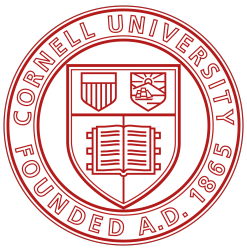


Cornell University

MATH 6370: Algebraic Number Theory

Lecturer: Dr. David Zywina
Notes By: Caleb McWhorter

Spring 2018

Last Updated: January 15, 2019

Contents

0 Introduction

MATH 6370: An introduction to number theory focusing on the algebraic theory. Topics include, but are not limited to, number fields, Dedekind domains, class groups, Dirichlet's unit theorem, local fields, ramification, decomposition and inertia groups, and the distribution of primes.

Recommended Text References

- Marcus, *Number Fields*. 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 and freely available.
- Lang, *Algebraic Number Theory*
- Murty, Esmonda, *Problems in Algebraic Number Theory*. This book was designed for self study. Lots of exercises with full solutions.
- Janusz, *Algebraic Number Fields*

These notes were taken in Spring 2018 in a course taught by Professor David Zywina at Cornell University. In some places, notation/material has been changed or added. Any errors in this text should be attributed to the typist — Caleb McWhorter — and not the instructor or any referenced text.

1 The Ring of Integers

1.1 Number Fields

Algebraic Number Theory studies the arithmetic of number fields — the ring of integers of number fields and its ideals, units, and factorizations. Number theoretic questions are posed in terms of these algebraic objects and their properties. To begin, we recall the definition of the basic object of study — number fields.

Definition (Number Field)**.** A number field is a finite extension of $\mathbb{Q}$, i.e.

$$\begin{array}{c} K \\ \Big| \, [K:\mathbb{Q}] = \dim_{\mathbb{Q}} K \\ \mathbb{Q} \end{array}$$

Example 1.1 (Number Fields)**.**

(i) $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$.

(ii) $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity.

(iii) $\mathbb{Q}(\alpha)$, where α is a root of $x^3 + 2x^2 + 1$.

These simple extensions of $\mathbb{Q}$ are not arbitrarily constructed elementary examples of number fields. In fact, every number field arises in this way. Recall given a field extension E/F, an element $\alpha \in E$ is called a primitive element for E/F if $E = F(\alpha)$. Every number field possesses a primitive element.

Theorem 1.1 (Primitive Element Theorem)**.** *If K is a number field, then $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{Q}$.*

Generally, if E/F is a separable extension of finite degree, then $E = F(\alpha)$ for some $\alpha \in E$. Of course, the definition of a number field excludes infinite extensions of $\mathbb{Q}$ such as $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}(\{\sqrt[n]{2} \colon n \in \mathbb{N}\})$. Of course, there are even examples when the extension is simple, e.g. $K = \mathbb{Q}(e)$ or $K = \mathbb{Q}(\pi)$.

The traditional object of interest in number theory is $\mathbb{Z} \subseteq \mathbb{Q}$. What is the analog for a general number field K, i.e. what should the object $\mathcal{O} \subseteq K$ be so that factoring is 'interesting'. The first goal for this course will be to define such an object and to study its properties.

1.2 Ring of Integers

Let K be a number field. Take $\alpha \in K$ and $n = [K : \mathbb{Q}]$. Let $\phi : \mathbb{Q}[\alpha] \to K$ be the homomorphism of $\mathbb{Q}$-algebras given by $x \mapsto \alpha$. This map is not injective (it is a map

of an infinite dimensional vector space to a finite dimensional vector space). Then the kernel is nonzero and must be principal since $\mathbb{Q}[x]$ is a PID. This induces an isomorphism $\tilde{\phi} : \mathbb{Q}[x]/(p_\alpha(x)) \to K$, where $p_\alpha(x)$ is the minimal monic irreducible polynomial in $\mathbb{Q}[x]$ with α as a root. Denote by $\mathbb{Q}[\alpha]$ the image of $\tilde{\phi}$ in K, i.e. the $\mathbb{Q}$-algebra generated by α. Since $p_\alpha(x)$ is irreducible, $(p_\alpha(x))$ is maximal and hence $\mathbb{Q}[x]/(p_\alpha(x))$ is a field. But since $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(p_\alpha(x))$, we must have $\mathbb{Q}[\alpha] \cong \mathbb{Q}(\alpha)$. Note that since $\mathbb{Q} \subseteq K$, certainly $\mathbb{Z} \subsetneq K$. Now recall that $\alpha \in K/\mathbb{Q}$ is an algebraic number if $p_\alpha(x) \in \mathbb{Q}[x]$. [We cannot have α transcendental since we assume that K is a number field.] We are interested in a very special type of algebraic number.

