod{\sigma_a^{-1}\mathfrak{l}},$$

or taking σ_a, we get

$$\zeta_p^{-a} \equiv s^{r_a} \pmod{\mathfrak{l}}.$$

Note that $\mathcal{O}_K/\mathfrak{l} \cong \mathbb{F}_\ell$ as $f(\mathfrak{l}|\ell) = 1$. Let $0 \leq b < \ell$ be an integer such that $\zeta_p^{-1} \equiv s^b \pmod{\ell}$. Note that $\zeta_p \not\equiv 1 \pmod{\ell}$, so $\zeta_p \pmod{\ell}$ has order p, so b is a multiple of $\frac{\ell-1}{p}$. Let $0 < c < p$ be an integer such that $b = \frac{\ell-1}{p}c$. Then, we have

$$r_a \equiv ab = \frac{\ell - 1}{p}ac \pmod{\ell - 1}.$$

Note that this quantity is never 0 mod $(\ell - 1)$ as $0 < a < p$. Now note that $G(\chi)G(\overline{\chi}) = \ell$, so $r_a \leq v_{\sigma_a^{-1}\mathfrak{L}}(\ell) = \ell - 1$. Thus, r_a is the unique integer $0 < r_a < \ell - 1$ such that $r_a \equiv \frac{\ell-1}{p}ac$, or more concisely,

$$r_a = (\ell - 1)\left\{\frac{ac}{p}\right\},$$

where $\{x\} := x - \lfloor x \rfloor$.

This looks weird, but in fact is something that is built in the element θ; notice that

$$(\ell - 1)\sigma_c\theta = \sum_{a=1}^{p-1}(\ell - 1)\left\{\frac{ac}{p}\right\}\sigma_a^{-1} = \sum_{a=1}^{p-1} r_a\sigma_a^{-1}.$$

Note now that

$$(G(\chi)^{\ell-1}) = \prod_{a=1}^{p-1} \sigma_a^{-1} \mathfrak{L}^{(\ell-1)r_a} = \prod_{a=1}^{p-1} \sigma_a^{-1} \mathfrak{l}^{r_a} = (\ell-1)\sigma_c\theta\mathfrak{l},$$

so this implies that $(\ell-1)\sigma_c\theta \in \mathbb{Z}[G]$ annihilates the ideal class $[\mathfrak{l}] \in \mathrm{Cl}(K)$.

Now we claim that, for any $\beta \in \mathbb{Z}[G]$ such that $\beta\theta \in \mathbb{Z}[G]$ (so that $\beta\theta \in I$), $\beta\theta[\mathfrak{l}] = 0$ in $\mathrm{Cl}(K)$. Note that $[\mathfrak{l}] \in \mathrm{Cl}(K) \cong \mathrm{Gal}(H_K/K)$ can be regarded as the Frobenius $\mathrm{Fr}(\mathfrak{L}|\ell)$ by the global class field theory, as $H_K/\mathbb{Q}$ is Galois (as any automorphism $\mathbb{C} \to \mathbb{C}$ fixes K by Galoisness of $K/\mathbb{Q}$, so it fixes its maximal unramified extension, H_K), and therefore $\mathrm{Fr}(\mathfrak{L}|\ell) \in \mathrm{Gal}(H_K/\mathbb{Q})$ is something that is sent to $\ell \in \mathrm{Gal}(K/\mathbb{Q})$, which is 1 as $\ell \equiv 1 \pmod{p}$, and restricts to $[\mathfrak{l}] \in \mathrm{Gal}(H_K/K) \cong \mathrm{Cl}(K)$. By the Chebotarev density theorem, given an ideal class $c \in \mathrm{Cl}(K)$, there exists infinitely many ℓ such that $c = [\mathfrak{l}]$, which implies that the claim proves the Stickelberger's theorem.

To prove the claim, let $\gamma = \sigma_c^{-1}\beta G(\chi) \in M$. Then, $\gamma^{\ell-1} = \sigma_c^{-1}\beta G(\chi)^{\ell-1} \in K$, and

$$(\gamma)^{\ell-1} = \sigma_c^{-1}\beta(G(\chi)^{\ell-1}) = (\ell-1)\sigma_c^{-1}\beta\sigma_c\theta\mathfrak{l} = (\ell-1)\beta\theta\mathfrak{l} = (\beta\theta\mathfrak{l})^{\ell-1}.$$

This implies that $\beta\theta\mathfrak{l}$ is principal if seen as a fractional ideal in M. What we want is to show that this is principal as a fractional ideal of K, which will follow if we show that $\gamma \in K$. Note that $K(\gamma)/K$ being a subextension of M/K is totally ramified at primes over ℓ, so $K(\gamma) \otimes_K K_\mathfrak{l}$ is a local field which is a totally ramified extension of $K_\mathfrak{l}$. On the other hand, simply $K(\gamma) \otimes_K K_\mathfrak{l} = K_\mathfrak{l}(\gamma)$. Since $v_\mathfrak{l}(\gamma^{\ell-1})$ is divisible by $\ell-1$, $v_\mathfrak{l}(\gamma)$ is an integer, so we can modify γ by a power of a uniformizer of $K_\mathfrak{l}$ so that $K_\mathfrak{l}(\gamma) = K_\mathfrak{l}(u^{\frac{1}{\ell-1}})$ for some $u \in \mathcal{O}_{K_\mathfrak{l}}^\times$. By the discriminant computation, this is an unramified extension of $K_\mathfrak{l}$, so in particular $K_\mathfrak{l}(\gamma) = K_\mathfrak{l}$, and $K(\gamma) = K$, which implies that $\gamma \in K$, as desired. □

Proof of Herbrand's theorem, Theorem 20.18. Since, for any $(d,p) = 1$,

$$(d-\sigma_d)\theta = \sum_{a=1}^{p-1} \left(\frac{ad}{p} - \left\{ \frac{ad}{p} \right\} \right) \sigma_a^{-1} = \sum_{a=1}^{p-1} \left\lfloor \frac{ad}{p} \right\rfloor \sigma_a^{-1} \in \mathbb{Z}[G],$$

the Stickelberger's theorem says that $(d-\sigma_d)\theta$ annihilates $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$, so $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p$. Since the decomposition $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p = \bigoplus_{a=0}^{p-2} \mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$ is a decomposition as $\mathbb{Z}_p[G]$-modules, it follows that $(d-\sigma_d)\theta$ annihilates each $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$. For $x \in \mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$,

$$(d-\sigma_d)\theta x = \varepsilon_i(d-\sigma_d)\theta x = (d-\omega^i(d))\varepsilon_i\theta x = (d-\omega^i(d))\frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-i}(a)\varepsilon_i x = (d-\omega^i(d))B_{1,\omega^{-i}}x.$$

Let $3 \le i \le p-2$ be odd. Then, if d is a primitive root mod p, then $(d-\omega^i(d))$ is not divisible by p, so the above observation implies that $B_{1,\omega^{-i}}x = 0$, which is what we desired. □

Remark 20.21. It may sound reasonable that the analytic class number formula, Herbrand, and Converse to Herbrand altogether implies that $|\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]| = (B_{1,\omega^{-i}})_p$, but we cannot say this as we do not know the group structure of the p-group $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$. It can be proved that, if $(p, h_{\mathbb{Q}(\zeta_p)^+}) = 1$, then $\mathrm{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]$ is a finite cyclic group for all odd $3 \le i \le p-2$. From the numerical computations, we suspect this is always the case.

Conjecture 20.22 (Vandiver's conjecture)**.** *Let p be a prime. Then, $(p, h_{\mathbb{Q}(\zeta_p)^+}) = 1$.*

Namely, if we assume Vandiver's conjecture, then for all odd $3 \leq i \leq p-2$, $|\operatorname{Cl}(\mathbb{Q}(\zeta_p))_p[\omega^i]| = (B_{1,\omega^{-i}})_p$ holds.

Vandiver's conjecture is wide open. In fact, we have very little idea how to approach the conjecture, and it is so clueless that some people suspect that the conjecture may be false actually. We have not found any counterexample yet.

Remark 20.23. Similar to Theorem 20.16(2), the relative class number arises as an index:

Theorem 20.24 (Iwasawa)**.** *Let $K = \mathbb{Q}(\zeta_{p^m})$, $p^m > 2$, $R = \mathbb{Z}[G]$ and $R^- \subset R$ be the minus-part of R, i.e. $R^- = \{x \in R \ : \ \overline{x} = -x\}$, where $\bar{\cdot}$ is the complex conjugation. Let $I \subset R$ be the Stickelberger ideal, and $I^- = I \cap R^- = R\theta \cap R^-$. Then,*

$$[R^- : I^-] = h_K^-.$$

– –

Exercise 20.1.

(1) Show that the Bernoulli polynomials $B_n(X)$ can be defined by the equation

$$\frac{Ze^{XZ}}{e^Z - 1} = \sum_{n=0}^{\infty} \frac{B_n(X)}{n!} Z^n.$$

(2) Show that $B_{n+1}(X+1) - B_{n+1}(X) = (n+1)X^n$.

(3) Let $n, m \in \mathbb{N}$. Show that

$$\sum_{a=1}^{m} a^n = \frac{B_{n+1}(m) - B_{n+1}(0)}{n+1} = \frac{1}{n+1} \sum_{j=0}^{n} (-1)^j \binom{n+1}{j} B_j m^{n+1-j}.$$

This is called the **Faulhaber's formula**.

(4) Let p be an odd prime and $n > 0$ be even integer not divisible by $p-1$. Using (3), show that

$$\sum_{a=1}^{p} a^n \equiv pB_n \pmod{p^2}.$$

(5) Let $b \in \mathbb{N}$, $(b, p) = 1$. Show that, for $1 \leq a \leq p$, if $ab = px_a + r_a$ for $x_a, r_a \in \mathbb{Z}$, $0 \leq r_a < p$,

$$(ab)^n \equiv r_a^n + pn(ab)^{n-1} \left\lfloor \frac{ab}{p} \right\rfloor \pmod{p^2}.$$

By adding the above equation over $1 \leq a \leq p$, show

$$(b^n - 1) \sum_{a=1}^{p} a^n \equiv pnb^{n-1} \sum_{a=1}^{p-1} a^{n-1} \left\lfloor \frac{ab}{p} \right\rfloor \pmod{p^2}.$$

(6) Let p be an odd prime and a, b be positive even integers such that $a \equiv b \not\equiv 0 \pmod{p-1}$ and a, b are coprime to p. Using (4), (5), show that

$$\frac{B_a}{a} \equiv \frac{B_b}{b} \pmod{p}.$$

This is called the **Kummer's congruences**.

Exercise 20.2.

(1) Let p be an odd prime. Recall that the Teichmüller character $\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ takes a to the $(p-1)$-st root of unity congruent to a mod p. Show that, for $1 \leq a \leq p-1$,

$$\omega(a) \equiv a + \frac{a^{p-1} - 1}{a^{p-2}} \pmod{p^2}.$$

(2) Let p be an odd prime, and let $3 \leq i \leq p-2$ be an odd integer. Using Question 1, show that

$$B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} \pmod{p}.$$

This implies that one may replace $B_{1,\omega^{-i}}$ with B_{p-i} in the statement of Herbrand's theorem.

Exercise 20.3. Let p be a prime, and let $1 \leq a \leq b$. Show that the norm map

$$N_{\mathbb{Q}(\zeta_{p^b})/\mathbb{Q}(\zeta_{p^a})} : \mathrm{Cl}(\mathbb{Q}(\zeta_{p^b})) \to \mathrm{Cl}(\mathbb{Q}(\zeta_{p^a})),$$

is surjective. Deduce that $h_{\mathbb{Q}(\zeta_{p^a})}$ divides $h_{\mathbb{Q}(\zeta_{p^b})}$.

Hint. Show that, for any subextension $\mathbb{Q}(\zeta_{p^b})/K/\mathbb{Q}(\zeta_{p^a})$, the unique prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_{p^a})$ over p is ramified in $K/\mathbb{Q}(\zeta_{p^a})$. Deduce that $H_{\mathbb{Q}(\zeta_{p^a})} \cap \mathbb{Q}(\zeta_{p^b}) = \mathbb{Q}(\zeta_{p^a})$.

Exercise 20.4. Let $p \equiv 3 \pmod{4}$ be a prime. Let $K = \mathbb{Q}(\sqrt{-p})$, and let χ_p be the quadratic Dirichlet character of modulus p (cf. Definition 19.14).

(1) Show that Theorem 19.17(1) reads

$$h_K = -\frac{1}{p}\sum_{a=1}^{p} \chi_p(a)a = \frac{1}{p}\left(-2\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a)a + p\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a)\right).$$

Hint. We know exactly what the value of $G(\chi_p)$ is.

(2) Show that (1) can be massaged into

$$h_K = \frac{1}{p}\left(-4\sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)a + p\sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)\right).$$

Hint. $\chi(2a) = -\chi(p-2a)$.

(3) Show that (1) and (2) together gives

$$h_K = \frac{1}{2 - \chi_p(2)} \sum_{a=1}^{\frac{p-1}{2}} \chi_p(a).$$

Deduce that there are more quadratic residues than non-residues in the interval $(0, \frac{p}{2})$.

(4) If $p \equiv 1 \pmod 4$ is a prime, show that the number of quadratic residues in the interval $(0, \frac{p}{2})$ is the same as the number of quadratic non-residues.

List of theorems without proofs

In the later part of the course, we stated some big difficult theorems without proofs. It takes a long time (or even a whole semester-long course) to prove these theorems. Our goal in this course is to rather expose the students to more modern developments of number theory, so we will not try to prove these theorems, but rather focus on seeing how useful these big theorems are.

The following is the list of unproven major theorems in the lecture notes.

- Kronecker–Weber theorem, Theorem 9.9. It is usually dealt in a typical graduate-level algebraic number theory course, but in fact it also easily follows from the local Kronecker–Weber theorem below.
- Local Kronecker–Weber theorem, Theorem 15.2. An elementary proof alluded in the footnote can be found in [Lub].
- The local class field theory, in particular Theorem 15.10 (local Artin reciprocity) and Theorem 15.11 (local existence theorem). This is usually proven in a typical graduate-level algebraic number theory course.
- Chebotarev density theorem, Theorem 16.10.
- The global class field theory, in particular Theorem 16.14 (Artin reciprocity) and Theorem 16.15 (existence theorem). These are usually proven in a typical graduate-level algebraic number theory course.
- Lemma 16.26, whose proof may be found in some of the class field theory textbooks, such as Artin–Tate, Neukirch, Lang, etc.
- Hilbert reciprocity law, Theorem 16.33.
- Analytic class number formula, Theorem 19.7. The proof is elementary but long.
- Conductor-discriminant formula, Theorem 20.5. It can be proved by showing an equality of "local discriminant" and the product of local conductors, and this requires more refined study of ramification in local fields.
- Theorem 20.14, that $p|h_{\mathbb{Q}(\zeta_p)}$ if and only if $p|h^-_{\mathbb{Q}(\zeta_p)}$.
- Ribet's Converse to Herbrand's theorem, Theorem 20.19.
- Theorem 20.24, that the index of the Stickelberger ideal captures the relative class number.

