Math 6370: Algebraic Number Theory

Taught by David Zywina

Notes by David Mehrle
dmehrle@math.cornell.edu

Cornell University

Spring 2018

Last updated May 13, 2018.
The latest version is online here.

Contents

Contents by Lecture

1 Introduction

The main objects of algebraic number theory are number fields.

Definition 1.1. A **number field** is an extension field of $\mathbb{Q}$ of finite degree, i.e. $K \supseteq Q$ with $[K\colon \mathbb{Q}] = \dim_{\mathbb{Q}} K < \infty$.

Example 1.2. $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $Q(\sqrt{-3})$, $Q(\sqrt[3]{5})$.

Theorem 1.3 (Primitive Element)**.** *For any number field* K, $K = \mathbb{Q}(\alpha)$ *for some* α.

In number theory, we study the integers $\mathbb{Z} \subseteq \mathbb{Q}$. The integers are nice because we can factor any element into a product of primes. When we work over other number fields, we want something analogous: what do the integers look like in a number field?

Let K be a finite field extension of $\mathbb{Q}$ of degree n. Take any $\alpha \in K$. Define a homomorphism of $\mathbb{Q}$-algebras

$$\begin{tikzcd} \mathbb{Q}[x] \arrow[r] & K \\ x \arrow[r, mapsto] & \alpha \end{tikzcd}$$

Since $\mathbb{Q}[x]$ is a principal ideal domain (PID), the kernel of this map is generated by a single element, say $\langle p_\alpha(x)\rangle$. The polynomial $p_\alpha(x)$ is the **minimal polynomial of** α, a monic polynomial in $\mathbb{Q}[x]$ of minimal degree with root α.

We write the image of ${}^{\mathbb{Q}[x]}\big/_{\langle p_\alpha(x)\rangle}$ in K as $\mathbb{Q}[\alpha]$ to denote the $\mathbb{Q}$-algebra generated by α; it is a field. We often write $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

Definition 1.4 (Working definition)**.** We say that $\alpha \in K$ is an **algebraic integer** if $p_\alpha(x)$ has coefficients in $\mathbb{Z}$.

Definition 1.5. Let $\mathcal{O}_K$ be the set of algebraic integers in K. This is the **ring of algebraic integers of** K**.**

We will prove this later that $\mathcal{O}_K$ is a ring. This fact isn't obvious.

Example 1.6. If $K = \mathbb{Q}$, and $\alpha \in \mathbb{Q}$, then $p_\alpha(x) = (x - \alpha)$. The polynomial $p_\alpha(x)$ has integer coefficients if and only if $\alpha \in \mathbb{Z}$. Therefore, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

Example 1.7. Let $K = \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{C}$. Elements of this field are $a + b\sqrt{-2}$ for a, b rational.

Let $\alpha = a + b\sqrt{-2}$. If $b = 0$, then $\alpha \in \mathbb{Q}$ and $p_\alpha(x) = (x - a)$. So $\alpha \in \mathcal{O}_K$ in this case precisely when $a \in \mathbb{Z}$.

If $b \neq 0$, then

$$p_\alpha(x) = (x - (a + b\sqrt{-2}))(x - (a - b\sqrt{-2})) = x^2 - 2ax + (a^2 + 2b^2).$$

In this case, $\alpha \in \mathcal{O}_K$ if and only if $2a \in \mathbb{Z}$ and $a^2 + 2b^2 \in \mathbb{Z}$. **Exercise:** this is equivalent to $a, b \in \mathbb{Z}$.

Therefore, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$.

If we had replaced $\sqrt{-2}$ by $\sqrt{-3}$ in the previous example, the algebraic integers would be slightly larger than the naïve thing we might expect. Moreover, $\mathbb{Z}[\sqrt{-2}]$, like $\mathbb{Z}$, is a unique factorization domain (UFD), but this isn't always the case.

Number fields are useful to solve Diophantine equations, as the next example shows.

Example 1.8. Find all solutions of $y^2 = x^3 - 2$ with $x, y \in \mathbb{Z}$. Right away, we can see a few solutions for small numbers: $(3, \pm 5)$, but there aren't other obvious ones. Are these the only ones?

To solve this, work in the larger ring $\mathbb{Z}[\sqrt{-2}]$. We may factor this equation

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

We may factor x in $\mathbb{Z}[\sqrt{-2}]$ as $x = u_1 \pi_1^{e_1} \cdots \pi_r^{e_r}$ with $u_i \in \mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$, $\pi_i \in \mathbb{Z}[\sqrt{-2}]$ irreducible, and $e_i \geq 0$. Assume moreover that $\pi_i \neq \pm \pi_j$ for $i \neq j$. When we substitute this expression into the equation above,

$$u_i^3 \pi_1^{3e_1} \cdots \pi_r^{3e_r} = x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Claim 1.9. $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime in $\mathbb{Z}[\sqrt{-2}]$, i.e. the only common divisors are units.

Proof. To prove this claim, take an irreducible π dividing both. Then π divides $(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2} = -(\sqrt{-2})^3$. We may assume by uniqueness that $\pi = \sqrt{-2}$. Then π divides $y + \sqrt{-2}$ implies that $y + \sqrt{-2} = \sqrt{-2}(a + b\sqrt{-2}) = -2b + a\sqrt{-2}$ for some $a, b \in \mathbb{Z}$. Hence, $y = -2b$, so $x^3 = 2 + y^2 \equiv 2 \pmod 4$. This is impossible in the integers. So we have demonstrated the claim. □

Now we may use the claim in the example. For each $1 \leq i \leq r$, $\pi_i^{3e_i}$ divides $y + \sqrt{-2}$ or $y - \sqrt{-2}$. Therefore,

$$y + \sqrt{-2} = u \prod_{i \in I} \pi_i^{3e_i}$$

for some $I \subseteq \{1, \ldots, r\}$ and $u \in \mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$. Therefore, $y + \sqrt{-2}$ is a cube in $\mathbb{Z}[\sqrt{-2}]$.

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3$$

for some $a, b \in \mathbb{Z}$. Expand:

$$y + \sqrt{-2} = (a^3 - 6ab^2) + (3a^2 b - 2b^3)\sqrt{-2}$$

Returning to $\mathbb{Z}$, we find that $y = a^3 - 6ab^2$ for integers a, b such that $3a^2b - 2b^3 = 1$. For this second equation, we can factor out b to learn that $b(3a^2 - 2b^2) = 1$, but b is an integer, so $b = \pm 1$. This reduces the three equations and four unknowns to three equations with three unknowns and two cases.

If $b = +1$, then we have a system of equations

$$\begin{cases} y = a^3 - 6a \\ 3a^2 - 2 = 1 \\ y^2 = x^3 - 2 \end{cases}$$

We may solve these first two equations to discover that $y = \pm 5$, and we can solve for x to see that there are solutions $(3, \pm 5)$.

If $b = -1$, then $3a^2(-1) - 2(-1)^3 = 1$, or equivalently $3a^2 = 1$. This has no solutions in the integers.

So the only solutions to $y^2 = x^3 - 2$ in the integers is $(3, \pm 5)$.

The point of this example is that, even when working over the integers, we are obliged to consider larger rings.

Example 1.10 (Non-example)**.** One could try the same thing for $y^3 = x^3 - 61$. Solve for x^3, and then factor the right hand side using $\sqrt{-61}$.

$$x^3 = y^2 + 61 = (y - \sqrt{-61})(y + \sqrt{-61}).$$

Assuming that $\mathbb{Z}[\sqrt{-61}]$ is a UFD, one can show that there are no solutions for $x, y \in \mathbb{Z}$.

However, $8^2 = 5^3 - 61$; $\mathbb{Z}[\sqrt{-61}]$ is *not* a UFD. Indeed,

$$5^3 = (8 + \sqrt{-61})(8 - \sqrt{-61})$$

and $5, 8 + \sqrt{-61}$ and $8 - \sqrt{-61}$ are all three irreducible.

How do we cope with the loss of unique factorization? Here's an idea due to Kummer from around 1846: if unique factorization fails, its because we don't have enough numbers yet; we should be able to add some "ideal numbers" and recover unique factorization. For example, where $5^3 = (8 + \sqrt{-61})(8 - \sqrt{-61})$, we may have $5 = \mathfrak{p}\mathfrak{q}$, $8 + \sqrt{-61} = \mathfrak{p}^3$ and $8 - \sqrt{-61} = \mathfrak{q}^3$.

Later, Dedekind defined **ideals** of a ring while trying to make sense of Kummer's work. Later, we will see that every nonzero ideal of $\mathcal{O}_K$ factors uniquely as a product of prime ideals. To make sense of the previous paragraph, we just add brackets to denote "the ideal generated by..."

$$\langle 5 \rangle = \mathfrak{p}\mathfrak{q}, \qquad \langle 8 + \sqrt{-61} \rangle = \mathfrak{p}^3, \qquad \langle 8 - \sqrt{-61} \rangle = \mathfrak{q}^3$$

where $\mathfrak{p}, \mathfrak{q}$ are (not necessarily principal) prime ideals.

In this course, we will study number fields and their rings of integers, and then use these to study the integers and Diophantine equations. Here are some things we want to understand:

- $\mathcal{O}_K$ is a ring;
- the structure of the abelian group $(\mathcal{O}_K, +)$;
- the structure of the group of units $\mathcal{O}_K^\times$;
- unique factorization into prime ideals in $\mathcal{O}_K$;
- how to measure how badly unique factorization fails in $\mathcal{O}_K$;
- the prime ideals of $\mathcal{O}_K$.

1.1 Administrivia

There is a class website here.

There will be approximately four homework assignments and no exams.

There is no textbook for the class, but there are several recommended references (available for free online to Cornell affiliates).

- Marcus, *Number Fields*. This has been recommended to me. It is a apparently good for beginners and has lots of exercises. Chapter 1 is motivational and can be skipped if desired. It avoids local fields and Dedekind domains.
- Neukirch, *Algebraic Number Theory*. This text is more advanced and treats the subject from the general point of view of arithmetic geometry (which may seem strange to those without the geometric background).
- Milne, *Algebraic Number Theory*. Milne's course notes (in several subjects) are always good.
- Lang, *Algebraic Number Theory*.
- Murty, Esmonde, *Problems in Algebraic Number Theory*. This book was designed for self study. Lots of exercises with full solutions.
- Janusz, *Algebraic Number Fields*

2 Algebraic integers

Recall that a **number field** K is a field extension of $\mathbb{Q}$ of finite degree, e.g. $\mathbb{Q}(\sqrt[3]{2})$. Fix a number field K of degree $n := [K\colon \mathbb{Q}] = \dim_{\mathbb{Q}} K$.

Proposition 2.1. *Let $\alpha \in K$. The following are equivalent.*

(a) $p_\alpha(x) \in \mathbb{Z}[x]$, where $p_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α over $\mathbb{Q}$;

(b) $f(\alpha) = 0$ for some monic $f(x) \in \mathbb{Z}[x]$;

(c) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module;

(d) there is a nonzero finitely generated subgroup $M \subseteq K$ such that $\alpha M \subseteq M$.

Proof. $(a) \implies (b)$: Take $f(x) = p_\alpha(x) \in \mathbb{Z}[x]$. By definition of minimal polynomial, α is a root of $p_\alpha(x)$.

$(b) \implies (c)$: Consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[\alpha]$ given by $x \mapsto \alpha$. This is a surjective homomorphism, which gives another surjection

$$\mathbb{Z}[x]/\langle f \rangle \twoheadrightarrow \mathbb{Z}[\alpha].$$

This exhibits $\mathbb{Z}[\alpha]$ as a quotient of the $\mathbb{Z}$-module $\mathbb{Z}[x]/\langle f \rangle$, and $\mathbb{Z}[x]/\langle f \rangle$ is finitely generated by $1, x, x^2, \ldots, x^{d-1}$. Hence, $\mathbb{Z}[\alpha]$ is finitely generated as well.

$(c) \implies (d)$: Take $M = \mathbb{Z}[\alpha]$. Then $\alpha M \subseteq M$.

$(d) \implies (b)$: Take generators $\beta_1, \ldots, \beta_r$ for M. Since M is a subgroup of the additive group of the field K, it must have no torsion. So $M = \mathbb{Z}\beta_1 \oplus \ldots \oplus \mathbb{Z}\beta_r$. Since $\alpha M \subseteq M$, We must have

$$\alpha\beta_i = \sum_{j=1}^{r} c_{ij}\beta_j$$

for some $c_{ij} \in \mathbb{Z}$. This gives a matrix $C = (c_{ij})_{i,j=1}^{r}$ with integer coefficients; set $f(x) = \det(xI - C) \in \mathbb{Z}[x]$. By the Cayley-Hamilton theorem, $f(C) = 0$, and therefore multiplication by $f(\alpha)$ on M is zero. Therefore $f(\alpha) = 0$ since M is nonzero and has no torsion.

$(b) \implies (a)$: We have $f(\alpha) = 0$, so $f(x) = p_\alpha(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. Since f is monic, both p_α and g must be monic as well. Claim that both $p_\alpha(x)$ and $g(x)$ are in $\mathbb{Z}[x]$.

Suppose not. Fix a prime p dividing the denominator of a coefficient of $p_\alpha(x)$ or $g(x)$. Take $a, b \geq 0$ minimal such that $p^a p_\alpha(x)$ and $p^b g(x)$ have coefficients with no p's in the denominators. Then

$$p^{a+b} f = p^a p_\alpha(x) p^b g(x)$$

Now consider this equation mod p. The right hand side is nonzero mod p because we chose a and b minimal to clear the denominators. Hence $p^{a+b}f \not\equiv 0 \pmod{p}$. But $f \in \mathbb{Z}[x]$ is monic, so we must have $a = b = 0$. So there cannot be a prime p dividing the denominator of any coefficient in either $p_\alpha(x)$ or $g(x)$. □

Definition 2.2. We say that $\alpha \in K$ is an **algebraic integer** if any one of the equivalent conditions in Proposition 2.1 hold.

Example 2.3. $\mathbb{Z}\left[\frac{1}{2}\right]$ is not finitely generated as a $\mathbb{Z}$-module because any finite set of elements cannot give you every power of 2 in the denominator.

Definition 2.4. Let $\mathcal{O}_K$ be the set of algebraic integers in K.

Proposition 2.5. *$\mathcal{O}_K$ is a subring of K.*

Proof. First, notice that $0, 1 \in \mathcal{O}_K$. To show that this is a ring, we must show that it is closed under addition, subtraction, and multiplication.

Take any $\alpha, \beta \in \mathcal{O}_K$. The $\mathbb{Z}$-modules $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$, are finitely generated by $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ and $1, \beta, \beta^2, \ldots, \beta^{e-1}$, respectively. Then $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module, generated by $\alpha^i\beta^j$ with $0 \leq i < d$ and $0 \leq j < e$.

Let $M = \mathbb{Z}[\alpha, \beta]$. We have $0 \neq M \subseteq K$, and moreover $(\alpha \pm \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$. So by Proposition 2.1, $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers. Hence, $\alpha \pm \beta, \alpha\beta \in \mathcal{O}_K$. □

Exercise 2.6. For a challenge, use either condition (a) or condition (b) from Proposition 2.1 to prove that $\alpha + \beta$ or $\alpha\beta$ are algebraic integers for algebraic integers α and β.

Proposition 2.7. *Some properties of rings of algebraic integers:*

(a) If $L \supseteq K$ is an extension of number fields, then $\mathcal{O}_L \cap K = \mathcal{O}_K$. In particular, $\mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$.

(b) For any $\alpha \in K$, there is an integer $m \geq 1$ such that $m\alpha \in \mathcal{O}_K$.

Proof of (b). Let $\alpha \in K$ and take any polynomial $f(x) = x^2 + c_1x^{d-1} + \ldots + c_d \in \mathbb{Q}[x]$ with $f(\alpha) = 0$. Multiply by m^d for any integer $m \geq 1$:

$$m^d f(x) = (mx)^d + c_1 m(mx)^{d-1} + \ldots + m^d c_d.$$

Choose m so large that

$$x^d + c_1 m x^{d-1} + \ldots + m^d c_d$$

has integer coefficients. Then $m\alpha$ is a root of this polynomial. □

2.1 Trace and Norm

Definition 2.8. Let $K/\mathbb{Q}$ be a field extension of degree n (a number field). For $\alpha \in K$, define a $\mathbb{Q}$-linear homomorphism $\mu_\alpha \colon K \to K$ by $x \mapsto \alpha x$.

- The **norm** $N_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$ is the map $\alpha \mapsto \det(\mu_\alpha)$.
- The **trace** $\mathrm{Tr}_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$ is the map $\alpha \mapsto \mathrm{tr}(\mu_\alpha)$.

Example 2.9. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ any squarefree integer. This is a degree 2 field extension of K. As a $\mathbb{Q}$-vector space, K has basis $1, \sqrt{d}$. Take any $\alpha = a + b\sqrt{d} \in K$ with $a, b \in \mathbb{Q}$. Then

$$\begin{aligned} \alpha \cdot 1 &= a + b\sqrt{d} \\ \alpha \cdot \sqrt{d} &= bd + a\sqrt{d} \end{aligned}$$

So as a matrix in the basis $1, \sqrt{d}$, we have

$$[\mu_\alpha]_{\{1,\sqrt{d}\}} = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

Therefore, $N_{K/\mathbb{Q}}(\alpha) = a^2 - db^2$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$.

Proposition 2.10. *Basic properties of the trace and norm:*

- *The norm is multiplicative, i.e.* $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$.
- $N_{K/\mathbb{Q}}(c) = c^n$ *for* $c \in \mathbb{Q}$.

These properties imply that $N_{K/\mathbb{Q}} \colon K^\times \to \mathbb{Q}^\times$ *is a group homomorphism.*

- $\mathrm{Tr}_{K/\mathbb{Q}} \colon K \to \mathbb{Q}$ *is* $\mathbb{Q}$*-linear.*

Example 2.11. We can use this to show that $x^2 - 2y^2 = 1$ has infinitely many solutions. Consider $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Q}(\sqrt{2})$. There is a correspondence between solutions to this equation and elements of $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $N_{K/\mathbb{Q}}(\alpha) = 1$.

$$\begin{array}{ccc} \left\{(a,b) \in \mathbb{Z}^2 \mid a^2 - 2b^2 = 1\right\} & \longrightarrow & \left\{\alpha \in \mathbb{Z}[\sqrt{2}] \mid N_{K/\mathbb{Q}}(\alpha) = 1\right\} \\ (a,b) & \longmapsto & a + b\sqrt{2} \end{array}$$

Let $G = \left\{\alpha \in \mathbb{Z}[\sqrt{2}] \mid N_{K/\mathbb{Q}}(\alpha) = 1\right\}$. Claim that G is a subgroup of $\mathbb{Z}[\sqrt{2}]^\times$.

- Clearly, $1 \in G$
- If $\alpha, \beta \in G$, then $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = 1 \cdot 1 = 1$ so $\alpha\beta \in G$.
- If $\alpha = a + b\sqrt{2} \in G$, then $\alpha^{-1} = a - b\sqrt{2} \in G$ as well.

$$\alpha\alpha^{-1} = a^2 - 2b^2 = 1$$

Now take $\varepsilon = 3 + 2\sqrt{2} \in G$. Powers of ε are all different, since $\varepsilon > 1$. We have constructed infinitely many elements of norm 1, and therefore infinitely may solutions to this equation.

In fact, $G = \pm\langle\varepsilon\rangle = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$. However, $\mathbb{Z}\left[\sqrt{2}\right]^\times = \pm\langle 1 + \sqrt{2}\rangle$, and G is a subgroup of $\mathbb{Z}\left[\sqrt{2}\right]^\times$ of index 2. Note that $(1+\sqrt{2})^2 = 3 + 2\sqrt{2} = \varepsilon$.

Remark 2.12. In general, $x^2 - dy^2 = 1$ with $d > 1$ squarefree has infinitely many solutions. For example, for the equation $x^2 - 1141y^2 = 1$, the corresponding group is

$$G = \left\{\alpha \in \mathbb{Z}[\sqrt{1141}] \mid N_{K/\mathbb{Q}}(\alpha) = 1\right\} = \pm\langle\varepsilon\rangle$$

with

$$\varepsilon = 1036782394157223963237125215 + 30693385322765657197397208\sqrt{1141}$$

These are special cases of the following theorem, which we will prove much later.

Theorem 2.13 (Dirichlet Unit Theorem)**.** *Let $K/\mathbb{Q}$ be a number field. Let r be the number of embeddings $K \hookrightarrow \mathbb{R}$ and let $2s$ be the number of embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$.*

Example 2.14. For a quadratic number field $K = \mathbb{Q}(\sqrt{d})$, with $d > 0$ squarefree, $r = 2$ and $s = 0$. So $\mathcal{O}_K^\times$ has rank 1 in the example above.

Example 2.15. In general, $\mathcal{O}_K \neq \mathbb{Z}\left[\sqrt{d}\right]$ when $K = \mathbb{Q}(\sqrt{d})$. Let $\alpha = \frac{1}{2}(-1 + \sqrt{-3})$. Notice that $\alpha^3 = 1$, so α is a root of $x^3 - 1$ and therefore an algebraic integer in $\mathbb{Q}(\sqrt{-3})$. But it is not an element of $\mathbb{Z}[\sqrt{-3}]$.

To understand the norm and the trace, we will study the characteristic polynomial $\det(xI - \mu_\alpha) \in \mathbb{Q}[x]$, because

$$\det(xI - \mu_\alpha) = x^n - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)x^{n-1} + \ldots + (-1)^n N_{K/\mathbb{Q}}(\alpha).$$

Remark 2.16. The definition of the norm and the trace doesn't depend on the fact that we have a number field, only that there is a finite field extension. For any finite extension of fields L/K, we may similarly define $\mathrm{Tr}_{L/K}$ and $N_{L/K}$.

Example 2.17. $K = \mathbb{Q}(\omega)$ where $\omega = \sqrt[3]{2}$. The minimal polynomial of ω is $p_\omega(x) = x^3 - 2$. K is therefore a degree 3 extension of $\mathbb{Q}$ with $\mathbb{Q}$-basis $1, \omega, \omega^2$. Any element $\alpha \in K$ may be written as $a + b\omega + c\omega^2$ for $a, b, c \in \mathbb{Q}$.

To find the norm and trace of α, we write μ_α as a matrix by checking the action of α on the basis $1, \omega, \omega^2$.

$$[\mu_\alpha]_{\{1,\omega,\omega^2\}} = \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix}$$

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) &= \mathrm{tr}[\mu_\alpha]_{\{1,\omega,\omega^2\}} = 3a \\ N_{K/\mathbb{Q}}(\alpha) &= \det[\mu_\alpha]_{\{1,\omega,\omega^2\}} = a^3 + 2b^3 + 4c^3 - 6abc \end{aligned}$$

When does $N_{K/\mathbb{Q}}(\alpha) = \pm 1$? Certainly when $\alpha = \pm 1$, but also when $\alpha = \varepsilon = 1 + \omega + \omega^2$, and then all powers of ε.

It turns out that $\mathcal{O}_K = \mathbb{Z}[\omega]$ and $\mathcal{O}_K^\times = \{\pm\varepsilon^n \mid n \in \ Z\}$.

2.2 Complex embeddings

Consider the action of μ_α on $K \otimes_{\mathbb{Q}} \mathbb{C}$. If we choose a primitive element β such that

$$K = \mathbb{Q}(\beta) \cong {}^{\mathbb{Q}[x]}\big/_{\langle p_\beta(x)\rangle},$$

where $p_\beta(x)$ is the minimal polynomial of β. Then we may write

$$K \otimes_{\mathbb{Q}} \mathbb{C} = {}^{\mathbb{C}[x]}\big/_{\langle p_\beta(x)\rangle}.$$

This ring is almost certainly *not* a field, since $p_\beta(x)$ factors into linear terms over $\mathbb{C}$. Write $p_\beta(x) = \prod_{i=1}^n (x - \beta_i)$ for distinct $\beta_i \in \mathbb{C}$. So by the Chinese remainder theorem:

$$K \otimes_{\mathbb{Q}} \mathbb{C} = {}^{\mathbb{C}[x]}\big/_{\langle p_\beta(x)\rangle} \cong \prod_{i=1}^n {}^{\mathbb{C}[x]}\big/_{\langle (x - \beta_i)\rangle} \cong \prod_{i=1}^n \mathbb{C} = \mathbb{C}^n.$$

With this isomorphism, μ_α acts on $K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^n$. To understand this, consider the composite

$$\begin{tikzcd} \sigma_i\colon K \arrow[r] & K \otimes_{\mathbb{Q}} \mathbb{C} \arrow[r, "\cong"] & \mathbb{C}^n \arrow[r, "\mathrm{pr}_i"] & \mathbb{C} \\ \alpha \arrow[r, mapsto] & \alpha \otimes 1 \end{tikzcd}$$

Each $\sigma_i\colon K \hookrightarrow \mathbb{C}$ is a homomorphism of fields with $\sigma_i(\beta) = \beta_i$.

Definition 2.18. The field homomorphisms $\sigma_1, \ldots, \sigma_n\colon K \hookrightarrow \mathbb{C}$ are the **complex embeddings** of K.

On the level of simple tensors, an explicit isomorphism $K \otimes_{\mathbb{Q}} \mathbb{C} \to \mathbb{C}^n$ is given by

$$\begin{tikzcd} K \otimes_{\mathbb{Q}} \mathbb{C} \arrow[r, "\cong"] & \mathbb{C}^n \\ \alpha \otimes z \arrow[r, mapsto] & (z\sigma_1(\alpha), \ldots, z\sigma_n(\alpha)) \end{tikzcd}$$

Or alternatively,

$$\begin{tikzcd} i\colon K \arrow[r, hook] & K \otimes_{\mathbb{Q}} \mathbb{C} \arrow[r, "\cong"] & \mathbb{C}^n \\ \alpha \arrow[rr, mapsto] & & (\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) \end{tikzcd}$$

The action of μ_α on $K \otimes_{\mathbb{Q}} \mathbb{C}$ translates to the action on $\mathbb{C}^n$ given by the matrix

$$\begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix}$$

From this diagonal representation of μ_α, we get the following.

Proposition 2.19. *For a number field $K/\mathbb{Q}$ of degree n,*

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha) &= \prod_{i=1}^{n} \sigma_i(\alpha) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) &= \sigma_1(\alpha) + \ldots + \sigma_n(\alpha). \end{aligned}$$

where $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ are the complex embeddings of K.

Example 2.20. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a squarefree integer. This is, as before, a quadratic extension of $\mathbb{Q}$. We consider $K \subseteq \mathbb{Q}$ already for convenience. The two embeddings $\sigma_1, \sigma_2 \colon K \hookrightarrow \mathbb{C}$ are

$$\begin{aligned} \sigma_1(a + b\sqrt{d}) &= a + b\sqrt{d} \\ \sigma_2(a + b\sqrt{d}) &= a - b\sqrt{d} \end{aligned}$$

The norm and trace are

$$\begin{aligned} N_{K/\mathbb{Q}}(a + b\sqrt{d}) &= (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \\ \mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) &= (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \end{aligned}$$

Recall that we wanted to study the polynomial $\det(xI - \mu_\alpha) \in \mathbb{Q}[x]$. We have now discovered that

$$\det(xI - \mu_\alpha) = \prod_{i=1}^{n} (x - \sigma_i(\alpha))$$

Notice that each $\sigma_i(\alpha)$ is a root of $p_\alpha(x)$, since p_α has rational coefficients and σ_i is a morphism of $\mathbb{Q}$-algebras.

$$p_\alpha(\sigma_i(\alpha)) = \sigma_i(p_\alpha(\alpha)) = \sigma_i(0) = 0$$

Therefore,

$$\det(xI - \mu_\alpha) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = p_\alpha(x)^m$$

for some integer m. The degree of p_α is $[\mathbb{Q}(\alpha) \colon \mathbb{Q}]$, and the degree of $\det(xI - \mu_\alpha)$ is $n = [K \colon \mathbb{Q}]$. Therefore, m must be $[K \colon \mathbb{Q}(\alpha)]$. We have shown:

Proposition 2.21. *Let $K/\mathbb{Q}$ be a number field and choose any $\alpha \in K$. Let $\mu_\alpha \colon K \to K$ denote multiplication by α. Then*

$$\det(xI - \mu_\alpha) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)) = p_\alpha(x)^{[K \colon \mathbb{Q}(\alpha)]},$$

where $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ are the complex embeddings of K.

Corollary 2.22. *For $\alpha \in \mathcal{O}_K$, $N_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ are integers.*

Proof. From the previous proposition, we have

$$\det(xI - \mu_\alpha) = p_\alpha(x)^{[K \colon \mathbb{Q}(\alpha)]}.$$

Since $p_\alpha(x) \in \mathbb{Z}$, all coefficients of the left hand side must be integers as well. And we have

$$\det(xI - \mu_\alpha) = x^n - \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)x^{n-1} + \ldots + (-1)^n N_{K/\mathbb{Q}}(\alpha).$$

□

Example 2.23. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a squarefree integer. What is $\mathcal{O}_K$? If $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$ for $a, b \in \mathbb{Q}$, we know from the previous corollary that $N_{K/\mathbb{Q}}(\alpha), \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Hence, $a^2 - db^2, 2a \in \mathbb{Z}$.

Multiplying the first by 4, we find that $(2a)^2 - d(2b)^2, 2a \in \mathbb{Z}$, which implies that $d(2b)^2, 2a \in \mathbb{Z}$. Since d is squarefree, this means that $2a, 2b \in \mathbb{Z}$.

Therefore, $2\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Hence, we have inclusions of abelian groups

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K \subseteq \frac{1}{2}\mathbb{Z}[\sqrt{d}].$$

Notice that the quotient group $\frac{1}{2}\mathbb{Z}[\sqrt{d}]/\mathbb{Z}[\sqrt{d}]$ is a group of order 4 with coset representatives 0, $\frac{1}{2}$, $\frac{\sqrt{d}}{2}$, and $\frac{1+\sqrt{d}}{2}$.

To determine what $\mathcal{O}_K$ is, we will figure out which of these representatives are actually algebraic integers. Clearly, $0 \in \mathcal{O}_K$ and $\frac{1}{2} \notin \mathcal{O}_K$. The minimal polynomial of $\frac{\sqrt{d}}{2}$ is $x^2 - \frac{d}{4}$ which is *not* in $\mathbb{Z}[x]$ because d is squarefree. Hence, $\frac{\sqrt{d}}{2} \notin \mathcal{O}_K$. Finally, the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is

$$\left(1 - \tfrac{1+\sqrt{d}}{2}\right)\left(x - \tfrac{1-\sqrt{d}}{2}\right) = x^2 - x + \tfrac{1-d}{4}.$$

So $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ when $d \equiv 1 \pmod 4$.

Therefore,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Example 2.24. Why don't we always use $\mathbb{Z}[\sqrt{d}]$? Why is $\mathcal{O}_K$ the right thing to study? Well, for example, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is a UFD, but $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

Proposition 2.25. *An algebraic integer $\alpha \in \mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. ($\Longrightarrow$). If α is a unit, then there is some β such that $\alpha\beta = 1$. We have $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(1) = 1$. Since $N_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\beta)$ are integers, we must have $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

($\Longleftarrow$). Assume that $K \subseteq \mathbb{C}$ and $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ are the complex embeddings with $\sigma_1 = \mathrm{id}$. We have

$$\pm 1 = N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha) = \alpha \cdot \sigma_2(\alpha)\cdots\sigma_n(\alpha).$$

A candidate for the inverse is $\beta = \sigma_2(\alpha)\cdots\sigma_n(\alpha)$. This is in K since $\alpha \in K$, so we need only check that β is an algebraic integer. But β is an algebraic integer because $\sigma_i(\alpha)$ are themselves algebraic integers, since they are roots of the minimal polynomial $p_\alpha(x) \in \mathbb{Z}[x]$. So $\alpha\beta = 1$ with $\beta \in \mathcal{O}_K$. □

2.3 $\mathcal{O}_K$ as an abelian group

Our next goal is to understand the additive abelian group structure of $\mathcal{O}_K$. We will learn that $\mathcal{O}_K \cong \mathbb{Z}x_1 \oplus \mathbb{Z}x_2 \oplus \ldots \oplus \mathbb{Z}x_n \cong \mathbb{Z}^n$.

Definition 2.26. The set $\{x_1, \ldots, x_n\}$ is an **integral basis** of $\mathcal{O}_K$. We sometimes also say that it is an integral basis of K, meaning the same thing.

Any integral basis is also a basis of K as a $\mathbb{Q}$-vector space. The image of these basis elements under the map

$$\begin{aligned} K &\longrightarrow \textstyle\prod_\sigma \mathbb{C} \\ \alpha &\longmapsto (\sigma(\alpha))_\sigma \end{aligned}$$

will lie in a smaller $\mathbb{R}$-vector space, which we define below.

For $\delta \colon K \to \mathbb{C}$, denote by $\overline{\sigma} \colon K \hookrightarrow \mathbb{C}$ the complex-conjugate embedding. For any $\alpha \in K$, we have

$$\overline{\sigma(\alpha)} = \overline{\sigma}(\alpha).$$

Definition 2.27. $K_\mathbb{R} := \left\{(\alpha_\sigma)_\sigma \in \prod_\sigma \mathbb{C} \;\middle|\; \overline{\alpha}_\sigma = \alpha_{\overline{\sigma}}\right\}$.

We have a map

$$\begin{aligned} K &\lhook\joinrel\longrightarrow K_\mathbb{R} \\ \alpha &\longmapsto (\sigma(\alpha))_\sigma \end{aligned}$$

Remark 2.28. $K \otimes_{\mathbb{Q}} \mathbb{R} \cong K_{\mathbb{R}}$ and $\dim_{\mathbb{R}} K_{\mathbb{R}} = \frac{1}{2} \dim_{\mathbb{R}} (\prod_\sigma \mathbb{C}) = n$, since if $\sigma = \overline{\sigma}$, then $\alpha_\sigma \in \mathbb{R}$, and if $\sigma \neq \overline{\sigma}$, then $\overline{a}_\sigma = a_{\overline{\sigma}}$, so knowing a_σ is enough to determine $a_{\overline{\sigma}}$.

Definition 2.29. An additive subgroup H of $\mathbb{C}^n$ (or $\mathbb{R}^n$) is **discrete** if $H \cap X$ is finite for any compact $X \subseteq \mathbb{C}^n$ (or $X \subseteq \mathbb{R}^n$).

Example 2.30. $\mathbb{Z} \subseteq \mathbb{C}$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subseteq \mathbb{C}$ are discrete, but $\mathbb{R} \subseteq \mathbb{C}$ is not.

Example 2.31. If $K = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, then $\mathcal{O}_K = K[\sqrt{2}]$. There are two embeddings $K \hookrightarrow \mathbb{C}$,

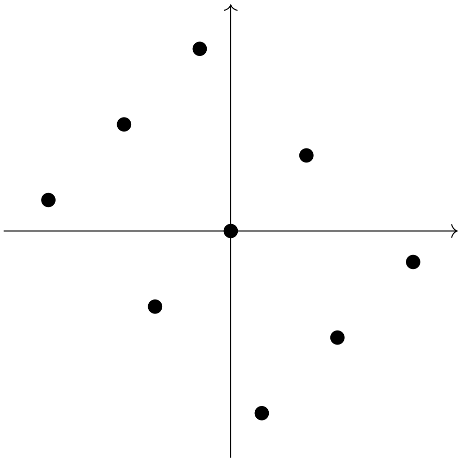
$$\begin{aligned} \sigma_1(a + b\sqrt{2}) &= a + b\sqrt{2} \\ \sigma_2(a + b\sqrt{2}) &= a - b\sqrt{2} \end{aligned}$$

These embeddings are self-conjugate, so $K_{\mathbb{R}} = \mathbb{R}^2$, and the map $K \hookrightarrow K_{\mathbb{R}} = \mathbb{R}^2$ is given by $\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha))$.

Example 2.32. $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ is not discrete, but the image of the embedding

$$\begin{aligned} \mathbb{Z}[\sqrt{2}] &\lhook\joinrel\longrightarrow \mathbb{R}^2 \\ a + b\sqrt{2} &\longmapsto (a + b\sqrt{2}, a - b\sqrt{2}) \end{aligned}$$

is discrete. The picture of this embedding is the lattice in $\mathbb{R}^2$ generated by the vectors $(1, -1)$ and $(\sqrt{2}, -\sqrt{2})$.



Proposition 2.33. *Under the inclusion* $i \colon K \hookrightarrow K_{\mathbb{R}}$, $i(\mathcal{O}_K)$ *is a discrete subgroup of the* $\mathbb{R}$*-vector space* $K_{\mathbb{R}}$.

Proof. Take any $r > 0$. It suffices to show that there are only finitely many $\alpha \in \mathcal{O}_K$ with $|\sigma(\alpha)| \leq r$ for all $\sigma \colon K \hookrightarrow \mathbb{C}$. Take such an α. Then

$$\prod_{\sigma}(x - \sigma(\alpha)) = p_\alpha(x)^{[K\colon \mathbb{Q}(\alpha)]} \in \mathbb{Z}[x]$$

since $\alpha \in \mathcal{O}_K$. The coefficients of the product on the left hand side are bounded in terms of r and the degree n, because $|\sigma(\alpha)| \leq r$. Hence, there are only finitely many possibilities for $\prod_\sigma(x - \sigma(\alpha))$ since $\mathbb{Z} \subseteq \mathbb{R}$ is discrete. Hence, there are only finitely many such α. □

The next proposition has little to do with number theory aside from its applications, but it is very useful so we'll prove it now.

Proposition 2.34. *Let* H *be a discrete subgroup of* $\mathbb{R}^n$*. Then* H *is a free* $\mathbb{Z}$*-module of rank at most* n*. Any* $\mathbb{Z}$*-basis of* H *is linearly independent over* $\mathbb{R}$*.*

Proof. Let $V = \operatorname{Span}_{\mathbb{R}}(H)$. By choosing a basis for V in H, we may assume that $\mathbb{Z}^r \subseteq H \subseteq \mathbb{R}^r$ with $r = \dim_{\mathbb{R}} V \leq n$. Replacing $\mathbb{R}^n$ by V if necessary, we may reduce to the case that $\mathbb{Z}^n \subseteq H \subseteq \mathbb{R}^n$.