Definition (Algebraic Integer)**.** We say $\alpha \in K$ is an algebraic integer if $p_\alpha(x)$ has coefficients in $\mathbb{Z}$, i.e. $p_\alpha(x) \in \mathbb{Z}[x]$.

Definition (Ring of Integers)**.** Define $\mathcal{O}_K$ to be the set of $\alpha \in K$ so that α is an algebraic integer.

It is not immediately clear that $\mathcal{O}_K$ is even a ring. We shall prove this later.

Example 1.2. Take $A = \mathbb{Q}$. If $\alpha \in \mathbb{Q}$, then $p_\alpha(x) = x - \alpha$. Now $p_\alpha(x) \in \mathbb{Z}[x]$ if and only if $\alpha \in \mathbb{Z}$. One can check that $\mathcal{O}_K = \mathbb{Z}$. Then the ring of integers does indeed reproduce the basic example of $\mathbb{Z} \subseteq \mathbb{Q}$. ◁

Example 1.3. Take $K = \mathbb{Q}(\sqrt{-2}) = \{a + b\colon a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ and $\alpha = a + b\sqrt{-2} \in K$. We have two cases:

$b = 0$: If $b = 0$, then $a \in \mathbb{Q}$. But then we are in the case from Example **??** so that $\alpha \in \mathcal{O}_K$ if and only if $\alpha \in \mathbb{Z}$.

$b \neq 0$: If $b \neq 0$, then $p_\alpha(x)$ factors as $p_\alpha(x) = (x - (a + b\sqrt{-2}))(x - (a - b\sqrt{-2})) = x^2 - 2ax + (a^2 + 2b^2)$. Then $\alpha \in \mathcal{O}_K$ if and only if $2a \in \mathbb{Z}$ and $a^2 + 2b^2 \in \mathbb{Z}$. Let $n = a^2 + 2b^2$. Since $2a \in \mathbb{Z}$, we have $a = \frac{r}{2}$ for some $r \in \mathbb{Z}$. Then we have $a^2 + 2b^2 = \frac{r^2}{4} + 2b^2 = n$. But then $r^2 + 8b^2 = 4n$ so that r cannot be odd. Therefore, $a \in \mathbb{Z}$. This shows that $2b^2 = n - a^2 \in \mathbb{Z}$ which implies $b^2 = \frac{s}{2}$ for some $s \in \mathbb{Z}$, where without loss of generality, we assume $(s, 2) = 1$. Write $b = \frac{u}{v}$, where $u, v \in \mathbb{Z}$ and $(u, v) = 1$. Then $\frac{u^2}{v^2} = \frac{s}{2}$ which implies $2u^2 = sv^2$. Now $2 \mid (2u^2)$ so that $2 \mid (sv^2)$. As $(s, 2) = 1$, it must be that $2 \mid v^2$. Therefore, $2 \mid v$ and $v = 2q$ for some $q \in \mathbb{Z}$. Therefore, $2u^2 = 4sq^2$ which implies $u^2 = 2sq^2$. As $2 \mid (2sq^2)$, $2 \mid u^2$ which implies $2 \mid u$. But then $(u, v) \geq 2$, a contradiction. Therefore, we must have $b \in \mathbb{Z}$.

This shows that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}\colon a, b\mathbb{Z}\}$. Furthermore, $\mathbb{Z}[\sqrt{-2}]$ is a UFD, i.e. factorial. ◁

We question remains why we care about 'integers' in number fields rather than just considering the ordinary integers in $\mathbb{Q}$. The answer is simple: factorizations. In these larger

rings, we might have 'larger' and more 'interesting' factorizations that we could use to solve problems that are otherwise more difficult in $\mathbb{Z}$ alone.

Example 1.4. Find all solutions $x, y \in \mathbb{Z}$ for $y^2 = x^3 - 2$. After a bit of experimentation, one can see that $(3, \pm 5)$ is a solution. However, is this the only solution? Are there infinitely many solutions? It is true that there are infinitely many rational solutions to this equation. To solve the stated problem, we choose to work in $\mathbb{Z}[\sqrt{-2}]$ for the 'extra factorization'. We shall use the fact that $\mathbb{Z}[\sqrt{-2}]$ is a UFD and $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$ without proof.