Lecture 1.

Solution to Exercise 1.1.

As $\mathbb{F}_p^\times$ is cyclic, there is a primitive root x mod p, namely $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ and under this isomorphism $x \in \mathbb{F}_p^\times$ corresponds to $1 \in \mathbb{Z}/(p-1)\mathbb{Z}$. Then, $a = x^j$ for some $0 \leq j < p-1$, and $\left(\frac{a}{p}\right) = 1$ if and only if j is even. Note that $a^{\frac{p-1}{2}} = x^{\frac{p-1}{2}j}$, so it is 1 if j is even, and $x^{\frac{p-1}{2}}$ if j is odd. Note that $\left(x^{\frac{p-1}{2}}\right)^2 = x^{p-1} = 1$, so $x^{\frac{p-1}{2}}$ is a solution to $X^2 - 1$ that is not equal to 1, so $x^{\frac{p-1}{2}} = -1$. Thus, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$. □

Solution to Exercise 1.2.

(1) As p is odd, $p = x^2 + y^2$ implies that one of x^2, y^2 is odd and the other is even. Thus one of them is $\equiv 1 (\mathrm{mod}\, 4)$ and one of them is $\equiv 0 (\mathrm{mod}\, 4)$. Thus, $p \equiv 0 + 1 = 1 (\mathrm{mod}\, 4)$.

(2) As $p|(n^2+1) = (n+i)(n-i)$, if p is irreducible, it means that either $p|(n+i)$ or $p|(n-i)$, but neither of them holds. Thus, p is reducible.

(3) As p is reducible, $p = z_1 \cdots z_r$ for $z_1, \cdots, z_r$ irreducible elements in $\mathbb{Z}[i]$ (the same element may repeat more than once). Taking the complex conjugate, we get $p = \overline{z}_1 \cdots \overline{z}_r$, so

$$p^2 = |z_1|^2 \cdots |z_r|^2.$$

Note that each $|z_i|^2$ is a positive integer. Furthermore, $|z_i|^2 \neq 1$, as otherwise it will mean $z_i \overline{z}_i = 1$, so z_i will be a unit. Thus, by prime factorization in integers, it follows that either $r = 1$ with $|z_1|^2 = p^2$, or $r = 2$ with $|z_1|^2 = |z_2|^2 = p$. Note that as p is reducible, $r > 1$. Thus, the only possibility is $r = 2$ with $|z_1|^2 = |z_2|^2 = p$. Let $z_1 = x + iy$, $x, y \in \mathbb{Z}$. Then $|z_1|^2 = p$ means $x^2 + y^2 = p$, as desired.

□

Lectures 2 and 3.

Solution to Exercise 2.1.

Let K be a quadratic field. By definition, $x \in K \backslash \mathbb{Q}$ is a root of a polynomial with rational coefficients that is not linear (as otherwise $x \in \mathbb{Q}$). As K is quadratic, it follows that x is a root of a qudaratic polynomial with rational coefficients, $p(X) = X^2 + aX + b$, $a, b \in \mathbb{Q}$. Note that $K = \mathbb{Q}(x)$ as $K \supset \mathbb{Q}(x) \supset \mathbb{Q}$ and $\mathbb{Q}(x) \neq \mathbb{Q}$ which leaves no possibilities but $K = \mathbb{Q}(x)$. Note also that $y = x + \frac{a}{2}$ is a root of a quadratic polynomial $q(X) = X^2 + b - \frac{a^2}{4}$. Note that as y is x plus a rational number, $\mathbb{Q}(y) = \mathbb{Q}(x)$, and on the other hand, $y = \sqrt{\frac{a^2}{4} - b}$, the square root of a rational number. Let $y = \sqrt{\frac{p}{q}}$, $p, q \in \mathbb{Z}$, $q > 0$. Then, $qy = \sqrt{pq}$, and $\mathbb{Q}(qy) = \mathbb{Q}(y)$. Thus, $K = \mathbb{Q}(\sqrt{pq})$. □

Solution to Exercise 2.2.

For $a \in A$ and $f \in \mathrm{Hom}_A(M,N)$, or $f : M \to N$ an A-module homomorphism,

$$a \cdot f : M \to N, \quad a \cdot f(m) = a \cdot (f(m)),$$

where $a \cdot (f(m))$ means you act by $a \in A$ on $f(m) \in N$ using the A-module structure on N.

Checking why this is an A-module is omitted (standard). □

Lecture 4.

Solution to Exercise 3.1.

By the lecture notes, $D(1,\alpha,\alpha^2) = (-1)^3 N_{K/\mathbb{Q}}(f'(\alpha)) = -N_{K/\mathbb{Q}}(3\alpha^2+a)$. Let $\alpha = x_1, x_2, x_3$ be the three roots of $f(X)$ in the normal closure of K. Then,

$$N_{K/\mathbb{Q}}(3\alpha^2+a) = (3x_1^2+a)(3x_2^2+a)(3x_3^2+a) = 27x_1^2x_2^2x_3^2+9a(x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2)+3a^2(x_1^2+x_2^2+x_3^2)+a^3.$$

Note that as $f(X) = (X-x_1)(X-x_2)(X-x_3)$ we have

$$x_1+x_2+x_3 = 0, \quad x_1x_2+x_1x_3+x_2x_3 = a, \quad x_1x_2x_3 = -b.$$

Thus

$$x_1^2x_2^2x_3^2 = b^2,$$
$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = (x_1x_2+x_1x_3+x_2x_3)^2 - 2x_1x_2x_3(x_1+x_2+x_3) = a^2,$$
$$x_1^2+x_2^2+x_3^2 = (x_1+x_2+x_3)^2 - 2(x_1x_2+x_1x_3+x_2x_3) = -2a.$$

So

$$N_{K/\mathbb{Q}}(3\alpha^2+a) = 27b^2+9a^3-6a^3+a^3 = 27b^2+4a^3.$$

Thus we get the result. □

Solution to Exercise 3.2.

(1) The primitive element theorem says that $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Let $p(X)$ be the minimal polynomial of α over $\mathbb{Q}$,

$$p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \quad a_{n-1}, \cdots, a_0 \in \mathbb{Q}.$$

Let d be the common denominator of the rational numbers $a_{n-1} \cdots, a_0$. Then, $\beta = d\alpha$ is a root of the polynomial $d^n p(X/d)$, which is

$$d^n p(X/d) = X^n + da_{n-1}X^{n-1} + \cdots + d^n a_0.$$

Note that $d^i a_{n-i} \in \mathbb{Z}$, as $da_{n-i} \in \mathbb{Z}$. Thus, $d^n p(X/d)$ is a monic polynomial with integer coefficients. By Gauss's lemma, as $p(X)$ is irreducible in $\mathbb{Q}[X]$, $d^n p(X/d)$ is irreducible in $\mathbb{Q}[X]$, so it is irreducible in $\mathbb{Z}[X]$. Thus $d\alpha \in \mathcal{O}_K$. Obviously $\mathbb{Q}(\alpha) = \mathbb{Q}(d\alpha)$. So we are done.

(2) Note that $D(1, \alpha, \cdots, \alpha^{n-1}) = \pm N_{K/\mathbb{Q}}(f'(\alpha))$, where $f(X)$ is the minimal polynomial of α over $\mathbb{Q}$. Since $K/\mathbb{Q}$ is separable, $f(X)$ and $f'(X)$ have no common roots, so $f'(\alpha) \neq 0$, so $N_{K/\mathbb{Q}}(f'(\alpha)) \neq 0$. Thus, $D(1, \alpha, \cdots, \alpha^{n-1}) \neq 0$. Note that

$$D(1, \alpha, \cdots, \alpha^{n-1}) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \operatorname{disc}(K),$$

so it follows that $\operatorname{disc}(K) \neq 0$.

□

Solution to Exercise 3.3.

(1) By Gauss's lemma, if $f(X)$ is reducible, it must be factorized into

$$f(X) = (X^m + b_{m-1}X^{m-1} + \cdots + b_0)(X^{n-m} + c_{n-m-1}X^{n-m-1} + \cdots + c_0).$$

Note that $b_0 c_0 = a_0$, so either b_0 or c_0 is divisible by p. Also, as p^2 does not divide a_0, exactly one is divisible by p. Without loss of generality, let $p|b_0$ and $(p, c_0) = 1$. Then we have $b_1 c_0 + b_0 c_1 = a_1$, and as b_0, a_1 are divisible by p, $b_1 c_0$ is divisible by p. As c_0 is copriem to p, p divides b_1. Continuing, we get every coefficient of $(X^m + b_{m-1}X^{m-1} + \cdots + b_0)$ is divisible by p, which is obviously a contradiction as it is monic. Thus, $f(X)$ is irreducible.

(2) By Hint, ζ_{p^a} is a root of $\Phi_{p^a}(X)$. Thus it suffices to show that $\Phi_{p^a}(X)$ is irreducible, or $\Phi_{p^a}(X+1)$ is. Note that the constant term of $\Phi_{p^a}(X+1)$ is $1+1+\cdots+1 = p$, so it satisfies Condition 2. Thus we are left with Condition 1, that $\Phi_{p^a}(X+1) \equiv X^{p^{a-1}(p-1)} \pmod{p}$. Note that

$$\Phi_{p^a}(X+1) = \frac{(X+1)^{p^a} - 1}{(X+1)^{p^{a-1}} - 1} \equiv \frac{X^{p^a} + 1 - 1}{X^{p^{a-1}} + 1 - 1} = \frac{X^{p^a}}{X^{p^{a-1}}} = X^{p^{a-1}(p-1)} \pmod{p}.$$

(3) Note that $\zeta_{p^a}^k$ for $1 \leq k \leq p^a$, $(k, p) = 1$, is also a root of $\Phi_{p^a}(X)$, and this exhausts all roots as we have enumerated all $\varphi(p^a) = p^{a-1}(p-1)$ roots. Thus, the conjugates of ζ_{p^a} are $\zeta_{p^a}^k$. Thus, $\Phi_{p^a}(X)$ is already split in $\mathbb{Q}(\zeta_{p^a})$, so $\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}$ is Galois. We have a natural map

$$\operatorname{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \to (\mathbb{Z}/p^a\mathbb{Z})^\times, \quad \sigma \mapsto r(\sigma), \quad \sigma(\zeta_{p^a}) = \zeta_{p^a}^{r(\sigma)},$$

which is injective as the automorphism of $\mathbb{Q}(\zeta_{p^a})$ is determined by where ζ_{p^a} goes. Thus the natural map is an injection between finite sets of the same order, so it is bijective, so it is an isomorphism.

□

Solution to Exercise 3.4.

(1) Note

$$D(1, \zeta_{p^a}, \cdots, \zeta_{p^a}^{p^{a-1}(p-1)-1}) = (-1)^{\frac{p^{a-1}(p-1)(p^{a-1}(p-1)-1)}{2}} N_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(\Phi'_{p^a}(\zeta_{p^a})).$$

Let's not worry about the sign part at the moment. We have

$$\Phi'_{p^a}(X) = \left(\frac{X^{p^a}-1}{X^{p^{a-1}}-1}\right)' = \frac{(X^{p^a}-1)'(X^{p^{a-1}}-1) - (X^{p^a}-1)(X^{p^{a-1}}-1)'}{(X^{p^{a-1}}-1)^2}$$

$$= \frac{p^a X^{p^a-1}(X^{p^{a-1}}-1) - p^{a-1}X^{p^{a-1}-1}(X^{p^a}-1)}{(X^{p^{a-1}}-1)^2}.$$

Let $\zeta_p = \zeta_{p^a}^{p^{a-1}}$, a primitive p-th root of unity. Then

$$\Phi'_{p^a}(\zeta_{p^a}) = \frac{p^a\zeta_{p^a}^{-1}(\zeta_p - 1) - 0}{(\zeta_p - 1)^2} = p^a \frac{1}{\zeta_{p^a}(\zeta_p - 1)}$$

Let D be the discriminant, $\pm$ be the sign part (to be determined later), and $K = \mathbb{Q}(\zeta_{p^a})$. Then

$$D = \pm \frac{N_{K/\mathbb{Q}}(p^a)}{N_{K/\mathbb{Q}}(\zeta_{p^a})N_{K/\mathbb{Q}}(\zeta_p - 1)} = \pm \frac{p^{ap^{a-1}(p-1)}}{(-1)^{p^{a-1}(p-1)}N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1)^{p^{a-1}}}.$$

Here we have used the transitivity of norms and that $\Phi_{p^a}(X)$ is the minimal polynomial of ζ_{p^a} to determine $N_{K/\mathbb{Q}}(\zeta_{p^a})$. Note also that ζ_p is a root of $X^{p-1} + \cdots + 1$, so $\zeta_p - 1$ is a root of $(X+1)^{p-1} + \cdots + (X+1) + 1$, so $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1}p$. Thus we have

$$D = \pm p^{ap^{a-1}(p-1)-p^{a-1}}.$$

So what is this sign? If p is odd, then looking at the expresion of $\pm$, one realizes that $\pm = (-1)^{\frac{p-1}{2}}$, so $D = (-1)^{\frac{p-1}{2}}p^{ap^{a-1}(p-1)-p^{a-1}}$. On the other hand, if $p = 2$, suppose first that $a \geq 3$. Then, $\pm = (-1)^{2^{a-2}(2^{a-1}-1)} = 1$. So, $D = p^{ap^{a-1}(p-1)-p^{a-1}}$. If $p^a = 4$, then $\pm = -1$, so $D = -p^{ap^{a-1}(p-1)-p^{a-1}}$. If $p^a = 2$, then $\pm = 1$, so $D = p^{ap^{a-1}(p-1)-p^{a-1}}$. So we have

$$D(1, \zeta_{p^a}, \cdots, \zeta_{p^a}^{p^{a-1}(p-1)-1}) = \begin{cases} p^{ap^{a-1}(p-1)-p^{a-1}} & \text{if } p \equiv 1 \pmod 4 \text{ or } p = 2 \text{ with } a \neq 2 \\ -p^{ap^{a-1}(p-1)-p^{a-1}} & \text{if } p \equiv 3 \pmod 4 \text{ or } p^a = 4 \end{cases}$$

(2) The minimal polynomial of ζ_{p^a} is $\Phi_{p^a}(X)$, so $1 - \zeta_{p^a}$ is a root of $\Phi_{p^a}(1-X)$. This polynomial has the constant coefficient p and the leading coefficient $(-1)^{p^{a-1}(p-1)}$, so the minimal polynomial of $1 - \zeta_{p^a}$ is $(-1)^{p^{a-1}(p-1)}\Phi_{p^a}(1-X)$, whose constant coefficient is $(-1)^{p^{a-1}(p-1)}p$. Thus, $N_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(1 - \zeta_{p^a}) = p$. This applies to any primitive p^a-th root of unity, so $N_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(1 - \zeta_{p^a}^k) = p$ for $k \in (\mathbb{Z}/p^a\mathbb{Z})^\times$. Thus the norm of $\frac{1-\zeta_{p^a}^k}{1-\zeta_{p^a}}$ is 1, which means it is a unit.