Now consider $H/\mathbb{Z}^n$. Every coset has a representative with $(a_1, \ldots, a_n) \in H \subseteq \mathbb{R}^n$ with $0 \leq a_i < 1$. Since H is discrete, there are only finitely many such $(a_1, \ldots, a_n)$ representing cosets in $H/\mathbb{Z}^n$. Hence, this quotient is finite.

Set $m := \#H/\mathbb{Z}^n$. Multiplying any element of $H/\mathbb{Z}^n$ by m must give the identity coset, so multiplying any element of H by m lands in $\mathbb{Z}^n$. So $\mathbb{Z}^n \subseteq H \subseteq \frac{1}{m}\mathbb{Z}^n$. Therefore, H must be free of rank n as a $\mathbb{Z}$-module. □

The application of this proposition is the following.

Proposition 2.35. $\mathcal{O}_K \cong \mathbb{Z}^n$ *as an additive abelian group.*

Proof. By Proposition 2.34, we know that $\mathcal{O}_K \cong i(\mathcal{O}_K) \subseteq K_{\mathbb{R}} \cong \mathbb{R}^n$. Therefore, $\mathcal{O}_K \cong \mathbb{Z}^r$ with $r \leq n$.

Take any basis $x_1, \ldots, x_n$ of K over $\mathbb{Q}$. Then by multiplying by some integer $m \geq 1$ if necessary, we may assume $x_i \in \mathcal{O}_K$. Therefore, $x_1, \ldots, x_n$ are independent in $(\mathcal{O}_K, +)$, so $r \geq n$.

Hence, $\mathcal{O}_K \cong \mathbb{Z}^n$ as an additive abelian group, with basis $x_1, \ldots, x_n$. □

2.4 Discriminants

How can we compute $\mathcal{O}_K$? So far we've only investigated quadratic extensions, but we don't know how to do this in general. If $K = \mathbb{Q}(\sqrt[3]{2})$, we might guess $\mathcal{O}_K \overset{?}{=} \mathbb{Z}\left[\sqrt[3]{2}\right]$. Discriminants will let us check our guesses efficiently.

Definition 2.36. An **order** of K is a subring $R \subseteq K$ that is isomorphic as an additive group to $\mathbb{Z}^n$, where $n = [K\colon \mathbb{Q}]$.

Example 2.37. $\mathbb{Z}[\sqrt[3]{2}]$ is an order of $\mathbb{Q}(\sqrt[3]{2})$. In Proposition 2.35, we showed that $\mathcal{O}_K$ is an order of K.

This next lemma shows that $\mathcal{O}_K$ is the maximal order of K. Often, $\mathcal{O}_K$ is defined this way.

Lemma 2.38. *For any order* $R \subseteq K$*, we have* $R \subseteq \mathcal{O}_K$*.*

Proof. Take any $\alpha \in R$. Then $\alpha R \subseteq R$, and R is a finitely generated $\mathbb{Z}$-submodule of K. This is one of the four equivalent definitions of algebraic integer, so $\alpha \in \mathcal{O}_K$. □

We have a symmetric $\mathbb{Q}$-bilinear pairing on K

$$\begin{aligned} \langle\ ,\ \rangle \colon K \times K &\longrightarrow \mathbb{Q} \\ (\alpha, \beta) &\longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) \end{aligned}$$

For any order R, this pairing lands in $\mathbb{Z}$, since the trace of an algebraic integer is an integer.

$$\begin{aligned} \langle\ ,\ \rangle \colon R \times R &\longrightarrow \mathbb{Z} \\ (\alpha, \beta) &\longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) \end{aligned}$$

Remark 2.39. This induces a pairing on $K \otimes_{\mathbb{Q}} \mathbb{R} \cong K_{\mathbb{R}}$ and gives it a Euclidean structure.

Fix a basis $x_1, \ldots, x_r$ of R as a $\mathbb{Z}$-module, and write $\alpha, \beta \in R$ as

$$\alpha = \sum_{i=1}^{r} a_i x_i$$
$$\beta = \sum_{i=1}^{r} b_i x_i$$

with $a_i, b_i \in \mathbb{Z}$. Then expanding linearly,

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = \sum_{i,j} a_i \,\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j) b_j = (a_1, \ldots, a_n) \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(x_1 x_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(x_1 x_r) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(x_r x_1) & \cdots & \mathrm{Tr}_{K/\mathbb{Q}}(x_r x_r) \end{pmatrix} \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$$

Definition 2.40. The **discriminant** of an n-tuple $(x_1, \ldots, x_n) \in \mathcal{O}_K^n$ is

$$\mathrm{disc}(x_1, \ldots, x_n) := \det\left(\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j)\right) \in \mathbb{Z}$$

Choose another basis $y_1, \dots, y_r$ of R such that

$$y_i = \sum_{j=1}^{r} B_{ij} x_j$$

for some $B_{ij} \in \mathbb{Z}$. The matrix B with these entries is invertible, $B \in \mathrm{GL}_n(\mathbb{Z})$. One can check that

$$\Big(\operatorname{Tr}_{K/\mathbb{Q}}(y_i y_j) \Big) = B \Big(\operatorname{Tr}_{K/\mathbb{Q}}(x_i x_j) \Big) B^T$$

Taking determinants, we learn that

$$\operatorname{disc}(y_1, \dots, y_n) = \det(B)^2 \operatorname{disc}(x_1, \dots, x_n),$$

but $\det(B) = \pm 1$, so the discriminants of the two bases are the same.

Definition 2.41. The **discriminant** of an order R is

$$\operatorname{disc}(R) := \operatorname{disc}(x_1, \dots, x_n)$$

for any $\mathbb{Z}$-basis $x_1, \dots, x_n$ of R.

This will later give us a formula for determining $\mathcal{O}_K$. We will show that for any order $R \subseteq \mathcal{O}_K$, $\operatorname{disc}(R) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K \colon R]^2$. Then, to find $\mathcal{O}_K$:

(1) make a guess; it will be an order R

(2) compute $\operatorname{disc}(R)$ to discover a finite number of possibilities for $[\mathcal{O}_K \colon R]$.

(3) Notice that $R \subseteq \mathcal{O}_K \subseteq \frac{1}{m} R$

Remark 2.42. $\operatorname{disc}(R) \neq 0$, since the pairing is non-degenerate. To prove this, suppose $\alpha \in R$, $\alpha \neq 0$. Then $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = [K \colon \mathbb{Q}] \neq 0$. There is some $m \geq 1$ such that $m\alpha^{-1} \in R$. Therefore, $\langle \alpha, \beta \rangle = m[K \colon \mathbb{Q}] \neq 0$.

Definition 2.43. The **discriminant** of K is $\operatorname{disc}(K) := \operatorname{disc}(\mathcal{O}_K)$.

Remark 2.44. There are many different notations for $\operatorname{disc}(K)$, with no standard convention. Basically anything reasonable is used: d_K, D_K, $\Delta_K, \dots$

Lemma 2.45. *Let* $R \subseteq K$ *be an order. Then* $\operatorname{disc}(R) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K \colon R]^2$.

To prove this lemma, we will use **Smith Normal Form**.

Theorem 2.46 (Smith Normal Form)**.** *Given any $n \times n$ integer matrix B of rank r, there are invertible $n \times n$ integer matrices $P, Q \in GL_n(\mathbb{Z})$ such that*

$$PBQ = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

with $d_i \geq 1$ and $d_i \mid d_{i+1}$.

Exercise 2.47. Prove the classification theorem of finitely generated abelian groups using Smith normal form.

Proof of Lemma 2.45. Write $\mathcal{O}_K = \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_n$ and let $R \subseteq \mathcal{O}_K$ be an order with $R = \mathbb{Z}y_1 \oplus \ldots \oplus \mathbb{Z}y_n$. We may write y_is as a linear combination of the x_is.

$$y_i = \sum_{j=1}^{n} B_{ij} x_i$$

for a unique $B \in M_n(\mathbb{Z})$ with $\det(B) \neq 0$. Observe that $[\mathcal{O}_K \colon R] = [\mathbb{Z}^n \colon B(\mathbb{Z}^n)]$. As before,

$$\operatorname{disc}(y_1, \ldots, y_n) = \det(B)^2 \operatorname{disc}(x_1, \ldots, x_n).$$

Therefore,

$$\operatorname{disc}(R) = \det(B)^2 \operatorname{disc}(\mathcal{O}_K).$$

So it remains to show that $\det(B) = \pm[\mathcal{O}_K \colon R]$. Without loss of generality, we may assume that B is in Smith normal form.

$$B = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

with $d_i \geq 1$ (we don't lose any generality because replacing B by PBQ does not change $[\mathbb{Z}^n \colon B\mathbb{Z}^n]$ or $\pm\det(B)$, since P and Q are invertible integer matrices, so have $\det(P), \det(Q) \in \{\pm 1\}$). Now we may write $\det(B) = d_1 d_2 \cdots d_n$ and therefore

$$B\mathbb{Z}^n = d_1\mathbb{Z} \times d_2\mathbb{Z} \times \cdots \times d_n\mathbb{Z}$$

and

$$\mathbb{Z}^n/_{B\mathbb{Z}^n} = \mathbb{Z}/_{d_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{d_n\mathbb{Z}},$$

which has cardinality $d_1 d_2 \cdots d_n$, as desired. □

Example 2.48. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ squarefree. Then we have an order $R = \mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. The discriminant of this order is

$$\begin{aligned} \operatorname{disc}(R) &= \operatorname{disc}(1, \sqrt{d}) \\ &= \det \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1 \cdot 1) & \mathrm{Tr}_{K/\mathbb{Q}}(1 \cdot \sqrt{d}) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d} \cdot 1) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d} \cdot \sqrt{d}) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d \end{aligned}$$

So $4d = \operatorname{disc}(R) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K \colon R]^2$. Therefore, $[\mathcal{O}_K \colon R] \in \{1, 2\}$ since d is squarefree. So

$$R \subseteq \mathcal{O}_K \subseteq \frac{1}{2}R.$$

Notice that $R/\frac{1}{2}R$ has coset representatives $1, \frac{1}{2}, \frac{\sqrt{d}}{2}$ and $\frac{1+\sqrt{d}}{2}$. Therefore,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

$$\operatorname{disc}(\mathcal{O}_K) = \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod 4 \\ d & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Remark 2.49. The discriminant of $\mathcal{O}_K$ determines a degree 2 extension $K/\mathbb{Q}$ up to isomorphism. We'll later see that up to isomorphism, there are only finitely many number fields of any degree with a given discriminant.

Lemma 2.50. *Let $\sigma_1, \ldots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ be the complex embeddings of K. Let A be the matrix*

$$X = \begin{pmatrix} \sigma_1(x_1) & \ldots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \ldots & \sigma_n(x_n) \end{pmatrix}$$

Then for $x_1, \ldots, x_n \in \mathcal{O}_K$, $\operatorname{disc}(x_1, \ldots, x_n) = \det(A)^2$.

Proof. Recall that

$$\operatorname{disc}(x_1, \ldots, x_n) = \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(x_1 x_1) & \mathrm{Tr}_{K/\mathbb{Q}}(x_1 x_2) & \ldots & \mathrm{Tr}_{K/\mathbb{Q}}(x_1 x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(x_n x_1) & \mathrm{Tr}_{K/\mathbb{Q}}(x_n x_2) & \ldots & \mathrm{Tr}_{K/\mathbb{Q}}(x_n x_n) \end{pmatrix}$$

And furthermore, $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x)$. Therefore,

$$\operatorname{disc}(x_1, \ldots, x_n) = \det\left(\left[\sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j) \right]_{i,j} \right) = \det(X^T X) = \det(X)^2.$$

□

Example 2.51. Let $K = \mathbb{Q}(\sqrt{d})$ for $d \neq 1$ squarefree. Let $R = \mathbb{Z}\left[\sqrt{d}\right]$. The two complex embeddings are

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$$
$$\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$$

We use the lemma to compute the discriminant of this order.

$$\begin{aligned} \operatorname{disc}(\mathbb{Z}\left[\sqrt{d}\right]) &= \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_1(\sqrt{d}) \\ \sigma_2(1) & \sigma_2(\sqrt{d}) \end{pmatrix}\right)^2 \\ &= \left(\det\begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right) \\ &= (-2\sqrt{d})^2 = 4d \end{aligned}$$

Definition 2.52. Recall that the **discriminant** of a monic $f(x) \in \mathbb{Q}[x]$ of degree $n \geq 1$ is

$$\operatorname{disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in \mathbb{Q}$$

where $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ are the roots of f in $\mathbb{C}$. If $f \in \mathbb{Z}[x]$, then $\operatorname{disc}(f) \in \mathbb{Z}$.

Example 2.53. Some special cases:

$$\begin{aligned} \operatorname{disc}(x^2 + bx + c) &= b^2 - 4c \\ \operatorname{disc}(x^3 + bx^2 + cx + d) &= b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd \\ \operatorname{disc}(x^3 + cx + d) &= -4c^3 - 27d^2 \end{aligned}$$

Lemma 2.54. *Take an $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. Hence, $\mathbb{Z}[\alpha]$ is an order of K. Then $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(p_\alpha(x))$, where $p_\alpha(x)$ is the minimal polynomial of α over $\mathbb{Q}$.*

Proof. Let $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ be the complex embeddings. The roots of $p_\alpha(x)$ in $\mathbb{C}$ are $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$. Take $\alpha_i = \sigma_i(\alpha)$.

The order $\mathbb{Z}[\alpha]$ has a $\mathbb{Z}$-basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. The discriminant of this order is

$$\begin{aligned} \operatorname{disc}(\mathbb{Z}[\alpha]) &= \operatorname{disc}(1, \alpha, \dots, \alpha^{n-1}) \\ &= \left(\det\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}\right)^2 \\ &= \left(\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)\right)^2 = \operatorname{disc}(p_\alpha(x)) \end{aligned}$$ □

Remark 2.55. A strategy for computing $\mathcal{O}_K$:

(1) Find an order $R \subseteq \mathcal{O}_K$.

(2) Bound $[\mathcal{O}_K \colon R]$ using $\operatorname{disc}(R) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K \colon R]^2$ and the prime factorization of $\operatorname{disc}(R)$.

(3) For a possible $m = [\mathcal{O}_K \colon R]$, check which cosets of R in $\frac{1}{m}R$ consist of algebraic integers.

Example 2.56. Let $K = \mathbb{Q}(\alpha)$ with α a root of $f(x) = x^3 + x + 1$. Then $\mathbb{Z}[\alpha]$ is an order of K with

$$\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(f) = -4(1)^3 - 27(1)^2 = -31.$$

We know that $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(\mathcal{O}_K)\left[\mathcal{O}_K \colon \mathbb{Z}[\alpha]\right]^2$, and since 31 is prime, we must have $[\mathcal{O}_K \colon \mathbb{Z}[\alpha]] = 1$. Therefore, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(K) = -31$.

Example 2.57. Let $K = \mathbb{Q}(\alpha)$ with α a root of $f(x) = x^3 - x^2 - 2x - 8$. Look at the order $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Then

$$\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(f) = -2012 = -2^2 \cdot 503.$$

This tells us that either $[\mathcal{O}_K \colon \mathbb{Z}[\alpha]] \in \{1, 2\}$. Hence,

$$\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K \subseteq \frac{1}{2}\mathbb{Z}[\alpha].$$

The group $\frac{1}{2}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]$ has coset representatives $\frac{a}{2} + \frac{b}{2}\alpha + \frac{c}{2}\alpha^2$ with $a, b, c \in \{0, 1\}$. We can then check which of these eight elements are algebraic integers.

In particular, claim that $\theta = (\alpha + \alpha)^2/2 \in \mathcal{O}_K$. To show this, recall that K has $\mathbb{Q}$-basis $1, \alpha, \alpha^2$. θ acts on this basis by

$$\begin{aligned}\theta \cdot 1 &= \quad \tfrac{1}{2}\alpha + \tfrac{1}{2}\alpha^2 \\ \theta \cdot \alpha &= 4 + \alpha + 2\alpha^2 \\ \theta \cdot \alpha^2 &= 8 + 6\alpha + 2\alpha^2\end{aligned}$$

So θ is a root of

$$\det\left(xI - \begin{pmatrix} 0 & 4 & 8 \\ 1/2 & 1 & 6 \\ 1/2 & 1 & 2 \end{pmatrix}\right) = x^3 - 3x^2 - 10x - 8.$$

So $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\theta$, where $\theta = \frac{1}{2}(\alpha + \alpha^2)$. Note that this is not the same as $\mathbb{Z}[\beta]$ for any $\beta \in \mathcal{O}_K$.

Lemma 2.58. $K = \mathbb{Q}(\alpha)$ *with* $\alpha \in \mathcal{O}_K$. *Let* $f \in \mathbb{Z}[x]$ *be the minimal polynomial of* α. *Then*

$$\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(f) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(f'(\alpha)).$$

Proof. We previously proved the first equality in Lemma 2.54, so we must prove the second one. Let $\sigma_1, : \sigma_n \colon K \hookrightarrow \mathbb{C}$ be the complex embeddings. We have

$$\begin{aligned}\operatorname{disc}(f) &= \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 \\ &= (-1)^{\binom{n}{2}} \prod_j \prod_{i \ne j} (\sigma_j(\alpha) - \sigma_i(\alpha)) \qquad (2.1)\end{aligned}$$

Let's compute the derivative of f: if $f = \prod_i (x - \sigma_i(\alpha))$, then

$$f' = \sum_j \prod_{i \ne j} (x - \sigma_i(\alpha)).$$

Therefore,

$$f'(\sigma_j(\alpha)) = \prod_{i \ne j} (\sigma_j(\alpha) - \sigma_i(\alpha))$$

Substituting into Eq. (2.1), we see

$$\begin{aligned}\operatorname{disc}(f) &= (-1)^{\binom{n}{2}} \prod_j f'(\sigma_j(\alpha)) \\ &= (-1)^{\binom{n}{2}} \prod_j \sigma_j(f'(\alpha))\end{aligned}$$

This last equality holds because f, and consequently f', has integer coefficients, and every complex embedding fixes the integers. □

2.5 Example: Cyclotomic Integers

Definition 2.59. Let p be an odd prime. Let $\zeta \ne 1$ be a p-th root of unity. Then $K = \mathbb{Q}(\zeta)$ is the p-th **cyclotomic field.**

Example 2.60. Let K be the p-th cyclotomic field with primitive element ζ. Define:

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x].$$

Notice that $f(\zeta) = 0$ and f is irreducible (because f is Eisenstein at p).

We have $[K\colon \mathbb{Q}] = p - 1$. What is $\mathcal{O}_K$? We guess $\mathbb{Z}[\zeta]$. Let's compute:

$$\operatorname{disc}(\mathbb{Z}[\zeta]) = (-1)^{\binom{p-1}{2}} N_{K/\mathbb{Q}}(f'(\zeta)).$$

To find the derivative of f, write

$$(x-1)f(x) = x^p - 1$$

and differentiate:

$$f(x) + (x-1)f'(x) = px^{p-1}$$

and plug in $x = \zeta$:

$$f(\zeta) + (\zeta-1)f'(\zeta) = p\zeta^{p-1}.$$

Since f is the minimal polynomial of ζ, $f(\zeta) = 0$. Now take norms:

$$N_{K/\mathbb{Q}}(\zeta-1)N_{K/\mathbb{Q}}(f'(\zeta)) = N_{K/\mathbb{Q}}(p)N_{K/\mathbb{Q}}(\zeta)^{p-1}.$$

We know that $N_{K/\mathbb{Q}}(p) = p^{[K:\,\mathbb{Q}]} = p^{p-1}$, and $N_{K/\mathbb{Q}}(\zeta) = \pm 1$ since ζ is a unit in $\mathcal{O}_K$. Hence,

$$N_{K/\mathbb{Q}}(\zeta-1)N_{K/\mathbb{Q}}(f'(\zeta)) = p^{p-1}(\pm 1)^{p-1} = p^{p-1},$$

the last equality since p is odd.

Now claim that $N_{K/\mathbb{Q}}(\zeta-1) = p$. This follows because

$$\begin{aligned} N_{K/\mathbb{Q}}(\zeta-1) &= (-1)^{p-1}N_{K/\mathbb{Q}}(1-\zeta) \\ &= N_{K/\mathbb{Q}}(1-\zeta) \\ &= \prod_{\sigma:\,K\hookrightarrow\mathbb{C}} \sigma(1-\zeta) \\ &= \prod_{\sigma}(1-\sigma(\zeta)) \\ &= f(1) = p \end{aligned}$$

Therefore, $\operatorname{disc}\mathbb{Z}[\zeta] = (-1)^{\frac{p-1}{2}}p^{p-2}$.

Suppose that $\mathcal{O}_K \supsetneq \mathbb{Z}[\zeta]$. Then $[\mathcal{O}_K\colon \mathbb{Z}[\zeta]] = p^e$ for some $e \geq 1$. This means that there is some $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}[\zeta]$ such that $p\alpha \in \mathbb{Z}[\zeta]$.

Now we use the fact that $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$, so we may write

$$\alpha = \frac{a_0}{p} + \frac{a_1}{p}(\zeta-1) + \ldots + \frac{a_p}{p}(\zeta-1)^{p-2}$$

with $a_i \in \mathbb{Z}$ but not all divisible by p. After subtracting an element in $\mathbb{Z}[\zeta]$, we may assume that for some $0 \leq i \leq p-1$, (remove the first $(i-1)$ terms with coefficient divisible by p.)

$$\alpha = \frac{a_i}{p} + \ldots + \frac{a_{p-2}}{p}(\zeta-1)^{p-2}$$

such that p does not divide a_i.

$$\frac{p\alpha}{(\zeta-1)^{i+1}} = \frac{a_i}{\zeta-1} + a_{i+1} + a_{i+2}(\zeta-1) + \ldots + a_{p-2}(\zeta-1)^{p-2-(i+1)}. \quad (2.2)$$

All but the first term lie in $\mathbb{Z}[\zeta]$. Note that

$$N_{K/\mathbb{Q}}\left(\frac{p\alpha}{(\zeta-1)^{i+1}}\right) = \frac{a_i^{p-1}}{p} \in \mathbb{Q}\setminus\mathbb{Z}.$$

This tells us that the first term in Eq. (2.2) is not an algebraic integer, since otherwise the whole expression would have integral norm.

$$\frac{a_i}{\zeta-1} \notin \mathcal{O}_K \implies \frac{p}{(\zeta-1)^{i+1}}\cdot\alpha \notin \mathcal{O}_K.$$

But since $\alpha \in \mathcal{O}_K$, we have

$$\frac{p}{(\zeta-1)^{i+1}} \notin \mathcal{O}_K.$$

Therefore, since $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$,

$$\frac{p}{(\zeta-1)^{i+1}} \notin \mathbb{Z}[\zeta].$$

We show that this is actually a contradiction in the next lemma, which demonstrates that $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

Lemma 2.61. $\dfrac{p}{(\zeta-1)^{i+1}} \in \mathbb{Z}[\zeta]$

Proof.

$$\begin{aligned} p &= N_{K/\mathbb{Q}}(\zeta-1) \\ &= \prod_{\sigma}(\sigma(\zeta)-1) \\ &= \prod_{i=1}^{p-1}(\zeta^i-1) \end{aligned}$$

Now write $\zeta^i - 1 = (\zeta-1)(1+\zeta+\ldots+\zeta^{i-1})$. Therefore, $(\zeta-1)^{p-1}$ divides p in $\mathbb{Z}[\zeta]$. □

Remark 2.62. We have that

$$\frac{p}{(\zeta-1)^{p-1}} \in \mathbb{Z}[\zeta].$$

Taking norms, we have

$$\frac{p^{p-1}}{p^{p-1}} = 1,$$

so $p = u(\zeta-1)^{p-1}$ for some $u \in \mathbb{Z}[\zeta]^\times$.

Remark 2.63. Take any $m \geq 1$, and let ζ_m be a primitive m-th root of unity. The ring of integers of $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$ and the discriminant of $\mathcal{O}_K$ divides $m^{\phi(m)}$, where ϕ is the Euler totient function.

3 The ideal class group

Proposition 3.1. *Let* $I \subseteq \mathcal{O}_K$ *be a nonzero ideal. Then* $\mathcal{O}_K/I$ *is a* ***finite*** *ring.*

Proof. Take $0 \neq \alpha \in I$. This gives a surjective homomorphism

$$\mathcal{O}_K/\alpha\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/I$$

Hence, we may assume that $I = \alpha\mathcal{O}_K$ is a principal ideal. Let $\mu_\alpha \colon \mathcal{O}_K \to \mathcal{O}_K$ be the multiplication by α map. Choose a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and write $\mu_\alpha = A \colon \mathbb{Z}^n \to \mathbb{Z}^n$, where A is the matrix for μ_α in this basis. Then

$$\#\left(\mathcal{O}_K/\alpha\mathcal{O}_K\right) = [\mathcal{O}_K \colon \alpha(\mathcal{O}_K)] = [\mathbb{Z}^n \colon A\mathbb{Z}^n].$$

Putting A in Smith normal form, we have

$$A' = PAQ^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$$

for some $P, Q \in GL_n(\mathbb{Z})$ with $d_i \geq 1$. We know that A is invertible because $\det(A) = \det(\mu_\alpha) = N_{K/\mathbb{Q}}(\alpha) \neq 0$. Hence,

$$\begin{aligned}
[\mathbb{Z}^n \colon A\mathbb{Z}^n] &= [\mathbb{Z}^n \colon A'(\mathbb{Z}^n)] \\
&= [\mathbb{Z}^n \colon d_1\mathbb{Z}^n \times \cdots \times d_n\mathbb{Z}^n] \\
&= d_1 d_2 \cdots d_n \\
&= \det(A') \\
&= \pm\det(A) = \pm N_{K/\mathbb{Q}}(\alpha)
\end{aligned}$$

Hence, for $\alpha \in \mathcal{O}_K$ nonzero,

$$\#\left(\mathcal{O}_K/\alpha\mathcal{O}_K\right) = |N_{K/\mathbb{Q}}(\alpha)|$$

The proposition follows. □

Remark 3.2. The proof above actually shows more: it gives a formula for the size of the quotient $\mathcal{O}_K/I$ when I is a principal ideal.

Definition 3.3. For an ideal $I \leq \mathcal{O}_K$, the **norm** of the ideal I is

$$N(I) = \#\left(\mathcal{O}_K/I\right).$$

In particular, we have $N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$. Note that the larger an ideal is, the smaller its norm.

Remark 3.4.

(a) Observe that there can only be finitely many ideals with a given norm: if $N(I) = m$, then $I \subseteq \mathcal{O}_K$ with index m as an additive group. Hence, $m\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$. If $\mathcal{O}_K \cong \mathbb{Z}^n$, then the index of $m\mathcal{O}_K \subseteq \mathcal{O}_K$ is m^n. So there can only be finitely many possible additive subgroups, and hence ideals, in between $m\mathcal{O}_K$ and $\mathcal{O}_K$.

(b) Let $I \neq 0$ be an ideal of $\mathcal{O}_K$. Then $I \cong \mathbb{Z}^n$ as additive groups. In particular, $\mathcal{O}_K$ is Noetherian.

(c) All nonzero prime ideals of $\mathcal{O}_K$ are maximal: if $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain. Recall that all finite integral domains are fields, so $\mathfrak{p}$ must be maximal.

3.1 Unique Factorization

The rings of integers $\mathcal{O}_K$ are nice, but they don't have everything we might want. Unique factorization may fail in $\mathcal{O}_K$.

Example 3.5. Let $K = \mathbb{Q}(\sqrt{-5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then we may factor 6 in two different ways:

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

For these to be genuinely different factorizations, 2 and 3 must not differ by a unit from $1 \pm \sqrt{-5}$. Claim that the units of $\mathcal{O}_K$ are just ± 1. Indeed, if $\alpha \in \mathcal{O}_K$, then $\alpha = a + b\sqrt{-5}$

$$\begin{aligned} \alpha \in \mathcal{O}_K^\times &\iff N_{K/\mathbb{Q}}(\alpha) = \pm 1 \\ &\iff a^2 + 5b^2 = \pm 1 \\ &\iff (a, b) = (\pm 1, 0) \\ &\iff \alpha = \pm 1 \end{aligned}$$

Claim that all of $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in $\mathcal{O}_K$. Consider first $1 + \sqrt{-5}$. If $1 + \sqrt{-5} = \alpha\beta$, then taking norms we see $6 = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$, where $N_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\beta)$ are positive integers. Therefore,

$$N_{K/\mathbb{Q}}(\alpha) \in \{1, 2, 3, 6\}$$

Let's check all four cases. If $N_{K/\mathbb{Q}}(\alpha) = 1$, then $\alpha \in \mathcal{O}_K^\times$. If $N_{K/\mathbb{Q}}(\alpha) = 6$, then $N_{K/\mathbb{Q}}(\beta) = 1$ and $\beta \in \mathcal{O}_K^\times$. If $N_{K/\mathbb{Q}}(\alpha) \in \{2, 3\}$, then write $\alpha = a + b\sqrt{-5}$. We have $a^2 + 5b^2 \in \{2, 3\}$, but this is impossible in the integers.

Nevertheless, we can recover a form of prime factorization if we work with ideals instead.

Theorem 3.6. *Let K be a number field. Every nonzero ideal of $\mathcal{O}_K$ can be uniquely expressed as a product of prime ideals up to reordering.*

This theorem is proved in Section 3.2.

Example 3.7. Consider $K = \mathbb{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Let $\mathfrak{p}$ be the ideal $\langle 2, 1+\sqrt{-5}\rangle \subseteq \mathcal{O}_K$. Claim that $\mathfrak{p}$ is prime.

To see this, check that the quotient is a field.

$$\mathcal{O}_K/_{\mathfrak{p}} = \mathbb{Z}[\sqrt{-5}]/_{\langle 2, 1+\sqrt{-5}\rangle} \cong \mathbb{Z}/_2$$

Notice that $\mathfrak{p}$ is non-principal. We have a factorization:

$$\mathfrak{p}^2 = \left\langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5} \right\rangle = \langle 2 \rangle$$

Define the ideals $\mathfrak{q}_1 = \langle 3, 1+\sqrt{-5}\rangle$ and $\mathfrak{q}_2 = \langle 3, 1-\sqrt{-5}\rangle$. These are both prime; $\mathcal{O}_K/\mathfrak{q}_i \cong \mathbb{Z}/3$. These ideals factor the ideal $\langle 3\rangle$.

$$\mathfrak{q}_1\mathfrak{q}_2 = \left\langle 9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6 \right\rangle = \langle 3 \rangle .$$

Therefore, we have a factorization

$$\langle 6 \rangle = \langle 2 \rangle \langle 3 \rangle = \mathfrak{p}^2 \cdot \mathfrak{q}_1\mathfrak{q}_2.$$

What about the other factorization $6 = (1+\sqrt{-5})(1-\sqrt{-5})$? We have

$$\begin{aligned} \mathfrak{p}\mathfrak{q}_1 &= \left\langle 6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, (1+\sqrt{-5})^2 \right\rangle = \left\langle 1+\sqrt{-5} \right\rangle \\ \mathfrak{p}\mathfrak{q}_2 &= \left\langle 6, 2-2\sqrt{-5}, 3-3\sqrt{-5}, (1-\sqrt{-5})^2 \right\rangle = \left\langle 1-\sqrt{-5} \right\rangle \end{aligned}$$

So there is another factorization

$$\langle 6 \rangle = \left\langle 1+\sqrt{-5} \right\rangle \left\langle 1-\sqrt{-5} \right\rangle = \mathfrak{p}\mathfrak{q}_1 \cdot \mathfrak{p}\mathfrak{q}_2$$

Remark 3.8. The theorem fails for every order $R \subseteq K$ except $\mathcal{O}_K$.

Assuming the theorem, how do we find and study prime ideals in $\mathcal{O}_K$? Given any nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$, we know that $\mathcal{O}_K/\mathfrak{p}$ is a finite field. If p is the characteristic of $\mathcal{O}_K/\mathfrak{p}$, we have an inclusion

$$\mathbb{Z}/_{\langle p \rangle} \hookrightarrow \mathcal{O}_K/_{\mathfrak{p}}$$

Hence, $p \in \mathfrak{p}$, and we may factor

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}.$$

Definition 3.9. p is **ramified** in K if $e_i > 1$ for some i in the factorization above.

Remark 3.10. Later, we will prove that p is ramified in K if and only if p divides the discriminant of K.

Since $p \in \mathfrak{p}$, we have

$$\mathfrak{p} \supseteq p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

so $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some i. Since every nonzero prime of $\mathcal{O}_K$ is maximal, this inclusion must be an equality: $\mathfrak{p} = \mathfrak{p}_i$ for some i. We have proved:

Fact 3.11. *Any nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ occurs in the factorization of $p\mathcal{O}_K$, where p is the characteristic of $\mathcal{O}_K/\mathfrak{p}$.*

Theorem 3.12 (Chinese Remainder Theorem)**.** *Let R be a unital commutative ring. If $I_1, \ldots, I_m$ are pairwise coprime ideals of R, then the homomorphism of rings*

$$\begin{aligned} \phi\colon R &\longrightarrow {}^{R}\!/_{I_1} \oplus \ldots \oplus {}^{R}\!/_{I_m} \\ r &\longmapsto (r + I_1, \ldots, r + I_m) \end{aligned}$$

is surjective with kernel $I_1 \cap I_2 \cap \cdots \cap I_m$.

If $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$, then

$$ {}^{\mathcal{O}_K}\!/_{p\mathcal{O}_K} \cong \bigoplus_{i=1}^{r} {}^{\mathcal{O}_K}\!/_{\mathfrak{p}_i^{e_i}}$$

by the Chinese Remainder Theorem.

Let's explain now how to factor $p\mathcal{O}_K$ into prime ideals. This procedure will work for most primes $p \in \mathbb{Z}$.

Let $K/\mathbb{Q}$ be any number field, and consider the order $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Let $g(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Take any prime p not dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Let $\overline{g}$ be the image of $g(x)$ in $\mathbb{F}_p[x]$. Factor $\overline{g}$ as

$$\overline{g} = \overline{g}_1^{e_1}\cdots\overline{g}_r^{e_r}$$

with $\overline{g}_i \in \mathbb{F}_p[x]$ monic, irreducible and distinct, and $e_i \geq 1$. For each $1 \leq i \leq r$, choose a preimage $g_i \in \mathbb{Z}[x]$ of $\overline{g}_i$ such that g_i is monic and has the same degree as $\overline{g}_i$. Define the ideals

$$\mathfrak{p}_i = \langle p, g_i(\alpha)\rangle \subseteq \mathcal{O}_K.$$

Proposition 3.13. *Each $\mathfrak{p}_i$ is a prime ideal. Moreover, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$.*

Example 3.14. Let $K = \mathbb{Q}(\sqrt{-5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Take $p = 3$ and let $\alpha = \sqrt{-5}$. Then $g(x) = x^2 + 5$, which factors as

$$x^2 + 5 \equiv (x-1)(x+1) \pmod 3.$$

So $g_1(x) = x + 1$ and $g_2(x) = x - 1$. Then

$$3\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2,$$

where $\mathfrak{q}_1 = \langle 3, 1+\sqrt{-5}\rangle$ and $\mathfrak{q}_2 = \langle 3, 1-\sqrt{-5}\rangle$.

Remark 3.15. Why doesn't this work for primes p dividing $\left[\mathcal{O}_K \colon \mathbb{Z}[\alpha]\right]$. The idea is that if

$$\phi \colon {}^{\mathbb{Z}[\alpha]}\!/_{\langle p\rangle} \to {}^{\mathcal{O}_K}\!/_{p\mathcal{O}_K}$$

is the homomorphism induced by the inclusion $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$, then the index

$$\left[{}^{\mathcal{O}_K}\!/_{p\mathcal{O}_K} \colon \phi\left({}^{\mathbb{Z}[\alpha]}\!/_{\langle p\rangle}\right)\right]$$

is a power of p since $\#(\mathcal{O}_K/p\mathcal{O}_K) = p^{[K \colon \mathbb{Q}]}$ and moreover divides $[\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$. The assumption that p does not divide $[\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$ implies that ϕ is surjective.

Remark 3.16. For any nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, we have $\mathfrak{p} \cap \mathbb{Z} = \langle p\rangle$, where p is the characteristic of $\mathcal{O}_K/\mathfrak{p}$.

Proposition 3.17. *Fix a prime p and an order $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ such that $p \nmid \left[\mathcal{O}_K \colon \mathbb{Z}[\alpha]\right]$. Let g be the minimal polynomial of α, and let $\overline{g} = g \pmod p$ be the image of $g(x)$ in $\mathbb{F}_p[x]$. Factor*

$$\overline{g} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$$

where the $\overline{g}_i \in \mathbb{F}_p[x]$ are distinct, monic, and irreducible. Let $f_i = \deg(\overline{g}_i)$, and for each i, choose $g_i(x) \in \mathbb{Z}[x]$ whose image mod p is $\overline{g}_i$.

Then $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i = \langle p, g_i(\alpha)\rangle \subseteq \mathcal{O}_K$ are distinct primes. Moreover, $[\mathcal{O}_K/\mathfrak{p}_i \colon \mathbb{F}_p] = f_i$.

Proof. We have a homomorphism

$$\phi \colon {}^{\mathbb{Z}[\alpha]}\!/_{\langle p\rangle} \to {}^{\mathcal{O}_K}\!/_{\langle p\rangle}$$

coming from the inclusion $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Note that both have cardinality p^n, since if $\mathcal{O}_K \cong \mathbb{Z}^n$, then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}^n/p\mathbb{Z}^n$. Now $\#\operatorname{coker}(\phi)$ must divide p^n, but $\left[\mathcal{O}_K \colon \mathbb{Z}[\alpha]\right]$ is relatively prime to p. Hence, the cokernel is trivial and ϕ is surjective. Therefore, ϕ is an isomorphism since both domain and codomain are finite sets.