In $\mathbb{Z}[\sqrt{-2}]$, we have $x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2})$. Write $x = u_1 \pi_1^{e_1} \cdots \pi_r^{e_r}$, where π_i is irreducible, $e_i \geq 1$, and $\pi_i \neq \pm \pi_j$ for $i \neq j$. Then $u_1^3 \pi_1^{3e_1} \cdots \pi_r^{3e_r} = (y + \sqrt{-2})(y - \sqrt{-2})$. We claim that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime: choose an irreducible dividing both, say π. Then $\pi \mid ((y + \sqrt{-2}) - (y - \sqrt{-2})) = 2\sqrt{-2} = (\sqrt{-2})^3$. By unique factorization, we must have $\pi = \sqrt{-2}$, up to units. Since $\pi \mid (y + \sqrt{-2})$, we have $y + \sqrt{-2} = \sqrt{-2}(a + b\sqrt{-2}) = -2b + a\sqrt{-2}$ for some $a, b \in \mathbb{Z}$. Then $y = -2b$ which implies $x^3 = 2 + y^2 \equiv 2 \mod 4$, a contradiction as no cube has residue 2 mod 4.

For each $1 \leq i \leq r$, $\pi_i^{3e_i}$ divides $y + \sqrt{-2}$ or $y - \sqrt{-2}$. Then $y + \sqrt{-2} = u \prod_{i \in \mathfrak{I}} \pi_i^{3e_i}$ for some $\mathfrak{I} \subseteq \{1, \ldots, r\}$ and $u \in \mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$. This implies $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ for some $a, b \in \mathbb{Z}$. Expanding yields, $y + \sqrt{-2} = (a^3 - 6ab^2) + (3a^2 b - 2b^3)\sqrt{-2}$. This forces $y = a^3 - 6ab^2$ and $3a^2 - 2b^3 = 1 - a$.

We now have a restriction on the possibilities for y! This is a restriction that would not have been as easily obtained working only in $\mathbb{Z}$. Now as $b(3a^2 - 2b^2) = 1$ with $a, b \in \mathbb{Z}$, it must be that $b \in \{\pm 1\}$. If $b = 1$, we have

$$y = a^3 - 6ab^2 \Leftrightarrow 3a^2 - 2 = 1 \Leftrightarrow 3a^2 = 3 \Leftrightarrow a = \pm 1$$

Then $y \in \{\mp 5\}$ which yields solutions $(3, \pm 5)$. These are the only solutions for if $b = -1$, then $3a^2(-1) - 2(-1)^3 = 1$, which implies $3a^2 = 1$, a contradiction. ◁

One must take care when using such an approach. Consider the following (non-)example.

Non-Example 1.1. Find all $(x, y) \in \mathbb{Z}^2$ satsifying $y^2 = x^3 - 61$. Using the factorization in $\mathbb{Z}[\sqrt{-61}]$, we have $x^3 = y^2 + 61 = (y + \sqrt{-61})(y - \sqrt{-61})$. Using the method of Example **??**, one can show that there are no such solutions. But $(5, \pm 8)$ are clearly solutions! ◁

The key to Example **??** was not just factorization but *unique* factorization. The fact that $\mathbb{Z}[\sqrt{-2}]$ was a UFD was essential. The problem in Example **??** is that $\mathbb{Z}[\sqrt{-61}]$ is not a UFD: $5^3 = 8^2 + 61 = (8 + \sqrt{-61})(8 - \sqrt{-61})$, where 5, $(8 + \sqrt{-61})$, and $(8 - \sqrt{-61})$ all irreducible. How does one cope with loss of unique factorization? Kummer (in approximately 1846) said there should be a further factorization into "ideal numbers" in order to recover unique factorization. This lead Dedekind to define the ideal of a ring. He later gave the correct notion of factorization instead using (prime) ideals. We shall see

every ideal of $\mathcal{O}_K$ factors uniquely as a product of prime ideals. Generally, we want to study the properties of $\mathcal{O}_K$ further. As a short list of goals, we want to...

- Show $\mathcal{O}_K$ is a ring.
- Study the structure of abelian group $(\mathcal{O}_K, +)$ and show $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$.
- Study the structure of units $\mathcal{O}_K^\times$.
- Show $\mathcal{O}_K$ has unique factorization into prime ideals.
- Measure failure of unique factorization, leading to the class group.
- Study the primes of $\mathcal{O}_K$ and how these primes 'split'.

We shall begin by showing that $\mathcal{O}_K$ is a ring. The proof, which is rather simple, will make use of some extra facts about algebraic integers.