(3) Note that $1+\zeta_{p^a}$ within a specific choice of $\zeta_{p^a} = e^{2\pi i/p^a}$ corresponds to a complex number

$$1 + \zeta_{p^a} \mapsto \left(1 + \cos\left(\frac{2\pi}{p^a}\right)\right) + i \sin\left(\frac{2\pi}{p^a}\right).$$

Note that $\frac{2\pi}{p^a} \leq \frac{2\pi}{5} < \frac{\pi}{2}$, so $\cos\left(\frac{2\pi}{p^a}\right) > 0$. Thus, the complex norm of $\left(1 + \cos\left(\frac{2\pi}{p^a}\right)\right) + i \sin\left(\frac{2\pi}{p^a}\right)$, which we denote as A, is larger than 1. Thus, $(1 + \zeta_{p^a})^k$ corresponds to a complex number that is of the norm A^k. This grows infinitely larger as $k \to \infty$, so $(1 + \zeta_{p^a})^k \neq 1$ for any $k > 0$. Thus $1 + \zeta_{p^a}$ is of infinite order.

□

Lecture 5.

Solution to Exercise 4.1.

Note that $\mathrm{disc}(\mathbb{Q}(\zeta_p))$ is $\pm$ a power of p. As $\mathrm{disc}(K)$ divides it, $\mathrm{disc}(K)$ must also be $\pm$a power of p. This excludes the case $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 2, 3 \pmod 4$, as then $\mathrm{disc}(K)$ is a multiple of 4 (recall we assumed that p is odd). For $d \equiv 1 \pmod 4$ to be a squarefree integer which is $\pm$ a power of p, the only possibilities are either $d = \pm p$ or $d = 1$. But $d \neq 0, 1$, so the only possibility is $d = \pm p$, and $d = p$ if $p \equiv 1 \pmod 4$ and $d = -p$ if $p \equiv 3 \pmod 4$. □

Solution to Exercise 4.2.

(1) Let $p_a(X) = X^n + d_{n-1}X^{n-1} + \cdots + d_0$ where $p | d_{n-1}, \cdots, d_0$ but p^2 does not divide d_0. Then $\alpha^n = -(d_{n-1}\alpha^{n-1} + \cdots + d_0)$, so $\frac{\alpha^n}{p} = -\left(\frac{d_{n-1}}{p}\alpha^{n-1} + \cdots + \frac{d_0}{p}\right) \in \mathbb{Z}[\alpha] \subset \mathcal{O}_K$, so $\alpha^n \in p\mathcal{O}_K$.

Thus, multiplying by α^{n-1}, we get

$$a_0\alpha^{n-1} + \alpha^n(a_1 + a_2\alpha + \cdots + a_{n-1}\alpha^{n-2}) \in p\mathcal{O}_K.$$

Since $\alpha^n \in p\mathcal{O}_K$, we have $a_0\alpha^{n-1} \in p\mathcal{O}_K$. Let $a_0\alpha^{n-1} = px$ with $x \in \mathcal{O}_K$. Then

$$N_{K/\mathbb{Q}}(a_0)N_{K/\mathbb{Q}}(\alpha)^{n-1} = N_{K/\mathbb{Q}}(p)N_{K/\mathbb{Q}}(x) = p^n N_{K/\mathbb{Q}}(x) \in p^n\mathbb{Z}.$$

On the other hand, by definition, $N_{K/\mathbb{Q}}(\alpha) = (-1)^n d_0$, so $N_{K/\mathbb{Q}}(\alpha)$ is an integer divisible by p but not p^2. Thus $N_{K/\mathbb{Q}}(\alpha)^{n-1}$ is an integer divisible by p^{n-1} but not by p^n. Tuhs, $N_{K/\mathbb{Q}}(a_0) = a_0^n \in p\mathbb{Z}$. Thus, $a_0 \in p\mathbb{Z}$. This implies that $a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = (a_0 + \cdots + a_{n-1}\alpha^{n-1}) - a_0 \in p\mathcal{O}_K$. Multiplying by α^{n-2}, we get $a_1\alpha^{n-1} \in p\mathcal{O}_K$, from which we again obtain $a_1 \in p\mathbb{Z}$. Repeating this, we get $a_0, \cdots, a_{n-1} \in p\mathbb{Z}$.

(2) Let d be the common denominator of $b_0, \cdots, b_{n-1}$. Then $dx \in \mathbb{Z}[\alpha] \cap d\mathcal{O}_K$. If there is a factor of p in the denominator, then $p|d$, so $dx \in \mathbb{Z}[\alpha] \cap p\mathcal{O}_K$. By (1), this means that $db_0, \cdots, db_{n-1} \in p\mathbb{Z}$. On the other hand, if b_i is the coefficient with the largest power of p dividing the denominator among $b_0, \cdots, b_{n-1}$, then db_i is coprime to p, which is a contradiction.

(3) If there is an order p element in $\mathcal{O}_K/\mathbb{Z}[\alpha]$, this means there is $x \in \mathcal{O}_K$ such that $px \in \mathbb{Z}[\alpha]$. But then x is then a $\mathbb{Q}$-linear combination of powers of α where each coefficient has denominator dividing p. By (2), this implies that each coefficient is in fact an integer, that $x \in \mathbb{Z}[\alpha]$. This means that there is no order p element in $\mathcal{O}_K/\mathbb{Z}[\alpha]$, as desired.

(4) Let $K = \mathbb{Q}(\sqrt[5]{2})$ and $\alpha = \sqrt[5]{2}$. Note $\operatorname{disc}(1, \cdots, \sqrt[5]{2^4}) = (-1)^{10} N_{K/\mathbb{Q}}(f'(\alpha))$ where $f(X) = X^5 - 2$ is the minimal polynomial of α over $\mathbb{Q}$ (it is the minimal polynomial because it is irreducible as it is obviously Eisenstein at 2). Thus $\operatorname{disc}(1, \cdots, \alpha^4) = N_{K/\mathbb{Q}}(5\alpha^4) = 5^5 N_{K/\mathbb{Q}}(\alpha)^4 = 5^5 2^4$.

Now 2 does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ by (3) as $X^5 - 2$ is Eisenstein at 2. So it remains to prove that 5 does not divide the index. Note that $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha - 2]$ where $\beta = \alpha - 2$ satisfies $f(X + 2) = (X + 2)^5 - 2$. This is again an irreducible polynomial in $\mathbb{Z}[X]$ (as $f(X)$ is irreducible), but note that it is also Eisenstein at 5: it is

$$f(X + 2) = (X + 2)^5 - 2 \equiv X^5 + 2^5 - 2 \equiv X^5 \pmod 5,$$

and its constant coefficient is $2^5 - 2 = 30$ which is not divisible by 5. Thus, $[\mathcal{O}_K : \mathbb{Z}[\beta]] = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is not divisible by 5 by (3).

□

Lecture 6.

Solution to Exercise 5.1.

(1) One direction is obvious. Suppose $M_1, M_2 \subset M$ such that $M_1 \cap N = M_2 \cap N$ and $\frac{M_1}{M_1 \cap N} = \frac{M_2}{M_2 \cap N}$. Let $M_3 = M_1 \cap N = M_2 \cap N$. Then it is a B-submodule of M, so there is a one-to-one correspondence between the B-submodules of $\frac{M}{M_3}$ and the B-submodules of M containing M_3. As $\frac{M_1}{M_3} = \frac{M_2}{M_3} \subset \frac{M}{M_3}$, it follows that $M_1 = M_2$.

(2) For such a module M with a generator m, define a map $B \to M$ by $b \mapsto bm$. By definition, it is surjective. Its kernel I is an ideal, as if $x \in B$ is sent to zero in M, this means $xm = 0$, so for any $y \in B$, $xym = 0$, so $xy \in I$.

(3) The base case is clear as Noetherianity of A implies that an ascending chain of ideals stabilizes. Now suppose M is an A-module with n generators $m_1, \cdots, m_n$. Let N be the submodule of M generated by $m_1, \cdots, m_{n-1}$. Let $M_1 \subset M_2 \subset$ be an increasing sequence of submodules of M. Then $M_1 \cap N \subset M_2 \cap \subset \cdots$ is an increasing sequence of submodules of N, which stabilizes by induction, say after $n \geq X$. Let $L = M_X \cap N$. Then we still have an ascending chain of submodules $\frac{M_X}{L} \subset \frac{M_{X+1}}{L} \subset \cdots$ of $\frac{M}{N}$. Since $\frac{M}{N}$ is generated by one element, again by induction this chain stabilizes. By (1), the original chain stabilizes.

□

Solution to Exercise 5.2.

(1) It is F-linear as A is an F-algebra. It is injective as it is an integral domain.

(2) It is a finite-dimensional F-vector space because that's literally what it means to be a finitely generated F-module. Thus, m_a is an injection between two F-vector spaces of the same finite dimension, so m_a is surjective by rank-nullity theorem.

(3) For $a \in A$ nonzero, let $a^{-1} = m_a^{-1}(1)$. Then a^{-1} is the desired multiplicative inverse to show that A is a field.

□

Lecture 7.

Solution to Exercise 6.1.

If $\mathfrak{a}$ is an integral ideal of A such that $\mathfrak{a} \supset I + J$, then both $\mathfrak{a} \supset I$ and $\mathfrak{a} \supset J$, so $\mathfrak{a}$ divides both I and J, which by the unique factorization means $I + J$ divides $\prod_{i=1}^n \mathfrak{p}_i^{\min(e_i, f_i)}$. On the other hand, for each i, $\mathfrak{p}_i^{e_i} \supset I, J$, so $\mathfrak{p}_i^{e_i} \supset I + J$, so $\mathfrak{p}_i^{e_i}$ divides $I + J$ for each i, so we get the formula for $I + J$.

The formula for $I \cap J$ is even easier, as $\mathfrak{a} \subset I \cap J$ if and only if $\mathfrak{a} \subset I$ and $\mathfrak{a} \subset J$. □

Solution to Exercise 6.2.

(1) It is obivous that it is sufficient to prove the case when $e_1, \cdots, e_n \geq 0$ with $b \in A$. Note that $\mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1}$ is an ideal of $A/\mathfrak{p}_i^{e_i+1}$ where

$$\frac{A/\mathfrak{p}_i^{e_i+1}}{\mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1}} = A/\mathfrak{p}_i^{e_i}.$$

As $\#A/\mathfrak{p}_i^k = N(\mathfrak{p}_i^k) = N(\mathfrak{p}_i)^k$, we have $\#\mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1} = N(\mathfrak{p}_i)^{e_i+1}/N(\mathfrak{p}_i)^{e_i} = N(\mathfrak{p}_i) > 1$, which means that $\mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1}$ is nonzero. This means that we can choose $x_i \in \mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1}$ that is not zero for each i. As in the hint, we can use the Chinese Remainder Theorem to find $b \in A$ such that $b \equiv x \pmod{\mathfrak{p}_i^{e_i+1}}$. This means that $b \in \mathfrak{p}_i^{e_i}$ but $b \notin \mathfrak{p}_i^{e_i+1}$. Thus, $(b) \subset \prod_{i=1}^n \mathfrak{p}_i^{e_i}$, or $\prod_{i=1}^n \mathfrak{p}_i^{e_i}$ divides (b), but for each i, $\mathfrak{p}_i^{e_i+1}$ does not divide (b). This is exactly what we want.

(2) Without loss of generalities, suppose that $e_1, \cdots, e_m < 0$ and $e_{m+1}, \cdots, e_n \geq 0$ (if all e_i's are nonnegative, then the strong approximation is the version of weak approximation we proved above, so there is nothing more to prove). By using the weak approximation theorem we proved, we can find $b \in A$ such that $(b) = \prod_{i=1}^m \mathfrak{p}_i^{-e_i} \prod_{j=1}^s \mathfrak{q}_j^{f_j}$ for $f_j > 0$ and $\mathfrak{q}_j$'s different from $\mathfrak{p}_i$'s. Also, by the weak approximation theorem we proved, we can find $b' \in A$ such that (b') is divisible by $\prod_{i=m+1}^n \mathfrak{p}_i^{e_i} \prod_{j=1}^s \mathfrak{q}_j^{f_j}$ and $\frac{(b')}{\prod_{i=m+1}^n \mathfrak{p}_i^{e_i} \prod_{j=1}^s \mathfrak{q}_j^{f_j}}$ is not divisible by any $\mathfrak{p}_i$'s or $\mathfrak{q}_j$'s. Then, $\frac{b'}{b} \in \mathrm{Frac}(A)$ satisfies the condition.

□

Lectures 8 and 9.

Solution to Exercise 7.1.

(1) Straightforward.

(2) Note that, in $\mathbb{F}_2[X]$, $X^2 - X = X(X-1)$ is reducible while $X^2 - X + 1$ is irreducible. One way to see that $X^2 - X + 1$ is irreducible is because, if it is reducible, it should be factored into a product of two linear factors, which means there should be a root in $\mathbb{F}_2$, but $0^2 - 0 + 1 = 1$ and $1^2 - 1 + 1 = 1$, so there is no root in $\mathbb{F}_2$. Thus, $f(X)$ is irreducible in $\mathbb{F}_2[X]$ iff $\frac{1-d}{4} \equiv 1 \pmod 2$.

(3) Note that $f(X) = (X - \frac{1}{2})^2 - \frac{d}{4}$, so for p odd, $f(X)$ is irreducible mod p iff $\frac{d}{4}$ is not a square mod p, or equivalently d is not a square mod p.

(4) This means that

$$(p) = \begin{cases} (2, \frac{\sqrt{d}+1}{2})(2, \frac{\sqrt{d}+3}{2}) & \text{if } p = 2,\ d \equiv 1 \pmod 8 \\ (2) & \text{if } p = 2,\ d \equiv 5 \pmod 8 \\ (p) & \text{if } p \text{ odd, } d \text{ not a square mod } p \\ (p, \frac{1+\sqrt{d}}{2} - \frac{p+1}{2})^2 & \text{if } p \text{ divides } d \\ (p, \frac{1+\sqrt{d}}{2} - \frac{p+1}{2} - a)(p, \frac{1+\sqrt{d}}{2} - \frac{p+1}{2} + a) & \text{if } p \text{ odd, } \frac{d}{4} \equiv a^2 \pmod p \text{ for } a \neq 0 \end{cases}$$

□

Solution to Exercise 7.2.