Now we have a string of isomorphisms

$$\begin{aligned} \mathcal{O}_K/p\mathcal{O}_K &\cong \mathbb{Z}[\alpha]/\langle p\rangle \\ &\cong \mathbb{Z}[x]/\langle p, g(x)\rangle \\ &\cong \mathbb{F}_p[x]/\langle \overline{g}\rangle \\ &\cong \prod_{i=1}^{r} \mathbb{F}_p[x]/\langle \overline{g}_i^{e_I}\rangle \end{aligned}$$

The homomorphisms $\mathcal{O}_K \twoheadrightarrow \mathbb{F}_p[x]/\langle \overline{g}_i^{e_i}\rangle$ have kernel $I_i = \langle p, g_i(\alpha)^{e_i}\rangle$. Hence,

$$\mathcal{O}_K/I_i \cong \mathbb{F}_p[x]/\langle \overline{g}_i^{e_i}\rangle$$

So the map

$$\mathcal{O}_K \twoheadrightarrow \prod_{i=1}^{r} \mathcal{O}_K/I_i$$

has kernel $p\mathcal{O}_K$ by the above, but also by the Chinese remainder theorem the kernel is $I_1 \cap I_2 \cap \ldots \cap I_r = I_1 I_2 \cdots I_r$. Therefore, $p\mathcal{O}_K = I_1 I_2 \cdots I_r$. Finally, one can check that $I_i = \mathfrak{p}_i^{e_i}$.

To see the claim about the index, we have

$$\left[\mathcal{O}_K/\mathfrak{p}_i \colon \mathbb{F}_p\right] = \left[\mathbb{F}_p[x]/\langle \overline{g}_i\rangle \colon \mathbb{F}_p\right] = \deg \overline{g}_i = f_i$$

□

Remark 3.18. The factors of $\mathfrak{p}$ appearing here are governed by the degree of the extension in the sense that

$$\sum_{i=1}^{r} e_i f_i = \sum_{i=1}^{r} e_i \deg(\overline{g}_i) = \deg \overline{g} = n = [K \colon \mathbb{Q}]$$

This in fact holds for all p.

Example 3.19. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a squarefree integer. Take any odd prime p, and let $\alpha = \sqrt{d}$. Let $g(x) = x^2 - d$. Notice that this prime satisfies our assumption that $p \nmid [\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$, since the index here is either 1 or 2.

We have $\sum_{i=1}^{r} e_i f_i = 2$, so there are a finite number of possibilities.

If $r = 2$ and $e_i = f_i = 1$, in which case $p\mathcal{O}_K = p_1 p_2$ and $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_p$. In this case, we say that p **splits** in K.

If $r = 1$, $e_1 = 2$ and $f_1 = 1$, then $p\mathcal{O}_K = \mathfrak{p}^2$ and $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$. In this case, we say that p **ramifies** in K.

If $r = 1$, $e_1 = 1$, and $f_1 = 2$, then $p\mathcal{O}_K = \mathfrak{p}$ and $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{p^2}$. In this case, we say that p is **inert** in K.

Given an odd prime p, which case are we in? We must factor $x^2 - d \pmod{p}$.

- p ramifies in K if and only if $p \mid d$.
- p splits in K if and only if $p \not| d$ and d is a square mod p.
- p is inert in K if and only if $p \not| d$ and d is not a square mod p.

If $p = 2$, there are fewer possibilities. If $d \not\equiv 1 \pmod 4$, then we didn't need to exclude it from the above and it ramifies. If $d \equiv 1 \pmod 4$, then take $\alpha = \frac{1+\sqrt{d}}{2}$ and $g(x) = x^2 - x + \frac{1-d}{4}$.

Remark 3.20. Quadratic reciprocity will describes the primes in these cases, depending only on p modulo $4d$. We will prove this later.

Example 3.21. Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \sqrt[3]{2}$. Let $g(x) = x^3 - 2$. Then

$$\begin{aligned} &x^3 - 2 \equiv (x-3)(x^2+3x+4) \pmod 5 \\ &x^2 - 2 \text{ is irreducible} \pmod 7 \\ &x^3 - 2 \equiv (x+11)(x+24)(x+27) \pmod{31} \end{aligned}$$

Hence, 5 and 31 splits, and 7 is inert in K.

3.2 Fractional Ideals

We extend our notion of ideals to capture factorization properties.

Definition 3.22. A **fractional ideal** of K is a nonzero finitely generated $\mathcal{O}_K$-submodule $I \subseteq K$.

Since K itself is not a finitely-generated $\mathcal{O}_K$-module, it cannot be a fractional ideal.

Definition 3.23. An **integral ideal** is a nonzero ideal of $\mathcal{O}_K$.

Note that integral ideals of $\mathcal{O}_K$ are fractional ideals since $\mathcal{O}_K$ is Noetherian.

Lemma 3.24. *Let I be a nonzero $\mathcal{O}_K$-submodule of K. Then the following are equivalent:*

(a) I *is a fractional ideal;*

(b) $dI \subseteq \mathcal{O}_K$ *for some* $d \geq 1$*;*

(c) $dI \subseteq \mathcal{O}_K$ *for some nonzero* $d \in \mathcal{O}_K$*;*

(d) $I = xJ$ *for some* $x \in K^\times$ *and a nonzero ideal* $J \subseteq \mathcal{O}_K$.

Proof. $(a) \implies (b)$. If $I = \mathcal{O}_K x_1 + \ldots + \mathcal{O}_K x_r$ for some $x_i \in K$, then there is some $d \geq 1$ such that $dx_i \in \mathcal{O}_K$. Therefore, $dI \subseteq \mathcal{O}_K$.

$(b) \implies (c)$. Regular integers are algebraic integers.

$(c) \implies (d)$. Let J be the ideal $dI \subseteq \mathcal{O}_K$. Then implies $I = d^{-1}J$ is a finitely generated $\mathcal{O}_K$-submodule of K.

$(d) \implies (a)$. If $I = xJ$, then I is a finitely generated $\mathcal{O}_K$-submodule of K since ideals of $\mathcal{O}_K$ are finitely generated. □

For any two fractional ideals I and J of K, we have another fractional ideal IJ. Here are some easy properties of fractional ideals.

Fact 3.25 (Easy properties of fractional ideals)**.**

(a) Multiplication of fractional ideals is commutative.

(b) Multiplication of fractional ideals is associative.

(c) $I \cdot \mathcal{O}_K = \mathcal{O}_K \cdot I = I$*, since* I *is an* $\mathcal{O}_K$*-module.*

Definition 3.26. Let $\mathfrak{I}_K$ be the set of fractional ideals of K.

Later, we will see that $\mathfrak{I}_K$ with multiplication is an abelian group with identity $\mathcal{O}_K$. For now, we need to show that inverses exist.

Definition 3.27. $\mathfrak{P}_K \subseteq \mathfrak{I}_K$ is the group of *principal* fractional ideals, i.e. $x\mathcal{O}_K$ with $x \in K^\times$.

This is more clearly a group than $\mathfrak{I}_K$ – the inverse of $x\mathcal{O}_K$ is $x^{-1}\mathcal{O}_K$.

Definition 3.28. The **ideal class group** of K is

$$C\ell_K := {}^{\mathfrak{I}_K}\!/_{\mathfrak{P}_K}.$$

Remark 3.29. This is not well-defined until we show that $\mathfrak{I}_K$ is a group. Later, we will prove that $C\ell_K$ is finite.

Example 3.30. $C\ell_{\mathbb{Q}(\sqrt{-5})} \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

For any $I \in \mathfrak{I}_K$, define

$$\widetilde{I} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}.$$

Claim that $\widetilde{I}$ is a fractional ideal. Indeed, fix a nonzero $\alpha \in I$, and then $\alpha\widetilde{I} \subseteq \mathcal{O}_K$. By one of the equivalent definitions for algebraic integers, this shows that $\widetilde{I}$ is a finitely generated $\mathcal{O}_K$-module.

Lemma 3.31. *If* $J \in \mathfrak{I}_K$ *satisfies* $IJ = \mathcal{O}_K$*, then* $\widetilde{I} = J$*.*

Proof. Notice that $JI = \mathcal{O}_K$, so $J \subseteq \widetilde{I}$. Therefore, multiplying by I

$$\mathcal{O}_K = IJ \subseteq I\widetilde{I} \subseteq \mathcal{O}_K.$$

Hence, $I\widetilde{I} = \mathcal{O}_K$. Then

$$\widetilde{I} = \mathcal{O}_K\widetilde{I} = JI \cdot \widetilde{I} = J\mathcal{O}_K = J \qquad \square.$$

Lemma 3.32. *Eery nonzero ideal* I *of* $\mathcal{O}_K$ *contains a product of nonzero prime ideals.*

Proof. Suppose not. Consider all ideals that do not contain a product of nonzero prime ideals, and let I be largest among them with respect to inclusion. Note that I cannot itself be prime. Then there are $a, b \in \mathcal{O}_K$ such that $ab \in I$ yet $a \notin I$, $b \notin I$. So the ideals $\langle a \rangle + I$ and $\langle b \rangle + I$ are strictly larger than I, so by the choice of I they must contain a product of nonzero primes

$$\langle a \rangle + I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$$
$$\langle b \rangle + I = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

However,

$$I = \langle ab \rangle + I = \big(\langle a \rangle + I\big)\big(\langle b \rangle + I\big) \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

So I does actually contain a product of prime ideals. $\square$

Example 3.33. Consider $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, with ideals $\mathfrak{q} = \langle 3, 1 + \sqrt{-5} \rangle$ and $\mathfrak{q}' = \langle 3, 1 - \sqrt{-5} \rangle$. We saw that $\mathfrak{q}\mathfrak{q}' = \langle 3 \rangle$, so $\mathfrak{q}(\frac{1}{3}\mathfrak{q}') = \mathcal{O}_K$. So

$$\widetilde{\mathfrak{q}} = \frac{1}{3}\mathfrak{q}' = \mathcal{O}_K + \left(\frac{1 - \sqrt{-5}}{3}\right)\mathcal{O}_K.$$

Proposition 3.34. *Let* $\mathfrak{p} \subseteq \mathcal{O}_K$ *be a nonzero prime ideal. Then* $\mathfrak{p}\widetilde{\mathfrak{p}} = \mathcal{O}_K$.

Proof. We will first prove that $\widetilde{\mathfrak{p}} \supsetneq \mathcal{O}_K$. We know that $\widetilde{\mathfrak{p}} \supseteq \mathcal{O}_K$. Take a nonzero $a \in \mathfrak{p}$. Then $\mathfrak{p} \supseteq \langle a \rangle$, and by the Lemma 3.32, $\langle a \rangle$ must contain a product of primes.

$$\mathfrak{p} \supseteq \langle a \rangle \supseteq \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r.$$

Assume that $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$ is a minimal product of primes: r is the least integer such that a product of r prime ideals is contained in $\langle a \rangle$. Since $\mathfrak{p}$ is prime, $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i; and moreover, $\mathfrak{p} = \mathfrak{p}_i$ since all primes in $\mathcal{O}_K$ are maximal.

If $r = 1$, then $\mathfrak{p} \supseteq \langle a \rangle \supseteq \mathfrak{p}_1$. Hence, $\mathfrak{p} = \langle a \rangle$ is a principal ideal, which has inverse $\frac{1}{a}\mathcal{O}_K$ as a fractional ideal, which strictly contains $\mathcal{O}_K$. In this case, $\widetilde{\mathfrak{p}} = \frac{1}{a}\mathcal{O}_K$.

If $r \geq 2$, assume without loss of generality that $\mathfrak{p} = \mathfrak{p}_1$. So

$$\langle a \rangle \supseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

and $\langle a \rangle \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$ by choice of r. Let $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin \langle a \rangle$. Define $x = {}^{b}/_{a} \in K^\times$; we have $x \notin \mathcal{O}_K$.

Claim that $x \in \widetilde{\mathfrak{p}}$, which would show that $\widetilde{\mathfrak{p}} \neq \mathcal{O}_K$. We have

$$b\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \langle a \rangle = a\mathcal{O}_K$$

Dividing by a, we see that $x\mathfrak{p} \subseteq \mathcal{O}_K$. Hence, $x \in \widetilde{\mathfrak{p}}$.

Now fix $x \in \widetilde{\mathfrak{p}} \setminus \mathcal{O}_K$. We have $x\mathfrak{p} \subseteq \mathcal{O}_K$, which implies that $\mathfrak{p} + x\mathfrak{p} \subseteq \mathcal{O}_K$. Since $\mathfrak{p}$ is a maximal ideal, there are two possibilities: either $\mathfrak{p} + x\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{p} + x\mathfrak{p} = \mathcal{O}_K$. We rule out the first possibility.

If $\mathfrak{p} = \mathfrak{p} + x\mathfrak{p}$, then $x\mathfrak{p} \subseteq \mathfrak{p}$. Note that $\mathfrak{p} \neq 0$ is a finitely generated $\mathbb{Z}$-submodule of K, which implies that $x \in \mathcal{O}_K$ by Proposition 2.1. This is a contradiction, since we chose $x \notin \mathcal{O}_K$. Note that this is where we use the ring of algebraic integers instead of a general order.

So we must have $\mathfrak{p} + x\mathfrak{p} = \mathcal{O}_K$. Hence, $\mathfrak{p}(\mathcal{O}_K + x\mathcal{O}_K) = \mathcal{O}_K$. Then by Lemma 3.31, $\mathcal{O}_K + x\mathcal{O}_K = \widetilde{\mathfrak{p}}$ since it is an inverse to $\mathfrak{p}$. □

Corollary 3.35. *Let $\mathfrak{p} \neq 0$ be a prime ideal of $\mathcal{O}_K$.*

(a) If $\mathfrak{p}I = \mathfrak{p}J$ for ideals I, J of $\mathcal{O}_K$, then $I = J$.

(b) Let $I \neq 0$ be an ideal of $\mathcal{O}_K$. Then $\mathfrak{p} \supseteq I \iff I = \mathfrak{p}J$ for some unique ideal J.

(c) For a nonzero ideal I, $\mathfrak{p}I \subsetneq I$.

Proof.

(a) Multiply both sides by $\widetilde{\mathfrak{p}}$ on the left to cancel.

(b) If $\mathfrak{p} \supseteq I$, then take $J = \widetilde{\mathfrak{p}}I \subseteq \mathcal{O}_K$ to see $I = \mathfrak{p}J$. Conversely, if $I = \mathfrak{p}J$ then clearly $\mathfrak{p} \supseteq I$.

(c) Assume for contradiction that $\mathfrak{p}I = I$. Then $I = \mathfrak{p}I = \mathfrak{p}^2 I = \mathfrak{p}^3 I = \ldots = \mathfrak{p}^n I \subseteq \mathfrak{p}^n$. Since $\#(\mathcal{O}_K/I)$ is finite, then $\mathfrak{p}^{n+1} = \mathfrak{p}^n$ for n sufficiently large. Multiplying this equation by $\widetilde{\mathfrak{p}}^n$, we see that $\mathfrak{p} = \mathcal{O}_K$. Contradiction. □

Proof of Theorem 3.6. Let $I \subseteq \mathcal{O}_K$ be a non-zero proper ideal. This ideal contains a product of nonzero primes:

$$I \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

We induct on r. If $r = 1$, then $I \supseteq \mathfrak{p}_1 \implies I = \mathfrak{p}_1$ since primes are maximal in $\mathcal{O}_K$.

If $r > 1$, write $I \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{r+1}$. Choose a maximal ideal $\mathfrak{p} \supseteq I$, so $\mathfrak{p} = \mathfrak{p}_i$ for some i. Assume that $\mathfrak{p} = \mathfrak{p}_{r+1}$. Then multiplying by $\widetilde{\mathfrak{p}}$, we get:

$$\mathcal{O}_K = \widetilde{\mathfrak{p}}I \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

By induction, we may factor $\widetilde{\mathfrak{p}}I = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$ into a product of primes. Multiplying by $\mathfrak{p}$, we have

$$I = \mathfrak{p}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

This proves existence.

To prove uniqueness, suppose that

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s$$

with $\mathfrak{q}_i, \mathfrak{p}_i$ nonzero prime ideals. Swapping the $\mathfrak{p}$'s and $\mathfrak{q}$'s if necessary, assume $s > r$. Since the left hand side is contained in $\mathfrak{p}_1$, we have $\mathfrak{p}_1 = \mathfrak{q}_i$ for some i. By reordering, we may assume that $\mathfrak{p}_1 = \mathfrak{q}_1$. Now multiply by $\widetilde{\mathfrak{p}}_1$ and recurse. After reordering, $\mathfrak{p}_1 = \mathfrak{q}_1, \ldots, \mathfrak{p}_r = \mathfrak{q}_r$, and

$$\mathcal{O}_K = \mathfrak{q}_{r+1}\mathfrak{q}_{r+2} \cdots \mathfrak{q}_s.$$

This is impossible unless $r = s$. □

Corollary 3.36. $\mathfrak{I}_K$ *is a group.*

Proof. We need only check that each element of $\mathfrak{I}_K$ has an inverse. Let $I \in \mathfrak{I}_K$. Then $dI \subseteq \mathcal{O}_K$ for some $d \geq 1$, and $dI = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$. Hence, $I = \frac{1}{d}\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$, which has inverse $d\widetilde{\mathfrak{p}}_1\widetilde{\mathfrak{p}}_2 \cdots \widetilde{\mathfrak{p}}_r$. □

Definition 3.37 (Notation)**.** Since inverses always exist in $\mathfrak{I}_K$, we will write $I^{-1} := \widetilde{I}$ from now on.

Remark 3.38. Every $I \in \mathfrak{I}_K$ has a unique factorization

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$$

where the product is taken over all nonzero primes $\mathfrak{p}$ with $e_{\mathfrak{p}} \in \mathbb{Z}$ and $e_{\mathfrak{p}} = 0$ for all but finitely many $\mathfrak{p}$.

Remark 3.39. How different is this from multiplication in the field K? Inside of $\mathfrak{I}_K$ we have a group $\mathfrak{P}_K$ of principal fractional ideals of K. $\mathfrak{P}_K$ behaves a lot like multiplication in $K^\times$, with elements $x\mathcal{O}_K$ for $x \in K^\times$, and inverses $\frac{1}{x}\mathcal{O}_K$. The **class group** of K is $C\ell_K = \mathfrak{I}_K / \mathfrak{P}_K$, which measures this difference. We will later prove that this is a finite abelian group, so this difference cannot be too large.

Example 3.40. Find all solutions $x, y \in \mathbb{Z}$ to $y^2 = x^3 - 5$. We will use that $C\ell_{\mathbb{Q}(\sqrt{-5})} \cong \mathbb{Z}/2$.

$K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Fix a pair (x, y) solving this equation. Over $\mathcal{O}_K$, we may factor the right hand side:

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

Claim that the ideals $\langle y + \sqrt{-5}\rangle$ and $\langle y - \sqrt{-5}\rangle$ are relatively prime.

If not, then there is a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ with $y \pm \sqrt{-5} \in \mathfrak{p}$, so $2\sqrt{-5} = (y + \sqrt{-5}) - (y - \sqrt{-5}) \in \mathfrak{p}$. Hence, $2 \cdot 5 \in \mathfrak{p}$, so either $2 \in \mathfrak{p}$ or $5 \in \mathfrak{p}$. We also know that

$$x^3 = (y + \sqrt{-5})(y - \sqrt{-5}) \in \mathfrak{p},$$

which means that $x \in \mathfrak{p}$. Recall that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, where p is the characteristic of $\mathcal{O}_K/\mathfrak{p}$. Since x is an integer, we know $x \in \mathfrak{p} \cap \mathbb{Z}$, so $x \in 2\mathbb{Z}$ or $x \in 5\mathbb{Z}$. So either $2 \mid x$ or $5 \mid x$. We have $y^2 = x^3 - 5$, yet neither $y^2 = -5 \pmod 4$ nor $y^2 = -5 \pmod{25}$ have solutions. This gives a contradiction, so the ideals must be relatively prime.

Now factor the ideal generated by x into primes:

$$x\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}.$$

In particular,

$$\langle y + \sqrt{-5}\rangle\langle y - \sqrt{-5}\rangle = x^3\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{3e_i}.$$

and the ideals $\langle y \pm \sqrt{-5}\rangle$ are relatively prime, so we must have

$$\langle y + \sqrt{-5}\rangle = \prod_{i \in J} \mathfrak{p}_i^{3e_i}$$

for some $J \subseteq \{1, \dots, r\}$. Rewrite this as

$$\langle y + \sqrt{-5}\rangle = I^3$$

for $I = \prod_{i \in J} \mathfrak{p}_i$. In $C\ell_K = \mathfrak{I}_K / \mathfrak{P}_K$, the element $[I]$ cubes to the identity, since I^3 is principal. Since $C\ell_K \cong \mathbb{Z}/2$, then $[I]$ is trivial. Hence, I is a principal ideal in $\mathcal{O}_K$:

$$\langle y + \sqrt{-5}\rangle = \langle a + b\sqrt{-5}\rangle^3.$$

for some $a, b \in \mathbb{Z}$. Up to a unit in $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$,

$$y + \sqrt{-5} = \pm(a + b\sqrt{-5})^3.$$

Changing a and b if necessary, we may assume that the unit is 1, since -1 is a cube. Hence,

$$y + \sqrt{-5} = (a + b\sqrt{-5})^3.$$

We have

$$y + \sqrt{-5} = (a^3 + 3ab^2(-5)) + (3a^2b + b^2(-5))\sqrt{-5}.$$

Equating real and imaginary parts, we have the following system of equations in the integers:

$$\begin{cases} y = a^3 - 15ab^2 \\ 1 = 3a^2b - 5b^3 \end{cases}$$

For the second equation, we may factor out a b to see that

$$1 = \pm(3a^2 - 5) \implies 3a^2 = 5 \pm 1$$

The equations $3a^2 = 4$ and $3a^2 = 6$ have no integer solutions. Hence, the original equation $y^2 = x^3 - 5$ has no integer solutions.

3.3 Ramification

Given any integer prime p, factor

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i$ are distinct prime ideals and $e_i \geq 1$.

Definition 3.41. The integer e_i is the **ramification index** of $\mathfrak{p}$ over p.

Definition 3.42. We say that $\mathfrak{p}$ is **ramified** in K if $e_i > 1$ for some i. If $e_i = 1$ for all i, then $\mathfrak{p}$ is **unramified**.

Definition 3.43. The **inertia degree** of $\mathfrak{p}_i$ over p is $f_i := \left[{}^{\mathcal{O}_K}/_{\mathfrak{p}_i} \colon \mathbb{F}_p\right]$.

Theorem 3.44. *Given any integer prime p, factor $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i$ are distinct prime ideals and $e_i \geq 1$. Let f_i be the inertia degree of $\mathfrak{p}_i$. Then*

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

In particular, $r \leq [K \colon \mathbb{Q}]$.

Remark 3.45. Actually, $r = [K \colon \mathbb{Q}]$ for infinitely many integral primes p.

Example 3.46. Suppose $[K \colon \mathbb{Q}] = 3$ and p is unramified, so $e_i = 1$ for all i. We could have:

- $r = 3, f_1 = f_2 = f_3 = 1$,
- $r = 2, f_1 = 1, f_2 = 2$,
- $r = 1, f_1 = 3$.

In $K = \mathbb{Q}(\sqrt[3]{2})$, all three cases occur, and in fact all three cases occur infinitely often. In $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + x^2 - 2x - 1$, the case $r = 2$ does not occur.

Recall that for a nonzero ideal $I \subseteq \mathcal{O}_K$, the norm of I is $N(I) := \#\left({}^{\mathcal{O}_K}/_{I}\right)$.

Proposition 3.47. *For any two ideals I and J of $\mathcal{O}_K$, we have $N(IJ) = N(I)N(J)$. In particular, if $I = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ for distinct primes, $\mathfrak{p}_i$, $N(I) = N(\mathfrak{p}_1)^{b_1} \cdots N(\mathfrak{p}_r)^{b_r}$.*

Proof. We need only check the last statement. Note that for $i \neq j$, $\mathfrak{p}_i^{b_i} + \mathfrak{p}_j^{b_j} = \mathcal{O}_K$; if not, then there is a maximal ideal $\mathfrak{q}$ such that $\mathfrak{p}_i^{b_i} + \mathfrak{p}_j^{b_j} \subseteq \mathfrak{q} \implies \mathfrak{q} = \mathfrak{p}_i$ and $\mathfrak{q} = \mathfrak{p}_j$. Then by the Chinese Remainder Theorem,

$$ {}^{\mathcal{O}_K}/_{I} = {}^{\mathcal{O}_K}/_{\mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_r^{b_r}} \cong {}^{\mathcal{O}_K}/_{\mathfrak{p}_1^{b_1}} \times {}^{\mathcal{O}_K}/_{\mathfrak{p}_2^{b_2}} \cdots \times {}^{\mathcal{O}_K}/_{\mathfrak{p}_r^{b_r}} $$

Hence, $N(I) = \prod_i N(\mathfrak{p}_i^{b_i})$.

It remains to show that for some prime $\mathfrak{p}$, $N(\mathfrak{p}^a) = N(\mathfrak{p})^a$. Consider the chain

$$\mathcal{O}_K \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \ldots \supseteq \mathfrak{p}^a.$$

Then

$$N(\mathfrak{p}^e) = \#\left({}^{\mathcal{O}_K}/_{\mathfrak{p}^e}\right) = \prod_{i=1}^{e} \#\left({}^{\mathfrak{p}^{i-1}}/_{\mathfrak{p}^i}\right)$$

where $\mathfrak{p}^0 = \mathcal{O}_K$. So we need only show that $\#\left({}^{\mathfrak{p}^{i-1}}/_{\mathfrak{p}^i}\right) = N(\mathfrak{p})$.

Let $M = {}^{\mathfrak{p}^{i-1}}/_{\mathfrak{p}^i}$; we know that $M \neq 0$ because if it was, then $\mathfrak{p}^{i-1} = \mathfrak{p}^i$, which implies that $\mathfrak{p}_i = \mathcal{O}_K$. So take any $x \in \mathfrak{p}^{i-1} \setminus \mathfrak{p}^i$. We have a homomorphism of $\mathcal{O}_K$-modules $\phi \colon \mathcal{O}_K \to M$ given by $b \mapsto bx$.

Claim that ϕ is surjective. If ϕ is not surjective, then there is an $\mathcal{O}_K$-module $0 \subsetneq \operatorname{im}(\phi) \subsetneq M$. So there is an $\mathcal{O}_K$-submodule J of M with $\mathfrak{p}^i \subsetneq J \subsetneq \mathfrak{p}^{i-1}$, hence $\mathfrak{p} \subsetneq (\mathfrak{p}^{i-1})^{-1} J \subsetneq \mathcal{O}_K$. This contradicts the maximality of $\mathfrak{p}$.

Hence, $\phi \colon \mathcal{O}_K \twoheadrightarrow {}^{\mathfrak{p}^{i-1}}/_{\mathfrak{p}^i} \neq 0$. The kernel of ϕ contains $\mathfrak{p}$, so there is a surjection

$$ {}^{\mathcal{O}_K}/_{\mathfrak{p}} \twoheadrightarrow {}^{\mathfrak{p}^{i-1}}/_{\mathfrak{p}^i}. $$

Since the left hand side is a field, this means that $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{i-1}/\mathfrak{p}^i$. Hence, $\#|\mathfrak{p}^{i-1}/\mathfrak{p}^i| = N(\mathfrak{p})$. □

Proof of Theorem 3.44. The idea is to compute $N(p\mathcal{O}_K)$ in two different ways. If $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$, then Proposition 3.47 implies

$$N(p\mathcal{O}_K) = N(\mathfrak{p}_1)^{e_1}N(\mathfrak{p}_2)^{e_2}\cdots N(\mathfrak{p}_r)^{e_r}.$$

Moreover,

$$N(\mathfrak{p}_i) = \#\left({}^{\mathcal{O}_K}\!/_{\mathfrak{p}_i}\right) = p^{f_i}.$$

Combining, we find that

$$N(\mathfrak{p}\mathcal{O}_K) = \prod_{i=1}^{r}\left(p^{f_i}\right)^{e_i} = p^{\sum_{i=1}^{r} e_i f_i}.$$

On the other hand, $\mathcal{O}_K \cong \mathbb{Z}^n$ as an abelian group, where $n = [K\colon \mathbb{Q}]$. Then we have the following chain of isomorphisms of abelian groups:

$$ {}^{\mathcal{O}_K}\!/_{p\mathcal{O}_K} \cong {}^{\mathbb{Z}^n}\!/_{p\mathbb{Z}^n} \cong \left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^n$$

This shows us that $N(p\mathcal{O}_K) = p^n$. Hence,

$$p^{\sum_{i=1}^{r} e_i f_i} = p^n. \qquad \square$$

Theorem 3.48. *A prime p is ramified in K if and only if p divides the discriminant of K. In particular, only finitely many primes p ramify in K.*

Remark 3.49. Here are some neat facts that we won't prove.

(a) Take number fields K_1 and K_2. Suppose that their discriminants are relatively prime. Then $K_1 \cap K_2 = \mathbb{Q}$.

(b) Given an integer $n \geq 1$ and a finite set S of primes, then up to isomorphism, there are only finitely many number fields K such that K has degree n and K is unramified at all $p \notin S$.

This second fact is actually a very hard theorem.

To prove Theorem 3.48, we must first extend the definition of discriminant.

Definition 3.50. Consider rings $A \subseteq B$, where B is a free A-module of rank n. Choose an A-basis $x_1, \ldots, x_n$ of B, and define

$$\operatorname{disc}(x_1, \ldots, x_n) := \det\left(\operatorname{Tr}_{B/A}(x_i x_j)\right) \in A$$

where $\operatorname{Tr}_{B/A}(x)$ is the trace of the A-linear map $B \to B$, $b \mapsto xb$.

For another A-basis $y_1, \dots, y_n$,

$$\operatorname{disc}(y_1, \dots, y_n) = \operatorname{disc}(x_1, \dots, x_n)(\det C)^2,$$

where $C \in \mathrm{GL}_n(A)$ is the change of basis matrix satisfying

$$y_i = \sum_{j=1}^{n} C_{ij} x_j.$$

Since C is an invertible matrix, $\det(C) \in A^\times$. So $\operatorname{disc}(y_1, \dots, y_n)$ and $\operatorname{disc}(x_1, \dots, x_n)$ differ by the square of a unit in A.

Definition 3.51. The **discriminant** of B over A is $\operatorname{disc}_A(B) = \operatorname{disc}(x_1, \dots, x_n)$ for any A-basis $x_1, \dots, x_n$ of B. This is well-defined up to an element of $(A^\times)^2$; it defines a coset $\operatorname{disc}(x_1, \dots, x_n) \cdot (A^\times)^2$.

Fact 3.52. *For $A \subseteq B_1$ and $A \subseteq B_2$, $\operatorname{disc}_A(B_1 \times B_2) = \operatorname{disc}_A(B_1) \operatorname{disc}_A(B_2)$.*

Proof of Theorem 3.48. Now let $x_1, \dots, x_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\overline{x}_1, \dots, \overline{x}_n$ is an $\mathbb{F}_p$-basis of $\mathcal{O}_K / p\mathcal{O}_K$.

$$\operatorname{disc}(K) = \operatorname{disc}(x_1, \dots, x_n) \equiv \operatorname{disc}(\overline{x}_1, \dots, \overline{x}_n) \pmod{p}$$

This class represents an element of the coset $\operatorname{disc}_{\mathbb{F}_p}\left({}^{\mathcal{O}_K}/_{p\mathcal{O}_K}\right)$. So $p \mid \operatorname{disc}(K)$ if and only if $\operatorname{disc}_{\mathbb{F}_p}\left({}^{\mathcal{O}_K}/_{p\mathcal{O}_K}\right) = 0$. Recall

$${}^{\mathcal{O}_K}/_{p\mathcal{O}_K} \cong \prod_{i=1}^{r} {}^{\mathcal{O}_K}/_{\mathfrak{p}_i^{e_i}}.$$

So $p \mid \operatorname{disc}(K)$ if and only if $\operatorname{disc}_{\mathbb{F}_p}\left(\prod_i {}^{\mathcal{O}_K}/_{\mathfrak{p}_i^{e_i}}\right) = \prod_i \operatorname{disc}_{\mathbb{F}_p}\left({}^{\mathcal{O}_K}/_{\mathfrak{p}_i^{e_i}}\right) = 0$, if and only if $\operatorname{disc}_{\mathbb{F}_p}\left({}^{\mathcal{O}_K}/_{\mathfrak{p}_i^{e_i}}\right) = 0$ for some i. The theorem will follow from the next lemma. □

Lemma 3.53. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime, and let e be its ramification index. Then the discriminant of $\mathcal{O}_K / \mathfrak{p}^e$ over $\mathbb{F}_p$ is zero if and only if $e \geq 2$.*

Proof. Suppose $e \geq 2$. Fix a basis $x_1, \dots, x_n$ of $B = \mathcal{O}_K / \mathfrak{p}^e$ over $\mathbb{F}_p$ with $x_1^2 = 0$. We may choose x_1 this way since

$$x_i \in {}^{\mathfrak{p}^{e-1}}/_{\mathfrak{p}^e} \implies x_1^2 \in \left(\mathfrak{p}^{e-1}\right)^2 \subseteq \mathfrak{p}^e.$$

The last inclusion holds since $e \geq 2$. Define a linear map $B \to B$ by $b \mapsto x_1 x_j b$. This is represented by an $n \times n$ matrix M in $\mathbb{F}_p$, and $M^2 = 0$ since $x_1^2 = 0$. Now

$$\operatorname{Tr}_{B/\mathbb{F}_p}(x_1 x_j) = \operatorname{tr}(M) = 0$$

since the eigenvalues of M are all zero. Then

$$\operatorname{disc}(x_1, \ldots, x_n) = \det(\operatorname{Tr}_{B/\mathbb{F}_p}(x_i x_j)) = 0,$$

since the first row is zero. Hence,

$$\operatorname{disc}_{\mathbb{F}_p}({}^{\mathcal{O}_K}/_{\mathfrak{p}^e}) = 0.$$

If $e = 1$, we want to show that $\operatorname{disc}_{\mathbb{F}_p}({}^{\mathcal{O}_K}/_{\mathfrak{p}^e}) \neq 0$. We will show that in fact, for a finite field extension L/K of separable fields, $\operatorname{disc}(L/K) \neq 0$. The separable assumption gives us $L = K(\alpha)$ for some α, and $1, \alpha, \ldots \alpha^{n-1}$ is a K-basis of L, where $n = [L\colon K]$. As before,

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

where $\sigma_1, \ldots, \sigma_n \colon L \hookrightarrow \overline{K}$ are the K-embeddings of L into an algebraic closure $\overline{K}$ of K. The product on the right-hand-side is nonzero, and in fact it will be nonzero up to a unit squared. Hence, $\operatorname{disc}_K(L) \neq 0$. □

3.4 Dedekind Domains

Although we were working with of rings of integers of number fields, we could have done everything in this section in a more general setting. We only needed to know that the ring $\mathcal{O}_K$ is a Dedekind domain to establish unique factorization.

Definition 3.54. A ring R is **integrally closed** if for each monic $f(x) \in R[x]$ with root $\alpha \in K$ (where K is the field of fractions of R), then $\alpha \in R$.

Definition 3.55. A **Dedekind domain** is an integral domain R satisfying:

(a) R is Noetherian;

(b) R is integrally closed;

(c) every nonzero prime ideal in R is maximal.

Example 3.56. If K is a number field, then $\mathcal{O}_K$ is a Dedekind domain. Indeed, we have already showed that $\mathcal{O}_K$ is Noetherian and every nonzero prime ideal in $\mathcal{O}_K$ is maximal. To show that $\mathcal{O}_K$ is integrally closed, take any $\alpha \in K$ such that $f(\alpha) = 0$ with $f \in \mathcal{O}_K[x]$ monic. Define $M := \mathcal{O}_K[\alpha] \subseteq K$. Note that M is a finitely generated $\mathcal{O}_K$-module since f is monic. Therefore, M is a finitely generated $\mathbb{Z}$-module. Then $\alpha M \subseteq M \implies \alpha \in \mathcal{O}_K$ by Proposition 2.1.

We won't prove the following theorem, but it justifies generalizing to Dedekind domains.

Theorem 3.57. *Let R be an integral domain. Then R is a Dedekind domain if and only if every nonzero ideal has a unique factorization into primes.*

The proof that Dedekind domains have unique factorization is as before in Section 3.2, with minor changes.

Example 3.58.

(a) Any PID is a Dedekind domain.

(b) $R = \mathbb{C}[x, y]/\langle y^2 - x^3 - 1\rangle$ is a Dedekind domain, but it is not a PID. The nonzero prime ideals are $\langle x - a, y - b\rangle$ with $b^2 = a^3 + 1$ for $a, b \in \mathbb{C}$. Moreover, if C is a non-singular affine curve over any field k, then its coordinate ring $k[C]$ is a Dedekind domain.

Remark 3.59. For any Dedekind domain R, we may also define the ideal class group $C\ell_R$, but it will not necessarily be finite as it is when R is the ring of integers of a number field. When R is the coordinate ring of the affine plane curve $y^3 = x^3 - 1$, then $C\ell_R \cong \mathbb{R}^2/\mathbb{Z}^2$.

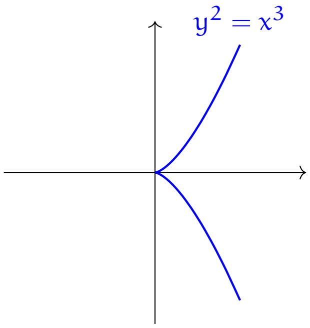
Definition 3.60. Let R be a ring with fraction field K. Let L be a finite field extension of K. The **integral closure of** R **in** L is the ring

$$S = \left\{\alpha \in L \mid f(\alpha) = 0 \text{ for some monic } f(x) \in R[x]\right\}.$$

Proposition 3.61. *Let R be a Dedekind domain with fraction field K. Let L be a finite field extension of K, and let S be the integral closure of R in L. Then S is a Dedekind domain.*

$$\begin{tikzcd}
L \arrow[r, phantom, "\supseteq"] \arrow[d, dash] & S \arrow[d, dash] \\
K \arrow[r, phantom, "\supseteq"] & R
\end{tikzcd}$$

Example 3.62. Let $R = \mathbb{C}[x, y]/\langle y^2 - x^3\rangle$. This is not a Dedekind domain that is not integrally closed. Indeed, the curve $y^2 - x^3$ is singular at the origin.