Proposition 1.1. *If $\alpha \in K$ is an algebraic integer, then the following are equivalent:*

(i) $p_\alpha(x) \in \mathbb{Z}[x]$

(ii) $f(\alpha) = 0$ *for some monic polynomial* $f(x) \in \mathbb{Z}[x]$

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

(iv) there exists a nonzero finitely generated subgroup $M \subseteq K$ *such that* $\alpha M \subseteq M$

Proof.

(i)→(ii) This is immediate.

(ii)→(iii) If $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ has α as a root, then we can express the numbers $\{\alpha^i\}_{i \geq n}$ in terms of lower powers of α. For example, since $f(\alpha) = 0$, we have $\alpha^n = -(a_1\alpha^{n-1} + \cdots + a_n)$ and $\alpha^{n+1} = -\alpha(a_1\alpha^{n-1} + \cdots + a_n) = -a_1\alpha^n - \cdots - a_n\alpha = -a_1(a_1\alpha^{n-1} + \cdots + a_n) - \cdots - a_n\alpha$. More concretely, there is a surjection $\mathbb{Z}[x] \to \mathbb{Z}[\alpha]$ given by $x \mapsto \alpha$. This gives a surjection $\mathbb{Z}[x]/(f) \to \mathbb{Z}[\alpha]$. But $\mathbb{Z}[x]/(f)$ is generated by $1, x, \ldots, x^{d-1}$, where $d = \deg(f)$. Then it must be that $\mathbb{Z}[\alpha]$ is finitely generated.

(iii)→(iv) Take $M = \mathbb{Z}[\alpha]$.

(iv)→(ii) We have $M = \oplus_{i=1}^r \mathbb{Z}\beta_i$ for some collection $\{\beta_i\}_{i=1}^r$. But then for each i, we can write $\alpha\beta_i = \sum_{j=1}^r C_{ij}\beta_j$ for some matrix $C = (C_{ij})$. By the Cayley-Hamilton Theorem, C is a root of its characteristic polynomial; that is, C is a root of $f(x) = \deg(xI - C) \in \mathbb{Z}[x]$. But then $C \in M_r(\mathbb{Z})$ so that $f(\alpha) = 0$.

(ii)→(i) Suppose that $f(\alpha) = 0$. We need only show that $f(x)$ is irreducible. Suppose to the contrary that $f(x) = p_\alpha(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. [Note, we have used the fact that the minimal polynomial must divide any polynomial having α as a root.] It must be that $g(x)$ is monic since $f(x) = p_\alpha(x)g(x)$ is monic. We claim that $p_\alpha(x), g(x) \in \mathbb{Z}[x]$. [This is really just Gauß' lemma but we shall show it directly here.] If not, then fix a p dividing the denominator of a coefficient of $p_\alpha(x)$ or $g(x)$. Take $e, f \geq 0$ such that $p^e p_\alpha(x)$ and $p^f g(x)$ have coefficients with no p's in the denominator. We have

$$p^{e+f} f(x) = p^e p_\alpha(x) \cdot p^f g(x) \not\equiv \mod p$$

But then $e + f = 0$ as $f(x)$ is monic. Since $e, f \geq 0$, we must have $e = f = 0$, a contradiction. □

We are now in a position to easily prove that $\mathcal{O}_K$ is a subring of K.

Proposition 1.2. *$\mathcal{O}$ is a subring of K.*

Proof. Observe that $0, 1 \in \mathcal{O}_K$ so that $\mathcal{O}_K$ is nonempty. In particular, $\mathbb{Z} \subseteq \mathcal{O}_K$. Let $\alpha, \beta \in \mathcal{O}_K$. Take $\alpha, \beta \in \mathcal{O}_K$. The $\mathbb{Z}$-modules $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated, say 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 finitely generated by $\{\alpha^i \beta^j\}_{\substack{0 \leq i < d \\ 0 \leq j < e}}$. But $\alpha \pm \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$ so that $(\alpha \pm \beta)\mathbb{Z}[\alpha, \beta]$ and $(\alpha\beta)\mathbb{Z}[\alpha, \beta]$ are contained in $\mathbb{Z}[\alpha, \beta]$. By Proposition **??**, $\alpha \pm \beta, \alpha\beta$ are algebraic integers and hence $\alpha \pm \beta, \alpha\beta \in \mathcal{O}_K$. □

Exercise: Prove Proposition **??** using (i) and (ii) of Proposition **??**.