(1) Suppose that p is ramified in L,

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \subset \mathcal{O}_L,$$

with $e_1 > 1$. Then $\mathfrak{p}_1^2$ divides (p). Let $\mathfrak{q}$ be any prime ideal in $\mathcal{O}_K$ lying over $\mathfrak{p}_1$. Then $\mathfrak{q}^2$ divides $p\mathcal{O}_K$, so p is ramified in K.

(2) Suppose that p is completely split in K. Then by (1) firstly p is unramified in L. Let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal lying over p. We want to show that $f(\mathfrak{p}|p) = 1$. Let $\mathfrak{q} \subset \mathcal{O}_K$ be any prime ideal lying over $\mathfrak{p}$, i.e. $\mathfrak{q} \cap \mathcal{O}_L = \mathfrak{p}$. Then $\mathcal{O}_L/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{q}$ is a subfield. Also $f(\mathfrak{q}|p) = 1$ so $\mathcal{O}_K/\mathfrak{q} = \mathbb{F}_p$ which means that $\mathcal{O}_L/\mathfrak{p} = \mathbb{F}_p$ which means $f(\mathfrak{p}|p) = 1$ as desired.

□

Solution to Exercise 7.3.

Note that $\operatorname{disc}(\mathbb{Q}(\sqrt{d})) = d$ in this case. Thus $\operatorname{Fr}_p = 1$ if and only if p splits completely in $\mathbb{Q}(\sqrt{d})$, which is, when p is odd, when d a square mod p. □

Lecture 10.

Solution to Exercise 8.1.

That p is inert means that $f = [K : \mathbb{Q}]$, so $D(\mathfrak{p}|p)$ is a cyclic group of order $f = [K : \mathbb{Q}]$, for any prime ideal $\mathfrak{p}$ lying over p. Since $D(\mathfrak{p}|p)$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$, which is of order $[K : \mathbb{Q}]$, it follows that $D(\mathfrak{p}|p) \cong \mathrm{Gal}(K/\mathbb{Q})$, so it is a cyclic group. □

Lecture 11.

Solution to Exercise 9.1.

(1) This is because there is no primitive n-th root of unity in $\mathbb{R}$.

(2) Note K^+ is fixed by $\sigma_{-1} \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma_{-1}(\zeta_n) = \zeta_n^{-1}$, so $[K : K^+] \geq 2$. Note that ζ_n is a root of a quadratic polynomial $f(X) \in K^+[X]$, $f(X) = X^2 - (\zeta_n + \zeta_n^{-1})X + 1$, so $[K : K^+] \leq 2$, so $[K : K^+] = 2$.

(3) Let $\iota : K^+ \hookrightarrow \mathbb{C}$ be any embedding and we can find $\zeta_n \in \mathbb{C}$ so that the induced embedding $K \hookrightarrow \mathbb{C}$ restricts to the given embedding ι (you can take the root of $f(X)$ in $\mathbb{C}$ which is possible because $\mathbb{C}$ is algebraically closed). Then ζ_n has complex norm 1, so ζ_n^{-1} is the complex conjugate of ζ_n, so $\zeta_n + \zeta_n^{-1}$ is a real number, so $K^+ \subset \mathbb{R}$.

(4) Note that $\mathcal{O}_{K^+} = \mathcal{O}_K \cap K^+$, so $\mathcal{O}_{K^+} \supset \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Conversely, if $x \in \mathcal{O}_{K^+}$, then $x = \sum_{j=0}^{n-1} a_j \zeta_n^j$, $a_j \in \mathbb{Z}$. Since $x \in K^+$, it is fixed by σ_{-1}, so $x = \sigma_{-1}(x) = \sum_{j=0}^{n-1} a_j \zeta_n^{n-j}$, so $a_j = a_{n-j}$ (with $a_n := a_0$). Thus it a $\mathbb{Z}$-linear combination of $1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \cdots$. Thus it is sufficient to prove that $\zeta_n^j + \zeta_n^{-j} \in K$ for all $j \in \mathbb{N}$. We prove this by induction on j. Obviously $j = 0$, $j = 1$ case holds. Also,

$$(\zeta_n^{j-1} + \zeta_n^{-j+1})(\zeta_n + \zeta_n^{-1}) = (\zeta_n^j + \zeta_n^{-j}) + (\zeta_n^{j-2} + \zeta_n^{-j+2}),$$

so by induction we get the desired result.

□

Lectures 12 and 13.

Solution to Exercise 10.1.

(1) The Minkowski bound is $\frac{2}{4}\sqrt{20} = \sqrt{5}$.

(2) Note (2) factors in K as $(2) = (2, \sqrt{6} + 2)^2$, so $\mathfrak{p} = (2, \sqrt{6} + 2)$.

(3) Note that $2 = (\sqrt{6} + 2)(\sqrt{6} - 2)$, so $\mathfrak{p} = (2 + \sqrt{6})$, so it is principal.

□

Solution to Exercise 10.2.

(1) Minkowski bound is $\frac{2}{4}\sqrt{40} = \sqrt{10}$.

(2) Note (2) factorizes as $(2) = (2, \sqrt{10}+2)^2$, so $\mathfrak{p}_2 = (2, \sqrt{10}+2)$. Note $N(\mathfrak{p}_2) = \sqrt{N((2))} = \sqrt{4} = 2$.

(3) If $\mathfrak{p}_2$ is principal, then there is $\alpha \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha) = \pm 2$. If $\alpha = x + y\sqrt{10}$, then $N_{K/\mathbb{Q}}(\alpha) = x^2 - 10y^2$, so we want to see if $x^2 - 10y^2 = \pm 2$ has any integer solutions. If there is an integer solution, mod 5, $x^2 \equiv \pm 2 \pmod 5$, so a contradiction.

(4) Note $X^2 - 10 = X^2 - 1 = (X-1)(X+1) \pmod 3$, so $(3) = (3, \sqrt{10}-1)(3, \sqrt{10}+1)$. Let $\mathfrak{p}_3 = (3, \sqrt{10}-1)$ and $\mathfrak{p}_3' = (3, \sqrt{10}+1)$. As $f = 1$, $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$.

(5) Note that $N_{K/\mathbb{Q}}(4+\sqrt{10}) = 6$, so the prime ideal factorization of $(4+\sqrt{10})$ is consisted of $\mathfrak{p}_2$ and some prime ideal of norm 3. On the other hand $4+\sqrt{10} \in \mathfrak{p}_3'$, so we see $(4+\sqrt{10}) = \mathfrak{p}_2\mathfrak{p}_3'$. Therefore in $\mathrm{Cl}(K)$, $[\mathfrak{p}_2] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_3']^{-1} = [\mathfrak{p}_3]$, so we see that $[\mathfrak{p}_2] = [\mathfrak{p}_3] = [\mathfrak{p}_3']$ and they are nontrivial elements of order 2. Thus $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z}$.

□

Solution to Exercise 10.3.

(1) Note that $\mathbb{Q}(\sqrt{-14})$ is of discriminant -56. Thus, using the algorithm, we seek for $a, b, c \in \mathbb{Z}$, $a, c > 0$, $56 = 4ac - b^2$, $-a < b \leq a$, $c \geq a$, and if $b < 0$, $c > a$. First we look for $1 \leq a \leq \sqrt{56/3}$, so $1 \leq a \leq 4$.

If $a = 1$, then $-1 < b \leq 1$, so $0 \leq b \leq 1$. Since b is even, $b = 0$. Then $c = 14$. This corresponds to $X^2 + 14Y^2$.

If $a = 2$, then $-2 < b \leq 2$. Since $4ac$ and 56 are both multiples of 8, b must be a multiple of 4. So, $b = 0$, and $c = 7$. This corresponds to $2X^2 + 7Y^2$.

If $a = 3$, then $-3 < b \leq 3$. Since b is even, either $b = 0$ or $b = \pm 2$. As 56 is not a multiple of 3, $b \neq 0$. If $b = \pm 2$, then $56 = 12c - 4$, so $60 = 12c$, so $c = 5$. These correspond to $3X^2 + 2XY + 5Y^2$ and $3X^2 - 2XY + 5Y^2$.

If $a = 4$, then $-4 < b \leq 4$. Since $4ac$ and 56 are both multiples of 8, b must be a multiple of 4. So either $b = 0$ or $b = 4$. In both cases $4ac$ and b^2 are multiples of 16, so 56 must be a multiple of 16, which is not the case, so a contradiction.

From the generalities, we see that p is properly represented by either of the four forms if and only if -56 is a square mod p, or, as $p \neq 2$, -14 is a square mod p.

(2) If $p = X^2 + 14Y^2$, then X is odd, so $p \equiv 1 - 2Y^2 \pmod 8$. Also $Y^2 \equiv 0, 1 \pmod 4$, so $p \equiv 1, -1 \pmod 8$. If $p = 2X^2 + 7Y^2$, then Y is odd, so $p \equiv 2X^2 - 1 \pmod 8$. Also $X^2 \equiv 0, 1 \pmod 4$, so $p \equiv 1, -1 \pmod 8$.

(3) If $p = 3X^2 \pm 2XY + 5Y^2$, then $3p = 9X^2 \pm 6XY + 15Y^2 = (3X \pm Y)^2 + 14Y^2$. If $3p = Z^2 + 14W^2$, then firstly, we want to show that either $p = 3$ or Z, W are both coprime to 3. Indeed, $0 \equiv Z^2 - W^2 \pmod 3$, so if either Z or W is divisible by 3, in fact both must be divisible by 3, in which case $3p$ is divisible by 9, so p is divisible by 3. Thus,

only one of the two cases, $Z \equiv W \pmod 3$ or $Z \equiv -W \pmod 3$, should hold. In that case one may express $Z = 3X \pm W$ for some $X \in \mathbb{Z}$, and $3p = Z^2 + 14W^2$ reduces to $p = 3X^2 \pm 2XW + 5W^2$.

Thus, in this case, $3p = Z^2 + 14W^2 \equiv Z^2 - 2W^2 \pmod 8$, in which case by the same reasoning $3p \equiv 1, -1 \pmod 8$, or $p \equiv 3, -3 \pmod 8$.

(4) If $p = 2X^2 + 7Y^2$, then $2p = 4X^2 + 14Y^2 = (2X)^2 + 14Y^2$. If $2p = Z^2 + 14W^2$, then Z is even, so $Z = 2X$ so that $2p = 4X^2 + 14W^2$, or $p = 2X^2 + 7W^2$.

(5) So either p or $2p = X^2 + 14Y^2$ if and only if $\left(\frac{-14}{p}\right) = 1$ and $p \equiv 1, 7 \pmod 8$. Since $p \equiv 1, 7 \pmod 8$ is equivalent to $\left(\frac{2}{p}\right) = 1$, we can change the condition into $p \equiv 1, 7 \pmod 8$, $\left(\frac{-7}{p}\right) = 1$. On the other hand, the quadratic reciprocity we proved had an intermediate consequence that $\left(\frac{(-1)^{\frac{q-1}{2}}q}{p}\right) = \left(\frac{p}{q}\right)$, so $\left(\frac{-7}{p}\right) = \left(\frac{p}{7}\right)$, so we get the desired result.

(6) If there is p where $X^2 + 14Y^2$ represents both p and $2p$, then there are two elementst $\alpha, \beta \in \mathbb{Z}[\sqrt{-14}]$ such that $N(\alpha) = p$, $N(\beta) = 2p$. Thus $\mathfrak{p} = (\alpha)$ is a prime ideal lying over p of norm p, and $(\beta) = \mathfrak{p}_2\mathfrak{p}'$ where $\mathfrak{p}_2 = (2, \sqrt{-14})$ is the unique prime ideal lying over 2, and $\mathfrak{p}'$ is another prime ideal lying over p of norm p. Note that either $\mathfrak{p} = \mathfrak{p}'$ or $\mathfrak{p}\mathfrak{p}' = (p)$, so $[\mathfrak{p}] = [\mathfrak{p}']^{\pm 1}$. On the other hand, as $\mathfrak{p}$ is principal, it follows that $[\mathfrak{p}'] = 1$, so this contradicts $1 = [(\beta)] = [\mathfrak{p}_2][\mathfrak{p}'] = [\mathfrak{p}_2]$ which is not true as we saw in the ntoes.

□

Solution to Exercise 10.4.

(1) Note that $[z]$ is the ideal class of a fractional ideal $\mathbb{Z} + \mathbb{Z} \cdot z$, so indeed $\overline{\mathbb{Z} + \mathbb{Z} \cdot (-\overline{z})} = \mathbb{Z} + \mathbb{Z} \cdot z$. Thus it suffices to show that $\mathfrak{a}\overline{\mathfrak{a}}$ is a principal ideal for any ideal $\mathfrak{a}$. We can prove this when $\mathfrak{a}$ is a prime ideal, and in that case the statement readily follows as we know how the rational prime splits; if p is inert, $\mathfrak{a}$ is already principal and $\overline{\mathfrak{a}} = \mathfrak{a}$, if p splits completely $\overline{\mathfrak{a}}\mathfrak{a} = (p)$, and if p is totally ramified, $\mathfrak{a} = \overline{\mathfrak{a}}$ and $\mathfrak{a}^2 = (p)$.

(2) Note that $-\overline{z} = \frac{b+\sqrt{d}i}{2a}$, so $z \mapsto -\overline{z}$ has the effect of changing the sign of b. Thus $[a, b, c]^2 = 1$ if and only if $[a, b, c] = [a, -b, c]$. This is the case when either $b = 0$ or $[a, -b, c]$ violates one of the representative conditions, $d = 4ac - b^2$, $-a < b \leq a$, $c \geq a$, and if $b < 0$, $c > a$. This can be the case when $b = a$ or when $c = a$ and $b > 0$.

We show the converse. If $b = 0$, then obviously $[a, b, c] = [a, -b, c]$. If $a = b$, this in terms of the complex number in $\mathbb{H}$ means $\mathrm{Re}(z) = \frac{1}{2}$, so $-\overline{z} = -1 + z$ which is again in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit. If $a = c$, this means that $d = 4a^2 - b^2$, so $|z| = \frac{b^2+d}{4a^2} = 1$. So $-\overline{z} = \frac{-1}{z} = Sz$ where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. In any case, $b = 0$, $a = b$ or $a = c$ implies $[a, b, c]^2 = 1$.

(3) Note that h_K is odd if and only if there is only one a, b, c with $[a, b, c]^2 = 1$, or either $b = 0$, $b = a$ or $c = a$. Let $K = \mathbb{Q}(\sqrt{-m})$ with m squarefree. Suppose that $m \equiv 3 \pmod 4$. Then $\mathrm{disc}(K) = -m = -d$. In particular d is odd and squarefree. If $d = 4ac - b^2$, then b must be odd. Thus $b = 0$ has no solution.

- If $b = a$, then $d = 4bc - b^2 = b(4c - b)$, where $c \geq b$, $b, c > 0$. Note that $d \equiv 3 \pmod 4$, so for any factor $m|d$, which must be odd, $\frac{d}{m} \equiv dm \equiv -m \pmod 4$, as $m^2 \equiv 1 \pmod 4$, so $\frac{d}{m} = 4x - m$ for some $x \in \mathbb{Z}$. In particular, if we let $m = 1$, then $d = 4x - 1$, and $x \geq 1$ as $d \geq 3$. This always give rise to at least one solution for $[a, b, c]^2 = 1$.