We may parameterize the curve $y^2 - x^3$ by $t \mapsto (t^2, t^3)$. When $t \neq 0$, we may recover it from a point (x, y) on the curve as $t = \frac{y}{x}$.

By abuse of notation, let $x, y \in R$ be the cosets of x and y, respectively, in R. In the fraction field K of R, define $t = y/x$. Then

$$\begin{aligned} t^2 &= \frac{y^2}{x^2} = \frac{x^3}{x^2} = x \\ t^3 &= \frac{y^3}{x^3} = \frac{y^3}{y^2} = y \end{aligned}$$

In this way, we see that $R \subseteq \mathbb{C}[t]$, and $\mathbb{C}[t]$ is a PID. Hence, $\mathbb{C}[t]$ is the integral closure of R in K.

3.5 Discrete Valuation Rings

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. For any $x \in K^\times$, write

$$x\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}(x)}$$

We have $\nu_\mathfrak{p}(x) \in \mathbb{Z}$ and $\nu_\mathfrak{p}(x) = 0$ for all but finitely many $\mathfrak{p}$. We declare $\nu_\mathfrak{p}(0) = \infty$.

Definition 3.63. The function $\nu_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}$ is the $\mathfrak{p}$**-adic valuation** of K.

Fact 3.64. *The valuation satisfies the following properties:*

(a) $\nu_\mathfrak{p}(xy) = \nu_\mathfrak{p}(x) + \nu_\mathfrak{p}(y)$

(b) $\nu_\mathfrak{p}(x + y) \geq \min\{\nu_\mathfrak{p}(x), \nu_\mathfrak{p}(y)\}$

Definition 3.65. Define $\mathcal{O}_\mathfrak{p} := \{x \in K \mid \nu_\mathfrak{p}(x) \geq 0\}$. If $\nu_\mathfrak{p}(x) \geq 0$, then we say that x **is integral at** $\mathfrak{p}$**.**

Note that $\mathcal{O}_\mathfrak{p}$ is a ring by the above properties of $\nu_\mathfrak{p}$. If we choose any $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, then $\nu_\mathfrak{p}(\pi) = 1$.

Lemma 3.66. *The nonzero ideals of* $\mathcal{O}_\mathfrak{p}$ *are* $\mathfrak{p}^n\mathcal{O}_\mathfrak{p} = \pi^n\mathcal{O}_\mathfrak{p}$ *for any* $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$.

Proof. Take any nonzero ideal $I \subseteq \mathcal{O}_\mathfrak{p}$. Let n be the smallest value of $\nu_\mathfrak{p}(x)$ over all $x \in I$. Since I is nonzero, there is some nonzero $x \in I$ and $\nu_\mathfrak{p}(x) \geq 0$. Hence, $n \geq \nu_\mathfrak{p}(x) \geq 0$.

Choose any $\pi \in \mathfrak{p}^2 \setminus \mathfrak{p}$ and consider $\pi^{-n}I$. If $x \in \pi^{-n}I$, then $\nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(\pi^{-n}b)$ for some nonzero $b \in I$, and

$$\nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(\pi^{-n}b) = -n + \nu_\mathfrak{p}(b) \geq 0.$$

Hence, $\pi^{-n}I \subseteq \mathcal{O}_\mathfrak{p}$ and is again an ideal.

Moreover, $\pi^{-n}I$ contains some $x \in \mathcal{O}_\mathfrak{p}$ with $v_\mathfrak{p}(x) = 0$, in which case $v_\mathfrak{p}(x^{-1}) = -v_\mathfrak{p}(x) = 0$, so $x^{-1} \in \mathcal{O}_\mathfrak{p}$ as well. Therefore, $\pi^{-n}I = \mathcal{O}_\mathfrak{p}$, so $I = \pi^n\mathcal{O}_\mathfrak{p}$. □

Definition 3.67. A **discrete valuation ring** (DVR) is a local PID, i.e. a PID with only one maximal ideal.

The previous lemma shows that $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring.

Lemma 3.68. $\mathcal{O}_\mathfrak{p} = \left\{ \dfrac{a}{b} \;\middle|\; a \in \mathcal{O}_K, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}$

Proof. Write $R_\mathfrak{p}$ for the right hand side. If $\frac{a}{b} \in R_\mathfrak{p}$, then

$$v_\mathfrak{p}\left(\tfrac{a}{b}\right) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b) = v_\mathfrak{p}(a) - 0 \geq 0,$$

since $b \notin \mathfrak{p}$ (when we factor $b\mathcal{O}_K$, $\mathfrak{p}$ doesn't show up at all). Hence, $R_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$.

Conversely, take any nonzero $\alpha \in \mathcal{O}_\mathfrak{p}$. Factor the principal ideal generated by α as

$$\alpha\mathcal{O}_K = IJ^{-1}$$

where I, J are ideals of $\mathcal{O}_K$ and $\mathfrak{p}$ doesn't divide J. Essentially, we factored $\alpha\mathcal{O}_K$ into primes and collected all of the primes with positive exponents into I and collected all of the primes with negative exponents into J^{-1}. We may assume $\mathfrak{p}$ doesn't divide J since $v_\mathfrak{p}(\alpha) \geq 0$.

The prime ideal $\mathfrak{p}$ doesn't divide J if and only if $J \not\subseteq \mathfrak{p}$. So we may choose some $b \in J \setminus \mathfrak{p}$. Then

$$b\alpha\mathcal{O}_K = I(bJ^{-1})$$

Notice that $bJ^{-1} \subseteq \mathcal{O}_K$, since $JJ^{-1} = \mathcal{O}_K$. Hence, $I(bJ^{-1}) \subseteq I$. Write $b\alpha = a \in I$. So $\alpha = \frac{a}{b}$. We have chosen $a \in I \subseteq \mathcal{O}_K$ and $b \in J \setminus \mathfrak{p} \subseteq \mathcal{O}_K \setminus \mathfrak{p}$. Hence, $\alpha \in R_\mathfrak{p}$, and $\mathcal{O}_\mathfrak{p} \subseteq R_\mathfrak{p}$. □

Remark 3.69. $\mathcal{O}_\mathfrak{p}$ is the localization of $\mathcal{O}_K$ at $\mathfrak{p}$. To show that $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring, we could have (instead of defining $v_\mathfrak{p}$) noted that $\mathcal{O}_\mathfrak{p}$ is necessarily local and demonstrated that it was a PID.

Theorem 3.70. *If R is a Noetherian integral domain, then R is Dedekind if and only if $R_\mathfrak{p}$ is a DVR for all nonzero primes $\mathfrak{p} \subseteq R$.*

This gives us another proof that $\mathcal{O}_K$ is a Dedekind domain, although quite a bit more roundabout.

3.6 Extensions of number fields.

Much of what we have done for $K/\mathbb{Q}$ also applies to extensions of number fields L/K.

Let L/K be an extension of number fields. Let $\mathfrak{p} \in \mathcal{O}_K$ be a non-zero prime ideal. Then

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})}$$

where $e(\mathfrak{q}/\mathfrak{p})$ is the **ramification index** of $\mathfrak{q}$ over $\mathfrak{p}$. The **inertia degree of** $\mathfrak{q}$ **over** $\mathfrak{p}$ is

$$f(\mathfrak{q}/\mathfrak{p}) = \left[\mathcal{O}_L/\mathfrak{q} \colon \mathcal{O}_K/\mathfrak{p}\right]$$

Theorem 3.71. $\displaystyle\sum_{\mathfrak{q}|\mathfrak{p}} e\left(\mathfrak{q}/\mathfrak{p}\right) f(\mathfrak{q}/\mathfrak{p}) = [L \colon K]$

We can also have a tower of field extensions. Consider the tower

$$\begin{tikzcd} M \arrow[d, dash] & \mathfrak{l} \arrow[d, phantom, "\rotatebox{90}{$\subseteq$}"] \\ L \arrow[d, dash] & \mathfrak{q} \arrow[d, phantom, "\rotatebox{90}{$\subseteq$}"] \\ K & \mathfrak{p} \end{tikzcd}$$

where $\mathfrak{l}, \mathfrak{q}, \mathfrak{p}$ are prime ideals in $\mathcal{O}_M, \mathcal{O}_L, \mathcal{O}_K$, respectively.

Proposition 3.72. *We have*

(a) $\varepsilon\left(\mathfrak{l}/\mathfrak{p}\right) = e\left(\mathfrak{l}/\mathfrak{q}\right) e\left(\mathfrak{q}/\mathfrak{p}\right)$

(b) $f\left(\mathfrak{l}/\mathfrak{p}\right) = f\left(\mathfrak{l}/\mathfrak{q}\right) f\left(\mathfrak{q}/\mathfrak{p}\right)$

Proof. (a)

$$\begin{aligned} \mathfrak{p}\mathcal{O}_M &= \mathfrak{p}\mathcal{O}_L \cdot \mathcal{O}_M \\ &= \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})} \\ &= \prod_{\mathfrak{q}|\mathfrak{p}} \left(\mathfrak{q}\mathcal{O}_M\right)^{e(\mathfrak{q}/\mathfrak{p})} \\ &= \prod_{\mathfrak{q}|\mathfrak{p}} \left(\prod_{\mathfrak{l}|\mathfrak{q}} \mathfrak{q}^{e(\mathfrak{l}/\mathfrak{q})}\right)^{e(\mathfrak{q}/\mathfrak{p})} \\ &= \prod_{\mathfrak{q}|\mathfrak{p}} \prod_{\mathfrak{l}|\mathfrak{q}} \mathfrak{q}^{e(\mathfrak{l}/\mathfrak{q}) e(\mathfrak{q}/\mathfrak{p})} \end{aligned}$$

(b) This proof relies on the fact that degrees of field extensions are multiplicative. In particular, we have a tower of fields

$$\begin{tikzcd} \mathcal{O}_M/\mathfrak{l} \arrow[d, no head] \\ \mathcal{O}_L/\mathfrak{q} \arrow[d, no head] \\ \mathcal{O}_K/\mathfrak{p} \end{tikzcd}$$

The degree of $\mathcal{O}_M/\mathcal{O}_L$ is $f(\mathfrak{l}/\mathfrak{q})$ and the degree of $\mathcal{O}_L/\mathcal{O}_K$ is $f(\mathfrak{q}/\mathfrak{p})$.

□

Proof of Theorem 3.71. Compute $N(\mathfrak{p}\mathcal{O}_L)$ in two ways. First,

$$\begin{aligned} N(\mathfrak{p}\mathcal{O}_L) &= N\left(\prod_{\mathfrak{q}\mid\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})}\right) \\ &= \prod_{\mathfrak{q}\mid\mathfrak{p}} N(\mathfrak{q})^{e(\mathfrak{q}/\mathfrak{p})} \\ &= \prod_{\mathfrak{q}\mid\mathfrak{p}} \left(N(\mathfrak{p})^{f(\mathfrak{q}/\mathfrak{p})}\right)^{e(\mathfrak{q}/\mathfrak{p})} \\ &= N(\mathfrak{p})^{\left(\sum_{q\mid p} e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p})\right)}. \end{aligned}$$

On the other hand, $N(p\mathcal{O}_L) = \#(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)$.

If $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, then $\mathcal{O}_L \cong \mathcal{O}_K^{[L\colon K]}$, and hence

$$\left({}^{\mathcal{O}_L}/_{\mathfrak{p}\mathcal{O}_L}\right) \cong \left({}^{\mathcal{O}_K}/_{\mathfrak{p}}\right)^{[L\colon K]}$$

as $\mathcal{O}_K$-modules.

Of course, we may not have that $\mathcal{O}_L$ is free over $\mathcal{O}_K$. To address this, localize at $\mathfrak{p}$. To ease notation, let $A = \mathcal{O}_K$ and let $B = \mathcal{O}_L$. We have $A \subseteq B$. Let $S = A \setminus \mathfrak{p}$. After localization, we get $S^{-1}A = A_{\mathfrak{p}}$ and $S^{-1}B$. We know that $S^{-1}A$ is a PID and $S^{-1}B$ is a finitely generated $S^{-1}A$-module. Hence, $S^{-1}B$ is a free $S^{-1}A$-module. The following exercise then shows us that

$$\dim_{A/_{\mathfrak{p}}} {}^{B}/_{\mathfrak{p}B} = \dim_{S^{-1}A/_{\mathfrak{p}S^{-1}A}} {}^{S^{-1}B}/_{\mathfrak{p}S^{-1}B} = [L\colon K]$$

as before. Hence, $\#\left({}^{B}/_{\mathfrak{p}B}\right) = N(\mathfrak{p})$. □

Exercise 3.73. Using the notation of the previous proof, the following are isomorphisms:

$$\begin{aligned} {}^{A}/_{\mathfrak{p}} &\to {}^{S^{-1}A}/_{\mathfrak{p}S^{-1}A} \\ {}^{B}/_{\mathfrak{p}B} &\to {}^{S^{-1}B}/_{\mathfrak{p}S^{-1}B} \end{aligned}$$

Example 3.74. Let X and Y be compact connected Riemann surfaces with a non-constant holomorphic map $\phi\colon Y \to X$. Let $\mathcal{M}_X$ and $\mathcal{M}_Y$ be the field of meromorphic functions on X and Y, respectively. There is an inclusion $\phi^*\colon \mathcal{M}_X \hookrightarrow \mathcal{M}_Y$ given by $f \mapsto f \circ \phi$. The degree n of the extension $\mathcal{M}_Y/\mathcal{M}_X$ is called the **degree of** ϕ.

Fix a point $p \in X$. Let $\mathcal{O}_p = \{f \in \mathcal{M}_X \mid f \text{ holomorphic at } p\}$. This is a ring; in fact, it is a DVR with maximal ideal $\mathfrak{p}$ consisting of those holomorphic f vanishing at p.

Let B be the integral closure of $\mathcal{O}_\mathfrak{p}$ in $\mathcal{M}_Y$. It is a Dedekind domain. We have

$$\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$$

for distinct primes $\mathfrak{q}_i$ with $f_i = \left[{}^{B}/_{\mathfrak{q}_i} \colon {}^{\mathcal{O}_p}/_{\mathfrak{p}}\right] = [\mathbb{C}\colon \mathbb{C}] = 1$. Moreover, if $\phi^{-1}(\{p\}) = \{q_1, \ldots, q_r\}$, then $\mathcal{O}_{q_i} = B_{\mathfrak{q}_i}$.

Geometrically, considering p as a divisor, $\phi^{-1}(p) = \sum_{i=1}^{r} e_i q_i$; the degree of this divisor is $\sum_{i=1}^{r} e_i = n$.

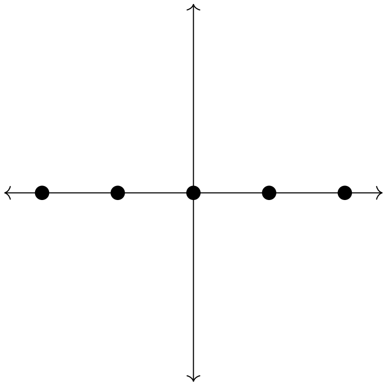
4 Geometry of Numbers (Minkowski Theory)

Definition 4.1. A **Euclidean space** is a finite dimensional real inner product space V.

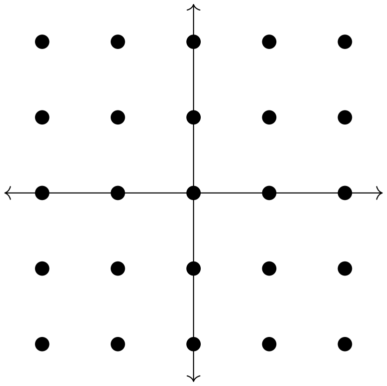
Choose any Euclidean space V with inner product $\langle\, ,\, \rangle\colon V \times V \to \mathbb{R}$. (You really lose nothing by thinking about $\mathbb{R}^n$ with the dot product.)

Recall that if H is an additive subgroup of V, H is **discrete** if and only if H is a free $\mathbb{Z}$-module generated by vectors linearly independent over $\mathbb{R}$.

Example 4.2. $\mathbb{Z} \subseteq \mathbb{C}$ is discrete, as is $\mathbb{Z}^2 \subseteq \mathbb{R}^2$.



$\mathbb{Z} \subseteq \mathbb{C}$



$\mathbb{Z}^2 \subseteq \mathbb{R}^2$

Definition 4.3. A subgroup $\Lambda \subseteq V$ is a **lattice** if it is discrete and spans V over $\mathbb{R}$, that is,

$$\Lambda = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \oplus \mathbb{Z}v_n$$

with $v_1, \ldots, v_n$ a basis for V over $\mathbb{R}$.

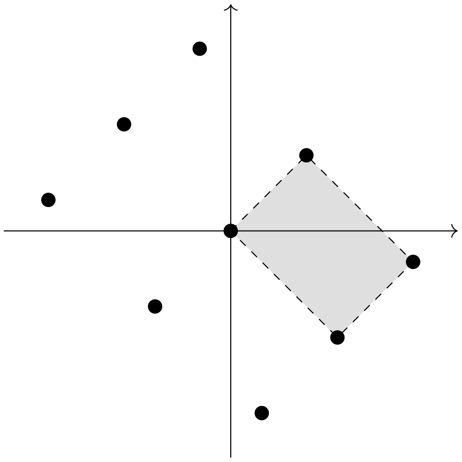
Remark 4.4. Warning: what we call a lattice is sometimes called a **complete** or **full** lattice.

Definition 4.5. Let $\Lambda \subseteq V$ be a lattice with $\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$. A **fundamental domain** for Λ is

$$\mathcal{F} = \{x_1 v_1 + \ldots + x_n v_n \mid 0 \leq x_i < 1\}$$

We have $V = \bigcup_{\lambda \in \Lambda} (\lambda + \mathcal{F})$.

Example 4.6. A fundamental domain for the lattice in $\mathbb{R}^2$ generated by the vectors $(1, 1)$ and $(\sqrt{2}, -\sqrt{2})$ is shaded in the picture below.



Definition 4.7. The **Haar measure** μ on V is given by

$$\mu\left(\{x_1 e_1 + \ldots + x_n e_n \mid 0 \leq x_i < 1\}\right) = 1$$

with $e_1, \ldots, e_n$ an orthonormal basis for V: $\langle e_i, e_j \rangle = \delta_{ij}$.

The Haar measure essentially assigns volume 1 to the fundamental domain. We say that

$$\mathrm{vol}(\mathcal{F}) = \mu(\mathcal{F}).$$

Definition 4.8. The **covolume of** $\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$ is $\mathrm{covol}(\Lambda) := \mathrm{vol}(F) = \mu(\mathcal{F})$.

The covolume of Λ is independent of the v_i. If $e_1, \ldots, e_n$ is an orthonormal basis for V, write

$$v_i = \sum_{j=1}^{n} A_{ij} e_j$$

for a unique $A \in \mathrm{GL}_n(\mathbb{R})$. Then $\mathrm{vol}(\mathcal{F}) = |\det(A)|$. The matrix B with entries $B_{ij} = \langle v_i, v_j \rangle$ satisfies $B = AA^T$, and $\mathrm{covol}(\Lambda) = \mathrm{vol}(\mathcal{F}) = \sqrt{|\det(B)|}$.

Remark 4.9. The quotient map $V \to V/\Lambda$ relates the volume and covolume. Note that V/Λ is compact and has a measure $\overline{\mu}$ induced from the one on V.

$$\mathrm{vol}\,(V/\Lambda) = \overline{\mu}(V/\Lambda) = \mu(F) = \mathrm{covol}(\Lambda).$$

4.1 Algebraic integers as a lattice

Let K be a number field of degree n. Recall that

$$K_{\mathbb{R}} := \left\{ (a_\sigma)_\sigma \in \prod_\sigma \mathbb{C} \mid \overline{a_\sigma} = a_{\overline{\sigma}} \forall \sigma \right\}$$

where σ runs over all complex embeddings $\sigma\colon K \to \mathbb{C}$. Recall also that $\overline{\sigma}$ is the complex conjugate embedding of σ given by complex conjugation following σ.

$K_{\mathbb{R}}$ is a real vector space of dimension n. There is a map

$$\begin{aligned} K &\xrightarrow{\ \ i\ \ } K_{\mathbb{R}} \\ \alpha &\longmapsto (\sigma(\alpha))_\sigma \end{aligned}$$

that induces an isomorphism of $\mathbb{R}$-algebras

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}}.$$

We saw that $\Lambda := i(\mathcal{O}_K)$ is a lattice in $K_{\mathbb{R}}$. Indeed, we have $\mathcal{O}_K \cong \mathbb{Z}^n \subseteq K \cong \mathbb{Q}^n$ as additive abelian groups.

For a nonzero ideal $I \subseteq \mathcal{O}_K$, $i(I)$ is a lattice in $K_{\mathbb{R}}$.

We want an inner product on $K_{\mathbb{R}}$. Recall that we had a pairing

$$\begin{aligned} K \times K &\longrightarrow Q \\ (\alpha, \beta) &\longmapsto \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) \end{aligned}$$

where

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta) = \sum_{\sigma\colon K \hookrightarrow \mathbb{C}} \sigma(\alpha)\sigma(\beta).$$

Define the pairing

$$\begin{aligned} K_{\mathbb{R}} \times K_{\mathbb{R}} &\xrightarrow{\ \langle\, ,\rangle\ } \mathbb{R} \\ \big((a_\sigma)_\sigma, (b_\sigma)_\sigma\big) &\longmapsto \textstyle\sum_\sigma a_\sigma b_\sigma \end{aligned}$$

Why does this land in $\mathbb{R}$? This is easy to check.

$$\overline{\sum_\sigma a_\sigma b_\sigma} = \sum_\sigma \overline{a_\sigma}\overline{b_\sigma} = \sum_\sigma a_{\overline{\sigma}} b_{\overline{\sigma}} = \sum_\sigma a_\sigma b_\sigma.$$

For $\alpha, \beta \in K$, we have

$$\langle i(\alpha), i(\beta) \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta).$$

Let r be the number of embeddings $\sigma\colon K \hookrightarrow \mathbb{R}$ and let s be the number of complex conjugate pairs of embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$. We have $n = r + 2s$, and we may order the embeddings such that

- $\sigma_1, \ldots, \sigma_r$ are the real embeddings of K
- $\sigma_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}$ are the complex embeddings of K.

Then $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{R}^{2s} \cong \mathbb{R}^n$ via

$$(a_\sigma)_\sigma \mapsto \left(a_{\sigma_1}, \ldots, a_{\sigma_r}, \mathrm{Re}(a_{\sigma_{r+1}}), \ldots, \mathrm{Re}(a_{\sigma_{r+s}}), \mathrm{Im}(a_{\sigma_{r+1}}), \ldots, \mathrm{Im}(a_{\sigma_{r+s}})\right)$$

The inner product on the left hand side is given by

$$\begin{aligned}\langle (a_\sigma), (b_\sigma) \rangle &= \sum_\sigma a_\sigma b_\sigma \\ &= \sum_{i=1}^{r} a_{\sigma_i} b_{\sigma_i} + \sum_{i=r+1}^{r+s} \left(a_{\sigma_i} b_{\sigma_i} + \overline{a_{\sigma_i}}\overline{b_{\sigma_i}}\right) \\ &= \sum_{i=1}^{r} a_{\sigma_i} b_{\sigma_i} + \sum_{i=r+1}^{r+s} \left(2\mathrm{Re}(a_{\sigma_i})\mathrm{Re}(b_{\sigma_i}) + 2\mathrm{Im}(a_{\sigma_i})\mathrm{Im}(b_{\sigma_i})\right)\end{aligned}$$

So the inner product on $\mathbb{R}^n$ that we want to use is a weird one:

$$\langle x, y \rangle = \sum_{i=1}^{r} x_i y_j + 2 \sum_{i=r+1}^{s} x_i y_i$$

What is the covolume of $\mathcal{O}_K$? Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then $i(x_1), \ldots, i(x_n)$ is a $\mathbb{Z}$-basis for $i(\mathcal{O}_K)$.

$$\begin{aligned}\mathrm{covol}(\mathcal{O}_K) &= \left|\det\left(\langle i(x_i), i(x_j)\rangle\right)\right|^{1/2} \\ &= \left|\det\left(\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j)\right)\right|^{1/2} \\ &= |\mathrm{disc}(K)|^{1/2}\end{aligned}$$

This is worth writing down as a proposition. We have proved the following:

Proposition 4.10. $i(\mathcal{O}_K)$ *is a latice in* $(K_{\mathbb{R}}, \langle\ ,\ \rangle)$ *with covolume* $\sqrt{\mathrm{disc}(K)}$.

4.2 Minkowski's Theorem

Definition 4.11. Let V be a Euclidean space.

(a) We say that a subset $X \subseteq V$ is **symmetric** if $x \in X \implies -x \in X$.

(b) We say that X is **convex** if $x, y \in X \implies tx + (1-t)y \in X$ for all $0 \leq t \leq 1$.

Theorem 4.12 (Minkowski)**.** *Let Λ be a lattice in a Euclidean space V of dimension n. Let X be a nonempty measurable subset of V that is symmetric and convex. Assume one of the following:*

(a) $\mathrm{vol}(X) > 2^n \,\mathrm{covol}(\Lambda)$*, or*

(b) $\mathrm{vol}(X) \geq 2^n \,\mathrm{covol}(\Lambda)$ *and* X *is compact.*

Then X *contains a non-zero element of* Λ*.*

Lemma 4.13. *If* $\mathrm{vol}(X) > \mathrm{covol}(\Lambda)$*, then there are two distinct points* $x, y \in X$ *such that* $x - y \in \Lambda$*.*

Proof. Consider the quotient map $\phi\colon V \to V/\Lambda$. If $\phi|_X$ is injective, then $\mathrm{vol}(X) = \mu(X) = \overline{\mu}(X)$, and therefore $\mathrm{vol}(X) \leq \overline{\mu}(V/\Lambda) = \mathrm{covol}(\Lambda)$. This is a contradiction of our assumption!

So $\phi|_X$ cannot be injective. Hence, there are distinct $x, y \in X$ such that $\phi(x) = \phi(y)$, and $\phi(x - y) = 0 \implies x - y \in \Lambda$. □

Proof of Theorem 4.12. Assume (a). Define $X' = \frac{1}{2}X$, so

$$\mathrm{vol}(X') = \frac{1}{2^n}\,\mathrm{vol}(X) > \mathrm{covol}(\Lambda)$$

by assumption. By the lemma, there are distinct $x, y \in X'$ such that $x - y \in \Lambda$. It remains to show that $x - y \in X$. Write

$$x - y = \frac{1}{2}(2x - 2y).$$

with $2x, 2y \in 2X' = X$. Since $2y \in X$, then $-2y \in X$ since X is symmetric. Since X is convex, we know that the average

$$x - y = \tfrac{1}{2}(2x) + \tfrac{1}{2}(-2y)$$

lies in X.

Now assume (b). Take any $\varepsilon > 0$, and scale X by $(1+\varepsilon)$. The shape $(1+\varepsilon)X$ has volume strictly greater than $2^n \,\mathrm{covol}(\Lambda)$. By the previous paragraph, $(1+\varepsilon)X$ contains a nonzero element in Λ. For $0 < \varepsilon' < \varepsilon$, $(1+\varepsilon')X \subseteq (1+\varepsilon)X$ using convexity and the fact that $0 \in X$ by symmetry and convexity. Then the intersection

$$\bigcap_{\varepsilon > 0}\Big((1+\varepsilon)X \cap (\Lambda \setminus \{0\})\Big)$$

is the intersection of compact and nonempty sets, and is therefore itself nonempty. So there exists some $\lambda \in \Lambda \setminus \{0\}$ such that $\lambda \in (1+\varepsilon)X$ for all $\varepsilon > 0$. Hence, $\lambda \in X$ because X is compact. □

Remark 4.14. Compactness is needed if we assume (b). If $\Lambda = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_n$, then

$$X = \left\{ \sum_{i=1}^{n} x_i v_i \;\middle|\; -1 < x_i < 1 \right\}$$

has $\mathrm{vol}(X) = 2^n \,\mathrm{covol}(\Lambda)$ yet $X \cap \Lambda = \{0\}$.

A classical application of Minkowski's theorem is the following, due to LaGrange.

Theorem 4.15 (LaGrange)**.** *All integers $n \geq 1$ are the sum of four squares.*

Lemma 4.16. *It suffices to show that primes are the sum of four squares.*

Proof. Let $\mathbb{H}$ be the ring of quaternions. Take $\alpha = a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$. Its conjugates is $\overline{\alpha} = a - bi - cj - dk$. We have $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$, and we may use the conjugation to define a norm:

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2.$$

For $\alpha, \beta \in \mathbb{H}$, we have

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

The left hand side is a sum of four squares, and the two terms on the right-hand side are each sums of four squares as well. □

Lemma 4.17. *For any odd prime p, there exist $r, s \in \mathbb{Z}$ such that $r^2 + s^2 + 1^2 + 0^2 \equiv 0 \pmod{p}$.*

Proof. Recall that $(\mathbb{F}_p^\times)^2$ is cyclic of order $\frac{p-1}{2}$. There are $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ possible residues for $r^2 \pmod{p}$ and likewise, $\frac{p+1}{2}$ possible residues for $-1 - s^2 \pmod{p}$. Since

$$\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p,$$

then by the pigeonhole principle we may find $r, s \in \mathbb{F}_p$ such that $r^2 = -1 - s^2$. □

Proof of Theorem 4.15. By Lemma 4.16, it suffices to prove the theorem for primes. The theorem is easy for $p = 2$. So take any odd prime p and choose, by Lemma 4.17, two integers r, s such that $r^2 + s^2 + 1 \equiv 0 \pmod{p}$. Define

$$A = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in M_4(\mathbb{Z}).$$

Let Λ be the lattice $\Lambda := A\mathbb{Z}^4 \subseteq \mathbb{R}^4$, where $\mathbb{R}^4$ is equipped with the usual dot product. The covolume of Λ is $\mathrm{covol}(\Lambda) = |\det(A)| \, \mathrm{covol}(\mathbb{Z}^4) = p^2$.

Claim that for all $\lambda \in \Lambda$, $\|\lambda\|^2 \equiv 0 \pmod{p}$. If

$$\lambda = A \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} pa + rc + sd \\ pb + sc - rd \\ c \\ d \end{pmatrix}$$

Then

$$\begin{aligned}\|\lambda\|^2 &= (pa + rc + sd)^2 + (pb + sc - rd)^2 + c^2 + d^2 \\ &\equiv (r^2 + s^2 + 1)c^2 + (s^2 + r^2 + 1)d^2 \pmod p \\ &\equiv 0 \pmod p\end{aligned}$$

Now take $X = \{v \in \mathbb{R}^4 \mid \|v\|^2 < 2p\}$. If Minkowski's theorem applies, $\lambda \in \Lambda \setminus \{0\}$ lies inside X, then $0 < \|\lambda\|^2 < 2p$ and $\|\lambda\|^2 \in \mathbb{Z}$ is divisible by p by the above. Hence, $\|\lambda\|^2 = p$, so p is a sum of four squares, since

$$\left\| \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \right\|^2 = a^2 + b^2 + c^2 + d^2.$$

So it remains to show that Minkowski's theorem applies to X. We have

$$\operatorname{vol}(X) = \frac{1}{2}\pi^2 \left(\sqrt{2p}\right)^4 = 2\pi^2 p^2 > 2^4 p^2 = 2^4 \operatorname{covol}(\Lambda),$$

which verifies assumption (a) in Theorem 4.12. □

4.3 The class group is finite

Let K be a number field of degree n. Let r be the number of real embeddings $K \hookrightarrow \mathbb{R}$. Let s be the number of conjugate pairs of embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$ with $\sigma(K) \subsetneq \mathbb{R}$.

Theorem 4.18. *Let I be any nonzero ideal of $\mathcal{O}_K$. Then I contains an element α satisfying*

$$|N_{K/\mathbb{Q}}(\alpha)| \le \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{disc}(K)|} \cdot N(I)$$

We call the number $(\frac{4}{\pi})^s \frac{n!}{n^n} \sqrt{|\operatorname{disc}(K)|}$ **Minkowski's constant** for K. Note that it doesn't depend on the ideal I.

Remark 4.19. We may reinterpret this inequality: if $\alpha \in I$ then $\alpha\mathcal{O}_K \subseteq I$. We have

$$[I\colon \alpha\mathcal{O}_K] = \frac{[\mathcal{O}_K\colon \alpha\mathcal{O}_K]}{[\mathcal{O}_K\colon I]} = \frac{N(\alpha\mathcal{O}_K)}{N(I)} = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(I)} \le \left(\frac{4}{\pi}\right)^2 \frac{n!}{n^n} \sqrt{|\operatorname{disc} K|}$$

Notice that the bound depends only on the field K; it is independent of both α and I. So this says that principal ideals and ideals are relatively close to each other, because the index $[I\colon \alpha\mathcal{O}_K]$ is bounded.

Note, however, that the element α depends on I in Theorem 4.18. If we are allowed to choose α, we may make $[I\colon \alpha\mathcal{O}_K]$ as large as we like. For example, we may scale the given α by any integer to make $|N_{K/\mathbb{Q}}(\alpha)|$ as large as we like.

Corollary 4.20. *Every class in the class group $\mathcal{C}\ell_K$ contains an integral ideal of norm at most $\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|}$. In particular, $\mathcal{C}\ell_K$ is finite.*

Proof of Corollary 4.20. Take any $\mathfrak{k} \in \mathcal{C}\ell_K$. Choose an integral ideal I such that $[I] = \mathfrak{k}^{-1}$. Set $C = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|}$. By the theorem, there is a nonzero $\alpha \in I$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \le C \cdot N(I).$$

Let $J = \alpha I^{-1} \subseteq \mathcal{O}_K$. By definition, we have $[J] = [I^{-1}] = [I]^{-1} = \mathfrak{k}$. This is an ideal of $\mathcal{O}_K$. By the calculation

$$N(J)N(I) = N(JI) = N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)| \le C \cdot N(I)$$

we have $N(J) \le C$.

Finally, $\mathcal{C}\ell_K$ is finite since there are only finitely many ideals of $\mathcal{O}_K$ with a given norm. □

Example 4.21. Let $K = \mathbb{Q}(i)$. In this case, $C = (4/\pi)^1 \frac{2!}{2^2}\sqrt{|-4|} = 4/\pi < 2$. Hence, every element of $\mathcal{C}\ell_{\mathbb{Q}(i)}$ contains an ideal of norm 1. Since $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, then $\mathcal{C}\ell_{\mathbb{Q}(i)} = \{[\mathcal{O}_K]\}$ is trivial.

Corollary 4.22. *$\mathcal{C}\ell_K$ is generated by classes $[\mathfrak{p}]$ with $N(\mathfrak{p}) \le \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\operatorname{disc} K|}$.*

Proof Sketch. Write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ so $[I] = [\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_r]^{e_r}$ in the class group and $N(I) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$. Then use the Corollary 4.20. □

Example 4.23. Consider $K = \mathbb{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have already shown that $\mathcal{O}_K$ is not a PID, which means that the class group is necessarily nontrivial.

There are no real embeddings and 2 complex embeddings (an embedding and its conjugate). Then Minkowski's bound is

$$M_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{|-20|} \approx 2.8.$$

What are the ideals of norm at most 2? The only ideal of norm 1 is $\mathcal{O}_K$, and we have seen that $\langle 2\rangle = \mathfrak{p}^2$ with $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle$. Hence, $\mathfrak{p}$ has norm 2.

Then $\mathcal{C}\ell_K = \{[\mathcal{O}_K], [\mathfrak{p}]\} \cong \mathbb{Z}/2\mathbb{Z}$.

Note that $\mathfrak{p}$ is not a principal ideal: if it were, say $\mathfrak{p} = \langle\alpha\rangle$ for some $\alpha \in \mathcal{O}_K$, then $|N_{K/\mathbb{Q}}(\alpha)| = N(\mathfrak{p}) = 2$. Yet if $\alpha = a + b\sqrt{-5}$, then $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2$, which is never 2.

Example 4.24. Let $K = \mathbb{Q}(\sqrt{-26})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-26}]$. We have $n = 2$, $r = 0$ and $s = 1$, and $\operatorname{disc}(K) = -104$. In this case, Minkowski's constant is approximately 6.49. Hence, $C\ell_K$ is generated by prime ideals $\mathfrak{p}$ with $N(\mathfrak{p}) \le 6 < 6.49$. In particular, $N(\mathfrak{p}) \in \{2, 3, 4, 5\}$. Let's do these case-by-case.

- If $N(\mathfrak{p}) = 2$,
  $$x^2 + 26 \equiv x^2 \pmod 2.$$
  This gives one ideal $\mathfrak{p}_2$ with $\mathfrak{p}_2^2 = \langle 2 \rangle$ and $\mathfrak{p}_2 = \langle 2, \sqrt{-26} \rangle$.
- If $N(\mathfrak{p}) = 3$,
  $$x^2 + 26 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod 3$$
  This gives two ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ such that $\langle 3 \rangle = \mathfrak{p}_3\mathfrak{p}_3'$ with $\mathfrak{p}_3 = \langle 3, \sqrt{-26} + 1 \rangle$ and $\mathfrak{p}_3' = \langle 3, \sqrt{-26} - 1 \rangle$.
- If $N(\mathfrak{p}) = 5$,
  $$x^2 + 26 \equiv x^2 + 1 \equiv (x+2)(x+3) \pmod 5.$$
  There are two ideals $\mathfrak{p}_5$ and $\mathfrak{p}_5'$ with $\langle 5 \rangle = \mathfrak{p}_5\mathfrak{p}_5'$ and $\mathfrak{p}_5 = \langle 5, \sqrt{-26} + 2 \rangle$ and $\mathfrak{p}_5' = \langle 5, \sqrt{-26} + 3 \rangle$.

The two relations $\mathfrak{p}_3\mathfrak{p}_3' = \langle 3 \rangle$ and $\mathfrak{p}_5\mathfrak{p}_5' = \langle 5 \rangle$ give relations in the class group

$$[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$$
$$[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$$

For $a + b\sqrt{-26} \in \mathcal{O}_K$,

$$|N_{K/\mathbb{Q}}(a + b\sqrt{-26})| = a^2 + 26b^2.$$

The right hand side is never $2, 3$ or 5, so $\mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_5$ are not principal. So we learn that $C\ell_K$ is therefore generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$. Let's find the relations between these.