If $\mathbb{Q} \subseteq K \subseteq L$ are number fields, it is immediate that $\mathcal{O}_L \cap K = \mathcal{O}_K$. In particular, $\mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$. It is clear that $\mathcal{O}$ is an integral domain since $\mathcal{O} \subseteq K$. Now for any $\alpha \in K$, there is an integer $m \geq 1$ such that $m\alpha \in \mathcal{O}_K$. Take any $\alpha \in K$ and $f(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Q}[x]$ with $f(\alpha) = 0$. For $m \geq 1$, $m\alpha$ is a root of $x^d + mc_1 x^{d-1} + \cdots + m^d c_d$. Choosing m sufficiently large, we can also assure that the coefficients are in $\mathbb{Z}$. That is, α is 'not far' from being an algebraic integer.

1.3 Trace and Norm

Suppose that $K/\mathbb{Q}$ has degree n. For $\alpha \in K$, define $\mu_\alpha : K \to K$ via $x \mapsto \alpha x$. This is a $\mathbb{Q}$-linear map so, fixing a basis, we can represent μ_α by a $n \times n$ matrix.

Definition (Norm)**.** Define $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ via $\alpha \mapsto \det(\mu_\alpha)$.

Definition (Trace)**.** Define $Tr_{K/\mathbb{Q}} : K \to \mathbb{Q}$ via $\alpha \mapsto \text{trace}(\mu_\alpha)$.

Remark. The definitions of norm and trace do not depend on the fact that K is a number field, only that the field extension is finite. So given any fields K, F with K/F finite, we may define $N_{K/F}$ and $Tr_{K/F}$.

Remark. While choosing different a different basis for $K/\mathbb{Q}$ will change the matrix μ_α, the trace and determinant of resulting matrix are invariant. This is because the new basis is conjugate to the old one and trace/determinant are invariant under conjugation.

Example 1.5. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ a squarefree integer. This is a degree 2 extension and K has basis $\{1, \sqrt{d}\}$. Take $\alpha = a + b\sqrt{d} \in K$, where $a, b \in \mathbb{Q}$. We have

$$\alpha \cdot 1 = a + b\sqrt{d}$$
$$\alpha \cdot \sqrt{d} = bd + a\sqrt{d}$$

Then relative to this basis, we have

$$\mu_\alpha = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

We then have $N_{K/\mathbb{Q}} = a^2 - db^2$ and $Tr_{K/\mathbb{Q}} = 2a$. ◁

Example 1.6. Let $K = \mathbb{Q}(\omega)$, where $\omega = \sqrt[3]{2}$. The minimal polynomial of ω over $\mathbb{Q}$ is $p_\omega(x) = x^3 - 2$. Therefore, K is a degree 3 extension of $\mathbb{Q}$ with possible $\mathbb{Q}$-basis being $\{1, \omega, \omega^2\}$. Then for $\alpha \in K$, we may write $a + b\omega + c\omega^2$ for $a, b, c \in \mathbb{Q}$. With respect to the chosen basis, we have

$$[\mu_\alpha] = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$$

$$Tr_{K/\mathbb{Q}}(\alpha) = \text{trace}[\mu_\alpha] = 3a$$
$$N_{K/\mathbb{Q}}(\alpha) = \det[\mu_\alpha] = a^3 + 2b^3 - 4c^3 - 6abc$$

Now when does $N_{K/\mathbb{Q}}(\alpha) = \pm 1$? Certainly when $\alpha = \pm 1$, $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. But this is also true for $\alpha = \epsilon$, where $\epsilon = 1 + \omega + \omega^2$. Since the norm is multiplicative, every power of ϵ has norm 1. It turns out, $\mathcal{O}_K = \mathbb{Z}[\omega]$ and $\mathcal{O}_K^\times = \{\pm\epsilon^n : n \in \mathbb{Z}\}$. ◁

From the properties of determinants and traces, it is routine to verify

Proposition 1.3.