  Suppose d is a composite number, $d = p_1 \cdots p_r$ with $p_1, \cdots, p_r$ distinct. Suppose that p_1 is the smallest prime factor. Then for there to be no other solution of $[a, b, c]^2 = 1$, we need $\frac{p_2 \cdots p_r + p_1}{4} < p_1$, or $p_2 \cdots p_r < 3p_1$. Note that this is impossible if $r \geq 3$ as $p_2 \cdots p_r \geq p_2 p_3 \geq p_1^2 \geq 3p_1$ as $p_1 \geq 3$. If $r = 2$, then this can be possible precisely if $p_2 < 3p_1$.

- If $c = a$, then because of the solution in the case $b = a$, we must have no solution. The equation becomes $d = 4a^2 - b^2$ with $a > 0$, $a \geq b \geq 0$. Note $d = (2a - b)(2a + b)$. We know from the previous case that the only possible case is when either d is a prime or $d = p_1 p_2$ with $p_1 < p_2 < 3p_1$. If d is a prime, then $2a - b = 1$ and $2a + b = d$, whence $a = \frac{d+1}{4}$ and $b = \frac{d-1}{2}$, so $a \geq b$ implies $\frac{d+1}{4} \geq \frac{d-1}{2}$, or $d + 1 \geq 2d - 2$, or $d \leq 3$, so $d = 3$. But then this is included in the case $a = b$ as $a = 1$ and $b = 1$. Thus anyways in the case d a prime, $c = a$ adds no more solution.

  If $d = p_1 p_2$ with $p_1 < p_2 < 3p_1$, we may take $2a - b = p_1$ and $2a + b = p_2$ so that $a = \frac{p_1 + p_2}{4}$ and $b = \frac{p_2 - p_1}{2}$. Then $a \geq b$ means $\frac{p_1 + p_2}{4} \geq \frac{p_2 - p_1}{2}$, or $p_1 + p_2 \geq 2p_2 - 2p_1$, or $3p_1 \geq p_2$. This holds as $3p_1 > p_2$. This is also a different solution as $a > b$ precisely because $3p_1 > p_2$. Thus, d composite case will add an additional solution in $c = a$ case.

Thus we have seen that in the case of $m \equiv 1 \pmod 4$, h_K is odd if and only if m is a prime.

Now suppose $m \equiv 1, 2 \pmod 4$, so that $d = 4m$. In particular d is a multiple of 4, so b is even. Thus $b = 0$ has a solution whenever $m = ac$, $c \geq a$. Thus this automatically excludes the case when m is a composite number. If $m = 1$, then $[1, 0, 1]$ is a solution to $[a, b, c]^2 = 1$. It is easy to see that $m = 1$ case has h_K odd as $\mathbb{Q}(\sqrt{-1})$ is a PID. If $m = p$ is a prime, then $[1, 0, p]$ is a solution to $[a, b, c]^2 = 1$. Thus the other cases, $b = a$ or $c = a$, must have no solutions.

If $b = a$, then $4p = b(4c - b)$, with $c \geq b$, $b > c > 0$. If we take $b = 2$, then $c = \frac{p+1}{2}$ would be a solution if $\frac{p+1}{2} \geq 2$, or $p \geq 3$. Thus $m \geq 3$ cases are excluded, and we are only left with $\mathbb{Q}(\sqrt{-2})$, which we know is a PID. Thus we see that if $m \equiv 1, 2 \pmod 4$, then h_K is odd iff $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$.

□

Lecture 14.

Solution to Exercise 11.1.

(1) Straightforward.

(2) As $v(1) = v(1) + v(1)$, $v(1) = 0$. Thus, $v(n) \geq \min(v(1), \cdots, v(1)) = 0$ for all $n \in \mathbb{N}$. Also $v(1) = v(-1) + v(-1)$ implies $v(-1) = 0$, so $v(n) = v(-n)$ which means that $v(n) \geq 0$ for all $n \in \mathbb{Z}$. Let $I = \{n \in \mathbb{Z} \mid v(n) > 0\}$. This is an ideal as, if $n \in I$, then for all $x \in \mathbb{Z}$, $v(xn) = v(x) + v(n) \geq v(n) > 0$, so $xn \in I$. Furthermore, if $xy \in I$, $x, y \in \mathbb{Z}$, then $v(xy) = v(x) + v(y) > 0$, so $v(x), v(y) \geq 0$ implies that either $v(x)$ or $v(y)$ is strictly positive, so either x or y is in I. Thus, I is a prime ideal of $\mathbb{Z}$, $I = (p)$ for some rational prime p. This implies that $v(n) = 0$ for $n \in \mathbb{Z}$ coprime to p. Also, if $x \in I$, then $x = py$ for some $y \in \mathbb{Z}$, so $v(x) = v(p) + v(y) \geq v(p)$. Thus, $v(p)$ is the minimum possible positive value of $v(x)$. As v is normalized, $v(p) = 1$. From $v(p) = 1$ and $v(n) = 0$ for n coprime to p, we can determine $v(n)$ for all $n \in \mathbb{Q}$, and see that $v = v_p$.

□

Solution to Exercise 11.2.

We just define $g(a/s) = f(a)f(s)^{-1}$ for $a \in A$ and $s \in S$, which is a well-defined ring homomorphism (check) and thus exhibits the existence part. This formula is forced upon us as $f(a)$ and $f(s)$ are forced, so this shows the uniqueness part. □

Solution to Exercise 11.3.

(1) Note that $\mathbb{Z}_p$ is an integral domain (check). Let $v : \mathbb{Z}_p \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ be defined as $v(a_1, a_2, \cdots) = \min(n \mid a_n \neq 0 \pmod{p^n}) - 1$ (if there are no such n, we interpret it as ∞, which is exactly when $(a_1, a_2, \cdots) = 0$). This is a discrete valuation (check). Note also that $(p, p, \cdots)$ is not invertible and not zero, so $\mathbb{Z}_p$ is not a field. So, $\mathbb{Z}_p$ is a discrete valuation ring.

(2) We can just take $n^{-1} \pmod{p^k}$ for each k. By Question 2, we get a natural map $\mathbb{Z}_{(p)} \to \mathbb{Z}_p$. Since no nonzero element is sent to 0, this is an injection.

(3) Note that $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ is countable. On the other hand, $\mathbb{Z}_p$ is not countable; informally speaking, choosing a_n given a_{n-1} has p possibilities, so the cardinality of $\mathbb{Z}_p$ is $p^{\mathbb{N}}$, which is uncountable. More precisely, we have a surjective map $f : \mathbb{Z}_p \twoheadrightarrow 2^{\mathbb{N}}$, where $2^{\mathbb{N}}$ is the set of subsets of $\mathbb{N}$, where $n \in f(a_1, \cdots)$ if and only if $0 \leq a_n \leq p^{n-1}$ as a congruence class mod p^n. This is surjective since, given $I \subset \mathbb{N}$, we can take $(a_1, \cdots)$ to be $a_n = b_1 + \cdots + b_n p^{n-1}$, $b_i = \begin{cases} 0 & \text{if } i \in I \\ 1 & \text{if } i \notin I \end{cases}$. Thus the cardinality of $\mathbb{Z}_p$ is at least that of $2^{\mathbb{N}}$, which is uncountable. Thus $\mathbb{Z}_p$ is uncountable as desired. This shows that $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ can't be surjective, and also $\mathbb{Q}_p$, also uncountable, is strictly bigger than $\mathbb{Q}$.

□

Lecture 15.

Solution to Exercise 12.1.

We can deduce this if we show that the discriminant $\operatorname{disc}(K/L)$ is a unit ideal. Note that we can see K as $K = L(\frac{1+\sqrt{p}}{2}) = L(\frac{1+\sqrt{q}}{2})$. Note that $\operatorname{Gal}(K/L) = \{1, \sigma\}$ where $\sigma(\sqrt{p}) = -\sqrt{p}$ and $\sigma(\sqrt{q}) = -\sqrt{q}$. Thus if we let $e_1 = 1$, $e_2 = \frac{1+\sqrt{p}}{2}$ and $e_3 = \frac{1+\sqrt{q}}{2}$, then $D(e_1, e_2) = \det \begin{pmatrix} 1 & \frac{1+\sqrt{p}}{2} \\ 1 & \frac{1-\sqrt{p}}{2} \end{pmatrix}^2 = p$, and $D(e_1, e_3) = q$ by the same calculation. Since $\operatorname{disc}(K/L)$ contains the ideal generated by $D(e_1, e_2) = p$ and $D(e_1, e_3) = q$, this implies that $\operatorname{disc}(K/L)$ is the unit ideal. □

Solution to Exercise 12.2.

(1) Suppose not and say all prime factors of $f(n)$ are less than N. Let $f(X) = a_n X^n + \cdots + a_0$. Then

$$\frac{f(M!a_0)}{a_0} = a_n a_0^{n-1}(M!)^n + \cdots + a_2 a_0 (M!)^2 + a_1 M! + 1 \equiv 1 \pmod{M!}.$$

Thus, $\frac{f(M!a_0)}{a_0}$ is an integer that is $\equiv 1 \pmod{p}$ for any $p \leq M$. Note that $\lim_{m\to\infty} |f(m)| = \infty$. Thus, if we take $M \geq N$ to be very big, we have $\frac{|f(M!a_0)|}{a_0} \geq 2$, so that a prime factor of $\frac{f(M!a_0)}{a_0}$ must be not less than N, a contradiction.

From this, this implies that $f(X)$ has a root mod p for infinitely many rational primes p.

(2) Let $K = \mathbb{Q}(\alpha)$ for $\alpha \in \mathcal{O}_K$ which is possible by primitive root theorem. Let $f(X)$ be the minimal polynomial of α over $\mathbb{Q}$. Then we can use Dedekind's criterion for all but finitely many primes, and for then we see that there are infinitely many rational primes p such that $f(X) \pmod{p}$ has a linear factor, which implies that there is a prime ideal lying over p in $\mathcal{O}_K$ whose residue degree is 1.

(3) Suppose not, so there are finitely many prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_n \subset \mathcal{O}_L$ splitting completely in K. Let M be the Galois closure of K over $\mathbb{Q}$. By (2), and as $K/\mathbb{Q}$ is Galois, there are infinitely many primes p such that p splits completely in K. This implies that p splits completely in L and any prime of L lying over p splits completely in K. This contradicts the finiteness assumption.

□

Lectures 16 and 17.

Solution to Exercise 13.1.

(1) By symmetry, it is sufficient to prove that $D(b, r) \subset D(a, r)$. If $x \in D(b, r)$, this means $|b - x| < r$, but then $|a - x| \leq \max(|a - b|, |b - x|) < r$, so $x \in D(a, r)$, as desired.

(2) It is clear that $|\cdot|^{-1}((a,b))$ is open for $a<b$, so it is continuous.

(3) Note that as $|\cdot|$ is discrete, the condition $|a-x|<r$ is equivalent to $|a-x|\le r-\epsilon$ for some small $\epsilon>0$, as long as $|\cdot|$ does not take value in any number in between $r-\epsilon$ and r. Thus, an open disk is closed by (2).

(4) One side is obvious. If $\lim_{n\to\infty} a_n = 0$, then by the strong triangle inequality, $\sum_{n=1}^{N} a_n$ is a Cauchy sequence, so it converges.

□

Solution to Exercise 13.2.

(1) Obvious.

(2) Immediate from (1).

(3) Obvious.

(4) Note that formally e^x and $\log(1+x)$ give inverses to each other, and they are real inverses whenever they converge, so (2) and (3) imply the desired result.

□

Solution to Exercise 13.3.

(1) Note $[K:L]=n$ and $e_{K/L}\ge n$ so the result follows.

(2) Hint is self-explanatory, as $1^n=1$.

(3) If we let π_L be a uniformizer of L, $\frac{\pi_K^n}{\pi_L}$ is a unit in K. You can multiply π_L by a unit in L so that $\frac{\pi_K^n}{\pi_L}\equiv 1 \pmod{\pi_K}$, and then by (2) this itself is an n-th power of a unit, so we can modify π_K by this unit to obtain a uniformizer π_K' as desired.

□

Solution to Exercise 13.4.

(1) Obvious by Hensel's lemma (this is about finding the solution of X^2-u).

(2) We cannot directly use Hensel's lemma to X^2-u. Indeed it is necessary to have $u\equiv 1 \pmod 8$. On the other hand, if $u\equiv 1 \pmod 8$, then X^2-u has a solution mod 4, and the two solutions are not the same. Now we can use Hensel's lemma to lift two different mod 4 solutions to $\mathbb{Z}_2$. To be more precise, we want $X=1+4Y$ to be a square-root of u for $Y\in\mathbb{Z}_2$, which is the same as $(1+4Y)^2-u=0$, or $16Y^2+8Y+1-u=0$, or $2Y^2+Y+\frac{1-u}{8}=0$. This indeed has a root mod 2, as mod 2 this polynomial becomes $Y+\frac{1-u}{8}$. By Hensel's lemma, this means that $2Y^2+Y+\frac{1-u}{8}$ has a linear factor whose mod 2 reduction is $Y+\frac{1-u}{8}$, so this gives a root.

(3) The statement in Hint is clear. By (2), $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has 8 elements, $2^{\mathbb{Z}/2\mathbb{Z}}\times\{1,3,5,7 \pmod 8\}$, and the 7 nontrivial elements correspond to quadratic extensions. Note that anything corresponding to a multiple of 2 is ramified as the minimal polynomial is X^2-(that number), which is Eisenstein. For $a \equiv 3,7 \pmod 8$, the minimal polynomial for $\sqrt{a}$ is X^2-a, but if you plug $X+1$ we get $X^2+2X+1-a$, which is again Eisenstein, so $a \equiv 3,7 \pmod 8$ case is also ramified. The remaining case, $a \equiv 5 \pmod 8$ case, is actually unramified, namely $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified (this is a genuine field extension as 5 is not $1 \pmod 8$ by (2)). This is because, for example, if you take $z = x+y\sqrt{5} \in \mathbb{Q}_2(\sqrt{5})$, $x,y \in \mathbb{Q}_2$, then the canonical extension of the normalized discrete valuation v_2 on $\mathbb{Q}_2$ to $\mathbb{Q}_2(\sqrt{5})$ satisfies

$$v_2(z) = \frac{1}{2}v_2(N_{\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2}(z)) = \frac{v_2(x^2-5y^2)}{2},$$

and this is always an integer, namely $v_2(x^2-5y^2)$ is always a multiple of 2 whenever $x,y \in \mathbb{Q}_2$. This is because if $v_2(x) \neq v_2(y)$ then obvious, and if $v_2(x) = v_2(y)$ then without loss of generality we may assume $v_2(x) = v_2(y) = 0$, then $x^2-5y^2 \equiv 1-5 \equiv 4 \pmod 8$, so $v_2(x^2-5y^2) = 2$. Thus only $\mathbb{Q}_2(\sqrt{5})$ is unramified and all the other quadratic extensions ($\mathbb{Q}_2(\sqrt{\pm 2})$, $\mathbb{Q}_2(\sqrt{\pm 6})$, $\mathbb{Q}_2(\sqrt{3})$, $\mathbb{Q}_2(\sqrt{-1})$) are ramified.