Consider $\alpha = 2 + \sqrt{-26}$. Then $N_{K/\mathbb{Q}}(\alpha) = 30 = 2 \cdot 3 \cdot 5$. We have $\alpha = 2 + \sqrt{-26} \in \mathfrak{p}_2$ but also $\alpha = 3 + (\sqrt{-26} - 1) \in \mathfrak{p}_3'$ and $\alpha = 2 + \sqrt{-26} \in \mathfrak{p}_5$. Therefore,

$$\langle \alpha \rangle = \mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_5,$$

which gives a relation in the class group

$$1 = [\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5],$$

so we may eliminate $[\mathfrak{p}_5]$ from our set of generators.

Notice that $[\mathfrak{p}_2]$ has order 2, because we know that $\mathfrak{p}_2$ is not principal and moreover $\langle 2\rangle = \mathfrak{p}_2^2$, so $[\mathfrak{p}_2]^2 = 1$ in the class group.

Similarly, claim that $[\mathfrak{p}_3]$ has order 3. Let $\alpha = 1 + \sqrt{-26}$. $N_{K/\mathbb{Q}}(\alpha) = 27$. So now if we write

$$\langle \alpha \rangle = \mathfrak{p}_3^a (\mathfrak{p}_3')^b$$

the left hand side has norm 27 and the right side has order 3^{a+b}. So $a + b = 3$. If $a \geq 1, b \geq 1$, then $\alpha \in \mathfrak{p}_3\mathfrak{p}_3' = \langle 3 \rangle$. This is impossible because $\alpha/3 \notin \mathcal{O}_K$. So either $\langle \alpha \rangle = \mathfrak{p}_3^3$ or $\langle \alpha \rangle = (\mathfrak{p}_3')^3$. Note that $\alpha \in \mathfrak{p}_3$, so $\langle \alpha \rangle = \mathfrak{p}_3^3$. The fact that $\mathfrak{p}_3$ is not principal and this relation gives $[\mathfrak{p}_3]^3 = 1$ in the class group.

So we have found that $C\ell_K$ is generated by $[\mathfrak{p}_2]$ of order 2 and $[\mathfrak{p}_3]$ of order 3. There are no relations between the two, so

$$C\ell_K \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{3\mathbb{Z}} \cong {}^{\mathbb{Z}}/_{6\mathbb{Z}}.$$

In fact, $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3]$ is a generator of this group of order 6; we could have checked this directly.

Proof of Theorem 4.18. Consider the embedding $i \colon \mathcal{O}_K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^n$ given by

$$(a_\sigma)_\sigma \mapsto \left(a_{\sigma_1}, \ldots, a_{\sigma_r}, \mathrm{Re}(a_{\sigma_{r+1}}), \ldots, \mathrm{Re}(a_{\sigma_{r+s}}), \mathrm{Im}(a_{\sigma_{r+1}}), \ldots, \mathrm{Im}(a_{\sigma_{r+s}})\right) \tag{4.1}$$

Recall that the inner product on this space is given by

$$\langle x, y \rangle = \sum_{i=1}^{n} e_i x_i y_i$$

with $e_i = 1$ for $1 \leq i \leq r$ and $e_i = 2$ for $r + 1 \leq i \leq r + s$.

Recall also that $i(\mathcal{O}_K)$ is a lattice of covolume $\sqrt{|\operatorname{disc} K|}$. The image of any nonzero ideal $I \subseteq \mathcal{O}_K$ under i is also a lattice $i(I) \subseteq \mathbb{R}^n$ of covolume $N(I) \cdot \sqrt{|\operatorname{disc} K|}$.

Take any $\alpha \in I$. We have

$$|N_{K/\mathbb{Q}}(\alpha)| = \left| \prod_{\sigma} \sigma(\alpha) \right| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2 \tag{4.2}$$

By the AMGM inequality, we have

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2 \leq \left(\frac{1}{n} \sum_{i=1}^{r} |\sigma_i(\alpha)| + \frac{2}{n} \sum_{i=r+1}^{r+s} |\sigma_i(\alpha)| \right)^n$$

For $t > 0$, define

$$X_t := \left\{ x \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^{r} |x_i| + 2 \sum_{i=r+1}^{r+s} \sqrt{x_i^2 + x_{i+s}^2} \leq t \right\}.$$

If $i(\alpha) \in X_t$, then $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{t^n}{n^n}$. Note that $X_t \subseteq \mathbb{R}^n$ is compact, symmetric, and convex. So we may apply Minkowski's Theorem (Theorem 4.12). If $\operatorname{vol}(X_t) \geq 2^n \operatorname{covol}(i(I))$, then there is a non-zero $\alpha \in I$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq {}^{t^n}/_{n^n}.$$

The theorem then follows from Exercise 4.33: once we know that

$$\operatorname{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!},$$

choose $t > 0$ such that $2^r \pi^s \frac{t^n}{n!} = 2^n \sqrt{|\operatorname{disc} K|} \cdot N(I)$. Therefore,

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{disc} K|} N(I).$$

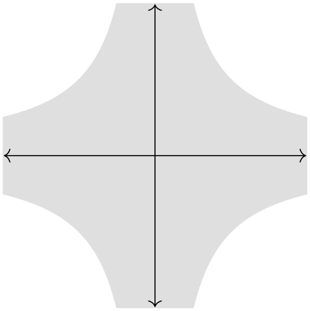
□

Exercise 4.25 (Boring Exercise)**.** Show that $\operatorname{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}$.

Remark 4.26. In the proof above, it would be more straightforward to pick the region

$$Y_t := \left\{ y \in \mathbb{R}^n \;\middle|\; \prod_{i=1}^{r} |y_i| \prod_{i=r+1}^{r+s} (y_i^2 + y_{i+s}^2) \leq t \right\}$$

by analogy to (4.4). But this isn't convex or necessarily compact! In fact, if $s = 0$ and $r = 2$, then $Y_t = \{(x, y) \in \mathbb{R}^2 \mid |xy| \leq t\}$ looks like the shaded region below



4.4 Bounds on the Discriminant

Recall that every class of $C\ell_K$ contains an integral ideal of norm at most Minkowski's bound $(\frac{4}{\pi})^s \frac{n!}{n^n} \sqrt{|\operatorname{disc} K|}$. Since the norm of an ideal is always at least 1, this gives a lower bound on the discriminant: solving the inequality

$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{disc} K|} \geq 1$$

for disc(K), we learn

$$\sqrt{|\operatorname{disc}(K)|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}.$$

A slightly weaker inequality is obtained using $\pi/4 < 1$ and $s \leq n/2$.

$$|\operatorname{disc}(K)|^{1/2} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}$$

Now consider the sequence

$$a_n = \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}.$$

The ratio of terms is

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2} \left(1 + \frac{1}{n}\right)^n$$

which converges to $\sqrt{\frac{\pi}{4}} \cdot e$ as $n \to \infty$, so $a_n \to \infty$ as $n \to \infty$ by the ratio test. We have proved:

Proposition 4.27. *For any integer d, there are only finitely many $n \geq 1$ for which there is a number field K of degree n and discriminant d.*

If $K \neq \mathbb{Q}$ (and hence $n \geq 2$), then in particular

$$\sqrt{|\operatorname{disc}(K)|} \geq \left(\frac{\pi}{4}\right)^{2/2} \frac{2^2}{2!} = \frac{\pi}{2} > 1$$

Hermite used this to show the following:

Theorem 4.28 (Hermite)**.** *For any number field $K \neq \mathbb{Q}$, we have* $\operatorname{disc}(K) \neq \pm 1$. *In particular, there is a prime p that ramifies in K.*

Corollary 4.29.

Corollary 4.30. $C\ell_K$ *is generated by classes* $[\mathfrak{p}]$ *with* $N(\mathfrak{p}) \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{disc} K|}$.

Proof Sketch. Write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ so $[I] = [\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_r]^{e_r}$ in the class group and $N(I) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$. Then use the Corollary 4.20. □

Example 4.31. Consider $K = \mathbb{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have already shown that $\mathcal{O}_K$ is not a PID, which means that the class group is necessarily nontrivial.

There are no real embeddings and 2 complex embeddings (an embedding and its conjugate). Then Minkowski's bound is

$$M_K = \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2} \sqrt{|-20|} \approx 2.8.$$

What are the ideals of norm at most 2? The only ideal of norm 1 is $\mathcal{O}_K$, and we have seen that $\langle 2\rangle = \mathfrak{p}^2$ with $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle$. Hence, $\mathfrak{p}$ has norm 2.

Then $C\ell_K = \{[\mathcal{O}_K], [\mathfrak{p}]\} \cong \mathbb{Z}/2\mathbb{Z}$.

Note that $\mathfrak{p}$ is not a principal ideal: if it were, say $\mathfrak{p} = \langle \alpha\rangle$ for some $\alpha \in \mathcal{O}_K$, then $|N_{K/\mathbb{Q}}(\alpha)| = N(\mathfrak{p}) = 2$. Yet if $\alpha = a + b\sqrt{-5}$, then $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2$, which is never 2.

Example 4.32. Let $K = \mathbb{Q}(\sqrt{-26})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-26}]$. We have $n = 2$, $r = 0$ and $s = 1$, and $\operatorname{disc}(K) = -104$. In this case, Minkowski's constant is approximately 6.49. Hence, $C\ell_K$ is generated by prime ideals $\mathfrak{p}$ with $N(\mathfrak{p}) \le 6 < 6.49$. In particular, $N(\mathfrak{p}) \in \{2,3,4,5\}$. Let's do these case-by-case.

- If $N(\mathfrak{p}) = 2$,
$$x^2 + 26 \equiv x^2 \pmod{2}.$$
This gives one ideal $\mathfrak{p}_2$ with $\mathfrak{p}_2^2 = \langle 2\rangle$ and $\mathfrak{p}_2 = \langle 2, \sqrt{-26}\rangle$.

- If $N(\mathfrak{p}) = 3$,
$$x^2 + 26 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod{3}$$
This gives two ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ such that $\langle 3\rangle = \mathfrak{p}_3\mathfrak{p}_3'$ with $\mathfrak{p}_3 = \langle 3, \sqrt{-26}+1\rangle$ and $\mathfrak{p}_3' = \langle 3, \sqrt{-26}-1\rangle$.

- If $N(\mathfrak{p}) = 5$,
$$x^2 + 26 \equiv x^2 + 1 \equiv (x+2)(x+3) \pmod{5}.$$
There are two ideals $\mathfrak{p}_5$ and $\mathfrak{p}_5'$ with $\langle 5\rangle = \mathfrak{p}_5\mathfrak{p}_5'$ and $\mathfrak{p}_5 = \langle 5, \sqrt{-26}+2\rangle$ and $\mathfrak{p}_5' = \langle 5, \sqrt{-26}+3\rangle$.

The two relations $\mathfrak{p}_3\mathfrak{p}_3' = \langle 3\rangle$ and $\mathfrak{p}_5\mathfrak{p}_5' = \langle 5\rangle$ give relations in the class group
$$[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$$
$$[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$$

For $a + b\sqrt{-26} \in \mathcal{O}_K$,
$$|N_{K/\mathbb{Q}}(a + b\sqrt{-26})| = a^2 + 26b^2.$$

The right hand side is never $2, 3$ or 5, so $\mathfrak{p}_2, \mathfrak{p}_3$ and $\mathfrak{p}_5$ are not principal. So we learn that $C\ell_K$ is therefore generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$. Let's find the relations between these.

Consider $\alpha = 2 + \sqrt{-26}$. Then $N_{K/\mathbb{Q}}(\alpha) = 30 = 2\cdot 3\cdot 5$. We have $\alpha = 2 + \sqrt{-26} \in \mathfrak{p}_2$ but also $\alpha = 3 + (\sqrt{-26} - 1) \in \mathfrak{p}_3'$ and $\alpha = 2 + \sqrt{-26} \in \mathfrak{p}_5$. Therefore,
$$\langle\alpha\rangle = \mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_5,$$

which gives a relation in the class group

$$1 = [\mathfrak{p}_2][\mathfrak{p}_3][\mathfrak{p}_5],$$

so we may eliminate $[\mathfrak{p}_5]$ from our set of generators.

Notice that $[\mathfrak{p}_2]$ has order 2, because we know that $\mathfrak{p}_2$ is not principal and moreover $\langle 2\rangle = \mathfrak{p}_2^2$, so $[\mathfrak{p}_2]^2 = 1$ in the class group.

Similarly, claim that $[\mathfrak{p}_3]$ has order 3. Let $\alpha = 1 + \sqrt{-26}$. $N_{K/\mathbb{Q}}(\alpha) = 27$. So now if we write

$$\langle \alpha \rangle = \mathfrak{p}_3^a (\mathfrak{p}_3')^b$$

the left hand side has norm 27 and the right side has order 3^{a+b}. So $a+b=3$. If $a \geq 1, b \geq 1$, then $\alpha \in \mathfrak{p}_3\mathfrak{p}_3' = \langle 3\rangle$. This is impossible because $\alpha/3 \notin \mathcal{O}_K$. So either $\langle\alpha\rangle = \mathfrak{p}_3^3$ or $\langle\alpha\rangle = (\mathfrak{p}_3')^3$. Note that $\alpha \in \mathfrak{p}_3$, so $\langle\alpha\rangle = \mathfrak{p}_3^3$. The fact that $\mathfrak{p}_3$ is not principal and this relation gives $[\mathfrak{p}_3]^3 = 1$ in the class group.

So we have found that $C\ell_K$ is generated by $[\mathfrak{p}_2]$ of order 2 and $[\mathfrak{p}_3]$ of order 3. There are no relations between the two, so

$$C\ell_K \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \oplus {}^{\mathbb{Z}}/_{3\mathbb{Z}} \cong {}^{\mathbb{Z}}/_{6\mathbb{Z}}.$$

In fact, $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3]$ is a generator of this group of order 6; we could have checked this directly.

Proof of Theorem 4.18. Consider the embedding $i\colon \mathcal{O}_K \hookrightarrow K_\mathbb{R} \cong \mathbb{R}^n$ given by

$$(a_\sigma)_\sigma \mapsto \big(a_{\sigma_1}, \ldots, a_{\sigma_r}, \mathrm{Re}(a_{\sigma_{r+1}}), \ldots, \mathrm{Re}(a_{\sigma_{r+s}}), \mathrm{Im}(a_{\sigma_{r+1}}), \ldots, \mathrm{Im}(a_{\sigma_{r+s}})\big) \tag{4.3}$$

Recall that the inner product on this space is given by

$$\langle x, y\rangle = \sum_{i=1}^n e_i x_i y_i$$

with $e_i = 1$ for $1 \leq i \leq r$ and $e_i = 2$ for $r+1 \leq i \leq r+s$.

Recall also that $i(\mathcal{O}_K)$ is a lattice of covolume $\sqrt{|\operatorname{disc} K|}$. The image of any nonzero ideal $I \subseteq \mathcal{O}_K$ under i is also a lattice $i(I) \subseteq \mathbb{R}^n$ of covolume $N(I) \cdot \sqrt{|\operatorname{disc} K|}$.

Take any $\alpha \in I$. We have

$$|N_{K/\mathbb{Q}}(\alpha)| = \left|\prod_\sigma \sigma(\alpha)\right| = \prod_{i=1}^r |\sigma_i(\alpha)| \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2 \tag{4.4}$$

By the AMGM inequality, we have

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{i=1}^r |\sigma_i(\alpha)| \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2 \leq \left(\frac{1}{n}\sum_{i=1}^r |\sigma_i(\alpha)| + \frac{2}{n}\sum_{i=r+1}^{r+s} |\sigma_i(\alpha)|\right)^n$$

For $t > 0$, define

$$X_t := \left\{ x \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^{r} |x_i| + 2 \sum_{i=r+1}^{r+s} \sqrt{x_i^2 + x_{i+s}^2} \leq t \right\}.$$

If $i(\alpha) \in X_t$, then $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{t^n}{n^n}$. Note that $X_t \subseteq \mathbb{R}^n$ is compact, symmetric, and convex. So we may apply Minkowski's Theorem (Theorem 4.12). If $\mathrm{vol}(X_t) \geq 2^n \operatorname{covol}(i(I))$, then there is a non-zero $\alpha \in I$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq {}^{t^n}/_{n^n}.$$

The theorem then follows from Exercise 4.33: once we know that

$$\mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!},$$

choose $t > 0$ such that $2^r \pi^s \frac{t^n}{n!} = 2^n \sqrt{|\operatorname{disc} K|} \cdot N(I)$. Therefore,

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\operatorname{disc} K|} N(I).$$

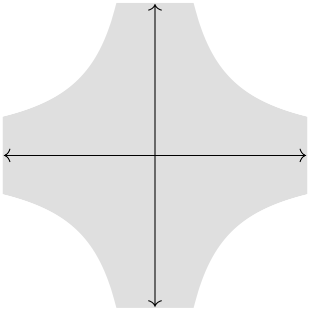
□

Exercise 4.33 (Boring Exercise)**.** Show that $\mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}$.

Remark 4.34. In the proof above, it would be more straightforward to pick the region

$$Y_t := \left\{ y \in \mathbb{R}^n \;\middle|\; \prod_{i=1}^{r} |y_i| \prod_{i=r+1}^{r+s} (y_i^2 + y_{i+s}^2) \leq t \right\}$$

by analogy to (4.4). But this isn't convex or necessarily compact! In fact, if $s = 0$ and $r = 2$, then $Y_t = \{(x, y) \in \mathbb{R}^2 \mid |xy| \leq t\}$ looks like the shaded region below



4.5 Bounds on the Discriminant

Recall that every class of $C\ell_K$ *contains an integral ideal of norm at most Minkowski's bound* $(\frac{4}{\pi})^s \frac{n!}{n^n}\sqrt{|\operatorname{disc} K|}$*. Since the norm of an ideal is always at least* 1*, this gives a lower bound on the discriminant: solving the inequality*

$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\operatorname{disc} K|} \geq 1$$

for $\operatorname{disc}(K)$*, we learn*

$$\sqrt{|\operatorname{disc}(K)|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}.$$

A slightly weaker inequality is obtained using $\pi/4 < 1$ *and* $s \leq n/2$*.*

$$|\operatorname{disc}(K)|^{1/2} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}$$

Now consider the sequence

$$a_n = \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}.$$

The ratio of terms is

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2} \left(1 + \frac{1}{n}\right)^n$$

which converges to $\sqrt{\frac{\pi}{4}} \cdot e$ *as* $n \to \infty$*, so* $a_n \to \infty$ *as* $n \to \infty$ *by the ratio test. We have proved:*

Proposition 4.35. *For any integer* d*, there are only finitely many* $n \geq 1$ *for which there is a number field* K *of degree* n *and discriminant* d*.*

If $K \neq \mathbb{Q}$ *(and hence* $n \geq 2$*), then in particular*

$$\sqrt{|\operatorname{disc}(K)|} \geq \left(\frac{\pi}{4}\right)^{2/2} \frac{2^2}{2!} = \frac{\pi}{2} > 1$$

Hermite used this to show the following:

Theorem 4.36 (Hermite)**.** *For any number field* $K \neq \mathbb{Q}$*, we have* $\operatorname{disc}(K) \neq \pm 1$*. In particular, there is a prime* p *that ramifies in* K*.*

Let K *and* L *be number fields such that* $\operatorname{disc}(K)$ *and* $\operatorname{disc}(L)$ *are relatively prime. Then* $K \cap L = \mathbb{Q}$*.*

Proof. Let $E = K \cap L$. Suppose that p ramifies in E; then p must ramify in both K and L. Consider the tower

$$\begin{tikzcd}
K \arrow[d, dash] & \supseteq & \mathfrak{q} \arrow[d, dash] \\
E \arrow[d, dash] & \supseteq & \mathfrak{p} \arrow[d, dash] \\
\mathbb{Q} & \supseteq & \langle p \rangle
\end{tikzcd}$$

The ramification degree of $\mathfrak{p}$ over p must be more than 1, so

$$e(^{\mathfrak{q}}/_{p}) = e(^{\mathfrak{q}}/_{\mathfrak{p}})e(^{\mathfrak{p}}/_{p}) > 1$$

This implies that $p \mid \operatorname{disc}(K)$ and $p \mid \operatorname{disc}(L)$, but this is impossible by the assumption that $\operatorname{disc}(K)$ and $\operatorname{disc}(L)$ are coprime. So E, no primes ramify in E. Then by Theorem 4.36, $E = \mathbb{Q}$. □

Remark 4.37. Under the same assumption, if $F = KL$, then we have

(a) $\mathcal{O}_F = \mathcal{O}_K\mathcal{O}_L$

(b) If $x_1, \ldots, x_n$ is an integral basis of K and $y_1, \ldots, y_m$ is an integral basis of L, then $x_i y_j$ is an integral basis of F.

(c) $\operatorname{disc}(F) = \operatorname{disc}(K)^{[L\,:\,\mathbb{Q}]}\operatorname{disc}(L)^{[K\,:\,\mathbb{Q}]}$

Theorem 4.38. *For any $d \in \mathbb{Z}$, there are only finitely many number fields with discriminant d up to isomorphism.*

Proof. It suffices to consider number fields K of a fixed degree $n > 1$. Let $d = \operatorname{disc}(K)$. Consider $i\colon \mathcal{O}_K \hookrightarrow \mathbb{R}^n$ and enumerate the embeddings as before: we have r real embeddings

$$\sigma_1, \ldots, \sigma_r \colon K \hookrightarrow \mathbb{R}$$

and $2s$ complex embeddings

$$\begin{aligned}\sigma_{r+1}, \ldots, \sigma_{r+s} &\colon K \hookrightarrow \mathbb{C}\\ \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}} &\colon K \hookrightarrow \mathbb{C}\end{aligned}$$

The map $i\colon \mathcal{O}_K \to \mathbb{R}^n$ is given by

$$i(\alpha) = \big(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \operatorname{Im}(\sigma_{r+1}(\alpha)), \ldots, \operatorname{Im}(\sigma_{r+s}(\alpha)), \operatorname{Re}(\sigma_{r+1}(\alpha)), \ldots, \operatorname{Re}(\sigma_{r+s}(\alpha))\big)$$

Now fix a constanct $C > 0$. Define

$$X = \left\{x \in \mathbb{R}^n \;\middle|\; |x_1| \leq C,\ |x_i| \leq \tfrac{1}{2} \text{ for } i \geq 2\right\}$$

This is a compact, symmetric, convex set, with $\operatorname{vol}(X) \geq b_n C$ for some constant b_n depending on n. Take C large enough (depending on n and d) such that $\operatorname{vol}(X) \geq 2^n \operatorname{covol}(i(\mathcal{O}_K)) = 2^n\sqrt{|\operatorname{disc}(K)|}$.

By Minkowski's theorem there is some nonzero $\alpha \in \mathcal{O}_K$ with $i(\alpha) \in X$. For $i \geq 2$, we have $|\sigma_i(\alpha)| < 1$: for real σ_i, $|\sigma_i(\alpha)| \leq \frac{1}{2} < 1$, and for complex σ_i, $|\sigma_i(\alpha)| \leq \sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2} < 1$.

So we must have $|\sigma_1(\alpha)| > 1$, since

$$1 \leq |N_{K/\mathbb{Q}}(\alpha)| = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} |\sigma(\alpha)|$$

Now claim that $K = \mathbb{Q}(\alpha)$. Indeed, if p_α is the minimal polynomial of α, then

$$\prod_{\sigma\colon K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)) = p_\alpha(x)^{[K\colon \mathbb{Q}(\alpha)]}$$

We will show $\sigma_1(\alpha) \neq \sigma(\alpha)$ for $\sigma \neq \sigma_1$. Hence, $[K\colon \mathbb{Q}(\alpha)] = 1$, so $K = \mathbb{Q}(\alpha)$. To establish the claim, it remains to show that $\sigma_1(\alpha) \neq \sigma(\alpha)$ for $\sigma \neq \sigma_1$. For $\sigma \notin \{\sigma_1, \overline{\sigma}_1\}$, $|\sigma(\alpha)| < 1$. Therefore, $\sigma(\alpha) \neq \sigma_1(\alpha)$ since $|\sigma_1(\alpha)| > 1$. And moreover, $\sigma_1(\alpha) \neq \overline{\sigma}_1(\alpha)$, since $|\mathrm{Re}(\sigma_1(\alpha))| < \frac{1}{2} \implies \mathrm{Im}(\sigma_1(\alpha)) \neq 0$, the implication because $|\sigma_1(\alpha)| > 1$.

Note that $|\sigma(\alpha)|$ is bounded by a constant depended only on n and d for all $\sigma\colon K \hookrightarrow \mathbb{C}$. So the coefficients of $p_\alpha(x)$ are bounded in terms of n and d. Thus, there are only finitely many possible p_α since they must have integer coefficients. This means that there are only finitely many $K = \mathbb{Q}(\alpha)$ up to isomorphism. □

Example 4.39. There are non-isomorphic fields with the same discriminant. Let α be a root of $p_\alpha(x) = x^4 - 6$ and β be a root of $p_\beta(x) = x^4 - 24$. Let $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$. We have $\mathrm{disc}(K) = \mathrm{disc}(L) = 2 \cdot 3^3$. So how do we tell these fields apart?

We can look at how primes factor in these fields. In this example, 5 factors differently in the two fields: $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, while $5\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$.

5 The units of $\mathcal{O}_K$

As always, fix a number field K of degree n with r real embeddings and $2s$ complex embeddings (s pairs of conjugate embeddings). What are the units of the number ring $\mathcal{O}_K$?

Consider the map

$$\begin{aligned} \phi\colon K^\times &\longrightarrow \mathfrak{I}_K \\ \alpha &\longmapsto \alpha\mathcal{O}_K \end{aligned}$$

where $\mathfrak{I}_K$ is the group of fractional ideals of $\mathcal{O}_K$, which is the free abelian group on the prime ideals of $\mathcal{O}_K$ by the prime factorization theorem. The cokernel of ϕ is the class group:

$$\mathrm{coker}(\phi) = {}^{\mathfrak{I}_K}\!/_{\mathrm{im}(\phi)} = {}^{\mathfrak{I}_K}\!/_{\mathfrak{P}(K)} = C\ell_K\,.$$

What's the kernel of ϕ? If $\alpha\mathcal{O}_K = \mathcal{O}_K$ as fractional ideals, then $1 \in \alpha\mathcal{O}_K$, so there is some $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. Hence, $\ker(\phi) = \mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$.

Definition 5.1. The group μ_K of **roots of unity** of $\mathcal{O}_K$ is the torsion subgroup of $\mathcal{O}_K^\times$, i.e. the group of $\alpha \in \mathcal{O}_K^\times$ such that $\alpha^m = 1$ for some integer $m > 0$.

Define the homomorphism $\psi\colon \mathcal{O}_K^\times \to \mathbb{R}^{r+s}$ by

$$\alpha \mapsto \big(\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \ldots, 2\log|\sigma_{r+s}(\alpha)|\big)$$

Proposition 5.2. *The group $\psi(\mathcal{O}_K^\times)$ is discrete in $\mathbb{R}^{r+s}$. The kernel of ψ is the finite group μ_K.*

Proof. Take any $C \geq 1$. Consider the set $\mathcal{S}$ of $\alpha \in \mathcal{O}_K^\times$ such that $-C \leq \log|\sigma_i(\alpha)| \leq C$ for all $1 \leq i \leq r+s$.

Claim that $\mathcal{S}$ is finite. If $\alpha \in \mathcal{S}$, then $|\sigma_i(\alpha)| \leq e^C$ for all i. Since $i\colon \mathcal{O}_K \to \mathbb{R}^n$ has discrete image, there are only finitely many $\alpha \in \mathcal{O}_K$ with $|\sigma(\alpha)| \leq e^C$ for all $\sigma\colon K \hookrightarrow \mathbb{C}$. Hence, $\mathcal{S}$ is finite.

Since C is arbitrary and $\mathcal{S}$ is finite, $\psi(\mathcal{O}_K^\times)$ is discrete. Moreover, $\ker\psi \subseteq \mathcal{S}$ for any C. Since $\mathcal{S}$ is finite, $\ker(\psi)$ is a finite finite subgroup of $\mathcal{O}_K^\times$. Hence, $\ker(\psi) \subseteq \mu_K$. And finally, let $\zeta \in \mu_K$ such that $\zeta^m = 1$. Then for any embedding$\sigma\colon K \hookrightarrow \mathbb{C}$, $|\sigma(\zeta)|^m = 1$, so $|\sigma(\zeta)| = 1$ and $\zeta \in \ker\psi$. Hence $\mu_K \subseteq \ker\psi$. This shows $\mu_K = \ker\psi$. □

5.1 Dirichlet Unit Theorem and Examples

Theorem 5.3 (Dirichlet's Unit Theorem)**.** *Let K be a number field of degree n with r real embeddings and s conjugate pairs of complex embeddings. Then the abelian group $\mathcal{O}_K^\times$ is isomorphic to $\mu_K \times \mathbb{Z}^{r+s-1}$.*

In other words, there are $\mu_1, \ldots, \mu_{r+s-1} \in \mathcal{O}_K^\times$ such that every $\alpha \in \mathcal{O}_K^\times$ is of the form $\alpha = \zeta \cdot u_1^{n_1} \cdots u_{r+s-1}^{n_{r+s-1}}$ for unique $\zeta \in \mu_K$ and $n_i \in \mathbb{Z}$.

Example 5.4. If $K = \mathbb{Q}$, then $r = 1$ and $s = 0$. $r + s - 1 = 0$, and $\mathcal{O}_\mathbb{Q}^\times = \mathbb{Z}^\times = \{\pm 1\}$.

Example 5.5. If $K = \mathbb{Q}(\sqrt{d})$ for a squarefree integer $d < 0$, then $r = 0$, $s = 1$, and $r + s - 1 = 0$. In this case, $\mathcal{O}_K^\times = \mu_K$.

Indeed, if $d \not\equiv 1 \pmod 4$, take $\alpha = a + b\sqrt{d} \in \mathcal{O}_K \setminus \{0\}$. α is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ if and only if $a^2 - db^2 = \pm 1$. This equation only has solutions $(a, b) = (\pm 1, 0)$ (or $(a, b) = (0, \pm 1)$ if $d = -1$). Hence, $\alpha = \pm 1$ (or $\alpha = \pm i$ when $d = -1$). So we find that

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1\} & d \neq -1, -3 \\ \{\pm i\} & d = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\} & d = -3 \end{cases}$$

Example 5.6. If $K = \mathbb{Q}(\sqrt{d})$ for a squarefree integer $d > 1$, then $r = 2$ and $s = 0$. So $r + s - 1 = 1$ and $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}$. Since $K \subseteq \mathbb{R}$, and the only real roots of unity are ± 1, $\mu_K = \{\pm 1\}$. So under the isomorphism $\mathcal{O}_K \cong \mu_K \times \mathbb{Z}$, there is some $\varepsilon \in \mathcal{O}_K^\times$ such that $\mathcal{O}_K^\times = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$. If we take $\varepsilon > 1$, this is the **fundamental unit** of this ring of integers. s

$$\begin{array}{lll}
d = 2 & \varepsilon = 1 + \sqrt{2} & N_{K/\mathbb{Q}}(\varepsilon) = -1 \\
d = 10 & \varepsilon = 3 + \sqrt{10} & N_{K/\mathbb{Q}}(\varepsilon) = -1 \\
d = 93 & \varepsilon = \frac{29+3\sqrt{93}}{2} & N_{K/\mathbb{Q}}(\varepsilon) = -1 \\
d = 94 & \varepsilon = 2143295_2 21064\sqrt{94} &
\end{array}$$

Example 5.7. If $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ where $\zeta = \frac{-1+\sqrt{-3}}{2}$ is a cube root of unity. The order of K is $[K \colon \mathbb{Q}] = 6$. There are no real embeddings $(r = 0)$, and six complex embeddings $(s = 3)$, so $r + s - 1 = 2$. We have

$$\mu_K = \mu_6 = \{\pm 1, \pm\zeta, \pm\zeta^2\}.$$

Then $\mathcal{O}_K^\times = \mu_6\langle\varepsilon, \overline{\varepsilon}\rangle$. The fundamental unit is,

$$\varepsilon = \frac{-1 + 2\sqrt[3]{2} + (\sqrt[3]{2})^2}{3} + \frac{1 - \sqrt[3]{2} + (\sqrt[3]{2})^2}{3} \cdot \zeta.$$

In this case, the ring of integers is $\mathcal{O}_K = \mathbb{Z}[\varepsilon]$.

Example 5.8. If $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $r = 4$ and $s = 0$, so $r + s - 1 = 3$. The roots of unit are $\mu_K = \{\pm 1\}$, with fundamental units

$$\begin{aligned}
u_1 &= 1 + \sqrt{2} \\
u_2 &= \sqrt{2} + \sqrt{3} \\
u_3 &= \frac{\sqrt{2} + \sqrt{6}}{2}
\end{aligned}$$

Recall that an **order** of a number field K is a finite index subring of $\mathcal{O}_K$. The Dirichlet unit theorem also applies to these orders in a very similar form. In fact, this is the statement Dirichlet proved for $R = \mathbb{Z}[\alpha]$.

Corollary 5.9. *For any order $R \subseteq K$, we have $R^\times \cong \mu_R \times \mathbb{Z}^{r+s-1}$ where μ_R is the set of roots of unity in R.*

Proof. Let $N = [\mathcal{O}_K \colon R]$, and note that $N\mathcal{O}_K \subseteq R \subseteq \mathcal{O}_K$. Consider the homomorphism

$$R^\times \xrightarrow{\phi} \left({}^{\mathcal{O}_K}/_{N\mathcal{O}_K}\right)^\times.$$

Take any $\alpha \in \mathcal{O}_K^\times$ such that $\alpha \equiv 1 \pmod{N\mathcal{O}_K}$. We also have $\alpha^{-1} \equiv 1 \pmod{N\mathcal{O}_K}$, so

$$\alpha - 1, \alpha^{-1} - 1 \in N\mathcal{O}_K \subseteq R \implies \alpha, \alpha^{-1} \in R \implies \alpha \in R^\times$$

Then

$$[\mathcal{O}_K^\times : R^\times] \leq \# \left({}^{\mathcal{O}_K}/_{N\mathcal{O}_K} \right)^\times .$$

The right side of this inequality is finite, so $[\mathcal{O}_K^\times : R^\times]$ is finite. Since $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r+s-1$, then $R^\times$ must also be a finitely generated abelian group of rank $r+s-1$. □

5.2 Pell's Equation

Let's look at an application of this corollary. Fix a squarefree integer $d > 0$. What are the solutions $(x, y) \in \mathbb{Z}^2$ to

$$x^2 - dy^2 = 1?$$

This equation is called **Pell's Equation**.

We can rephrase this as follows: we are looking for elements $a + b\sqrt{d}$ of the order $R = \mathbb{Z}[\sqrt{d}]$ with $N(a + b\sqrt{d}) = 1$. Define

$$G := \left\{ a + b\sqrt{d} \in R^\times \;\middle|\; N(a + b\sqrt{d}) = 1 \right\} \leq R^\times .$$

This set is in bijection with the set of solutions

$$\left\{ (a, b) \in \mathbb{Z}^2 \;\middle|\; a^2 - db^2 = 1 \right\}.$$

We know that $R^\times \cong \mu_R \times \mathbb{Z}$ in this case, and G is index 1 or 2 in $R^\times$. $G = \pm\langle u \rangle \cong \mathbb{Z}/2 \times \mathbb{Z}$.

Example 5.10. For example, when $d = 10$, $x^2 - 10y^2 = 1$. The fundamental unit of $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ is $\varepsilon = 3 + \sqrt{10}$. The norm of this fundamental unit is $N_{K/\mathbb{Q}}(\varepsilon) = -1$. Here are a few solutions:

$$\begin{array}{ll} \varepsilon^2 = 19 + 6\sqrt{10} & \text{solution: } (19, 6) \\ (\varepsilon^2)^2 = 721 + 228\sqrt{10} & \text{solution: } (721, 228) \\ (\varepsilon^2)^3 = 27379 + 8658\sqrt{10} & \text{solution: } (27379, 8658) \end{array}$$

In fact, these are all solutions in the positive integers.

Example 5.11 (c.f. Example 2.11)**.** Find a solution (x, y) in positive integers to

$$x^2 - 1141y^2 = 1.$$

Let $K = \mathbb{Q}(\sqrt{1141}) \subseteq \mathbb{R}$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{1141}}{2}$ because $1141 \equiv 1 \pmod 4$.

$$\mathbb{Z}[\alpha] \cong \mathbb{Z} + \mathbb{Z}[\alpha] = \left\{ \tfrac{a+b\sqrt{1141}}{2} \;\middle|\; a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}$$

Problem: describe $\mathcal{O}_K^\times$, $R^\times$. Abstractly, Dirichlet's unit theorem tells us that $\mathcal{O}_K^\times = \pm\langle u\rangle$, for a fundamental unit $u > 1$ in $\mathcal{O}_K^\times$. So the problem is to find u.

Note that for $\beta \in K^\times$,

$$\beta\mathcal{O}_K = \mathcal{O}_K \iff \beta \in \mathcal{O}_K^\times.$$

The idea is to find β, γ with $\gamma\mathcal{O}_K = \beta\mathcal{O}_K$, so $\beta\gamma^{-1} \in \mathcal{O}_K^\times$.