- $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$
- $N_{K/\mathbb{Q}}(c) = c^n$ *for* $c \in \mathbb{Q}$

In particular, $N_{K/\mathbb{Q}} : K^\times \to \mathbb{Q}^\times$ *is a homomorphism of groups.*

- $Tr_{K/\mathbb{Q}} : K \to \mathbb{Q}$ *is* $\mathbb{Q}$*-linear*

Example 1.7 (Pell's Equation, $n = 2$)**.** Using the norm, we shall show that $x^2 - 2y^2 = 1$ has infinitely many solutions. We know $\mathbb{Z}[\sqrt{2}] \subseteq K := \mathbb{Q}(\sqrt{2})$. Observe $N_{K/\mathbb{Q}} = x^2 - 2y^2$. There is a correspondence

$$\{(a,b) \in \mathbb{Z}^2 \colon a^2 - 2b^2 = 1\} \iff \{\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{2}] \colon N_{K/\mathbb{Q}}(\alpha) = 1\}$$

Let $G = \{\alpha \in \mathbb{Z}[\sqrt{2}] \colon N_{K/\mathbb{Q}}(\alpha) = 1\}$. We 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 that $\alpha\beta \in G$.
- If $\alpha = a + b\sqrt{2} \in G$, then $\alpha^{-1} = a - b\sqrt{2} \in G$ as $\alpha\alpha^{-1} = a^2 - 2b^2 = 1$.

Now take $\epsilon = 3 + 2\sqrt{2} \in G$. Since $\epsilon > 1$, the powers of ϵ are all distinct. But then there are infinitely many elements of norm 1; hence, there are infinitely many solutions to $x^2 - 2y^2 = 1$. In fact, $G = \pm\langle\epsilon\rangle = \{\pm\epsilon^n \colon n \in \mathbb{Z}\}$. However, $\mathbb{Z}[\sqrt{2}]^\times = \pm\langle 1 + \sqrt{2}\rangle$ and G is a subgroup of $\mathbb{Z}[\sqrt{2}]^\times$ of index 2. Note that $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2} = \epsilon$. ◁

Example 1.8. In general, Pell's equation ($x^2 - dy^2 = 1$ with $d > 1$ squarefree) has infinitely many solutions. However, the first nontrivial solution (ones different from (1,0)), ϵ, can be large. For example given $x^2 - 1141y^2 = 1$, the corresponding group is

$$G = \{\alpha \in \mathbb{Z}[\sqrt{1141}] \colon N_{K/\mathbb{Q}}(\alpha) = 1\} = \pm\langle\epsilon\rangle,$$

where $\epsilon = 1036782394157223963237125215 + 30693385322765657197397208\sqrt{1141}$. ◁

These are special cases of a more general theorem, which will come later (see Section **??** and Section **??**):

Theorem ?? (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 a finitely generated abelian group with rank $r + s - 1$ and $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K are the roots of unity in $\mathcal{O}_K$.*

Example 1.9. For a quadratic number field $K = \mathbb{Q}(\sqrt{d})$, with $d > 0$ square free, $r = 2$ and $s = 0$ so that $\mathcal{O}_K^\times$ has rank $r + s - 1 = 1$. ◁

Example 1.10. The theorem also gives that when $K = \mathbb{Q}(\sqrt{d})$, it will not generally be the case that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. For instance, if $\alpha = \dfrac{-1 + \sqrt{-3}}{2}$. Observe that $\alpha^3 = 1$ so that α is a root of $x^3 - 1$; therefore, $\alpha \in \mathbb{Q}(\sqrt{-3})$ is an algebraic integer. However, $\alpha \notin \mathbb{Z}[\sqrt{-3}]$. ◁

1.4 Complex Embeddings: Norm & Trace Continued

In trying to study the norm and trace, it is natural to study the characteristic polynomial of $[\mu_\alpha]$, i.e. $\det(xI - \mu_\alpha) \in \mathbb{Q}[x]$, as

$$\det(xI - \mu_\alpha) = x^n - Tr_{K/\mathbb{Q}}(\alpha)x^{n-1} + \cdots + (-1)^n N_{K/\mathbb{Q}}(\alpha).$$

Now μ_α acts on K as a $\mathbb{Q}$-linear map. Extending scalars, μ_α acts on $K \otimes_{\mathbb{Q}} \mathbb{C}$. Choose a primitive element β for K. Then we have

$$K = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(p_\beta(x)),$$

where $p_\beta(x)$ is the minimal polynomial of β. [The isomorphism in the left direction is $x \mapsto \beta$ or assuming equality, $\beta = [x]$.] We may then write

$$K \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}[x]/(p_\beta(x)).$$

This ring is almost certainly not a field, since $\beta_b eta(x)$ factors into linear terms over $\mathbb{C}$ by the Fundamental Theorem of Algebra. It should then be clear that this is a field if and only if p_β has degree 1 if and only if $\beta \in \mathbb{Q}$ if and only if $K = \mathbb{Q}$. Now write $p_\beta(x) = \prod_{i=1}^n (x - \beta_i)$, where $\beta_i \in \mathbb{C}$ are the distinct roots of $p_\beta(x)$ in $\mathbb{C}$. By the Chinese Remainder Theorem,