□

Lecture 18.

Solution to Exercise 14.1.

(1) Let $\{v_i\}_{i\in I}$ be an L-basis of K_1. We define f to be

$$f(v_i \otimes 1) = f_1(v_i),$$

and extend K_2-linearly to define f for every element in $K_1 \otimes_L K_2$. This in particular implies that $f(x\otimes y) = f_1(x)f_2(y)$ for every $x \in K_1, y \in K_2$, which in particular implies that the construction is independent of the choice of basis. It is clear to see that this is an L-algebra homomorphism. This is unique because the algebra homomorphism structure forces the value of f on every element.

(2) You apply the universal property for S to $K_1 \otimes_L K_2$, you get a homomorphism $S \to K_1 \otimes_L K_2$. Vice versa, you get a homomorphism $K_1 \otimes_L K_2 \to S$. Their compositions, $S \to K_1 \otimes_L K_2 \to S$ and $K_1 \otimes_L K_2 \to S \to K_1 \otimes_L K_2$, must be the identities as the universal property gives a unique homomorphism. Thus, $S \cong K_1 \otimes_L K_2$.

(3) It is sufficient to show that the elements of the above form multiplied by $x \otimes y$ is still an element of the above forms, which is immediate.

(4) If there is R with $f_1, f_2 : K_1, K_2 \to R$, then define $f : X \to R$ as just $f(x\otimes y) = f_1(x)f_2(y)$. This is unique and there is nothing to think about. Now we need to show that $\ker f \supset I$. This is just showing things like $f_1(v_1+v_2)f_2(w)-f_1(v_1)f_2(w)-f_1(v_2)f_2(w) =$

0, etc, which are obvious. Thus, this induces a morphism $f : X/I \to R$. Since the value of f is again forced by the sturcture of algebra homomorphism, this implies that X/I satisfies the universal property.

□

Solution to Exercise 14.2.

(1) If $K = L(\zeta_n)$ with $(n, p) = 1$, then as $X^n - 1$ has no repeated roots mod p, the minimal polynomial of ζ_n over L, which must divide $X^n - 1$, has no repeated roots mod p, which implies that K/L is unramified. Conversely, if K/L is an unramified extension, then $k_K = k_L(\alpha)$ where $\alpha^{\#k_K - 1} = 1$. As $\#k_K - 1$ is coprime to p, one can lift α to $\zeta \in K$ such that $\zeta^{\#k_K - 1} = 1$. Note that $L(\zeta)/L$ is unramified with $k_{L(\zeta)} = k_K$, so it follows that $K = L(\zeta)$.

(2) Immediate from (1).

□

Solution to Exercise 14.3.

(1) Note that 2 is totally ramified in $\mathbb{Q}(\alpha)$ because α's minimal polynomial over $\mathbb{Q}$ is $X^4 - 2$, which is Eisenstein at 2. Similarly, 2 is totally ramified in $\mathbb{Q}(i)$ because we know how primes factorize there.

(2) We follow the **Hint**. Suppose $\mathbb{Q}_2(i) \subset \mathbb{Q}_2(\alpha)$. Then, $\sigma(\alpha) = i^n\alpha$ for some $n = 1, 2, 3$, but $\sigma^2 = 1$, so $i^{2n} = 1$, which implies that $n = 2$, or $\sigma(\alpha) = -\alpha$. This implies that $\sigma(\alpha^2) = \alpha^2$, so $\alpha^2 = \sqrt{2} \in \mathbb{Q}_2(i) = \mathbb{Q}_2(\alpha)^{\sigma=1}$. But we have seen that $\mathbb{Q}_2(\sqrt{-1})$ and $\mathbb{Q}_2(\sqrt{2})$ are not isomorphic by Exercise 13.4, because -1 and 2 are not the same as elements of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. So a contradiction.

(3) (2) implies that $\mathbb{Q}_2(\alpha, i)$ is a field of degree 8 over $\mathbb{Q}_2$. Thus, $K_2 \supset \mathbb{Q}_2(\alpha, i)$ must be equal to each other, so a field.

(4) We follow the **Hint**. Suppose not. Then, as $e_{K_2/\mathbb{Q}_2}$ is divisible by $e_{\mathbb{Q}_2(\alpha)/\mathbb{Q}_2}$, and as α is Eisenstein, $e_{\mathbb{Q}_2(\alpha)/\mathbb{Q}_2} = 4$, which implies that $e_{K_2/\mathbb{Q}_2}$ is either 4 or 8, and the 8 case is what we are excluding as assumption. Then, $f = 2$. This means that there is a maximal unramified extension in $K_2/\mathbb{Q}_2$, which is a quadratic extension of $\mathbb{Q}_2$. As $K_2/\mathbb{Q}_2$ is Galois with the same expression as $\mathrm{Gal}(K/\mathbb{Q})$, namely generated by the same s and t, we know precisely what quadratic fields appear as subextensions. Namely, they correspond to index 2 (=order 4) subgroups of D_4. By enumerating the three index two subgroups, we see that the quadratic subfields are $\mathbb{Q}_2(i)$, $\mathbb{Q}_2(\sqrt{2})$ and $\mathbb{Q}_2(\sqrt{-2})$. They are all ramified over $\mathbb{Q}_2$, so a contradiction.

(5) Note that such p is unramified in $\mathbb{Q}(\alpha)$. Since K is the Galois closure of $\mathbb{Q}(\alpha)$, K is the compositum of all $\mathbb{Q}(\alpha')$ for α' a conjugate of α. As p being unramified in $\mathbb{Q}(\alpha)$ only depends on the minimal polynomial of α (the discriminant is computed using the minimal polynomial), p is unramified in $\mathbb{Q}(\alpha')$ for all conjugates α', and therefore p is unramified in their compositum, K. More concretely, K is the compositum of $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i\sqrt[4]{2})$, and in both number fields, p is unramified, so it is unramified in K.

□

Lecture 19.

Solution to Exercise 15.1.

(1) An embedding $i : K \hookrightarrow \mathbb{C}$ lies over $j : L \hookrightarrow \mathbb{C}$ if j is the restriction of i on $L \subset K$.

(2) As $\mathbb{C}/\mathbb{R}$ is ramified, this means the following. If an archimedean prime $i : L \hookrightarrow \mathbb{C}$ is a complex embedding, then any archimedean prime of K lying over i is necesarily a complex embedding, so it is automatically unramified. If i is a real embedding, then we want every archimedean prime of K lying over i to be a real embedding.

(3) The only thing we need to prove is that $\mathbb{R}^\times/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ via $\mathrm{Art}_{\mathbb{R}}$. As $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$ is precisely $\mathbb{R}_{>0}$, we get the result.

(4) The local existence theorem says that

$$\{\text{Open finite index subgroups of } \mathbb{R}^\times\} \leftrightarrow \{\text{Finite abelian extensions of } \mathbb{R}\}.$$

Note that the finite extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$, and they are all abelian. Correspondingly, if $G \leq \mathbb{R}^\times$ is an open finite index subgroup, then firstly $1 \in G$, and an open neighborhood of 1 is in G. Therefore, there is some $\lambda > 1$ such that every real number between λ and 1 is in G. Taking the integer powers of these, we see that all positive real numbers must be in G. Then we see that there are exactly two possibilities for open finite index subgroups of $\mathbb{R}^\times$, either $\mathbb{R}^\times$ or $\mathbb{R}_{>0}$. We see that $\mathbb{R}^\times$ corresponds to $\mathbb{R}$ and $\mathbb{R}_{>0}$ corresponds to $\mathbb{C}$.

□

Lectures 20 and 21.

Solution to Exercise 16.1.

(1) The Minkowski bound is < 2, so $h_L = 1$.

(2) Note that $K = L(\sqrt{-1})$, so in this perspective $1, \sqrt{-1} \in \mathcal{O}_K$ is an L-basis of K, so $\mathrm{disc}(K/L)$ contains

$$\det \begin{pmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{pmatrix}^2 = -4 \in \mathrm{disc}(K/L).$$

On the other hand, $K = L(\sqrt{-3})$, so in this perspective $1, \frac{1+\sqrt{-3}}{2} \in \mathcal{O}_K$ is an L-basis of K, so $\mathrm{disc}(K/L)$ contains

$$\det \begin{pmatrix} 1 & \frac{1+\sqrt{-3}}{2} \\ 1 & \frac{1-\sqrt{-3}}{2} \end{pmatrix}^2 = -3 \in \mathrm{disc}(K/L).$$

So, $4 - 3 \in \mathrm{disc}(K/L)$, which means that $\mathrm{disc}(K/L) = (1)$ is the unit ideal, so all finite prime ideals of $\mathcal{O}_L$ is unramified in K.

(3) It's consistent because the archimedean primes of L ramify in K.

□

Solution to Exercise 16.2.

(1) Note that $J_{\mathbb{Q}}^m = \{(n) \ : \ n \in \mathbb{N},\ (n,m) = 1\}$, and $\mathrm{Art}^m_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ sends $(n) \in J_{\mathbb{Q}}^m$ to $n \in (\mathbb{Z}/m\mathbb{Z})^\times$, so $\ker \mathrm{Art}^m_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} = \{(n) \ : \ n \in \mathbb{N},\ n \equiv 1 \pmod m\}$. If $m = p_1^{e_1} \cdots p_r^{e_r}$ is a prime factorization, then

$$\ker \mathrm{Art}^m_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} = \{(n) \ : \ n \in \mathbb{N},\ n \equiv 1 \pmod m\} = \{(n) \ : \ n > 0,\ p_i^{e_i} | (n-1)\} = P_{\mathbb{Q}}^{m\infty}.$$

By the global existence theorem, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(m\infty)$ is the ray class field of modulus $m\infty$. This implies that $\mathfrak{f}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} | m\infty$. Note that $\mathfrak{f}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ is divisible by ∞, as $\mathbb{Q}(\zeta_m)$ has no real prime.

(2) Note that the ray class field $\mathbb{Q}(\mathfrak{f}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}})$ contains $\mathbb{Q}(\zeta_m)$, so $\mathbb{Q}(\zeta_n)$ contains $\mathbb{Q}(\zeta_m)$. Since $v_2(m) \neq 1$, $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ with $n|m$ implies that $n = m$.

(3) For m odd, $-\zeta_m$ is $2m$-th root of unity, so $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$. So (1), (2) implies the conclusion.

(4) Note that, if $N_{K/\mathbb{Q}_2}(K^\times) \supset 1 + 2\mathbb{Z}_2$, then $1 + 2\mathbb{Z}_2 = \mathbb{Z}_2^\times$, so $N_{K/\mathbb{Q}_2}(K^\times) \supset \mathbb{Z}_2^\times$, so $K/\mathbb{Q}_2$ is unramified. Thus, either $\mathfrak{f}_{K/\mathbb{Q}_2} = 0$ or $\mathfrak{f}_{K/\mathbb{Q}_2} \geq 2$.

(5) (3) and (4) imply that $\mathbb{Q}(m\infty) = \mathbb{Q}(\zeta_m)$. From this, $\mathbb{Q}(m) \subset \mathbb{Q}(\zeta_m)^+$. Note that $\mathrm{Cl}_K^m = J_{\mathbb{Q}}^m / P_{\mathbb{Q}}^m$, where $P_{\mathbb{Q}}^m = \{(n) \ : \ p_i^{e_i} | (n-1)\}$, so $\mathrm{Cl}_K^m \cong (\mathbb{Z}/m\mathbb{Z})^\times / \{\pm 1\}$, which implies that the ray class field of modulus m, $\mathbb{Q}(m)$, is index 2 subfield of $\mathbb{Q}(m\infty) = \mathbb{Q}(\zeta_m)$, which implies that $\mathbb{Q}(m) = \mathbb{Q}(\zeta_m)^+$.

□

Solution to Exercise 16.3.

(1) Note that all archimedean primes of K are complex, so K'/K is unramified in archimedean primes. Moreover, $K' = K(\sqrt{2})$ means that all primes of K coprime to 2 are unramified in K'. Moreover, $K' = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$, and 2 splits completely in $\mathbb{Q}(\sqrt{-7})$, as $x^2 + x + 2$ has a root mod 2. As 2 is totally ramified in $\mathbb{Q}(\sqrt{2})$, for $K'/\mathbb{Q}$, $e = 2$ and $f = 2$, so $g = 1$. As 2 is totally ramified in $\mathbb{Q}(\sqrt{-14})$, for the unique prime $\mathfrak{p}_2$ of K lying over 2, in K'/K, $e = 1, f = 2, g = 1$, so that K'/K is unramified in $\mathfrak{p}_2$. All in all, K'/K is unramified.

(2) Note that the identity in the problem shows that $K'' = K'(\sqrt{2\sqrt{2}-1}) = K'(\sqrt{-2\sqrt{2}-1})$. Note that these two descriptions imply that $\mathrm{disc}(K''/K') \ni 4(2\sqrt{2}-1), 4(-2\sqrt{2}-1)$, so $8 \in \mathrm{disc}(K''/K)$, so in particular any prime coprime to 2 is unramified in K''/K' (including the archimedean primes, as all archimedean primes are already complex).

(3) Note that $K'' = K'(\alpha)$. The discriminant of the polynomial $X^2 - (1+\sqrt{2})X + 1$ is $(1+\sqrt{2})^2 - 4 = 2\sqrt{2} - 1$, so in particular $2\sqrt{2}-1 \in \mathrm{disc}(K''/K')$. Since 7 is a multiple of $2\sqrt{2}-1$, $8-7 \in \mathrm{disc}(K''/K')$, which implies that $\mathrm{disc}(K''/K')$ is a unit ideal, so K''/K' is unramified.

(4) Note that we have four automorphisms K''/K,

$$\sigma_0 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{2\sqrt{2}-1} \mapsto \sqrt{2\sqrt{2}-1},$$

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{2\sqrt{2}-1} \mapsto -\sqrt{2\sqrt{2}-1},$$

$$\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{2\sqrt{2}-1} \mapsto \sqrt{-2\sqrt{2}-1},$$

$$\sigma_3 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{2\sqrt{2}-1} \mapsto -\sqrt{-2\sqrt{2}-1}.$$

Indeed one checks that these are four different automorphisms of K'' over K, so K''/K is Galois. Since any order four group is abelian, K''/K is abelian. Since K''/K is unramified, $H_K = K''$.