Start by factoring

$$3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{q}_3$$

with $\mathfrak{p}_3 = \langle 3, \alpha\rangle$ and $\mathfrak{q}_3 = \langle 3, \alpha - 1\rangle$.

$$x^2 - x - 285 \equiv x^2 - x \equiv x(x-1) \pmod 3.$$

Likewise,

$$5\mathcal{O}_K = \mathfrak{p}_5, \mathfrak{q}_5$$

where $\mathfrak{p}_5 = \langle 5, \alpha\rangle$ and $\mathfrak{q}_5 = \langle 5, \alpha - 1\rangle$.

$$x^5 - x - 285 \equiv x(x-1) \pmod 5.$$

Factor

$$\begin{aligned} 15 - \alpha &= \frac{29 - \sqrt{1141}}{2} \\ 15 + \alpha &= \frac{31 + \sqrt{1141}}{2} \\ 21 - \alpha &= \frac{41 - \sqrt{1141}}{2} \end{aligned}$$

$N_{K/\mathbb{Q}}(15-\alpha) = -75 = -3 \cdot 5^2$. We factor $\langle 15 - \alpha\rangle$ into primes in $\mathcal{O}_K$. We have $15 - \alpha \in \mathfrak{p}_3$, $15 - \alpha \in \mathfrak{p}_5$, and $15 - \alpha \notin \mathfrak{q}_5$; if it were, $15 - \alpha \in \mathfrak{p}_5\mathfrak{q}_5 = \langle 5\rangle$, yet $\frac{15-\alpha}{5} \notin \mathcal{O}_K$. We have therefore factored

$$\langle 15 - \alpha\rangle = \mathfrak{p}_3\mathfrak{p}_5^2$$

We may likewise factor

$$\begin{aligned} \langle 15 - \alpha\rangle &= \mathfrak{p}_3\mathfrak{p}_5^2 \\ \langle 15 + \alpha\rangle &= \mathfrak{p}_3^2\mathfrak{p}_5 \\ \langle 21 - \alpha\rangle &= \mathfrak{p}_3^2\mathfrak{q}_5 \end{aligned}$$

Therefore, multiplying this last equation by $\mathfrak{p}_5^2$ on the right and then dividing by $\langle 5\rangle$, we have an equation of fractional ideals

$$\langle \tfrac{21-\alpha}{5}\rangle = \mathfrak{p}_3^2\mathfrak{p}_5^{-1}.$$

To make units out of this, write

$$\begin{aligned}\langle 15-\alpha\rangle^{a}\langle 15+\alpha\rangle^{b}\left\langle \tfrac{21-\alpha}{5}\right\rangle^{c} &= (\mathfrak{p}_3\mathfrak{p}_5^2)^{a}(\mathfrak{p}_3^2\mathfrak{p}_5)^{b}(\mathfrak{p}_3^3\mathfrak{p}_5^{-1})^{c}\\ &= \mathfrak{p}_3^{a+2b+3c}\mathfrak{p}_5^{2a+b-c}\end{aligned}$$

To find a unit, we ask when this ideal is $\mathcal{O}_K$. This happens when $a = \frac{5}{3}c$ and when $b = -\frac{7}{3}c$. So try $(a, b, c) = (-5, 7, -3)$. Then

$$\varepsilon = -\left(15-\alpha\right)^{-5}\left(15+\alpha\right)^{7}\left(\frac{21-\alpha}{2}\right)^{-3}$$

is a unit in $\mathcal{O}_K$. Now, we have to be careful that this is not just ±1, but when we expand it out we have

$$\varepsilon = 618715978 + 37751109\alpha$$

In fact, ε is the fundamental unit of $\mathcal{O}_K^\times$.

However, we were searching for solutions $x^2 - 1141y^2 = 1$ and therefore searching for units in $R = \mathbb{Z}[\sqrt{1141}] \neq \mathcal{O}_K$. In particular, $\varepsilon \notin R$. But $\varepsilon^3 \in R^\times$ (in fact $R^\times = \pm\langle\varepsilon^3\rangle$) so this gives us a solution (x_0, y_0) with

$$\begin{aligned}x_0 &= 1036782394157223963237125215\\ y_0 &= 30693385322765657197397208.\end{aligned}$$

5.3 Proof of the Dirichlet Unit Theorem

Recall the homomorphism

$$\begin{aligned}\psi\colon K^\times &\longrightarrow \mathbb{R}^{r+s}\\ \alpha &\longmapsto (e_i \log|\sigma_i(\alpha)|)\end{aligned}$$

where

$$e_i = \begin{cases} 1 & (1 \le i \le r),\\ 2 & (r < i \le r+s).\end{cases}$$

We already proved the following in Section 5:

- ψ is a homomorphism of groups;
- $\psi(\mathcal{O}_K^\times) \subseteq \mathbb{R}^{r+s}$ is discrete;
- $\ker(\psi|_{\mathcal{O}_K^\times}) = \mu_K$;

Now define

$$V := \left\{ x \in \mathbb{R}^{r+s} \;\middle|\; \sum_{i=1}^{r+s} x_i = 0 \right\}.$$

Note that V is a $\mathbb{R}$-vector space of dimension $r+s-1$. Claim that $\psi(\mathcal{O}_K^\times) \subseteq V$. Indeed, for $\alpha \in \mathcal{O}_K^\times$,

$$1 = |N_{K/\mathbb{Q}}(\alpha)| = \prod_{\sigma} |\sigma(\alpha)| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{i=1}^{r+s} |\sigma_i(\alpha)|^2$$

Taking logarithms,

$$0 = \sum_{i=1}^{r} \log|\sigma_i(\alpha)| + 2\sum_{i=1}^{r+s} \log|\sigma_i(\alpha)|.$$

So $\psi(\alpha) \in V$. Then, the discreteness of $\psi(\mathcal{O}_K^\times)$ shows that

$$\mathcal{O}_K^\times/_{\mu_K} \cong \psi(\mathcal{O}_K^\times).$$

Hence, $\mathcal{O}_K^\times/\mu_K \cong \mathbb{Z}^m$ for some $m \le r+s-1$.

In fact, Dirichlet's unit theorem is equivalent to the statement that $\psi(\mathcal{O}_K^\times)$ is a lattice in V.

Definition 5.12. The number

$$\mathrm{Reg}_K := \frac{\mathrm{covol}(\psi(\mathcal{O}_K^\times))}{\sqrt{r+s}}$$

is called the **regulator** of K.

Alternatively, consider the $(r+s-1) \times (r+s)$ matrix

$$\Big(e_j \log|\sigma_j(u_i)| \Big) \tag{5.1}$$

where $u_1, \ldots, u_{r+s-1}$ are a basis for $\mathcal{O}_K^\times/\mu_K$ as an $\mathcal{O}_K^\times$-module.

Fact 5.13. *The columns of the matrix* (5.1) *sum to zero, and the regulator of* K *is the determinant of the matrix obtained by removing any column.*

It would be nice to know the regulator of a number field K. Indeed, if μ_K, $\alpha_1, \ldots, \alpha_{r+s-1}$ generate a subgroup $H \le \mathcal{O}_K^\times$ of rank $r+s-1$.

$$\frac{\mathrm{covol}(\psi(H))}{\mathrm{covol}(\psi(\mathcal{O}_K^\times))} = [\mathcal{O}_K^\times : H]$$

The denominator on the left hand side comes from the regulator, so if we know the index and the regulator, we can find the covolume of $\psi(H)$ and then try to figure out what the group H is.

Proof of Dirichlet's Unit Theorem (Theorem 5.3). Let's dispatch with the easy case $r+s-1=0$ first. In this case, $\psi(\mathcal{O}_K^\times) \subseteq V$ and $\dim_{\mathbb{R}} V = r+s-1=0$. Hence, $\psi(\mathcal{O}_K^\times) = 0$.

Now assume that $r+s-1>0$. Assume for the sake of contradiction that $\psi(\mathcal{O}_K^\times)$ has rank strictly less than $r+s-1$. Then there is a nonzero $\mathbb{R}$-linear map $f\colon V \to \mathbb{R}$ with $f(\psi(\mathcal{O}_K^\times)) = 0$. There are unique $c_i \in \mathbb{R}$ such that for all $v \in V \subseteq \mathbb{R}^{r+s}$,

$$f(v) = c_1 v_1 + \ldots + c_{r+s-1} v_{r+s-1}; \tag{5.2}$$

note that we do not nee v_{r+s} since $\sum_i v_i = 0$. Using (5.2), we extend f to an $\mathbb{R}$-linear map $f\colon \mathbb{R}^{r+s} \to \mathbb{R}$.

Define a real number

$$A := \sqrt{|\operatorname{disc}(K)|}\left(\frac{2}{\pi}\right)^s > 0$$

depending only on the number field K.

Goal: construct a sequence $\alpha_1, \alpha_2, \ldots$ of nonzero numbers in $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha_i)| \leq A$, and the values $f(\psi(\alpha_i))$ are distinct.

Assuming that we can prove this goal, then $N(\alpha_i \mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha_i)| \leq A$. Since there are only finitely many ideals in $\mathcal{O}_K$ of bounded norm, there are distinct α_n, α_m with $\alpha_n \mathcal{O}_K = \alpha_m \mathcal{O}_K$ and $f(\psi(\alpha_n)) \neq f(\psi(\alpha_m))$. Define $\beta = \alpha_n \alpha_m^{-1} \in K^\times$. Then $\beta \mathcal{O}_K = \mathcal{O}_K \implies \beta \in \mathcal{O}_K^\times$, yet

$$f(\psi(\beta)) = f(\psi(\alpha_n)) - f(\psi(\alpha_m)) \neq 0,$$

contradicting the choice of f such that $f(\psi(\mathcal{O}_K^\times)) = 0$.

Now it remains to construct this sequence. This is a geometry of numbers proof, so recall the embedding $i\colon \mathcal{O}_K \hookrightarrow \mathbb{R}^n$ from (4.3) such that $i(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ of covolume $\sqrt{|\operatorname{disc} K|}$. Define

$$X := \left\{ x \in \mathbb{R}^n \;\middle|\; \begin{array}{cc} |x_i| \leq b_i & (1 \leq i \leq r), \\ x_i^2 + x_{i+s}^2 \leq b_i^2 & (r+1 \leq i \leq r+s) \end{array} \right\}$$

with $b_i > 0$ fixed real numbers such that

$$b_1 \cdots b_r (b_{r+1} \cdots b_{r+s})^2 = A.$$

If $\alpha \in \mathcal{O}_K$ with $i(\alpha) \in X$, then $|\sigma_i(\alpha)| \leq b_i$ for $1 \leq i \leq r+s$. Therefore,

$$|N_{K/\mathbb{Q}}(\alpha)| = \left| \prod_{i=1}^{r+s} \sigma_i(\alpha) \cdot \prod_{i=1}^{s} \overline{\sigma_{r+i}}(\alpha) \right| \leq b_1 \cdots b_r (b_{r+1} \cdots b_{r+s})^2 = A$$

Note that X is compact, symmetric, and convex, and

$$\operatorname{vol}(X) = \prod_{i=1}^{r}(2b_i) \cdot \prod_{i=r+1}^{r+s} (\pi b_i^2) \cdot 2^s = 2^{r+s}\pi^s A = 2^n \sqrt{|\operatorname{disc}(K)|} = 2^n \operatorname{covol}(i\mathcal{O}_K)$$

So by Minkowski's theorem, there is some $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $i(\alpha) \in X$. Hence, $|N_{K/\mathbb{Q}}(\alpha)| \leq A$.

We will now prove, by varying the b_i, that we can find α as above with $f(\psi(\alpha)) \in \mathbb{R}$ arbitrarily large. This will prove the goal.

Claim that for $1 \leq i \leq r+s$,

$$^{b_i}/_A \leq |\sigma_i(\alpha)| \leq b_i.$$

The upper bound is from the construction of α, and the lower bound comes from

$$1 \leq |N_{K/\mathbb{Q}}(\alpha)| = |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)| \cdot \bigg(|\sigma_{r+1}(\alpha)| \cdots |\sigma_{r+s}(\alpha)| \bigg)^2$$

$$\leq |\sigma_i(\alpha)| \frac{b_1 \cdots b_r (b_{r+1} \cdots b_{r+s})^2}{b_i} = |\sigma_i(\alpha)| \frac{A}{b_i}$$

The idea is that $|\sigma_i(\alpha)|$ is "close" to b_i.

Then, plug $\psi(\alpha)$ in to $f(v) = \sum_{i=1}^{r+s-1} c_i v_i$ for $v \in \mathbb{R}^{r+s}$.

$$f(\psi(\alpha)) = \sum_{i=1}^{r+s-1} c_i e_i \log |\sigma_i(\alpha)|.$$

Approximating $|\sigma_i(\alpha)|$ by b_i, we have

$$\begin{aligned} \left| f(\psi(\alpha)) - \sum_{i=1}^{r+s-1} c_i e_i \log b_i \right| &\leq 2 \sum_{i=1}^{r+s-1} |c_i| \big| \log |\sigma_i(\alpha)| - \log b_i \big| \\ &\leq 2 \sum_{i=1}^{r+s-1} |c_i| \log \left(^{|\sigma_i(\alpha)|}/_{b_i} \right) \\ &\leq 2 \sum_{i=1}^{r+s-1} |c_i| \log A, \end{aligned}$$

the last inequality by the claim in the previous paragraph. This bound $2 \sum_{i=1}^{r+s-1} |c_i| \log A$ is some fixed number depending only on the number field K. By rearranging,

$$f(\psi(\alpha)) \geq \sum_{i=1}^{r+s-1} c_i e_i \log b_i - 2 \sum_{i=1}^{r+s-1} |c_i| \log A.$$

Since not all c_i are zero since $f \neq 0$, then we may choose $b_1, \ldots, b_{r+s-1}$ to be positive real numbers such that

$$\sum_{i=1}^{r+s-1} c_i e_i \log b_i$$

is arbitrarily large. Since b_{r+s} is absent from the sum, this choice of b_i is compatible with the condition we imposed on the b_i, namely the condition that $b_1 \cdots b_r(b_{r+1} \cdots b_{r+s})^2 = A$. □

Example 5.14. Let $K = \mathbb{Q}(\alpha)$, for α a root of $x^3 - 3x + 1$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is exactly what we expect. The cubic has three real roots, so there are three real embeddings and no complex embeddings. So $\mathcal{O}_K^\times$ has rank $r + s - 1 = 2$. In fact, $\mathcal{O}_K^\times = \pm\langle u_1, u_2\rangle$ where $u_1 = -\alpha + 1$ and $u_2 = \alpha^2 + \alpha - 1$.

Given $u = -14 + 32\alpha + 21\alpha^2 \in \mathcal{O}_K^\times$, how do we express it in terms of u_1 and u_2? We may compute the image of this unit under

$$\begin{aligned} \psi\colon \mathcal{O}_K^\times &\longrightarrow \mathbb{R}^3 \\ \alpha &\longmapsto \big(\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|, \log|\sigma_3(\alpha)|\big) \end{aligned}$$

Then we have

$$\begin{aligned} \psi(u_1) &= (-0.4266\ldots, -0.6309\ldots, 1.0575\ldots) \\ \psi(u_2) &= (-0.6309\ldots, 1.0575\ldots, -0.4266\ldots) \\ \psi(u) &= (-1.0395\ldots, 4.4346\ldots, -3.3950\ldots) \end{aligned}$$

Since $u = \pm u_1^m u_2^n$ for unique $m, n \in \mathbb{Z}$ and ψ is a homomorphism, then we may write $\psi(u) = m\psi(u_1) + n\psi(u_2)$; a numerical calculation shows $(m, n) \approx (-2.0002, 3.0001)$. So we expect that $u = \pm u_1^{-2}u_2^3$. We can then check that $u = u_1^{-2}u_2^3$.

6 Galois extensions of number fields

Let L/K be an extension of number fields. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime ideal. Recall that

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})}$$

where the product ranges over all prime ideals $\mathfrak{q}$ of $\mathcal{O}_L$ that divide $\mathfrak{p}\mathcal{O}_L$, and $e(\mathfrak{q}/\mathfrak{p})$ are the ramification degrees. We have

$$[L\colon K] = \sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p})f(\mathfrak{q}/\mathfrak{p})$$

where $f(\mathfrak{q}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q}\colon \mathcal{O}_K/\mathfrak{p}]$.

The problem we want to answer is: which factorizations occur as $\mathfrak{p}$ varies? To study this, we first review some Galois theory.

6.1 Galois Groups

Let K be a field. For simplicity, we can assume that K has characteristic zero or is finite (this ensures all finite extensions L/K are separable). Let L/K be a finite extension, and write $\mathrm{Aut}(L/K)$ for the group of field automorphisms of L that leave K fixed.

$$\mathrm{Aut}(L/K) := \left\{\sigma\colon L \xrightarrow{\cong} L \;\middle|\; \sigma(x) = x \;\forall x \in K\right\}.$$

For a subgroup $H \leq \mathrm{Aut}(L/K)$, let L^H be the field consisting of $x \in L$ such that $\sigma(x) = x$ for all $\sigma \in H$:

$$L^H := \left\{x \in L \;\middle|\; \sigma(x) = x \;\forall \sigma \in H\right\}.$$

Then we have

$$K \subseteq L^H \subseteq L.$$

Example 6.1 (Non-example)**.** An example of a non-separable field extension. Consider $K = \mathbb{F}_p(t)$ and choose a root u of the irreducible polynomial $x^p + t \in K[x]$. Let $L = K(u) = \mathbb{F}_p(u)$. Then

$$(x+u)^p = x^p + u^p = x^p + t,$$

so L/K is a splitting field but $\mathrm{Aut}(L/K) = 1$.

Example 6.2. Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\sqrt{d})$ for $d \neq 1$ a squarefree integer. Then $\mathrm{Aut}(L/K) = \{\mathrm{id}, \tau\}$ where $\tau(a + b\sqrt{d}) = a - b\sqrt{d}$. We have $L^{\mathrm{Aut}(L/K)} = \mathbb{Q}$.

Example 6.3. Let $L = \mathbb{Q}(\sqrt[3]{2})$. Then $\mathrm{Aut}(L/\mathbb{Q})$ is trivial, since for any $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$, $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2$; this polynomial $x^3 - 2$ has only one root in $L \subseteq \mathbb{R}$.

Proposition 6.4. *If L/K is a separable field extension, then $\#\,\mathrm{Aut}(L/K) \leq [L\colon K]$.*

Proof. We have $L = K(\alpha)$ by our assumption on K that guarantees L/K is separable. Let $f(x) \in K[x]$ be the minimal polynomial of α. Each $\sigma \in \mathrm{Aut}(L/K)$ is determined by $\sigma(\alpha)$ and $\sigma(\alpha)$ is also a root of $f(x)$, since $0 = \sigma(0)$ and $\sigma(f(\alpha)) = f(\sigma(\alpha))$ because the coefficients of f are in K. Hence,

$$\#\,\mathrm{Aut}(L/K) \leq \#(\text{roots of } f(x) \text{ in } L) \leq \deg(f) = [L\colon K]. \qquad \square$$

Definition 6.5. We say that L/K is **Galois** if it is a separable extension and one of the following equivalent conditions hold:

(a) $\#\,\mathrm{Aut}(L/K) = [L\colon K]$

(b) $L^{\mathrm{Aut}(L/K)} = K$

(c) L is the splitting field of a polynomial $f(x) \in K[x]$.

This last condition says that $L = K(\alpha_1, \ldots, \alpha_n)$ with $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$.

Definition 6.6. If L/K is Galois, then the **Galois group** of the field extension is

$$\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K).$$

Theorem 6.7 (Fundamental Theorem of Galois Theory)**.** *Let* L/K *be a finite Galois extension. There is an inclusion reversing bijection*

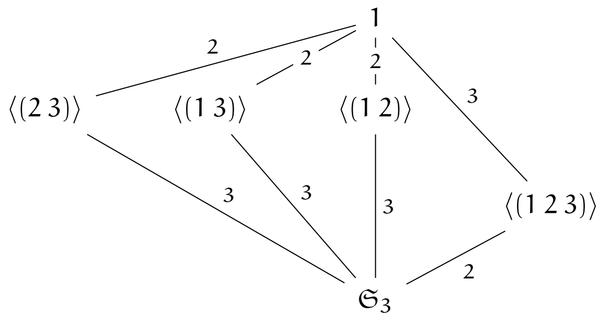
$$\left\{ \begin{matrix} \text{subgroups} \\ H \leq \mathrm{Gal}(L/K) \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{subfields} \\ K \subseteq F \subseteq L \end{matrix} \right\}$$

$$\begin{aligned} H &\longmapsto L^H \\ \mathrm{Gal}(L/F) = \mathrm{Aut}(L/F) &\longleftarrow\!\shortmid F \end{aligned}$$

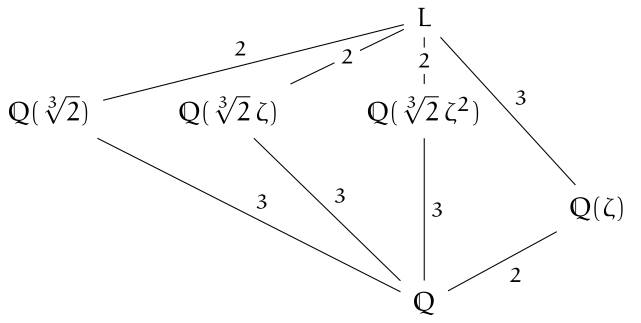
Remark 6.8. It's remarkably hard to try to prove that the set of intermediate fields $K \subseteq F \subseteq L$ is finite without this theorem.

Example 6.9. Let $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ where ζ is a cube root of unity. Then L is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$, which has roots $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\zeta$, and $\alpha_3 = \sqrt[3]{2}\,\zeta^2$.

There is an injective group homomorphism $\phi\colon \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathfrak{S}_3$ into the symmetric group $\mathfrak{S}_3$ such that $\sigma_{\alpha_i} = \alpha_{\phi(\sigma)i}$ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and $1 \leq i \leq 3$. In fact, this is an isomorphism in this case since $\#\mathrm{Gal}(L/\mathbb{Q}) = [L\colon \mathbb{Q}] = 6$ and likewise $\#\mathfrak{S}_3 = 6$. The lattice of subgroups of $\mathfrak{S}_3$ is



The numbers on the lines indicate the degrees of the subgroups. The diagram of intermediate fields $\mathbb{Q} \subseteq K \subseteq L$ looks the same (but upside down), and even the degrees of the field extensions are the same!


L
2
2
2
3
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\sqrt[3]{2}\,\zeta)$
$\mathbb{Q}(\sqrt[3]{2}\,\zeta^2)$
3
3
3
$\mathbb{Q}(\zeta)$
2
$\mathbb{Q}$

Example 6.10. Consider the field extension $\mathbb{F}_{q^n} \geq \mathbb{F}_q$. This is a separable extension because $\mathbb{F}_{q^n}$ is the splitting field of $x^{q^n} - x$. In fact, this is a Galois extension and $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n generated by the **Frobenius** homomorphism

$$\begin{aligned} \mathrm{Frob}_q \colon \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_{q^n} \\ x &\longmapsto x^q \end{aligned}$$

We can see that Frob_q is generating because the order of Frob_q is the smallest integer d such that

$$\mathrm{Frob}_q^d(x) = x^{q^d} = x$$

for all $x \in \mathbb{F}_{q^n}$. Hence, $d = n$.

Intermediate fields $\mathbb{F}_q \subseteq F \subseteq \mathbb{F}_{q^n}$ correspond to subgroups of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, which are cyclic groups of order d for $d \mid n$.

Example 6.11 (Cyclotomic Extensions)**.** Let $L = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity. This is a Galois extension of $\mathbb{Q}$; the roots of $x^m - 1$ are ζ_m^i with $0 \leq i < m$. The minimal polynomial of ζ_m is

$$\Phi_m(x) = \prod_{\substack{a=1 \\ \gcd(a,m)=1}}^{m} (x - \zeta_m^a) \in \mathbb{Z}[x].$$

The degree of $\Phi_m(x)$ is the **Euler totient function** $\varphi(m)$, where $\varphi(m)$ is the number of positive integers coprime to m.

Take any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then σ is determined by $\sigma(\zeta_m)$.

$$\sigma(\zeta_m) = \zeta_m^a$$

with $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. There is an injective homomorphism

$$\Psi\colon \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right)^{\times}$$

given by $\sigma(\zeta_m) = \zeta_m^{\Psi(\sigma)}$ for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. In fact, this is an isomorphism since both groups have the same cardinality.

6.2 Splitting in Galois Number Fields

Now consider a finite *Galois* extension L/K of number fields. Let $G = \mathrm{Gal}(L/K)$. For $\alpha \in L$, recall the trace and norm maps:

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

Fact 6.12. *For any* $\sigma \in G$, $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.

Proof. Indeed, for $\alpha \in L$, the minimal polynomial of $\sigma(\alpha)$ is the same as the minimal polynomial of α, since σ commutes with the coefficients of this polynomial:

$$\sigma(p_\alpha(x)) = p_\alpha(\sigma(x)) = p_{\sigma(\alpha)}(x).$$

□

By this fact, we have a well-defined action of G on $\mathcal{O}_L$. Indeed, if $\sigma \in G$ and $I \leq \mathcal{O}_L$ is an ideal, then $\sigma(I) \subseteq \sigma(\mathcal{O}_L) = \mathcal{O}_L$ is also an ideal, and we have an isomorphism of rings

$$\begin{tikzcd} \mathcal{O}_L/I \arrow[r, "\cong"] & \mathcal{O}_L/\sigma(I) \\ x + I \arrow[r, mapsto] & \sigma(x) + \sigma(I) \end{tikzcd}$$

In particular, if $\mathfrak{q} \subseteq \mathcal{O}_L$ is prime, then $\sigma(\mathfrak{q}) \subseteq \mathcal{O}_L$ is also prime.

Take any nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, and write

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})}.$$

Given any $\sigma \in G$, we have

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{\mathfrak{q}} \sigma(\mathfrak{q})^{e(\mathfrak{q}/\mathfrak{p})},$$

where the first equality holds since $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ and $\mathfrak{p} \subseteq K$ and σ fixes K.

Then by unique factorization, the Galois group G acts on the set

$$\left\{ \mathfrak{q} \subseteq \mathcal{O}_L \text{ prime} \;\middle|\; \mathfrak{q} \mid \mathfrak{p} \right\}.$$

Moreover, $e(\sigma(\mathfrak{q})/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p})$ and $f(\sigma(\mathfrak{q})/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p})$ since we have an isomorphism $\mathcal{O}_L/\mathfrak{q} \cong \mathcal{O}_L/\sigma(\mathfrak{q})$. We have proved:

Fact 6.13. *Let L/K be a Galois extension of number fields with Galois group G. Then for any $\sigma \in G$, $e(\sigma(\mathfrak{q})/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{p})$ and $f(\sigma(\mathfrak{q})/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{p})$.*

Proposition 6.14. *Let L/K be a Galois extension of number fields with Galois group G. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime ideal. Then G acts transitively on the set of $\mathcal{O}_L$-primes $\mathfrak{q}$ dividing $\mathfrak{p}$.*

Proof. Suppose not. Then there are two primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ in different G-orbits. By the Chinese remainder theorem, there is $x \in \mathcal{O}_L$ such that $x \in \mathfrak{q}_1, x \notin \sigma(\mathfrak{q}_2)$ for all $\sigma \in G$. So

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) = x \cdot \prod_{\substack{\sigma \in G \\ \sigma \neq 1}} \sigma(x) \in \mathfrak{q}_1$$

since $x \in \mathfrak{q}_1$. Hence,

$$\prod_{\sigma \in G} \sigma(x) = N_{L/K}(x) \in \mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p} \subseteq \mathfrak{q}_2.$$

Therefore, $\sigma(x) \in \mathfrak{q}_2$ for some $\sigma \in G$. So $x \in \sigma^{-1}(\mathfrak{q}_2)$, which contradicts the choice of x. □

By combining Fact 6.13 and Proposition 6.14, we arrive at the following theorem.

Theorem 6.15. *Let L/K be a Galois extension of number fields with Galois group G, and let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime ideal. Then*

(a) $\mathfrak{p}\mathcal{O}_L = (\mathfrak{q}_1 \cdots \mathfrak{q}_g)^e$ *for distinct primes* $\mathfrak{q}_i \subseteq \mathcal{O}_L$ *and a unique* $e \geq 1$*;*

(b) $f = f(\mathfrak{q}/\mathfrak{p})$ *is independent of the prime* $\mathfrak{q}$ *dividing* $\mathfrak{p}$.

(c) $[L \colon K] = \sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p}) = \sum_{\mathfrak{q}|\mathfrak{p}} ef = efg.$

Definition 6.16. Let L/K be a Galois extension of number fields with Galois group G. Fix a prime $\mathfrak{q}$ dividing $\mathfrak{p}$. Then the **decomposition group of** $\mathfrak{q}$ is the subgroup $D_\mathfrak{q}$ of G that fixes $\mathfrak{q}$.

$$D_\mathfrak{q} := \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

What is the size of the decomposition group? There is a bijection

$$\begin{tikzcd} {}^{G}/_{D_\mathfrak{q}} \arrow[r, "\cong"] & \{\mathfrak{q}' \mid \mathfrak{q}' \mid \mathfrak{p}\} \\ \sigma \arrow[r, mapsto] & \sigma(\mathfrak{q}) \end{tikzcd}$$

The right-hand-side of this bijection has g-many elements. Hence,

$$g = \left| {}^{G}/_{D_{\mathfrak{q}}} \right| = {}^{|G|}/_{|D_{\mathfrak{q}}|} = {}^{[L:K]}/_{|D_{\mathfrak{q}}|} = {}^{efg}/_{|D_{\mathfrak{q}}|}.$$

Therefore, $|D_{\mathfrak{q}}| = ef$.

Now take any $\sigma \in D_{\mathfrak{q}}$. Using the isomorphism

$$\begin{tikzcd} \mathbb{F}_{\mathfrak{q}} := {}^{\mathcal{O}_L}/_{\mathfrak{q}} \arrow[r, "\cong"] & {}^{\mathcal{O}_L}/_{\sigma(\mathfrak{q})} = {}^{\mathcal{O}_L}/_{\mathfrak{q}} = \mathbb{F}_{\mathfrak{q}} \\ x + \mathfrak{q} \arrow[r, mapsto] & \sigma(x) + \sigma(\mathfrak{q}) = \sigma(x) + \mathfrak{q} \end{tikzcd}$$

Therefore, each $\sigma \in G$ induces an automorphism of $\mathbb{F}_{\mathfrak{q}}$ that fixes $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$. Hence, there is a group homomorphism

$$\phi \colon D_{\mathfrak{q}} \longrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$$

The group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is a cyclic group of order equal to the degree of the extension $\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}$ of finite fields, which is $f = f(\mathfrak{q}/\mathfrak{p})$. It is generated by the Frobenius

$$x \mapsto x^{N(\mathfrak{p})},$$

where $N(\mathfrak{p}) = \#\mathbb{F}_{\mathfrak{p}} = \#\left({}^{\mathcal{O}_K}/_{\mathfrak{p}}\right)$ is the usual norm.

Lemma 6.17. *The homomorphism* $\phi \colon D_{\mathfrak{q}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ *is surjective.*

Proof. Use the Chinese remainder theorem. Take $\alpha \in \mathcal{O}_L$ such that

(i) $\mathbb{F}_{\mathfrak{p}}(\overline{\alpha}) = \mathbb{F}_{\mathfrak{q}}$ where $\overline{\alpha} = \alpha \pmod{\mathfrak{q}}$.

(ii) $\alpha \in \mathfrak{q}'$ for $\mathfrak{q}' \mid \mathfrak{p}$ with $\mathfrak{q}' \neq \mathfrak{q}$.

For any $\sigma \in G \setminus D_{\mathfrak{q}}$, we have $\sigma(\mathfrak{q}) \neq \mathfrak{q}$, and hence $\alpha \in \sigma(\mathfrak{q})$. Applying σ^{-1} to both sides, $\sigma(\alpha) \in \mathfrak{q}$ for all $\sigma \in G \setminus D_{\mathfrak{q}}$ ($G \setminus D_{\mathfrak{q}}$ is closed under inverses).

Define

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

Reducing mod $\mathfrak{q}$,

$$f(x) \equiv x^{|G \setminus D_{\mathfrak{q}}|} h(x) \pmod{\mathfrak{q}}$$

for some $h(x) \in \mathbb{F}_{\mathfrak{q}}[x]$. Note that $\overline{\alpha}$ is a root of $h(x)$; all terms in $h(x)$ come from those $\sigma \in D_{\mathfrak{q}}$, and in particular $(x - \alpha)$ is a root of $f(x)$, so $(x - \overline{\alpha})$ is a linear factor of $h(x)$ not accounted for in the $x^{|G \setminus D_{\mathfrak{q}}|}$.

Now take any $\tau \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$. Since $\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_{\mathfrak{p}}(\overline{\alpha})$, τ is determined by $\tau(\overline{\alpha})$. But $\overline{\alpha}$ is a root of $h(x) \in \mathbb{F}_{\mathfrak{p}}[x]$, so $\tau(\overline{\alpha})$ is a root of $h(x)$, so $\tau(\overline{\alpha}) \equiv \sigma(\alpha) \pmod{\mathfrak{q}}$ for some $\sigma \in D_{\mathfrak{q}}$.

To establish surjectivity of ϕ, we now have $\phi(\sigma) = \tau$. □

Since $D_{\mathfrak{q}}$ has cardinality ef and $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ has cardinality f, then the kernel of ϕ has cardinality e. This is another interesting group to think about.

Definition 6.18. The kernel $I_{\mathfrak{q}}$ of $\phi\colon D_{\mathfrak{q}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is called the **inertia group of** $\mathfrak{q}/\mathfrak{p}$.

There is a short exact sequence of groups

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \xrightarrow{\phi} \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \to 1.$$

This yields a chain of subgroups of G and the associated tower of fields, as below:

$$\begin{tikzcd}
1 \arrow[d, dash, "e"] & L \arrow[d, dash, "e"] & \mathfrak{q} \arrow[d, phantom, "\cup\!|"] \\
I_{\mathfrak{q}} \arrow[d, dash, "f"] & L^{I_{\mathfrak{q}}} \arrow[d, dash, "f"] & \mathfrak{q}_I := \mathfrak{q} \cap \mathcal{O}_{L^{I_{\mathfrak{q}}}} \arrow[d, phantom, "\cup\!|"] \\
D_{\mathfrak{q}} \arrow[d, dash, "g"] & L^{D_{\mathfrak{q}}} \arrow[d, dash, "g"] & \mathfrak{q}_D := \mathfrak{q} \cap \mathcal{O}_{L^{D_{\mathfrak{q}}}} \arrow[d, phantom, "\cup\!|"] \\
G & K = L^G & \mathfrak{p}
\end{tikzcd}$$

Definition 6.19. The field $L^{D_{\mathfrak{q}}}$ is called the **decomposition field at** $\mathfrak{q}$ and the field $L^{I_{\mathfrak{q}}}$ is called the **inertia field at** $\mathfrak{q}$.

We won't prove this next proposition, because it is quite tedious. The upshot is that in Galois extensions L/K, we can break up the splitting of a prime into cases that are simpler to study.

Proposition 6.20. *There are distinct splitting behaviors in these three extensions:*

- *In the extension $L^{D_{\mathfrak{q}}}/K$, the prime $\mathfrak{p}$ splits into g distinct primes ℓ_i such that $e(\ell_i/\mathfrak{p}) = 1$ and $f(\ell_i/\mathfrak{p}) = 1$ for all i; indeed one of the ℓ_i is $\mathfrak{q}_D$.*
- *In $L^{I_{\mathfrak{q}}}/L^{D_{\mathfrak{q}}}$, $\mathfrak{q}_D\mathcal{O}_{L^{I_{\mathfrak{q}}}} = \mathfrak{q}_I$ such that $e(\mathfrak{q}_I/\mathfrak{q}_D) = 1$ and $f(\mathfrak{q}_I/\mathfrak{q}_D) = f$.*
- *In $L/L^{I_{\mathfrak{q}}}$, $\mathfrak{q}_I\mathcal{O}_L = \mathfrak{q}^e$, where $e(\mathfrak{q}/\mathfrak{q}_I) = e$ and $f(\mathfrak{q}/\mathfrak{q}_I) = 1$.*

Fact 6.21. $L^{D_{\mathfrak{q}}}/L$ *is Galois, with Galois group* $D_{\mathfrak{q}}$.

6.3 Frobenius elements and quadratic reciprocity

Fix a Galois extension of number fields L/K with Galois group G. Fix $\mathfrak{p} \subseteq \mathcal{O}_K$ primes such that $\mathfrak{p}$ is unramified in L. Choose a prime ideal $\mathfrak{q} \subseteq \mathcal{O}_L$ such that $\mathfrak{q} \mid \mathfrak{p}$.

In this situation, $I_\mathfrak{q} = 1$ and $I_\mathfrak{q}$ has order $e_\mathfrak{p} = e(\mathfrak{q}/\mathfrak{p}) = 1$. So we have an isomorphism

$$D_\mathfrak{q} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}); \tag{6.1}$$

both are cyclic of order $f_\mathfrak{p}$.

Definition 6.22. When $\mathfrak{p}$ is unramified in L, the generator of the cyclic group $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is the **Frobenius automorphism**

$$\begin{tikzcd} \mathrm{Frob}_\mathfrak{q} \colon \mathbb{F}_\mathfrak{q} \arrow[r] & \mathbb{F}_\mathfrak{q} \\ x \arrow[r, mapsto] & x^{N(\mathfrak{p})} \end{tikzcd}$$

The corresponding element $\mathrm{Frob}_\mathfrak{q} \in D_\mathfrak{q}$ under the isomorphism (6.1) is called the **Frobenius element** of $\mathfrak{q}$ in G.

The Frobenius automorphism is the unique automorphism of L such that $\mathrm{Frob}_\mathfrak{q}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$ for all $x \in \mathcal{O}_L$.

Lemma 6.23. *For* $\tau \in G$*,*

$$\mathrm{Frob}_{\tau(\mathfrak{q})} = \tau \circ \mathrm{Frob}_\mathfrak{q} \circ \tau^{-1}.$$

Proof. We have

$$\mathrm{Frob}_\mathfrak{q}(\tau^{-1}x) \equiv \tau^{-1}(x)^{N(\mathfrak{p})} \pmod{\mathfrak{q}}.$$

So applying τ, we see that

$$\tau(\mathrm{Frob}_\mathfrak{q}(\tau^{-1}(x))) \equiv x^{N(\mathfrak{p})} \pmod{\tau(\mathfrak{q})}.$$

□

Definition 6.24. For $\mathfrak{p} \subseteq \mathcal{O}_K$ prime, we define $\mathrm{Frob}_\mathfrak{p}$ to be the conjugacy class in G containing $\mathrm{Frob}_\mathfrak{q}$ for any $\mathfrak{q}$ dividing $\mathfrak{p}$. This is well-defined by the previous lemma.