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

This isomorphism is canonical up to choice of ordering of the roots and β. Using this isomorphism, μ_α acts on $K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^n$ via multiplication by $\alpha \otimes 1$. Consider the composite

$$\sigma_i : K \longrightarrow K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\cong} \mathbb{C}^n \xrightarrow{\pi_i} \mathbb{C}$$

where the first map is $\alpha \mapsto \alpha \otimes 1$. Each map $\sigma_i : K \hookrightarrow \mathbb{C}$ is a nonzero homomorphism of fields, hence injective. Since the isomorphism is determined by its action on β (since the map will fix $\mathbb{Q}$), each embedding is characterized by the fact that $\sigma_i(\beta) = \beta_i$.

Definition (Complex Embeddings)**.** The field homomorphisms $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ are the complex embeddings of K into $\mathbb{C}$.

Remark. Note that if $K/\mathbb{Q}$ is a number field of degree n, the work above shows there are always exactly n such embeddings.

Considering simple tensors, an explicit isomorphism $K \otimes_{\mathbb{Q}} \mathbb{C} \to \mathbb{C}^n$ is given by $\alpha \otimes z \mapsto (z\sigma_1(\alpha), \ldots, z\sigma_n(\alpha))$, i.e. 'scaling'. The action on $K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^n$ can then be given by the diagonal matrix

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

From this characterization, the following becomes clear:

Proposition 1.4. *For a number field $K/\mathbb{Q}$ of degree n,*

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$
$$Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

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

Example 1.11. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension, where $d \neq 1$ is a squarefree integer. We assume $K \subseteq \mathbb{C}$ already for convenience. There are two embeddings $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{C}$:

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

Then the norm and trace are

$$N_{K/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$
$$Tr_{K/\mathbb{Q}}(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$$

◁

We had wanted to study more the relation between trace/norm and the characteristic polynomial of $[\mu_\alpha]$, i.e. $\det(xI - \mu_\alpha) \in \mathbb{Q}[x]$. The work above shows

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

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

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

Therefore,

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

for some m. But we know $\deg p_\alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $\deg \det(xI - \mu_\alpha) = n = [K : \mathbb{Q}]$. Therefore, we must have $m = [K : \mathbb{Q}(\alpha)]$. This proves the following:

Proposition 1.5. *Let $K/\mathbb{Q}$ be a number field and $\alpha \in K$. Let $\mu_\alpha : K \to K$ denote multiplication by α. Then*

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

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

Corollary 1.1. *For $\alpha \in \mathcal{O}_K$, $N_{K/\mathbb{Q}}(\alpha)$ and $Tr_{K/\mathbb{Q}}(\alpha)$ are integers.*

Proof. From Proposition **??**,

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

Since $p_\alpha(x) \in \mathbb{Z}[x]$, all the coefficients on the left side must also be integers. But we have

$$\det(xI - \mu_\alpha) = x^n - Tr_{K/\mathbb{Q}}(\alpha)x^{n-1} + \cdots + (-1)^n N_{K/\mathbb{Q}}(\alpha).$$

□

Example 1.12. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. We want to find $\mathcal{O}_K$. If $\alpha = a + b\sqrt{d} \in \mathcal{O}_K$, where $a, b \in \mathbb{Q}$, we know from Corollary **??** that $N_{K/\mathbb{Q}}(\alpha), Tr_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Hence, $a^2 - db^2, 2a \in \mathbb{Z}$. Multiplying $a^2 - db^2$ by 4, we obtain $(2a)^2 - d(2b)^2, 2a \in \mathbb{Z}$.

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

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

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

In order to determine $\mathcal{O}_K$, we need to determine which of these representatives are 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 $\mathbb{Z}[x]$ as d is square free. Hence, $\frac{\sqrt{d}}{4} \notin \mathcal{O}_K$. Finally, the minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is

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

Then $\frac{1+\sqrt{d}}{2}$ has minimal polynomial $p_\alpha(x) \in \mathbb{Z}[x]$. [That is, $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ if and only if $d \equiv 1 \mod 4$.] Therefore,

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

◁

In the previous example where $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer, we found