(5) Note that we can use $\alpha = \sqrt{2\sqrt{2}-1}$, whose minimal polynomial is $(\alpha^2+1)^2 = 8$, or $\alpha^4 + 2\alpha^2 - 7 = 0$. Its discriminant has prime factors in $2, 7$, so the statement follows.

□

Solution to Exercise 16.4.

Note that by Hint

$$1 = (bc^{-1}, ac^{-1}) = (b,a)(b,c^{-1})(c^{-1},a)(c^{-1},c^{-1}) = (b,a)(b,c)^{-1}(c,a)^{-1}(-c^{-1},c^{-1})(-1,c^{-1})$$

$$= (b,a)(c,b)(a,c)((-1)^n, c^{-1}) = (b,a)(a+b,b)(a,a+b),$$

as $((-1)^n, c^{-1}) = (-1,c^{-1})^n = 1$, so $(a,b) = (a,a+b)(a+b,b)$. □

Solution to Exercise 16.5.

(1) Note that $e = p-1$, so $(1+\pi^2\mathcal{O}_{K_\mathfrak{p}}, \times) \cong (\pi^2\mathcal{O}_{K_\mathfrak{p}}, +)$. Also, $(1+\pi^{p+1}\mathcal{O}_{K_\mathfrak{p}}, \times) \cong (\pi^{p+1}\mathcal{O}_{K_\mathfrak{p}}, +)$. Since $p(\pi^2\mathcal{O}_{K_\mathfrak{p}}, +) = (\pi^{p+1}\mathcal{O}_{K_\mathfrak{p}}, +)$ ($(p) = (\pi)^{p-1}$), so $(1+\pi^2\mathcal{O}_{K_\mathfrak{p}}, \times)^p = (1+\pi^{p+1}\mathcal{O}_{K_\mathfrak{p}}, \times)$.

(2) For $i+j \geq p-1$, e_{i+j} is a p-th power by (1). Thus, by Question 4, $(e_i, \pi^i e_j) = (e_i, e_{i+j})(e_{i+j}, \pi^i e_j) = 1$. Thus, $1 = (e_i, \pi^i e_j) = (e_i, \pi^i)(e_i, e_j)$. Since $(e_i, \pi^i) = (1-\pi^i, \pi^i) = 1$, we get the result.

(3) Hint is pretty much self-explanatory; the only issue is that x_j converges, which is also quite obvious as $e_j \equiv 1 \pmod{\pi^j}$ and $j \to \infty$.

(4) Note that, as K has only complex primes, the power reciprocity implies that $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = (a,b)_{\mathfrak{p}}$, so we need to show that $(a,b)_{\mathfrak{p}} = 1$. Note that by (3), $a = e_{\frac{p+1}{2}}^{m_{\frac{p+1}{2}}} \cdots e_p^{m_p} c^p$, $b = e_{\frac{p+1}{2}}^{n_{\frac{p+1}{2}}} \cdots e_p^{n_p} d^p$ for some $c, d \in \mathcal{O}_K^\times$, so

$$(a,b)_{\mathfrak{p}} = (e_{\frac{p+1}{2}}^{m_{\frac{p+1}{2}}} \cdots e_p^{m_p} c^p, e_{\frac{p+1}{2}}^{n_{\frac{p+1}{2}}} \cdots e_p^{n_p} d^p) = (e_{\frac{p+1}{2}}^{m_{\frac{p+1}{2}}} \cdots e_p^{m_p}, e_{\frac{p+1}{2}}^{n_{\frac{p+1}{2}}} \cdots e_p^{n_p})$$

$$= \prod_{i,j=\frac{p+1}{2}}^{p} (e_i, e_j)_{\mathfrak{p}}^{m_i n_j} = 1,$$

by (2), as desired.

□

Lecture 22.

Solution to Exercise 17.1.

(1) Let $u = \left\lfloor \frac{\sqrt{d}+1}{2} \right\rfloor + \frac{\sqrt{d}-1}{2}$. Then $\overline{u} = \left\lfloor \frac{\sqrt{d}+1}{2} \right\rfloor - \frac{\sqrt{d}+1}{2}$. As $\sqrt{d} > 1$, $u > \left\lfloor \frac{\sqrt{d}+1}{2} \right\rfloor > \left\lfloor \frac{2}{2} \right\rfloor = 1$. On the other hand, $-\overline{u} = \frac{\sqrt{d}+1}{2} - \left\lfloor \frac{\sqrt{d}+1}{2} \right\rfloor$, so $0 < -\overline{u} < 1$ (this is never 0 because $\frac{\sqrt{d}+1}{2}$ is never an integer), which implies that $-1 < \overline{u} < 0$, so that u has a purely periodic continued fraction.

(2) The proof is exactly the same as in the case of $d \not\equiv 1 \pmod 4$ case, noting that, for $u = x + y\frac{\sqrt{d}+1}{2}$ with $N(u) = \pm 1$, $x, y > 0$, we have $\left(x + y\frac{\sqrt{d}+1}{2}\right)\left(x + y\frac{-\sqrt{d}+1}{2}\right) = \left(x + \frac{y}{2}\right)^2 - \frac{dy^2}{4} = x^2 + xy + \frac{1-d}{4}y^2 = \pm 1$, so that

$$\left|\frac{\sqrt{d}-1}{2} - \frac{x}{y}\right| = \frac{\left|x - \frac{\sqrt{d}-1}{2}y\right|}{y} = \frac{\left(x + y\frac{\sqrt{d}+1}{2}\right)\left|x + y\frac{-\sqrt{d}+1}{2}\right|}{y\left(x + y\frac{\sqrt{d}+1}{2}\right)} = \frac{1}{y\left(x + y\frac{\sqrt{d}+1}{2}\right)}.$$

□

Solution to Exercise 17.2.

(1) The first statement is clear as the units of K are $\pm\epsilon^n$ and $N_{K/\mathbb{Q}}(\pm\epsilon^n) = N_{K/\mathbb{Q}}(\epsilon)^n$. If $\operatorname{disc}(K) = 4d$, then a unit is of the form $x + \sqrt{d}y$, and $N_{K/\mathbb{Q}}(x + \sqrt{d}y) = x^2 - dy^2$, so in this case $x^2 - dy^2 = -1$ has integer solutions, from which one gets integer solutions to $x^2 - 4dy^2 = -4$ by doubling x. If $\operatorname{disc}(K) = d$ (i.e. $d \equiv 1 \pmod 4$), then a unit is of the form $\frac{x+\sqrt{d}y}{2}$, $x \equiv y \pmod 2$, so $N_{K/\mathbb{Q}}(\frac{x+\sqrt{d}y}{2}) = \frac{x^2-dy^2}{4}$, so in this case $x^2 - dy^2 = -4$ has integer solutions.

(2) If $p|d$, $p \equiv 3 \pmod 4$, then if $N(K) = -1$, then $x^2 \equiv -4 \pmod p$ has a solution, which is impossible as $\left(\frac{-1}{p}\right) = -1$.

(3) Note that $\mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$ is an isomorphism if and only if $P_K^{\mathfrak{m}} \to P_K$ is an isomorphism. This means that, for any principal ideal (a), $a \in K^\times$, there exists a generator $b \in (a)$ such that $b, \overline{b} > 0$, where, for $b = x + \sqrt{d}y$, $\overline{b} = x - \sqrt{d}y$. By possibly replacing a with $-a$, we can assume that $a > 0$. If $\overline{a} < 0$, then this means that there exists a unit $u \in \mathcal{O}_K^\times$ such that $u > 0$ and $\overline{u} < 0$; the existence of such unit is equivalent to $\mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$ being isomorphism. Note that if there exists a unit v of norm -1, then either v or $-v$ is positive, and the positive unit will exactly have this property, as $v\overline{v} = -1$. On the other hand, if all units are of norm 1, then v and $\overline{v}$ will have the same sign for every unit v, so there is no such unit. Thus, this establishes the equivalence.

(4) By (2) and (3), if d has a prime factor $\equiv 3 \pmod 4$, then $\mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}(K)$, which is surjective, is not an isomorphism, so $K(\mathfrak{m})$ is strictly bigger than H_K. As $\mathfrak{m}_f = 1$, the ray class field $K(\mathfrak{m})$ satisfies the desired properties of L in the problem.

□

Lectures 23 and 24.

Solution to Exercise 18.1.

(1) Note that

$$\int_0^\infty y^{\frac{s}{2}} \frac{\widetilde{\theta}_\chi(iy)}{2} \frac{dy}{y} = \sum_{n \geq 1} \chi(n) n \int_0^\infty y^{\frac{s}{2}} \sqrt{y} e^{-\pi n^2 y} \frac{dy}{y} = \sum_{n \geq 1} \chi(n) n \Gamma\left(\frac{s+1}{2}\right) (\pi n^2)^{-\frac{s+1}{2}}$$

$$= \pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right) L(s, \chi).$$

(2) Note

$$\widetilde{\theta}_\chi(iy) = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n \in \mathbb{Z}} (mn + b) \sqrt{y} e^{-\pi (mn+b)^2 y} = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n \in \mathbb{Z}} f_{y,b}(n),$$

where $f_{y,b}(x) = (mx + b)\sqrt{y} e^{-\pi (mx+b)^2 y}$. By Poisson summation,

$$\widetilde{\theta}_\chi(iy) = \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n \in \mathbb{Z}} \widehat{f_{y,b}}(n).$$

Note that $f_{y,b}(x) = f(\sqrt{y}(mx + b))$, where $f(x) = xe^{-\pi x^2}$. As $\widehat{f}(x) = -ixe^{-\pi x^2}$,

$$\widehat{f_{y,b}}(x) = \frac{e^{\frac{2\pi i x b}{m}}}{m\sqrt{y}} \widehat{f}\left(\frac{x}{m\sqrt{y}}\right) = -i \frac{e^{\frac{2\pi i x b}{m}}}{m\sqrt{y}} \frac{x}{m\sqrt{y}} e^{-\frac{\pi x^2}{m^2 y}} = -\frac{ixe^{\frac{2\pi i x b}{m}}}{m^2 y} e^{-\frac{\pi x^2}{m^2 y}}.$$

Thus

$$\widetilde{\theta}_\chi(iy) = \sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) \sum_{n\in\mathbb{Z}} \left(-\frac{ine^{\frac{2\pi inb}{m}}}{m^2 y} e^{-\frac{\pi n^2}{m^2 y}} \right).$$

Note that

$$-\frac{iG(\chi)}{m\sqrt{y}} \widetilde{\theta}_{\overline{\chi}} \left(\frac{i}{m^2 y} \right) = -\frac{iG(\chi)}{m\sqrt{y}} \sum_{n\in\mathbb{Z}} \overline{\chi}(n) n \sqrt{\frac{1}{m^2 y}} e^{-\frac{\pi n^2}{m^2 y}}.$$

Again the identity follows from

$$\sum_{b\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(b) e^{\frac{2\pi inb}{m}} = G(\chi)\overline{\chi}(n).$$

□

Solution to Exercise 18.2.

(1) Really the whole sum is bounded by $\sum_p \sum_{n=1}^\infty p^{-ns} = \sum_p \frac{p^{-s}}{1-p^{-s}} < 2\sum_p p^{-s}$, so the right hand side is absolutely convergent. This thing by the similar reason uniformly converges on the region $\mathrm{Re}(s) > \sigma_0$ for any $\sigma_0 > 1$, so the right hand side defines a holomorphic function on $\mathrm{Re}(s) > 1$.

(2) Note that $\log L(s,\chi) - \sum_p \chi(p)p^{-s} = \sum_p \sum_{n=2}^\infty \frac{\chi(p)^n p^{-ns}}{n}$, so this difference is bounded above by

$$\sum_p \sum_{n=2}^\infty p^{-ns} = \sum_p \frac{p^{-2s}}{1-p^{-s}} < 2\sum_p \frac{1}{p^2} < 2\zeta(2).$$

(3) (2) implies the desired inequality. Note that $\log L(s,\chi)$, as $s \to 1^+$, goes to a finite number if $\chi \neq \mathbf{1}_n$ as $L(1,\chi) \neq 0$, and goes to $+\infty$ if $\chi = \mathbf{1}_n$. Thus, $\sum_{p \text{ prime}, p \equiv a \pmod n} p^{-s}$ diverges as $s \to 1^+$, which means that there are infinitely many primes that are $\equiv a \pmod n$.

□

Solution to Exercise 18.3.

(1) This is immediate as π_1 is a cube mod π_2 and vice versa.

(2) Note that $G(\chi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}} \equiv \left(\frac{p}{q}\right)\left(\frac{\pi}{q}\right) \pmod q$. Since any integer is a cube mod q, $\left(\frac{p}{q}\right) = 1$, so the equality follows.

(3)

$$G(\chi)^{q^2} \equiv \sum_{a=1}^{p-1} \chi(a)^{q^2} e^{\frac{2\pi iaq^2}{p}} = \sum_{a=1}^{p-1} \chi(a) e^{\frac{2\pi iaq^2}{p}} \pmod q.$$

(4) We have $\sum_{a=1}^{p-1}\chi(a)e^{2\pi iaq^2/p} = G(\chi)\chi(q^2)^{-1} = G(\chi)\chi(q)$, so (2) and this gives the cubic reciprocity.

□

Solution to Exercise 18.4.

(1) This is just $B_{n,\mathbf{1}} = B_n$.

(2) Note that $pB_n = \sum_{a=1}^{p}\sum_{i=0}^{n}\binom{n}{i}p^iB_ia^{n-i}$. So

$$pB_n = \sum_{a=1}^{p}(p^nB_n + a^n + \sum_{i=1}^{n-1}\binom{n}{i}p^{i-1}(pB_i)a^{n-i}),$$

so

$$(p-p^{n+1})B_n \in \mathbb{Z}_p,$$

so $pB_n \in \mathbb{Z}_p$.

(3) Note that

$$(p-p^{n+1})B_n \equiv \sum_{a=1}^{p}a^n + \sum_{a=1}^{p}npB_1a^{n-1} \equiv \sum_{a=1}^{p}a^n \pmod p.$$

Here, we use $v_p(npB_1) \geq 1$; this is obvious if p is odd, and if $p=2$, this is true because n is even. If n is not a multiple of $p-1$, $\sum_{a=1}^{p}a^n$ is a multiple of p. If not, $\sum_{a=1}^{p}a^n \equiv p-1 \pmod p$. Since $1-p^n \equiv 1 \pmod p$, $pB_n \equiv -1 \pmod p$.

□

Lecture 25.

Solution to Exercise 19.1.