Example 6.25. Let $L = \mathbb{Q}(\sqrt{d})$ for $d \neq 1$ squarefree. This is a degree 2 extension of $\mathbb{Q}$ with Galois group $G \cong \{\pm 1\}$. Take a prime p not dividing $2d$; it is unramified in L. Hence, $\mathrm{Frob}_p \in G$ has order f_p. We ask whether or not it is the trivial element.

If $x^2 - d \pmod{p}$ splits, then $f_p = 1$, and if $x^2 - d \pmod{p}$ is irreducible, then $f_p = 2$. Since the group has order 2, this determines Frob_p.

Define the **Legendre symbol** $\left(\frac{d}{p}\right)$ to be the image of Frob_p under the isomorphism

$$\begin{tikzcd} \mathrm{Gal}(L/\mathbb{Q}) \arrow[r, "\cong"] & \{\pm 1\} \\ \mathrm{Frob}_p \arrow[r, mapsto] & \left(\frac{d}{p}\right) \end{tikzcd}$$

Definition 6.26. The **Legendre symbol** of an integer d relative to a prime p is

$$\left(\frac{d}{p}\right) := \begin{cases} +1 & \text{if } d \text{ is a non-zero square mod } p, \\ -1 & \text{if } d \text{ is not a square mod } p, \\ 0 & \text{if } d \equiv 0 \pmod{p}. \end{cases}$$

Fact 6.27.

(a) *The Legendre symbol is multiplicative:* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(b) *The Legendre symbol* $\left(\frac{a}{p}\right)$ *only depends on the residue of* a *mod* p.

(c) *The number of solutions to* $a^2 \equiv d \pmod{p}$ *with* $a \in \mathbb{Z}/p\mathbb{Z}$ *is* $1 + \left(\frac{d}{p}\right)$.

We may understand the multiplicative property of the Legendre symbol as a group homomorphism

$$\begin{tikzcd} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \arrow[r, "\simeq"] & \{\pm 1\} \\ a \arrow[r, mapsto] & \left(\frac{a}{p}\right) \end{tikzcd}$$

Important cases of the Legendre symbol to understand are $\left(\frac{-1}{p}\right)$ and $\left(\frac{\ell}{p}\right)$ for $\ell \neq p$ prime.

Theorem 6.28 (Quadratic reciprocity)**.** *Let* p *and* ℓ *be distinct odd primes. Then*

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

Equivalently,

$$\left(\frac{p}{\ell}\right) = \begin{cases} \left(\frac{\ell}{p}\right) & \textit{if } p \equiv 1 \textit{ or } \ell \equiv 1 \pmod{4}, \\ -\left(\frac{\ell}{p}\right) & \textit{if } p \equiv \ell \equiv 3 \pmod{4}. \end{cases}$$

Theorem 6.29.

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

(b) $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \textit{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \textit{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

Example 6.30. Is 3 a square modulo $p = 144169$? We compute the Legendre symbol using quadratic reciprocity: $144169 \equiv 1 \pmod 4$, so

$$\left(\frac{3}{144169}\right) = \left(\frac{144169}{3}\right).$$

Then we reduce $144169 \pmod 3$, so

$$\left(\frac{3}{144169}\right) = \left(\frac{144169}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

So yes, 3 is a square modulo 144169.

Example 6.31. Is 31 a square modulo 103? Well, $31 \equiv 103 \equiv 3 \mod 4$, so

$$\left(\frac{31}{103}\right) \equiv -\left(\frac{103}{31}\right) = -\left(\frac{10}{31}\right) = -\left(\frac{2}{31}\right)\left(\frac{5}{31}\right) = -(+1)\left(\frac{31}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

No, 31 is not a square modulo 103.

We can reformulate questions of splitting in quadratic number fields using the Legendre symbol. Fix $d \in \mathbb{Z}$ squarefree, and set $L = \mathbb{Q}(\sqrt{d})$. Take any p not dividing $2d$. Then p splits in L if and only if $x^2 - d \pmod p$ has 2 distinct roots, if and only if $\left(\frac{d}{p}\right) = +1$.

Example 6.32. For which $p \not| 10$ does p split in $\mathbb{Q}(\sqrt{5})$? By the above, p splits when $\left(\frac{5}{p}\right) = 1$. Using quadratic reciprocity,

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 4 \pmod 5, \\ -1 & \text{if } p \equiv 2 \text{ or } 3 \pmod 5. \end{cases}$$

So when $p \equiv \pm 1 \pmod 5$, then p splits in $\mathbb{Q}(\sqrt{5})$.

6.4 Proof of Quadratic Reciprocity

To prove Theorem 6.28, recall that for L/K a Galois extension of number fields with Galois group G, there is a unique $\mathrm{Frob}_{\mathfrak{q}} \in G$ for any nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$ unramified in L and prime $\mathfrak{q} \subseteq \mathcal{O}_L$ dividing $\mathfrak{p}$, such that

- $\mathrm{Frob}_{\mathfrak{q}}(\mathfrak{q}) = \mathfrak{q}$,
- $\mathrm{Frob}_{\mathfrak{q}}$ induces the automorphism $x \mapsto x^{N(\mathfrak{p})}$ on $\mathbb{F}_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q}$.

Equivalently, there is a unique $\mathrm{Frob}_{\mathfrak{q}} \in G$ such that $\mathrm{Frob}_{\mathfrak{q}}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$ for all $x \in \mathcal{O}_L$. This is the **Frobenius element of $\mathfrak{q}$ in** G from Definition 6.22.

Note that $\mathrm{Frob}_{\mathfrak{q}} \in G$ has order $f_{\mathfrak{p}} := f(\mathfrak{q}/\mathfrak{p})$. The conjugacy class of $\mathrm{Frob}_{\mathfrak{q}}$ in G is denoted by $\mathrm{Frob}_{\mathfrak{p}}$, and does not depend on $\mathfrak{q} \mid \mathfrak{p}$. If G is abelian, then $\mathrm{Frob}_{\mathfrak{p}} \in G$ is a well-defined element in G (all conjugacy classes are a single element).

Example 6.33 (Cyclotomic Fields)**.** Fix an integer $m \geq 2$. Let $L = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity. We have an isomorphism

$$\Psi\colon \operatorname{Gal}(L/\mathbb{Q}) \xrightarrow{\cong} \left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right)^{\times}$$

such that $\sigma(\zeta_m) = \zeta_m^{\Psi(\sigma)}$ for any $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$.

Take any $p \not| m$; it is unramified in L. Choose $\mathfrak{q} \mid \mathfrak{p}$ with $\mathfrak{q} \subseteq \mathcal{O}_L$. We have $\operatorname{Frob}_{\mathfrak{q}}(\zeta_m) \equiv \zeta_m^p \pmod{\mathfrak{q}}$. Since p does not divide m, $x^m - 1$ is separable mod p, and both ζ_m^p and $\operatorname{Frob}_{\mathfrak{q}}(\zeta_m)$ are roots of $x^m - 1$. But they are equivalent mod $\mathfrak{q}$, so in fact $\operatorname{Frob}_{\mathfrak{q}}(\zeta_m) = \zeta_m^p$. Since the Galois group is abelian, there is no harm in writing $\operatorname{Frob}_p = \operatorname{Frob}_{\mathfrak{q}}$. Then the isomorphism Ψ is given by

$$\begin{tikzcd}
\operatorname{Gal}\left({}^{\mathbb{Q}(\zeta_m)}/_{\mathbb{Q}}\right) \arrow[r, "\Psi", "\cong"'] & \left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right)^{\times} \\
\operatorname{Frob}_p \arrow[r, mapsto] & p \mod m
\end{tikzcd}$$

Example 6.34. Set $m = 4$ in the previous example. The 4-th root of unity is typically called i, and the cyclotomic field in question is $\mathbb{Q}(i)$. Pick any odd prime p.

$$\begin{tikzcd}
\operatorname{Gal}\left({}^{\mathbb{Q}(i)}/_{\mathbb{Q}}\right) \arrow[r, "\Psi", "\cong"'] & \left({}^{\mathbb{Z}}/_{4\mathbb{Z}}\right)^{\times} \\
\operatorname{Frob}_p \arrow[r, mapsto] & p \mod 4
\end{tikzcd}$$

Note that f_p is the order of Frob_p. An odd prime p splits in $\mathbb{Q}(i)$ if and only if $f_p = 1$ if and only if $\operatorname{Frob}_p = 1 \in \operatorname{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ if and only if $p \equiv 1 \pmod 4$.

Earlier, we saw that p splits in $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ if and only if $\left(\frac{-1}{p}\right) = 1$. Combining, we recover Theorem 6.29(a).

The previous example computed the splitting of p in a cyclotomic field in two different ways, and so proved Theorem 6.29(a). This is the strategy we will use to prove quadratic reciprocity (Theorem 6.28).

Proof of Theorem 6.28. Fix an odd prime ℓ and set $L = \mathbb{Q}(\zeta_\ell)$. Then

$$\operatorname{Gal}(L/\mathbb{Q}) \overset{\Psi}{\cong} (\mathbb{Z}/\ell\mathbb{Z})^{\times} = \mathbb{F}_\ell^{\times}.$$

Let $K/\mathbb{Q}$ be the subfield of L corresponding to $(\mathbb{F}_\ell^{\times})^2$, i.e. the subfield fixed by $\Psi^{-1}((\mathbb{F}_\ell^{\times})^2)$. K is a quadratic extension of $\mathbb{Q}$.

$$\begin{tikzcd}
L \arrow[d, dash] & 1 \arrow[d, dash] \\
K \arrow[d, dash, "2"] & (\mathbb{F}_\ell^{\times})^2 \arrow[d, dash, "2"] \\
\mathbb{Q} & \mathbb{F}_\ell^{\times}
\end{tikzcd}$$

What is K? Claim that $K = \mathbb{Q}(\sqrt{\ell^*})$ where

$$\ell^* = (-1)^{\frac{\ell-1}{2}}\ell = \begin{cases} \ell & \text{if } \ell \equiv 1 \pmod 4, \\ -\ell & \text{if } \ell \equiv 3 \pmod 4. \end{cases}$$

Why do we use ℓ^* instead of ℓ? Well, L is unramified at all primes $p \neq \ell$, and $\operatorname{disc} L = \pm\ell^b$ for some b. Hence, K is also unramified at $p \neq \ell$, so $\operatorname{disc} K = \pm\ell$. Then if $K = \mathbb{Q}(\sqrt{d})$ for d squarefree,

$$\operatorname{disc}(K) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \not\equiv 1 \pmod 4. \end{cases}$$

So we must choose d such that $d = \pm\ell$ and $d \equiv 1 \pmod 4$. Hence, $K = \mathbb{Q}(\sqrt{\ell^*})$.

Now take a prime p that does not divide 2ℓ. When does p split in K? We will compute this in two ways.

(i) p splits in K if and only if $\left(\frac{\ell^*}{p}\right) = 1$.

(ii) Choose a prime $\mathfrak{q}$ of $\mathcal{O}_L$ dividing p; this yields a prime $\mathfrak{p}$ of $\mathcal{O}_K$ dividing p. Consider $\operatorname{Frob}_{\mathfrak{q}} \in \operatorname{Gal}(L/\mathbb{Q})$. For $x \in \mathcal{O}_K$, $\operatorname{Frob}_{\mathfrak{q}}(x) - x^p \in \mathfrak{q}$. Therefore, $\operatorname{Frob}_{\mathfrak{q}}(x) - x^p \in \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$, since $\operatorname{Frob}_{\mathfrak{q}}|_K \in \operatorname{Gal}(K/\mathbb{Q})$. This shows that $\operatorname{Frob}_{\mathfrak{q}}|_K = \operatorname{Frob}_{\mathfrak{p}}$.

Then p splits in K if and only if $f_p = f(\mathfrak{p}/p) = 1$, if and only if $\operatorname{Frob}_{\mathfrak{p}} = 1 \in \operatorname{Gal}(K/\mathbb{Q})$. This is equivalent to the statement that $\operatorname{Frob}_{\mathfrak{q}}$ fixes K, since $\operatorname{Frob}_{\mathfrak{q}}|_K = \operatorname{Frob}_{\mathfrak{p}}$, which is true if and only if $\Psi(\operatorname{Frob}_{\mathfrak{q}}) \in (\mathbb{F}_\ell^\times)^2$.

In fact, it suffices to show that $\Psi(\operatorname{Frob}_p) \in (\mathbb{F}_\ell^\times)^2$ because the Galois group is abelian, so the conjugacy class Frob_p is just $\operatorname{Frob}_{\mathfrak{q}}$. From Example 6.33, $\Psi(\operatorname{Frob}_p) \in (\mathbb{F}_\ell^\times)^2$ if and only if $p \mod \ell \in (\mathbb{F}_\ell^\times)^2$, if and only if $\left(\frac{p}{\ell}\right) = 1$.

Combining the two approaches, $\left(\frac{\ell^*}{p}\right) = 1$ if and only if p splits in K if and only if $\left(\frac{p}{\ell}\right) = 1$. Hence,

$$\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right).$$

To get the same algebraic formulation of Theorem 6.28,

$$\begin{aligned}\left(\frac{\ell^*}{p}\right) &= \left(\frac{(-1)^{\ell-1}2\ell}{p}\right) \\ &= \left(\frac{-1}{p}\right)^{\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{\ell-1}{2}}\left(\frac{\ell}{p}\right)\end{aligned}$$

□

Remark 6.35. It remains to prove Theorem 6.29(b). To do so, notice that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$. In fact, $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. So there is an extension of fields

$$\begin{tikzcd}
\mathbb{Q}(\zeta_8) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

The difficulty here is $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$ is not a cyclic group; it has three subgroups if index 2. So you have to figure out that $\mathbb{Q}(\zeta 2)$ corresponds to the subgroup $\{\pm 1\} \subseteq (\mathbb{Z}/8\mathbb{Z})^\times$.

6.5 Chebotarev Density Theorem

Let L/K be a (finite) Galois extension of number fields. Set $G = \mathrm{Gal}(L/K)$. Take a non-zero prime $\mathfrak{p} \subseteq \mathcal{O}_K$ unramified in L. Choose a prime $\mathfrak{q} \subseteq \mathcal{O}_L$ dividing $\mathfrak{p}$. Then there exists a unique $\mathrm{Frob}_\mathfrak{q} \in G$ such that

$$\mathrm{Frob}_\mathfrak{q}(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{q}}$$

for all $x \in \mathcal{O}_L$. Recall that $\mathrm{Frob}_\mathfrak{q}$ has order $f_\mathfrak{p} = f(\mathfrak{q}/\mathfrak{p})$. Denote by $\mathrm{Frob}_\mathfrak{p}$ the conjugacy class of $\mathrm{Frob}_\mathfrak{q}$ in G.

Fix a separable monic $h \in \mathcal{O}_K[x]$ whose splitting field is L, i.e. $L = K(\alpha_1, \ldots, \alpha_n)$ when

$$h(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Note that the α_i are distinct. The Galois group of L/K acts on the set of roots of h by permutations; there is an injective homomorphism

$$\Psi \colon G \hookrightarrow \mathfrak{S}_n$$

into the symmetric group on n letters. For $\sigma \in G$,

$$\sigma(\alpha_i) = \alpha_{\Psi(\sigma)i}.$$

Take a prime $\mathfrak{p}$ not dividing $\mathrm{disc}(h)$. We have

$$h \equiv h_1 h_2 \cdots h_r \pmod{p}$$

for distinct $h_i \in \mathbb{F}_p[x]$ monic and irreducible. Set $f_i = \deg(h_i)$. Note that $\sum_i f_i = n$.

Theorem 6.36. *For a prime $\mathfrak{q}$ of $\mathcal{O}_L$ dividing $\mathfrak{p}$,*

$$\Psi(\mathrm{Frob}_{\mathfrak{q}}) \in \mathfrak{S}_n$$

is a permutation of cycle type $(f_1, f_2, \ldots, f_r)$.

Remark 6.37. This gives the conjugacy class of $\Psi(\mathrm{Frob}_{\mathfrak{q}})$ in $\mathfrak{S}_n$.

Proof sketch. Define $\overline{\alpha}_i = \alpha_i \pmod{\mathfrak{q}}$. We have a bijection

$$\begin{tikzcd}
\{\alpha_1, \ldots, \alpha_n\} \arrow[r, "\sim"] & \{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\} \\
\alpha \arrow[r, mapsto] & \alpha \pmod{\mathfrak{q}}
\end{tikzcd}$$

since $\mathfrak{p}$ does not divide disc(h), so h is separable modulo $\mathfrak{p}$.

The action of Frob$_{\mathfrak{q}}$ corresponds to the action of

$$\begin{tikzcd}
\mathrm{Frob}\colon \mathbb{F}_{\mathfrak{q}} \arrow[r] & \mathbb{F}_{\mathfrak{q}} \\
x \arrow[r, mapsto] & x^{N(\mathfrak{p})}
\end{tikzcd}$$

where Gal$(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) = \langle$Frob$\rangle$. Observe an orbit of Frob on $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\}$ corresponds to the roots of an $h_i \in \mathbb{F}_{\mathfrak{p}}[x]$. □

Example 6.38. Let $L/\mathbb{Q}$ be the splitting field of $h(x) = x^4 + x + 5$. Note that disc$(h) = 31973$ is prime. Let's factor $h \pmod{p}$ for some small primes p.

- For $p = 2, 3$, h is irreducible. Hence, $\Psi(\mathrm{Frob}_2), \Psi(\mathrm{Frob}_3) \in \mathfrak{S}_4$ are 4-cycles.
- $h \equiv x(x+1)(x^2+4x+1) \pmod{5}$, so $\Psi(\mathrm{Frob}_5) \in \mathcal{S}_4$ is a 2-cycle.
- $h \equiv (x+6)(x^3+x^2+x+2) \pmod{7}$, so $\Psi(\mathrm{Frob}_7) \in \mathcal{S}_4$ is a 3-cycle.

In fact, $\Psi\colon \mathrm{Gal}(L/\mathbb{Q}) \to \mathfrak{S}_4$ must be an isomorphism since $\mathfrak{S}_4$ has no proper subgroups containing elements of order 4 and 3.

Example 6.39. Let $L/\mathbb{Q}$ be the splitting field of $h(x) = x^4 + 8x + 12$. The discriminant of h is disc$(h) = 2^{12}3^4$. We can factor h modulo p for p not dividing 6. Order the sequence $f_1, \ldots, f_r$ to be increasing.

For $5 \leq p \leq 10,000,000$, the following table shows how many primes have a given sequence $f_1, \ldots, f_r$, and the ratio of how many primes in this range have correspond to the given cycle type $f_1, \ldots, f_r$.

$f_1, \ldots, f_r$	$1,1,1,1$	$1,1,2$	$1,3$	$2,2$	4
number of p	55338	0	443017	166222	0
ratio	0..083268 . . .	0	0.666615 . . .	0.2501116 . . .	0

Notice that only odd cycles occur in the table: the cycle type $(1,1,1,1)$ occurs roughly $\frac{1}{12}$ of the time, the cycle type $(1,3)$ occurs roughly $\frac{2}{3}$ of the time, and the cycle type $(2,2)$ occurs roughly $\frac{1}{4}$ of the time. This leads us to the conjecture that $\Psi(\mathrm{Gal}(L/\mathbb{Q})) \subseteq \mathfrak{A}_4$, the alternating group on four letters.

To see this claim, consider

$$2^{12}3^4 = \mathrm{disc}(h) = \prod_{1\le i<j\le 4} (\alpha_i - \alpha_j)^2$$

where h has roots $\alpha_1, \dots, \alpha_4$. We have

$$\delta := \prod_{1\le i<j\le 4} (\alpha_i - \alpha_j) = 2^6 3^2 \in \mathbb{Q}^\times.$$

For $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$,

$$\begin{aligned}\delta = \sigma(\delta) &= \prod_{1\le i<j\le 4} (\sigma(\alpha_i) - \sigma(\alpha_j)) \\ &= \prod_{1\le i<j\le 4} (\alpha_{\Psi(\sigma)i} - \alpha_{\Psi(\sigma)j}) \\ &= \mathrm{sgn}(\Psi(\sigma)) \prod_{1\le i<j\le 4} (\alpha_i - \alpha_j)\end{aligned}$$

where $\mathrm{sgn}\colon \mathfrak{S}_4 \to \{\pm 1\}$ is the usual sign of a permutation; the homomorphism sgn has kernel $\mathfrak{A}_4$. Cancelling the δ on both sides of the above equation gives $\mathrm{sgn}(\Psi(\sigma)) = 1$. Hence, $\Psi(\mathrm{Gal}(L/\mathbb{Q})) \subseteq \mathfrak{A}_4$.

In fact, since $\Psi(\mathrm{Gal}(L/\mathbb{Q}))$ contains elements of order 2 and 3, we must have $\Psi(\mathrm{Gal}(L/\mathbb{Q})) = \mathfrak{A}_4$. So $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{A}_4$.

Definition 6.40. For a set $\mathcal{S}$ of prime ideals of $\mathcal{O}_K$, its **density** is

$$\delta(\mathcal{S}) := \lim_{x\to+\infty} \frac{\#\{\mathfrak{p} \in \mathcal{S} \mid N(\mathfrak{p}) \le x\}}{\#\{\mathfrak{p} \mid N(\mathfrak{p}) \le x\}}$$

when this limit exists.

Theorem 6.41 (Chebotarev Density)**.** *Let L/K be a Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/K)$. For any $C \subseteq G$ stable under conjugation by G, let $\mathcal{S}_C$ be the set of $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathfrak{p}$ is unramified in L and $\mathrm{Frob}_\mathfrak{p} \subseteq C$.*

$$\mathcal{S}_C = \left\{\mathfrak{p} \subseteq \mathcal{O}_K \mid \mathfrak{p} \textit{ unramified in } L \textit{ and } \mathrm{Frob}_\mathfrak{p} \subseteq C\right\}.$$

Then the density of $\mathcal{S}_C$ is the ratio of the size of C to the size of G.

$$\delta(\mathcal{S}_C) = \frac{\#C}{\#G}.$$

Example 6.42. Fix $m \geq 2$ and $a \in \mathbb{Z}$ relatively prime to m.

$$\begin{tikzcd}
\Phi\colon \operatorname{Gal}\left({}^{\mathbb{Q}(\zeta_m)}/_{\mathbb{Q}}\right) \arrow[r, "\cong"] & \left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right)^{\times} \\
\operatorname{Frob}_{\mathfrak{p}} \arrow[r, mapsto] & \mathfrak{p} \pmod{m}
\end{tikzcd}$$

Let $C = \Phi^{-1}([a])$ and let $\mathcal{S}_C = \left\{p \colon p \not| \, m, \operatorname{Frob}_p \in \Phi^{-1}([a])\right\}$ Then by Chebotarev Density (Theorem 6.41),

$$\delta(\mathcal{S}_C) = \frac{1}{\#\left({}^{\mathbb{Z}}/_{m\mathbb{Z}}\right)^{\times}} = \frac{1}{\phi(m)}$$

where $\phi(m)$ is the Euler totient function. Notice $\mathcal{S}_C = \left\{p \mid p \equiv a \pmod{m}\right\}$, so the density of primes p congruent to a modulo m is $1/\phi(m)$. This is a theorem of Dirichlet.

Corollary 6.43 (Dirichlet)**.** *Let $m \geq 2$. The set of primes $p \equiv a \pmod{m}$ has density $\frac{1}{\phi(m)}$, where ϕ is the Euler totient function. In particular there are infinitely many such p.*

Example 6.44. Let L/K be a Galois extension with Galois group G. Let $\mathcal{S}$ be the set of primes $\mathfrak{p} \subseteq \mathcal{O}_K$ that split completely in L, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ with $e(\mathfrak{q}_i/\mathfrak{p}) = 1$ and $f(\mathfrak{q}_i/\mathfrak{p}) = 1$ for all i. In this case, $r = [L \colon K]$. By Chebotarev Density (Theorem 6.41) with $C = \{1\}$,

$$\delta(\mathcal{S}) = \frac{1}{\#G} = \frac{1}{[L \colon K]}.$$

Proposition 6.45. *Take L and M Galois extensions of K. Write $\mathcal{S}_{L/K}$ for the set of primes of K that split completely in L, and likewise write $\mathcal{S}_{M/K}$ for the set of primes of K that split completely in M. Then $L \subseteq M$ if and only if $\mathcal{S}_{L/K} \supseteq \mathcal{S}_{M/K}$.*

Proof sketch. If $L \subseteq M$, then $\mathcal{S}_{L/K} \supseteq \mathcal{S}_{M/K}$.

Conversely, consider

$$\begin{tikzcd}
\operatorname{Gal}(LM/K) \arrow[r, hook] & \operatorname{Gal}(L/K) \times \operatorname{Gal}(M/K) \\
\sigma \arrow[r, mapsto] & (\sigma|_L, \sigma|_M)
\end{tikzcd}$$

One can check that $\operatorname{Frob}_{\mathfrak{p}} \mapsto \operatorname{Frob}_{\mathfrak{p}} \times \operatorname{Frob}_{\mathfrak{p}}$. So $\mathcal{S}_{LM/K} = \mathcal{S}_{L/K} \cap \mathcal{S}_{M/K}$. By assumption, $S_{L/K} \supseteq \mathcal{S}_{M/K}$, so $\mathcal{S}_{LM/K} = \mathcal{S}_{M/K}$. So

$$\frac{1}{[LM \colon K]} = \delta(\mathcal{S}_{LM/K}) = \delta(\mathcal{S}_{M/K}) = \frac{1}{[M \colon K]}.$$

Therefore, $[LM \colon K] = [M \colon K]$, so $LM = M \implies L \subseteq M$. □

7 Dedekind Zeta Functions

Recall the basics:

- K is a number field;
- n is the degree of K;
- r is the number of real embeddings $K \hookrightarrow \mathbb{R}$, denoted $\sigma_1, \dots, \sigma_r$;
- s is the number of conjugate pairs of complex embeddings $\sigma \colon K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$, denoted $\sigma_{r+1}, \dots, \sigma_{r+s}$ and $\overline{\sigma}_{r+1}, \dots, \overline{\sigma}_{r+s}$;
- $\operatorname{disc}(K)$ is the discriminant of K;
- $C\ell_K$ is the class number of K;
- $\omega_k = \#\mu_K$ with μ_K the group of roots of unity in K;
- $h_k = \# C\ell_K$ is the **class number** of K.

Definition 7.1 (Repeat of Definition 5.12)**.** If $\mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$, and ϕ is the function

$$\begin{aligned} \mathcal{O}_K^\times &\xrightarrow{\phi} V := \left\{ x \in \mathbb{R}^{r+s} \;\middle|\; \sum_{i=1}^{r+s} x_i = 0 \right\} \\ \alpha &\longmapsto \big(e_i \log|\sigma_i(\alpha)|\big) \end{aligned}$$

where

$$e_i = \begin{cases} 1 & 1 \le i \le r, \\ 2 & r+1 \le i \le r+s, \end{cases}$$

the **regulator of** K is the quantity

$$\operatorname{Reg}_K := \frac{1}{\sqrt{r+s}} \operatorname{covol}(\phi(\mathcal{O}_K^\times))$$

Question 7.2. How do you compute $C\ell_K$ and $\mathcal{O}_K^\times$?

Recall the class group is a finite abelian group, and the group of units of $\mathcal{O}_K$ is a finitely generated abelian group.

Here is an idea, assuming that we can numerically compute $h_K \cdot \operatorname{Reg}_K \in \mathbb{R}_{>0}$. By numerically compute, we mean compute an arbitrary number of digits of this real number.

(1) Compute the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ with
$$N(\mathfrak{p}_i) \le \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|}.$$
By Minkowski's theorem, these primes generate $C\ell_K$.

(2) Find many factorizations
$$\alpha_i \mathcal{O}_K = \mathfrak{p}_1^{a_{i,1}} \cdots \mathfrak{p}_m^{a_{i,m}}$$
with $1 \le i \le M$ and $\alpha_i \in K$.

(3) Define a "guess" for $C\ell_K$
$$C := \mathbb{Z}^m \big/ \langle (a_{i,1}, \ldots, a_{i,m}) \mid 1 \le i \le M \rangle.$$
There is a surjective group homomorphism $C \twoheadrightarrow C\ell_K$ given by $e_i \mapsto [\mathfrak{p}_i]$. This will be an isomorphism if we have found "enough" factorizations. Note that
$$(a_{i,1}, \ldots, a_{i,m}) \mapsto [\mathfrak{p}_1]^{a_{i,1}} \cdots [\mathfrak{p}_m]^{a_{i,m}} = [\alpha \mathcal{O}_K] = 1.$$

(4) Take any $(b_1, \ldots, b_M) \in \mathbb{Z}^M$ such that
$$\sum_{i=1}^{M} a_{i,j} b_i = 0$$
for all $1 \le j \le M$. Then
$$\prod_{i=1}^{M} \alpha_i^{b_i} \mathcal{O}_K = \mathcal{O}_K.$$
In that case, we have produced a unit $\prod_{i=1}^{M} \alpha_i^{b_i} \in \mathcal{O}_K^\times$.

Let $U \subseteq \mathcal{O}_K^\times$ be the group generated by these units and μ_K. We will have $U = \mathcal{O}_K^\times$ if we have taken "enough" factorizations in step (2). U is our guess for $\mathcal{O}_K^\times$.

(5) When are we done? Assume M is sufficiently large that C is finite and U has rank $r + s - 1 = \operatorname{rank}(\mathcal{O}_K^\times)$. Consider the positive integers $\#C/\#C\ell_K$ and
$$\frac{\operatorname{covol}(\phi(U))}{\operatorname{covol}(\phi(\mathcal{O}_K^\times))} = [\phi(\mathcal{O}_K^\times) \colon \phi(U)] = [\mathcal{O}_K^\times \colon U].$$
We have
$$\#C \cdot \frac{1}{\sqrt{r+s}} \operatorname{covol}(\phi(U)) = \frac{\#C}{\#C\ell_K} [\mathcal{O}_K^\times \colon U] \cdot h_K \operatorname{Reg}_K .$$

Both the quantities $h_K \operatorname{Reg}_K$ and $\#C\frac{1}{\sqrt{r+s}}\operatorname{covol}(\phi(U))$ can be computed numerically. Hence, we approximate the integer

$$\frac{\#C}{\#C\ell_K}[\mathcal{O}_K^\times : U]$$

by a real number. Rounding gets the actual value. We continue to add more factorizations until this value is 1, in which case $C \cong C\ell_K$ and $U = \mathcal{O}_K^\times$.

Note that this process is not yet algorithmic – step (2) is too vague.

7.1 Counting Ideals

The process above is nice, but it assumes we can numerically compute $h_K \operatorname{Reg}_K$. We will approach $h_K \operatorname{Reg}_K$ by counting ideals.

Definition 7.3. Let $x \in \mathbb{R}$. Define

$$\mathcal{A}(x) := \#\{I \subseteq \mathcal{O}_K \mid N(I) \leq x\}.$$

Note that $\mathcal{A}(x)$ is finite, because there are only finitely many ideals of a given norm, and norms are integers.

How does $\mathcal{A}(x)$ grow as $x \to +\infty$?

Theorem 7.4. *There is a constant $\kappa > 0$ such that $\mathcal{A}(x) \sim \kappa \cdot x$ as $x \to +\infty$, where*

$$\kappa = \frac{2^r(2\pi)^s h_K \operatorname{Reg}_K}{\omega_K\sqrt{|\operatorname{disc}(K)|}}.$$

This theorem states that the number of ideals of norm at most x grows linearly with x. More interestingly, all of the invariants of a number field appear at the same time in the constant κ.

Example 7.5. Consider $K = \mathbb{Q}$. In this case, $\mathcal{A}(x) = \#\{n \in \mathbb{Z} \mid n \leq x\}$, which grows approximately as $1 \cdot x$. Here, we have $r = 1$, $s = 0$, $h_\mathbb{Q} = 1$, $\operatorname{Reg}_\mathbb{Q} = 1$, $\omega_\mathbb{Q} = 2$ and $\operatorname{disc}(\mathbb{Q}) = 1$. Hence, $\kappa = 1$.

Remark 7.6. This gives a numerical approach to estimate $h_K \operatorname{Reg}_K$.

Proof sketch of Theorem 7.4. Fix $C \in C\ell_K$ and define

$$\mathcal{A}(x, C) = \#\left\{I \subseteq \mathcal{O}_K \,\middle|\, N(I) \leq x \text{ and } [I] = C\right\}.$$

Note that

$$\sum_{C \in C\ell_K} \mathcal{A}(x, C) = \mathcal{A}(x).$$

It suffices to prove

$$\mathcal{A}(x, C) \sim \frac{2^r(2\pi)^s \operatorname{Reg}_K}{\omega_K \sqrt{|\operatorname{disc}(K)|}} \cdot x.$$

We will give a proof when $K/\mathbb{Q}$ is quadratic. The general case involves a lot more bookkeeping and is no more enlightening.

Fix an ideal J with $[J] = C^{-1}$.

For I with $[I] = C$ and $N(I) \leq x$, we have $IJ = \langle \alpha \rangle$ for some $\alpha \in J$. Therefore,

$$|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha\mathcal{O}_K) = N(IJ) = N(I)N(J) \leq xN(J).$$

Conversely, take any nonzero $\alpha \in J$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq xN(J)$. Then $\langle \alpha \rangle \subseteq J$ implies that $I := \alpha J^{-1}$ is an ideal with

$$N(I) = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(J)} \leq \frac{xN(J)}{N(J)} = x.$$

Therefore,

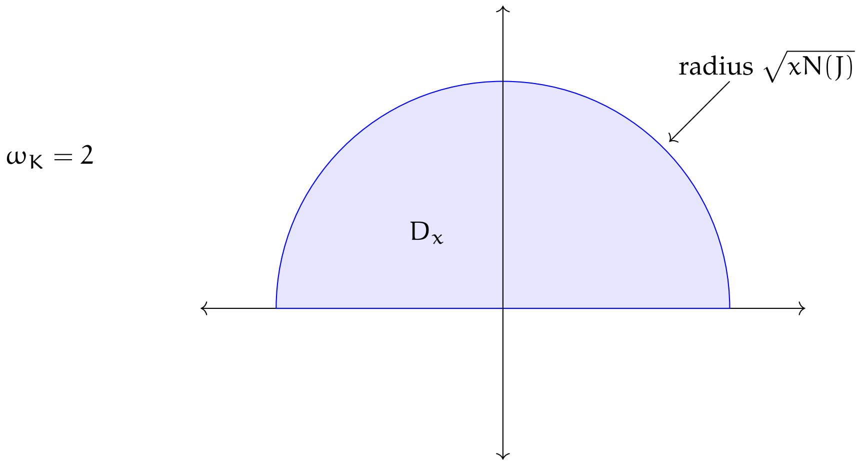
$$\mathcal{A}(x, C) = \#\left\{ \langle \alpha \rangle \;\middle|\; \alpha \in J \setminus \{0\} \text{ and } N_{K/\mathbb{Q}}(\alpha) \leq xN(J) \right\}.$$

We want to count $\alpha \in J$ (back to lattices) but $\langle u\alpha \rangle = \langle \alpha \rangle$ for $u \in \mathcal{O}_K^\times$.

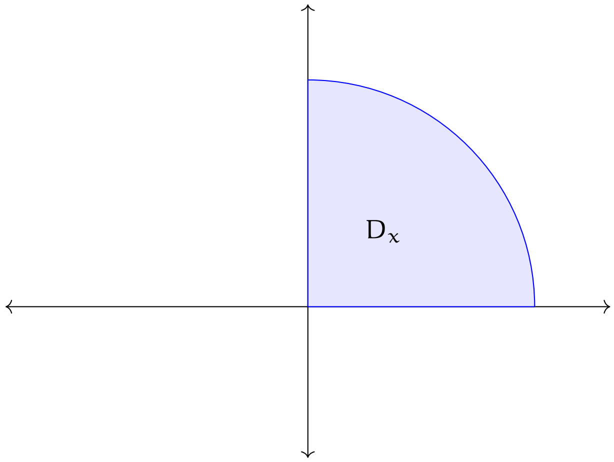
Case (1): Let's assume $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ is quadratic imaginary. Here, $\mathcal{O}_K^\times = \mu_K$ and $\mathcal{A}(x, C) = \#(J \cap D_x)$ where

$$D_x = \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \operatorname{Arg}(z) < \frac{2\pi}{\omega_K} \text{ and } z\overline{z} \leq xN(J) \right\}.$$

Note that any nonzero principal ideal of $\mathcal{O}_K$ has a unique generator α with $0 \leq \operatorname{Arg}(\alpha) < \frac{2\pi}{\omega_K}$ and $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} > 0$.



$\omega_K = 4$



As $x \to \infty$,

$$A(x, C) \sim \frac{\text{Area}(D_x)}{\text{covol}(J)} = \frac{1}{2}\frac{\pi\left(\sqrt{xN(J)}\right)^2/\omega_K}{N(J)\sqrt{|\text{disc}(K)|}} = \frac{2\pi}{\omega_K\sqrt{|\text{disc}\,K|}}\cdot x$$

Case (2): If $K \subseteq \mathbb{R}$ is real quadratic, then let $\tau\colon K \hookrightarrow \mathbb{R}$ be the non-identity embedding. We know $\mathcal{O}_K^\times = \pm\langle\varepsilon\rangle$ with $\varepsilon > 1$ the "fundamental unit." Consider the composite

$$\begin{tikzcd}
\phi\colon K^\times \arrow[r, hook, "\mathrm{id}\times\tau"] & \mathbb{R}^\times \times \mathbb{R}^\times \arrow[r] & \mathbb{R}^2 \\
& (a, b) \arrow[r, mapsto] & (\log|a|, \log|b|)
\end{tikzcd}$$

We have

$$\phi(\mathcal{O}_K^\times) = \mathbb{Z}\cdot(\log\varepsilon, -\log\varepsilon).$$

Note that $(1, 1)$ and $(\log\varepsilon, -\log\varepsilon)$ are linearly independent over $\mathbb{R}$.

$$(\log|a|, \log|b|) = \frac{\log|a| + \log|b|}{2}(1, 1) + \frac{\log|a| - \log|b|}{2\log\varepsilon}(\log\varepsilon, -\log\varepsilon).$$

For a nonzero $\alpha \in \mathcal{O}_K$, there is a unique $n \in \mathbb{Z}$ such that $\phi(\alpha\varepsilon^n) = c_1(1, 1) + c_2(\log\varepsilon, -\log\varepsilon)$ with $c_i \in \mathbb{R}$ and $0 \le c_2 < 1$. So

$$\mathcal{A}(x, C) = \#J \cap D_x,$$

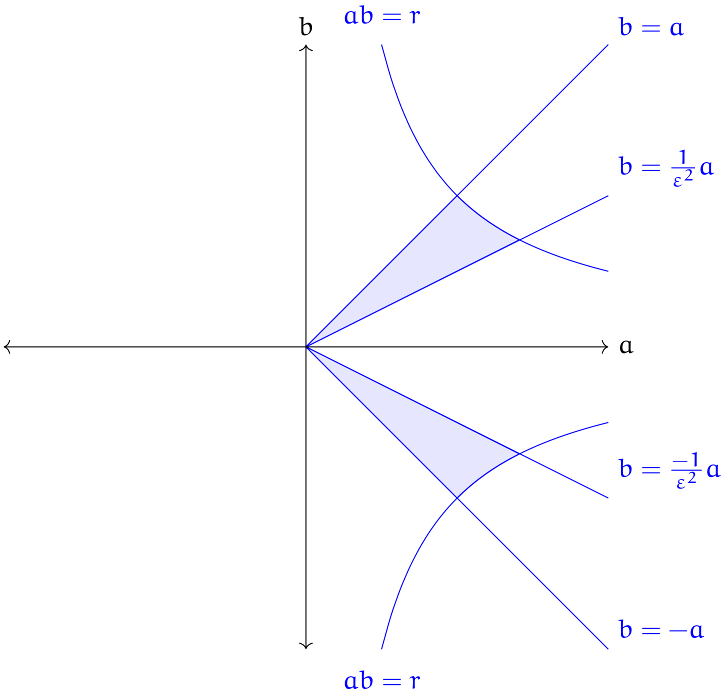
where

$$D_x = \left\{(a, b) \in \mathbb{R}^2 \;\middle|\; |ab| < xN(J) \text{ and } 0 \le \frac{\log|a| - \log|b|}{2\log\varepsilon} < 1 \text{ and } a > 0, b \neq 0\right\}.$$

Or equivalently, if we set $r = xN(J)$

$$D_x = \left\{(a, b) \in \mathbb{R}^2 \;\middle|\; a > 0, b \neq 0, |ab| \le r, 1 \le \frac{a}{|b|} < \varepsilon^2\right\}.$$

D_x is the region shaded in blue below, bounded by the indicated curves.


b
$ab = r$
$b = a$
$b = \frac{1}{\varepsilon^2} a$
a
$b = \frac{-1}{\varepsilon^2} a$
$b = -a$
$ab = r$

We can integrate this region to find

$$\mathcal{A}(x, C) \sim \frac{\text{Area}(D_x)}{\text{covol}(J)} = \frac{2 \log \varepsilon}{\sqrt{|\operatorname{disc} K|}} \cdot x,$$

as desired. □

7.2 Dirichlet Series and L-functions

We saw in the last section that for a number field $K/\mathbb{Q}$, the number of ideals $\mathcal{A}(x)$ of norm $N(I) \leq x$ is asymptotic to $\kappa \cdot x$, where

$$\kappa = \frac{2^r (2\pi)^s h_K \operatorname{Reg}_K}{\omega_K \sqrt{|\operatorname{disc} K|}} > 0.$$

This suggests a way to estimate $h_K \operatorname{Reg}_K$. In fact, we will see that

$$A(x) = \kappa \cdot x + O\left(x^{1 - 1/[K:\mathbb{Q}]}\right). \tag{7.1}$$

To do that, we need to first talk about Dedekind zeta functions and Dirichlet series.

Define:

$$\begin{aligned} D_x &= \left\{(a,b) \in \mathbb{R}^2 \mid \sqrt{a^2+b^2} \leq x\right\}, \\ N_x &= \#\left(\mathbb{Z}^2 \cap D_x\right). \end{aligned}$$

Notice that

$$\pi(x-1)^2 = \operatorname{Area}(D_{x-1}) \leq N_x \leq \operatorname{Area}(D_{x+1}) = \pi(x+1)^2,$$

and therefore $N_x = \pi x^2 + O(x)$.

Definition 7.7. The **Dedekind zeta function** of K is

$$\zeta_K(x) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where $a_n = \#\{I \subseteq \mathcal{O}_K \mid N(I) = n\}$.

Lemma 7.8 (Partial Summation)**.** *Let $a_1, a_2, \ldots$ be a sequence of complex numbers, and let $z \colon [1,\infty) \to \mathbb{C}$ be a C^1-function. Define*

$$A(x) := \sum_{n \leq x} a_n.$$

Then

$$\sum_{n \leq x} a_n z(n) = A(x)z(x) - \int_1^x A(t)z'(t)\, dt.$$

Proof sketch. Take $x \geq 1$ to be an integer. Then

$$\begin{aligned} \int_1^x A(t)z'(t)\, dt &= \sum_{n \leq x-1} \int_n^{n+1} A(t)z'(t)\, dt \\ &= \sum_{n \leq x-1} A(n) \int_n^{n+1} z'(t)\, dt \\ &= \sum_{n \leq x-1} A(n)(z(n+1) - z(n)) \end{aligned}$$

□

Lemma 7.9. *Fix a formal Dirichlet series*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

with $a_n \in \mathbb{C}$. Set

$$A(x) = \sum_{n \leq x} a_n$$

and suppose that $A(x) = \mathcal{O}(x^{\delta})$ *for some* $\delta > 0$*. Then*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

converges absolutely for $\mathrm{Re}(s) > \delta$ *and equals*

$$s \int_1^{\infty} \frac{A(t)}{t^{s+1}}\, dt.$$

In particular, it is holomorphic for $\mathrm{Re}(s) > \delta$*.*

Proof. Take $z(n) = n^{-s}$ with $z(x) = x^{-s} = e^{-s\log(x)}$; $z'(x) = e^{-s\log(x)}\left(\frac{-s}{x}\right) = \frac{-s}{x^{s+1}}$. Then by partial summation,

$$\sum_{n \le x} a_n n^{-s} = \frac{A(x)}{x^s} + s\int_1^x \frac{A(t)}{t^{s+1}}$$

The first term goes to zero as $x \to +\infty$, and the second term has order

$$O\left(\int_1^x \frac{1}{t^{\mathrm{Re}(s)-\delta+1}}\, dt\right) = O(1)$$

if $\mathrm{Re}(s) > \delta$. □

Example 7.10. Consider the Riemann zeta function

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

We have

$$\begin{aligned}\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= s\int_1^{\infty} \frac{\lfloor t \rfloor}{t^{s+1}}\, dt \\ &= s\int_1^{\infty} \frac{t}{t^{s+1}}\, dt + s\int_1^{\infty} \frac{\lfloor t \rfloor - t}{t^{s+1}}\, dt\end{aligned}$$

The right hand integral converges for $\mathrm{Re}(s) > 0$, since $|\lfloor t \rfloor - t| \le 1$. Hence, we arrive at

$$\zeta(s) = \frac{1}{s-1} + 1 + s\int_1^{\infty} \frac{\lfloor t \lfloor - t}{t^{s+1}} dt.$$

Therefore, $\zeta(s)$ has a unique analytic continuation to $\mathrm{Re}(s) > 0$ except with a simple pole at $s = 1$ with residue 1.

Remark 7.11. In fact, $\zeta(s)$ (and $\zeta_K(s)$) extends to a holomorphic function on $\mathbb{C} \setminus \{1\}$.

Example 7.12. Consider

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^{-s}}.$$

Since

$$A(x) = \sum_{n \leq x} a_n \sim \kappa \cdot x,$$

this implies that $\zeta_K(s)$ converges absolutely when $\mathrm{Re}(s) > 1$.

Now consider

$$\zeta_K(s) - \kappa\zeta(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

with $b_n = a_n - \kappa$. Taking partial sums of the b_n,

$$B(x) := \sum_{n \leq x} b_n = \sum_{n \leq x} a_n - \kappa\lfloor x \rfloor = A(x) - \kappa x + O(1) = O\left(x^{1-1/[K:\mathbb{Q}]}\right).$$

This proves Eq. (7.1). Moreover, it shows that

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

converges for $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$, and therefore $\zeta_K(s)$ has an analytic continuation to $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ except at $s = 1$. Finally, the function

$$\zeta_K(s) - \frac{\kappa}{s-1}$$

has analytic continuation to $\mathrm{Re}(s) > 0$.

Theorem 7.13 (Analytic class number formula)**.**

$$\mathrm{Res}_{s=1}\, \zeta_K(s) = \lim_{s \to 1} (s-1)\zeta_K(s) = \kappa$$

This gives us a way to find the number κ, which in turn allows us to find the value of $h_K \,\mathrm{Reg}_K$ to compute $C\ell_K$ and $\mathcal{O}_K^\times$.

Theorem 7.14 (Euler Product)**.** *For* $\mathrm{Re}(s) > 1$*, we have*

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \text{prime}}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

Proof. Fix a nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$. Then

$$\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{i=0}^{\infty} \frac{1}{N(\mathfrak{p})^{is}} = \sum_{i=0}^{\infty} \frac{1}{N(\mathfrak{p}^i)^s}$$

So

$$\begin{aligned}\prod_{\mathfrak{p}, N(\mathfrak{p}) \leq x} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} &= \prod_{\mathfrak{p}, N(\mathfrak{p}) \leq x} \sum_{i=0}^{\infty} \frac{1}{N(\mathfrak{p}^i)^s} \\ &= \sum_{I \in \mathcal{I}} \frac{1}{N(I)^s}\end{aligned}$$

where $\mathcal{I}$ is the set of ideals $I \subseteq \mathcal{O}_K$ whose prime factors $\mathfrak{p}$ satisfy $N(\mathfrak{p}) \leq x$; the equality uses unique factorization of ideals of $\mathcal{O}_K$.

Now

$$\left| \zeta_K(s) - \prod_{\mathfrak{p}, N(\mathfrak{p}) \leq x} \sum_{i=0}^{\infty} \frac{1}{N(\mathfrak{p}^i)^s} \right| = \left| \sum_{I \notin \mathcal{I}} \frac{1}{N(I)^s} \right| \leq \sum_{N(I) > x} \frac{1}{N(I)^{\mathrm{Re}(s)}}.$$

This right-hand term converges to zero since $\zeta_K(\mathrm{Re}(s))$ converges. Hence, the Euler product formula holds. □

Now let's focus on $K/\mathbb{Q}$ quadratic. Take a prime p

$$\prod_{\mathfrak{p} | p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \begin{cases} \left(1 - \frac{1}{p^s}\right)^{-1} & \text{if } p\mathcal{O}_K = \mathfrak{p}^2, \\ \left(1 - \frac{1}{p^s}\right)^{-2} & \text{if } p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \\ \left(1 - \frac{1}{p^{2s}}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 + \frac{1}{p^s}\right)^{-1} & \text{if } p\mathcal{O}_K = \mathfrak{p}. \end{cases}$$

Definition 7.15. Define

$$L(s, x) := \frac{\zeta_K(s)}{\zeta(s)} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

where

$$\chi(p) = \begin{cases} 0 & \text{if } p \text{ ramifies in } K, \\ 1 & \text{if } p \text{ splits in } K, \\ -1 & \text{if } p \text{ is inert in } K. \end{cases}$$

Extending χ to a function $\chi\colon \mathbb{N} \to \{-1, 0, +1\}$ multiplicatively, we have the L**-series**

$$L(s, x) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Note that

$$L(1,\chi) = \frac{2^{r_1}(2\pi)^{r_2} h_K \operatorname{Reg}_K}{\omega_K \sqrt{|\operatorname{disc}(K)|}},$$

where r_1 is the number of real embeddings $K \hookrightarrow \mathbb{R}$ and r_2 is the number of conjugate pairs of complex embeddings $K \hookrightarrow \mathbb{C}$. In particular, we have

$$h_K \operatorname{Reg}_K = \frac{\omega_K \sqrt{|\operatorname{disc}(K)|}}{2^{r_1}(2\pi)^{r_2}} L(1,\chi).$$

Dirichlet gives some closed forms for $h_K = \# C\ell_K$:

Theorem 7.16 (Dirichlet)**.** *Let* ε *be the fundamental unit of* $\mathcal{O}_K^\times$*.*

$$h_k = \begin{cases} \dfrac{\omega_K}{2|\operatorname{disc}(K)|}\left| \displaystyle\sum_{\substack{1 \le j \le |\operatorname{disc}(K)|/2 \\ (j,\operatorname{disc}(K))=1}} \chi(j) j \right| & \textit{if } \operatorname{disc}(K) < 0, \\ \dfrac{1}{\log \varepsilon}\left| \displaystyle\sum_{\substack{1 \le j \le |\operatorname{disc}(K)|/2 \\ (j,\operatorname{disc}(K))=1}} \chi(j) \log\left|\sin\left(\tfrac{\pi j}{|\operatorname{disc}(K)|}\right)\right| \right| & \textit{if } \operatorname{disc}(K) > 0. \end{cases}$$

Example 7.17. Let $K = \mathbb{Q}(\sqrt{5})$. We have $\operatorname{disc}(K) = 5$ and $h_K = 1$. Then

$$\log \varepsilon = |\log(\sin(\tfrac{\pi}{5})) - \log(\sin(\tfrac{2\pi}{5}))| = \log\left(\frac{\sin(\pi/5)}{\sin(2\pi/5)}\right).$$

Therefore, the fundamental unit is

$$\varepsilon = \frac{\sin(\pi/5)}{\sin(2\pi/5)}.$$

Example 7.18. Let $K = \mathbb{Q}(\sqrt{-5})$. We may check that the formula gives $h_K = 2$.

There are also useful non-closed forms.

Theorem 7.19. *Set* $d = \operatorname{disc}(K)$*. If* $d < 0$*, then*

$$h_K = \sum_{n=1}^{\infty} \chi(n)\left(\operatorname{erfc}\left(n\tfrac{\sqrt{\pi}}{|d|}\right) + \frac{\sqrt{d}}{\pi n} e^{-\pi n^2/|d|}\right).$$

If $d > 0$*, then*

$$h_K \log \varepsilon = \frac{1}{2}\sum_{n=1}^{\infty} \chi(n)\left(\frac{\sqrt{|d|}}{n}\operatorname{erfc}\left(n\tfrac{\sqrt{\pi}}{|d|}\right) + E_1\left(\tfrac{\pi n^2}{|d|}\right)\right)$$

where

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2}\, dt$$

$$E_1(x) = \int_x^\infty e^{-t} \frac{dt}{t}$$

Example 7.20. $K = \mathbb{Q}(\sqrt{94})$. Then $\operatorname{disc}(K) = 4 \cdot 94$. One can check that $h_K = 1$. We find that

$$\log \varepsilon = h_K \log \varepsilon = 15.271002103\ldots$$

Therefore, $\varepsilon = 4286589.9999997667\ldots$. What is the minimal polynomial of ε?

If $N_{K/\mathbb{Q}}(\varepsilon) = 1$, then it's

$$(x-\varepsilon)(x-\varepsilon^{-1}) = x^2 - (4286590.000\ldots)x + 1.$$

If $N_{K/\mathbb{Q}}(\varepsilon) = -1$, then

$$(x-\varepsilon)(x+\varepsilon^{-1}) = x^2 - (4286589.9999953\ldots)x + 1.$$

Note that the latter is not in $\mathbb{Z}[x]$, so it must be the former.

8 Local Fields

Definition 8.1. A **topological field** is a field K with a topology such that $+, -, \times \colon K \to K$ and $(-)^{-1} \colon K^\times \to K^\times$ are continuous functions.

Example 8.2. The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are topological fields with the usual topology.

Definition 8.3. A **local field** is a topological field with a non-discrete topology that is **locally compact**, i.e. every point has a neighborhood whose closure is compact.

8.1 $\mathfrak{p}$-adic fields

Let K be a number field. The fractional ideal generated by any $x \in K^\times$ factors uniquely:

$$x\mathcal{O}_K = \prod_{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K} \mathfrak{p}^{\nu_\mathfrak{p}(x)}$$

with $\nu_\mathfrak{p}(x) \in \mathbb{Z}$.

Fix $\mathfrak{p}$. Set $\nu_\mathfrak{p}(0) = +\infty$. Define

$$|-|_\mathfrak{p} \colon K \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$$

by $|x|_\mathfrak{p} = N(\mathfrak{p})^{-\nu_\mathfrak{p}(x)}$. This is an **absolute value** function:

- $|x|_\mathfrak{p} = 0 \iff x = 0$,
- $|xy|_\mathfrak{p} = |x|_\mathfrak{p}|y|_\mathfrak{p}$,
- $|x+y|_\mathfrak{p} \leq |x|_\mathfrak{p} + |y|_\mathfrak{p}$.

In fact, we have a strong triangle inequality:

$$|x+y|_\mathfrak{p} \leq \max\{|x|_\mathfrak{p}, |y|_\mathfrak{p}\}.$$

This norm $|-|_\mathfrak{p}$ gives a topology on K via the metric $d(x,y) = |x-y|_\mathfrak{p}$.

Definition 8.4. Given a number field K and a nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$, the topology induced by the norm $|-|_\mathfrak{p}$ is called the **$\mathfrak{p}$-adic topology**.

Remark 8.5. For $K = \mathbb{Q}$, this topology is very different from the usual one, and very weird at first. For example:

- all “triangles” are isosceles;
- if the intersection of two open balls $B(a,\varepsilon) = \{x \in K \mid |x-a|_\mathfrak{p} < \varepsilon\}$ is nonempty then one contains the other.

Given the topological field K under the metric topology given by the norm $|-|_\mathfrak{p}$, we may complete: let $\widehat{K}$ be the completion of K, i.e. the set of Cauchy sequences $\{a_n\}_{n\in\mathbb{N}}$ in K up to equivalence. If $\alpha \in \widehat{K}$ is the equivalence class of the Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$, then

$$|\alpha|_\mathfrak{p} = \lim_{n\to\infty} |a_n|_\mathfrak{p}.$$

Definition 8.6. Given a number field K and a nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$, we denote by $K_\mathfrak{p}$ the completion of K with respect to $|-|_\mathfrak{p}$. This is the **$\mathfrak{p}$-adic completion of** K.

Fact 8.7. $\sum_{n=1}^{\infty} a_n$ *converges if and only if* $a_n \to 0$ *as* $n \to \infty$.

Proof idea.

$$\left|\sum_{n=m}^{N} a_n\right| \leq \max\left\{|a_n| \;\middle|\; m \leq n \leq N\right\}.$$

□

Example 8.8. Consider the 2-adic topology on $\mathbb{Q}$. In the field $\mathbb{Q}_2$, the sequence

$$a_n = 1 + 2 + 2^2 + \ldots + 2^n = \frac{2^{n+1}-1}{2-1} = 2^{n+1} - 1$$

converges to -1 as $n \to \infty$.

Example 8.9. For $n \geq 0$, consider the rational number

$$\binom{1/2}{n} = \frac{1/2\,(1/2-1)\,(1/2-2)\cdots(1/2-n+1)}{n!}.$$

Claim that the denominator of this is a power of 2. To see this, take any odd prime p. It suffices to show that

$$\left|\binom{1/2}{n}\right|_p \leq 1 \iff \nu_{\mathfrak{p}}\left(\binom{1/2}{n}\right) \geq 0.$$

To that end, define $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ by

$$f(x) = \binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!},$$

and note that it is continuous. Now consider

$$\binom{\frac{p^m+1}{2}}{n} = f\left(\frac{p^m+1}{2}\right) \xrightarrow[m\to\infty]{} f(\frac{0+1}{2}) = \binom{1/2}{n}$$

On the left hand side, we have $\binom{\frac{p^m+1}{2}}{n} \in \mathbb{Z}$. Therefore,

$$\left|\binom{1/2}{n}\right|_p \leq 1$$

since

$$\left|\left(\frac{p^m+1}{2}\right)\right|_p \leq 1$$

for all $m \geq 1$.

Example 8.10. Consider $\mathbb{Q}_5$. Let

$$\alpha = \frac{1}{2}\sum_{n=0}^{\infty}(-1)^n\binom{1/2}{n}5^n.$$

To check that this is well-defined, we only need to know that each term individually goes to zero, which happens because

$$\left|(-1)^n\binom{1/2}{n}\right|_5 \leq 1$$

as in the previous example and $|5^n|_5 = 5^{-n} \to 0$ as $n \to \infty$.

For real $|x| < 1$,

$$\sqrt{1+x} = \sum_{n=0}^{\infty}\binom{1/2}{n}x^n.$$

Hence, there is an equality of formal power series:

$$1 + x = \left(\sum_{n=0}^{\infty} \binom{1/2}{n} x^n \right)^2 .$$

Now set $x = -5$.

$$-4 = \left(\sum_{n=0}^{\infty} \binom{1/2}{n} (-5)^n \right)^2 \in \mathbb{Q}_5 .$$

Therefore, $\alpha^2 = -1$. In particular, $\mathbb{Q}_5$ has a fourth root of unity!

Definition 8.11. The subring of $K_{\mathfrak{p}}$

$$\mathcal{O}_{\mathfrak{p}} := \left\{ x \in K_{\mathfrak{p}} \;\middle|\; |x_{\mathfrak{p}}| \leq 1 \right\}$$

is called the **ring of $\mathfrak{p}$-adic integers**.

If $K = \mathbb{Q}$, we write $\mathbb{Z}_p$ instead.

Proposition 8.12. *$\mathcal{O}_{\mathfrak{p}}$ is a discrete valuation ring.*

Proof sketch. $\nu_{\mathfrak{p}} \colon K^{\times} \to \mathbb{Z} \subseteq \mathbb{R}$ is continuous with respect to $|-|_{\mathfrak{p}}$, and extends uniquely to a continuous map

$$\nu_{\mathfrak{p}} \colon K_{\mathfrak{p}}^{\times} \to \mathbb{Z} \subseteq \mathbb{R}.$$

Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\nu_{\mathfrak{p}}(\pi) = 1$.

Let $\mathcal{O}_{\mathfrak{p}}^{\times} = \left\{ x \in K_{\mathfrak{p}} \;\middle|\; |x_{\mathfrak{p}}| = 1 \right\}$. Note that for $x \in \mathcal{O}_{\mathfrak{p}}^{\times}$, $|x^{-1}|_{\mathfrak{p}} = |x|_{\mathfrak{p}}^{-1}$. For $a \in \mathcal{O}_{\mathfrak{p}} \setminus \{0\}$,

$$\nu_{\mathfrak{p}}(a\pi^{-\nu_{\mathfrak{p}}(a)}) = 0.$$

Therefore, $|a\pi^{-\nu_{\mathfrak{p}}(a)}|_{\mathfrak{p}} = 1$, and it follows that $a\pi^{-\nu_{\mathfrak{p}}(a)} \in \mathcal{O}_{\mathfrak{p}}^{\times}$.

The nonzero ideals of $\mathcal{O}_{\mathfrak{p}}$ are $\pi^n \mathcal{O}_{\mathfrak{p}}$ with $n \geq 0$. Hence, $\mathcal{O}_{\mathfrak{p}}$ is a PID with a unique maximal ideal. □

Remark 8.13. We may related this to the discrete valuation ring $\mathcal{O}_K$ via an isomorphism

$$\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sim} \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\pi\mathcal{O}_{\mathfrak{p}}.$$

Notice that the left hand side is a finite field, and therefore $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ is a finite field as well.

8.2 How do you write down elements of $K_\mathfrak{p}$ or $\mathcal{O}_\mathfrak{p}$?

Remark 8.14. We will really concentrate on $\mathcal{O}_\mathfrak{p}$, because given any element of $K_\mathfrak{p}$, we may multiply by a sufficiently large power of $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ to get an element of $\mathcal{O}_\mathfrak{p}$.

Fix a finite set $S \subseteq \mathcal{O}_K$ representing the cosets of $\mathcal{O}_K/\mathfrak{p}$. Fix $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, i.e. $\pi \in \mathcal{O}_K$ and $v_\mathfrak{p}(\pi) = 1$.

Example 8.15. For $K = \mathbb{Q}$, and an integral prime p, $\pi = p$ and $S = \{0, 1, \dots, p-1\}$.

Theorem 8.16. *Any $x \in \mathcal{O}_\mathfrak{p}$ is of the form*

$$\sum_{n=0}^{\infty} a_n \pi^n$$

for unique $a_0, a_1, \dots \in S$. Conversely, any such series converges to an element of $\mathcal{O}_\mathfrak{p}$.

This gives us a way to represent elements of $\mathcal{O}_\mathfrak{p}$ on a computer, for instance.

Proof idea. Let $x \in \mathcal{O}_\mathfrak{p}$.

- $x \equiv a_0 \pmod{\mathfrak{p}\mathcal{O}_\mathfrak{p}}$ for a unique $a_0 \in S$.

$$\frac{x - a_0}{\pi} \in \mathcal{O}_\mathfrak{p}$$

- $\frac{x-a_0}{\pi} \equiv a_1 \pmod{\mathfrak{p}\mathcal{O}_\mathfrak{p}}$ for a unique $a_1 \in S$.

$$\frac{x - (a_0 + a_1\pi)}{\pi^2} \in \mathcal{O}_\mathfrak{p}$$

- Repeat.

$$x - (a_0 + a_1\pi + \ldots + a_n\pi^n) \in \pi^{n+1}\mathcal{O}_\mathfrak{p}$$

  with $a_i \in S$.

Finally,

$$\left| x - \sum_{i=0}^{n} a_i \pi^i \right|_\mathfrak{p} \leq |\pi|_\mathfrak{p}^{n+1} = \left(\frac{1}{N(\mathfrak{p})} \right)^{n+1} \xrightarrow[n\to\infty]{} 0. \qquad \square$$

Proposition 8.17. *$\mathcal{O}_\mathfrak{p}$ is compact.*

Proof idea. Suffices to prove sequential compactness since $K_\mathfrak{p}$ is a metric space. Consider any sequence $\{x_n\}$ in $\mathcal{O}_\mathfrak{p}$. Write each x_i as

$$x_i = \sum_{n=0}^{\infty} a_{ni}\pi^n$$

for $a_0, a_1, \ldots \in S$.

Of this sequence, there are infinitely many x_n with the same a_{0i} because S is finite. Of those, there are infinitely many x_n with the same $a_{1i} \in S$ again, since S is finite. Repeat. This yields a convergent subsequence in $\mathcal{O}_\mathfrak{p}$. □

Remark 8.18. For any $a \in K$, $a + \mathcal{O}_\mathfrak{p}$ is an open neighborhood of a that is compact. Hence, $K_\mathfrak{p}$ is a local field.

8.3 Extensions of $\mathbb{Q}_p$

Fix a prime p, and let $K/\mathbb{Q}_p$ be a finite extension of fields. Let B be the integral closure of $\mathbb{Z}_p$ in K.

$$\begin{tikzcd}
K \arrow[r, phantom, "\supseteq"] \arrow[d, dash] & B \arrow[d, dash] \\
\mathbb{Q}_p \arrow[r, phantom, "\supseteq"] & \mathbb{Z}_p
\end{tikzcd}$$

By a theorem we stated but didn't prove, B is a Dedekind domain, so pB factors uniquely as

$$pB = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Fact 8.19. *There is only one prime of* K *such that* $pB = \mathfrak{p}^e$.

Moreover, we have $[K\colon \mathbb{Q}_p] = ef$, where $f = [B/\mathfrak{p}\colon \mathbb{Z}_p/\langle p\rangle]$. There are valuations

$$\nu_\mathfrak{p}\colon K^\times \to \mathbb{Z}$$
$$\nu_p\colon \mathbb{Q}_p^\times \to \mathbb{Z}$$

such that $\nu_\mathfrak{p}|_{\mathbb{Q}_p^\times} = e\nu_p$.

Proposition 8.20. *The* p*-adic absolute value* $|-|_p$ *extends uniquely to* K.

Corollary 8.21. *The* p*-adic absolute value extends uniquely to* $\overline{\mathbb{Q}}_p = \overline{K}$.

Lemma 8.22 (Krasner's Lemma)**.** *Take* $\alpha, \beta \in \overline{K}$. *Let* $p_\alpha(x) \in K[x]$ *be the minimal polynomial of* α *for* $\overline{K}/K$. *Suppose that if* $\alpha' \in \overline{K} \setminus \{\alpha\}$ *is a root of* $p_\alpha(x)$, *then*

$$|\beta - \alpha|_p < |\alpha - \alpha'|_p.$$

Then $K(\alpha) \subseteq K(\beta)$.

The assumption of this lemma says that β is closer to α than any of α's conjugates.

Proof. Take any $\sigma\colon K(\alpha,\beta) \hookrightarrow \overline{K}$ that fixes $K(\beta)$. It suffices to show that $\sigma(\alpha) = \alpha$. We have

$$|\sigma(\alpha) - \beta|_p = |\sigma(\alpha) - \sigma(\beta)|_p = |\sigma(\alpha - \beta)|_p$$

Note that $|\sigma(-)|_p$ is an absolute value on $K(\alpha,\beta)$ that extends $|-|_p$ on $\mathbb{Q}_p$. But by Corollary 8.21, such an extension is unique and therefore $|\sigma(-)|_p = |-|_p$. Hence,

$$|\sigma(\alpha) - \beta|_p = |\sigma(\alpha) - \sigma(\beta)|_p = |\sigma(\alpha - \beta)|_p = |\alpha - \beta|_p.$$

Finally,

$$\begin{aligned} |\sigma(\alpha) - \alpha|_p &= |\sigma(\alpha) - \beta + \beta - \alpha|_p \\ &\leq \max\{|\sigma(\alpha) - \beta|_p, |\beta - \alpha|_p\} \\ &= |\sigma(\alpha) - \beta|_p. \end{aligned}$$

But $|\sigma(\alpha) - \beta| < |\sigma(\alpha) - \alpha|$ if $\sigma(\alpha) \neq \alpha$ by assumption. Hence, $\sigma(\alpha) = \alpha$. □

Krasner's Lemma is the key idea in the proof of the following proposition.

Proposition 8.23. *Fix $f(x) \in K[x]$ monic irreducible of degree n. Then for any $g(x) \in K[x]$ of degree n that is "sufficiently close with respect to $|-|_p$" to $f(x)$, $g(x)$ is irreducible and for any root $\alpha \in \overline{K}$ of f, there is some root $\beta \in \overline{K}$ of g such that $K(\alpha) = K(\beta)$.*

Proposition 8.24. *There is a number field L and a prime $\mathfrak{p} \subseteq \mathcal{O}_L$ dividing p such that $K = L_\mathfrak{p}$.*

Proof idea. Write $K = \mathbb{Q}_p(\alpha)$ by the primitive element theorem. Let $f(x) \in \mathbb{Q}_p[x]$ be the minimal polynomial of α over $\mathbb{Q}_p$. Then take $g(x) \in \mathbb{Q}[x]$ sufficiently close to $f(x)$ by Proposition 8.23 since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Then there is a root $\beta \in \overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}}_p$ of $g(x)$ such that $\mathbb{Q}_\mathfrak{p}(\alpha) = \mathbb{Q}_\mathfrak{p}(\beta)$. Then take $L = \mathbb{Q}(\beta)$. □

Theorem 8.25. *The local fields K of characteristic zero are (up to isomorphism)*

- *finite field extensions $K/\mathbb{Q}_p$, or*
- *the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$.*

Remark 8.26. The local fields K of characteristic $p > 0$ are (up to isomorphism) $\mathbb{F}_q((x))$ for q a power of a prime.

Recall that B is the integral closure of $\mathbb{Z}_p$ inside $K/\mathbb{Q}_p$. A consequence of the previous lemma is that $B = \mathcal{O}_\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$, where $K = L_\mathfrak{p}$.

Lemma 8.27 (Hensel's Lemma)**.** *Let* $f(x) \in B[x] = \mathcal{O}_\mathfrak{p}[x]$ *be monic, and let* $\overline{f}(x) \in \mathbb{F}_\mathfrak{p}[x]$ *be its reduction mod* $\mathfrak{p}$*. Assume* $a \in \mathbb{F}_\mathfrak{p}$ *is a simple root of* $\overline{f}$*. Then there is a unique* $\alpha \in \mathcal{O}_\mathfrak{p}$ *with* $\alpha \equiv a \pmod{\mathfrak{p}}$ *such that* α *is a root of* $f(x)$*.*

Proof sketch. Suppose we have an $\alpha_n \in \mathcal{O}_\mathfrak{p}$ such that $\alpha_n \equiv a \pmod{\mathfrak{p}}$ and $f(\alpha_n) \equiv 0 \pmod{\mathfrak{p}^n}$. (This is true if $n = 0$.) Then take $\pi \in \mathcal{O}_\mathfrak{p}$ with $\nu_\mathfrak{p}(\pi) = 1$. We want to solve

$$0 \overset{?}{\equiv} f(\alpha_n + b\pi^n) \equiv f(\alpha_n) + f'(\alpha_n)b\pi^n \pmod{\mathfrak{p}^{n+1}},$$

or equivalently, solve

$$f'(\alpha_n)b \equiv -\frac{f(\alpha_n)}{\pi^n} \pmod{\mathfrak{p}}.$$

But we know that $f'(\alpha_n)b \equiv f'(a)b \pmod{\mathfrak{p}}$, and $f'(a)b \not\equiv 0 \pmod{\mathfrak{p}}$ since a is a simple root. So we may solve the previous equation for $b \in \mathcal{O}_\mathfrak{p}$. Then $\alpha_{n+1} = \alpha_n + b\pi^n$. The sequence $\{\alpha_n\}$ will converge to a root. □

Remark 8.28. In fact, the proof of Hensel's lemma gives an algorithm for finding α.

Let $K/\mathbb{Q}_p$ be a finite field extension, with ring of p-adic integers $\mathcal{O}_\mathfrak{p} \subseteq K$. Consider the field extension

$$\begin{tikzcd}
\mathcal{O}_\mathfrak{p}/\mathfrak{p} \arrow[d, dash, "f"] \\
\mathbb{Z}_p/\langle p\rangle \cong \mathbb{F}_p
\end{tikzcd}$$

where $f = [\mathcal{O}_\mathfrak{p}/\mathfrak{p} \colon \mathbb{Z}_p/\langle p\rangle]$. Then $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ is the splitting field of $x^{p^f} - x \in \mathbb{F}_p[x]$. Since this polynomial is separable in $\mathbb{F}_p[x]$, then Hensel's lemma tells us that it is separable in $\mathcal{O}_\mathfrak{p}[x]$ as well; it factors into linear terms in $\mathcal{O}_\mathfrak{p}[x]$. So K contains $p^f - 1$ roots of unity!

We essentially get roots of unity for free from Hensel's lemma in the local field case, whereas before we had to work really hard to find roots of unity in number fields.

Let $\mu_{p^f-1} \subseteq K$ denote the roots of unity in K. We have an intermediate field $\mathbb{Q}_p(\mu_{p^f-1})$ fitting into the tower

$$\begin{tikzcd}
K \arrow[d, dash, "e"] \\
\mathbb{Q}_p(\mu_{p^f-1}) \arrow[d, dash, "f"] \\
\mathbb{Q}_p
\end{tikzcd}$$

The extension $K/\mathbb{Q}_p(\mu_{p^f-1})$ is totally ramified, whereas the extension $\mathbb{Q}_p(\mu_{p^f-1})$ is unramified.

Proposition 8.29. *Fix a prime* p *and integer* $n \geq 1$*. There are only finitely many extensions* $K/\mathbb{Q}_p$ *of degree* n*.*

Proof sketch. Any such extension $K/\mathbb{Q}_p$ is also a totally ramified extension of the intermediate field $\mathbb{Q}_p(\mu_{p^f-1})$ of degree e, for f dividing n. Set $F := \mathbb{Q}_p(\mu_{p^f-1})$. We need only show there are only finitely many totally ramified extensions K/F of degree e.

Take any **uniformizer** $\pi \in K$ with $\nu_K(\pi) = 1$. The minimal polynomial of π over F is Eisenstein at $\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$. A slight change in coefficients of this minimal polynomial does not change the extension field by Proposition 8.23, which describes an open cover of the compact set $\mathfrak{p}^{\times(e-1)} \times (\mathfrak{p} - \mathfrak{p}^2)$. There is a finite subcover of this open cover, so K can be obtained from one of these finitely many Eisenstein polynomials. □

We can use this proposition to prove something about number fields.

Theorem 8.30. *Let* K *be a number field. Let* S *be a finite set of primes of* $\mathcal{O}_K$ *and* $n \geq 1$ *an integer. Then there are only finitely many extensions* L/K *of degree* n *and unramified at all primes* $\mathfrak{p} \notin \mathcal{O}_K$*.*

Proof idea. Let's just consider the case $K = \mathbb{Q}$. We know that there are finitely many extensions $L/\mathbb{Q}$ of degree n with a given discriminant $\operatorname{disc}(L)$. The prime divisors of $\operatorname{disc}(L)$ are the ramified primes of the extension $L/\mathbb{Q}$. Then we may bound the powers of $\operatorname{disc}(L)$ that arise using the finiteness of extensions of $\mathbb{Q}_p$ with Proposition 8.29. □

8.4 Global and Local class field theory

The two theorems in this section are the beginning of the subjects of local class field theory and global class field theory.

Definition 8.31. A field extension L/K is **abelian** if it is Galois with an abelian Galois group.

Theorem 8.32. *Let* $K/\mathbb{Q}_p$ *be a finite field extension. There is an inclusion-reversing bijection between finite abelian extensions* L/K *in* $\overline{K}$ *and open finite index subgroups of* $K^\times$ *given by* $L \mapsto N_{L/K}(L^\times)$*.*

Definition 8.33. The **group of ideles of** K is

$$\mathbb{A}_K^\times = \left\{ (a_\nu) \in \prod_\nu K_\nu^\times \;\middle|\; a_\nu \in \mathcal{O}_\nu \text{ for most } \nu \right\},$$

where ν runs over all valuations of K.

$K^\times$ includes into $\mathbb{A}_K^\times$ via $a \mapsto (a)_v$

Definition 8.34. Define $C_K := \mathbb{A}_K^\times / K^\times$.

Theorem 8.35. *Let K be a number field. There is an inclusion reversing bijection between finite abelian extensions of K in $\overline{K}$ and open finite index subgroups of C_K.*