Let $K = \mathbb{Q}(\sqrt{-21})$. Then $\mathrm{disc}(K) = -84$. Then

$$84h_K = \pm\sum_{a=1}^{84}\chi_{-84}(a)a = \pm(\chi_{-84}(1)+5\chi_{-84}(5)+11\chi_{-84}(11)+13\chi_{-84}(13)+17\chi_{-84}(17)+19\chi_{-84}(19)$$

$$+23\chi_{-84}(23)+25\chi_{-84}(25)+29\chi_{-84}(29)+31\chi_{-84}(31)+37\chi_{-84}(37)+41\chi_{-84}(41)+43\chi_{-84}(43)$$

$$+47\chi_{-84}(47)+53\chi_{-84}(53)+55\chi_{-84}(55)+59\chi_{-84}(59)+61\chi_{-84}(61)+65\chi_{-85}(65)+67\chi_{-84}(67)$$

$$+71\chi_{-84}(71)+73\chi_{-84}(73)+79\chi_{-84}(79)+83\chi_{-84}(83))$$

$$=\pm((1-83)\chi_{-84}(1)+(5-79)\chi_{-84}(5)+(11-73)\chi_{-84}(11)+(13-71)\chi_{-84}(13)+(17-67)\chi_{-84}(17)$$

$$+(19-65)\chi_{-84}(19)+(23-61)\chi_{-84}(23)+(25-59)\chi_{-84}(25)+(29-55)\chi_{-84}(29)+(31-53)\chi_{-84}(31)$$

$$+(37-47)\chi_{-84}(37)+(41-43)\chi_{-84}(41))$$

$$= \pm(-82\chi_{-84}(1)-74\chi_{-84}(5)-62\chi_{-84}(11)-58\chi_{-84}(13)-50\chi_{-84}(17)-46\chi_{-84}(19)-38\chi_{-84}(23)$$
$$-34\chi_{-84}(25) - 26\chi_{-84}(29) - 22\chi_{-84}(31) - 10\chi_{-84}(37) - 2\chi_{-84}(41))$$
$$= \pm(-82 - 74\left(\frac{-84}{5}\right) - 62\left(\frac{-84}{11}\right) - 58\left(\frac{-84}{13}\right) - 50\left(\frac{-84}{17}\right) - 46\left(\frac{-84}{19}\right) - 38\left(\frac{-84}{23}\right)$$
$$-34 - 26\left(\frac{-84}{29}\right) - 22\left(\frac{-84}{31}\right) - 10\left(\frac{-84}{37}\right) - 2\left(\frac{-84}{41}\right))$$
$$= \pm(-82 - 74\left(\frac{1}{5}\right) - 62\left(\frac{4}{11}\right) - 58\left(\frac{7}{13}\right) - 50\left(\frac{1}{17}\right) - 46\left(\frac{11}{19}\right) - 38\left(\frac{8}{23}\right)$$
$$-34 - 26\left(\frac{3}{29}\right) - 22\left(\frac{9}{31}\right) - 10\left(\frac{27}{37}\right) - 2\left(\frac{-2}{41}\right))$$
$$= \pm(-82-74-62-58\left(\frac{13}{7}\right)-50+46\left(\frac{19}{11}\right)-38\left(\frac{2}{23}\right)-34-26\left(\frac{29}{3}\right)-22-10\left(\frac{3}{37}\right)-2)$$
$$= \pm(-326 - 58\left(\frac{-1}{7}\right) + 46\left(\frac{8}{11}\right) - 38 - 26\left(\frac{2}{3}\right) - 10\left(\frac{37}{3}\right))$$
$$= \pm(-364 + 58 + 46\left(\frac{2}{11}\right) + 26 - 10\left(\frac{1}{3}\right))$$
$$= \pm(-280 - 46 - 10) = 336.$$

Thus, $h_K = \frac{336}{84} = 4$. □

Solution to Exercise 19.2.

(1) This is immediate as $\epsilon_K = a + b\sqrt{d}$ where $a, b > 0$.

(2) By (1),

$$h_K = \frac{1}{\log|\epsilon_K|}\left|\sum_{a=1}^{2d}\chi_{4d}(a)\log\left(\sin\left(\frac{\pi a}{4d}\right)\right)\right| < \frac{1}{\log\sqrt{d}}\sum_{1\le a\le 2d,\ a\text{ odd}}\left|\log\left(\sin\left(\frac{\pi a}{4d}\right)\right)\right|.$$

Since $\sin\left(\frac{\pi a}{4d}\right) < 1$, $\left|\log\left(\sin\left(\frac{\pi a}{4d}\right)\right)\right| = -\log\left(\sin\left(\frac{\pi a}{4d}\right)\right)$. So, $h_K < -\frac{d}{\log\sqrt{d}}\log\left(\sin\left(\frac{\pi}{4d}\right)\right)$.

(3) For $0 < x < 1$, $\sin(\frac{\pi}{2}x) > x$ because $\sin(\frac{\pi}{2}x)$ is concave downward. Thus

$$\log(\sin(\pi/4d)) > \log(1/2d) = -\log(2d),$$

so

$$h_K < d\frac{\log(2d)}{\log\sqrt{d}} = d\frac{\log(2)+\log(d)}{\frac{1}{2}\log(d)} < 4d.$$

□

Lecture 26.

Solution to Exercise 20.1.

(1) Let $f(X,Z)[X^m]$ be the formal power series in Z arising as the X^m-coefficient of $f(X,Z)$. Then

$$\sum_{n=0}^{\infty} \frac{B_n(X)[X^m]}{n!} Z^n = \sum_{n=0}^{\infty} \frac{\binom{n}{n-m} B_{n-m}}{n!} Z^n = \sum_{n=0}^{\infty} \frac{\binom{n+m}{n} B_n}{(n+m)!} Z^{n+m},$$

$$\left(\frac{Ze^{XZ}}{e^Z - 1} \right) [X^m] = \frac{Z^m}{m!} \frac{Z}{e^Z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!m!} Z^{n+m}.$$

They coincide, which is what we want.

(2) Note that

$$\sum_{n=0}^{\infty} \frac{B_n(X+1) - B_n(X)}{n!} Z^n = \frac{Ze^{(X+1)Z} - Ze^{XZ}}{e^Z - 1} = \frac{Ze^{XZ}(e^Z - 1)}{e^Z - 1} = Ze^{XZ}.$$

Thus,

$$\frac{B_n(X+1) - B_n(X)}{n!} = (Ze^{XZ})[Z^n] = \frac{X^{n-1}}{(n-1)!},$$

which gives what we want.

(3) This is an immediate consequence of (2) and the definition of $B_n(X)$.

(4) Note that

$$\sum_{a=1}^{p} a^n = \frac{1}{n+1} \left((n+1) B_n p - \binom{n+1}{n-1} B_{n-1} p^2 + \cdots \right) \equiv p B_n \pmod{p^2}.$$

(5) Note that $x_a = \left\lfloor \frac{ab}{p} \right\rfloor$. From $ab = px_a + r_a$,

$$(ab)^n \equiv r_a^n + np \left\lfloor \frac{ab}{p} \right\rfloor r_a^{n-1} \pmod{p^2}.$$

The equation follows from $r_a \equiv ab \pmod{p}$.

Adding the equation over $1 \leq a \leq p$, we have

$$b^n \sum_{a=1}^{p} a^n \equiv \sum_{a=1}^{p} r_a^n + pnb^{n-1} \sum_{a=1}^{p-1} a^{n-1} \left\lfloor \frac{ab}{p} \right\rfloor \pmod{p^2}.$$

Since $\{r_1, r_2, \cdots, r_p\} \equiv \{1, 2, \cdots, p\} \pmod{p}$, we get the conclusion.

(6) Let s be a primitive root mod p. Then, for n even and not divisible by $p-1$,

$$pB_n \equiv \sum_{j=1}^{p} j^n \equiv \frac{pns^{n-1}\sum_{j=1}^{p-1} j^{n-1}\left\lfloor \frac{sj}{p}\right\rfloor}{s^n-1} \pmod{p^2},$$

so for $(n,p)=1$,

$$\frac{B_n}{n} \equiv \frac{ps^{n-1}\sum_{j=1}^{p-1} j^{n-1}\left\lfloor \frac{sj}{p}\right\rfloor}{s^n-1} \pmod{p}.$$

The right hand side only depends on the congruence class of n mod $p-1$, so we get the congruence.

□

Solution to Exercise 20.2.

(1) We want to find, for a, x such that $\omega(a) \equiv a+px \pmod{p^2}$. The requirement is that it is a $(p-1)$-st root of unity, so

$$(a+px)^{p-1} \equiv 1 \pmod{p^2},$$

so

$$a^{p-1} + (p-1)pxa^{p-2} \equiv 1 \pmod{p^2}.$$

So $px \equiv \frac{1-a^{p-1}}{(p-1)a^{p-2}} \equiv \frac{a^{p-1}-1}{a^{p-2}} \pmod{p^2}$.

(2) Note that $B_{1,\omega^{-i}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-i}(a)$. Thus, since $\omega^{p-1}(a)=1$, we want to show that

$$\sum_{a=1}^{p-1} a\omega^{-i}(a) = \sum_{a=1}^{p-1} a\omega^{p-i-1}(a) \equiv \frac{pB_{p-i}}{p-i} \pmod{p^2}.$$

We have

$$\omega^{p-i-1}(a) \equiv \left(a + \frac{a^{p-1}-1}{a^{p-2}}\right)^{p-i-1} \equiv a^{p-i-1} + (p-i-1)a^{p-i-2}\frac{a^{p-1}-1}{a^{p-2}}$$

$$\equiv a^{p-i-1} + (p-i-1)a^{p-i-1} - (p-i-1)\frac{1}{a^i} \equiv (p-i)a^{p-i-1} - (p-i-1)a^{p^2-p-i} \pmod{p^2},$$

so

$$\sum_{a=1}^{p-1} a\omega^{p-i-1}(a) \equiv (p-i)\sum_{a=1}^{p-1} a^{p-i} - (p-i-1)\sum_{a=1}^{p-1} a^{p^2-p-i+1}$$

$$\equiv (p-i)\sum_{a=1}^{p} a^{p-i} - (p-i-1)\sum_{a=1}^{p} a^{p^2-p-i+1} \equiv p((p-i)B_{p-i} - (p-i-1)B_{p^2-p-i+1}) \pmod{p^2},$$

since $p-i$ and $p^2-p-i+1$ are even and not divisible by $p-1$. Moreover, $p-i \equiv p^2-p-i+1 \pmod{p-1}$, so by Kummer congruence,

$$B_{p^2-p-i+1} \equiv \frac{p^2-p-i+1}{p-i} B_{p-i} \equiv \frac{-i+1}{-i} B_{p-i} = \frac{i-1}{i} B_{p-i} \pmod{p},$$

so

$$(p-i-1)B_{p^2-p-i+1} \equiv -(i+1)\frac{i-1}{i} B_{p-i} = \left(-i+\frac{1}{i}\right) B_{p-i} \pmod{p}.$$

Thus,

$$\sum_{a=1}^{p-1} a\omega^{p-i-1}(a) \equiv p((p-i)B_{p-i} - (p-i-1)B_{p^2-p-i+1}) \equiv p\left(p-i+i-\frac{1}{i}\right) B_{p-i} = p\frac{B_{p-i}}{-i} \equiv p\frac{B_{p-i}}{p-i} \pmod{p^2},$$

which is what we want.

□

Solution to Exercise 20.3.

Hint is obvious as $\mathfrak{p}$ is totally ramified in $\mathbb{Q}(\zeta_{p^b})$. As $K := H_{\mathbb{Q}(\zeta_{p^a})} \cap \mathbb{Q}(\zeta_{p^b})$ is a subextension of $\mathbb{Q}(\zeta_{p^b})/\mathbb{Q}(\zeta_{p^a})$ which is everywhere unramified over $\mathbb{Q}(\zeta_{p^a})$, by Hint, $K = \mathbb{Q}(\zeta_{p^a})$. Now the argument as in the proof Theorem 20.3(1) works in the same way. □

Solution to Exercise 20.4.

(1) This follows from what we proved in the analytic proof of the quadratic reciprocity law that $G(\chi_p) = i\sqrt{p}$.

(2) Note that

$$\sum_{a=1}^{p} \chi_p(a)a = \sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)2a + \sum_{a=\frac{p+1}{2}}^{p-1} \chi_p(2a)(2a-p) = \sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)2a + \sum_{a=1}^{\frac{p-1}{2}} \chi_p(2(p-a))(2(p-a)-p)$$

$$= \sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)2a + \sum_{a=1}^{\frac{p-1}{2}} \chi_p(2a)(2a-p),$$

which gives what we want.

(3) Note that $2\chi_p(2)$ times the expression in (1) minus the expression in (2) gives

$$(2\chi_p(2)-1)h_K = \chi_p(2)\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a),$$

or

$$h_K = \frac{\chi_p(2)}{2\chi_p(2)-1}\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a) = \frac{1}{2-\chi_p(2)}\sum_{a=1}^{\frac{p-1}{2}} \chi_p(a).$$

(4) Note that $\sum_{a=1}^{\frac{p-1}{2}}$ is the number of quadratic residues minus the number of quadratic non-residues. Since $2 - \chi_p(2)$ is either 1 or 3, we get the result.

□

Acknowledgements

I benefited a lot from the following lecture notes, resources and textbooks: *Class Field Theory* by Emil Artin and John Tate; *Gauss and Jacobi sums* by Bruce Berndt, Ronald Evans and Kenneth Williams; *A Course in Computational Algebraic Number Theory* by Henri Cohen; notes for "Algebraic Number Theory" taught by Brian Conrad (written by Aaron Landesman); various notes by Keith Conrad; *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication* by David A. Cox; notes for "Algebraic Number Theory" taught by Michael Harris; *Algebraic Number Fields* by Gerald Janusz; notes for "Local Fields" taught by Christian Johansson (written by Dexter Chua); *Number Fields* by Daniel Marcus; *Algebraic Number Theory* by James Milne; *Algebraic Number Theory* by Jürgen Neukirch; *Local Fields* by Jean-Pierre Serre; notes for "Number Theory I" taught by Andrew Sutherland; notes for "Algebraic Number Theory" taught by Yichao Tian; *Introduction to Cyclotomic Fields* by Lawrence Washington; *Algebraic Theory of Numbers* by Hermann Weyl.

I thank the students of GU4043 in Spring 2024 for their participation.

References

[BSD] E. S. Barnes, H. P. F. Swinnerton-Dyer. **The inhomogeneous minima of binary quadratic forms. I.** Acta Math. **87** (1952), 259-323.

[Har] Malcolm Harper. $\mathbb{Z}[\sqrt{14}]$ **is Euclidean.** Canad. J. Math. **56** (2004), no. 1, 55-70.

[Lub] Jonathan Lubin. **The local Kronecker–Weber theorem.** Trans. Am. Math. Soc. **267** (1981),133-138.

[Lut] Bernhard Lutzmann. **Quadratic Number Fields that are Euclidean but not Norm-Euclidean**. Master's Thesis. Universität Wien. 2007.

[Was] Lawrence Washington. **Introduction to cyclotomic fields**. Second edition. Grad. Texts in Math., **83**. Springer-Verlag, New York, 1997. xiv+487 pp.

Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027
E-mail address: gyujinoh@math.columbia.edu