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

But what is the point of this? Certainly, $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. Why not just use $\mathbb{Z}[\sqrt{d}]$? Why is $\mathcal{O}_K$ the 'right' thing to study? As a vague answer, $\mathcal{O}_K$ is 'nicer'. For example, take the case where $K = \mathbb{Q}(\sqrt{-3})$. We know $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ not $\mathbb{Z}[\sqrt{-3}]$. Why use $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$? Well, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is a UFD whereas $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is not. So the ring $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is a 'better' choice. There are under lying geometric considerations/connections here as well; the affine coordinate ring of $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is smooth whereas the one for $\mathbb{Z}[\sqrt{-3}]$ is not. But for now, let us return to relations between $\mathcal{O}_K$ and $N_{K/\mathbb{Q}}/Tr_{K/\mathbb{Q}}$.

Proposition 1.6. *$\alpha \in \mathcal{O}$ is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. ($\Longrightarrow$). If α is a unit, there is some $\beta \in K$ 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 $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

($\Longleftarrow$). Identify $K \subseteq \mathbb{C}$ and let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the complex embeddings of K into $\mathbb{C}$, relabeling if necessary, so that $\sigma_1 = \mathrm{id}$. Then

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

Define $\beta := \sigma_2(\alpha)\cdots\sigma_n(\alpha)$. Now $\beta \in K$ as $\alpha \in K$. We only need check that $\beta \in \mathcal{O}_K$. Now for all i, $\sigma_i(\alpha)$ is an algebraic integer since these are roots of the minimal polynomial $p_\alpha(x) \in \mathbb{Z}[x]$. But then $\beta := \sigma_2(\alpha)\cdots\sigma_n(\alpha)$ is a product of algebraic integers so that $\beta \in \mathcal{O}_K$. Then $\alpha\beta = 1$ with $\beta \in \mathcal{O}_K$. □

1.5 Integral Basis & Orders

We wanted to understand the additive abelian group structure of $\mathcal{O}_K$. Our next goal will be to prove that as an abelian group, $\mathcal{O}_K \cong \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n \cong \mathbb{Z}^n$. That is, $\{x_1, \ldots, x_n\}$ is an integral basis for $\mathcal{O}_K$.

Definition (Integral Basis)**.** A set of elements $\{x_1, \ldots, x_n\}$, where $x_i \in \mathcal{O}_K$ is called an integral basis for $\mathcal{O}_K$ if $\mathcal{O}_K \cong \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n \cong \mathbb{Z}^n$. We also say that this is an integral basis of K.

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

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

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

For $\delta : K \to \mathbb{C}$, denote by $\overline{\sigma} : K \hookrightarrow \mathbb{C}$ the embedding obtained by composing σ with complex conjugation. For $\alpha \in K$, we have $\overline{\sigma(\alpha)} = \overline{\sigma}(\alpha)$, essentially by definition.

Definition. $K_{\mathbb{R}} := \{(\alpha_\sigma)_\sigma \in \prod_\sigma \mathbb{C} \colon \overline{\alpha}_\sigma = \alpha_{\overline{\sigma}}\}$.

There is a map

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

But what is the dimension, as an $\mathbb{R}$-vector space, of $K_{\mathbb{R}}$? We know $K \otimes_{\mathbb{Q}} \mathbb{R} \cong K_{\mathbb{R}}$ and $\dim_{\mathbb{R}} K_{\mathbb{R}} = \frac{1}{2} \dim_{\mathbb{R}} (\prod_\sigma \mathbb{C})$, since if $\sigma = \overline{\sigma}$, then $\alpha_\sigma \in \mathbb{R}$, and if $\sigma \neq \overline{\sigma}$, then $\overline{\alpha}_\sigma = \alpha_{\overline{\sigma}}$, so knowing α_σ is enough to determine $\alpha_{\overline{\sigma}}$. [This is because $\overline{\alpha}_\sigma = \alpha_{\overline{\sigma}}$ if and only if $(\alpha_\sigma) = (\alpha_\sigma)$ and $\operatorname{Im}(\alpha_\sigma) = -\operatorname{Im}(\alpha_{\overline{\sigma}})$.] Then

$$\dim_{\mathbb{R}} K_{\mathbb{R}} = \frac{1}{2} \dim_{\mathbb{R}} \left(\prod_\sigma \mathbb{C} \right) = \frac{1}{2} \cdot 2n = n$$

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

Example 1.13.

(i) $\mathbb{Z} \subseteq \mathbb{R} \subseteq \mathbb{C}$ is discrete.

(ii) $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subseteq \mathbb{C}$ is discrete.

(iii) $\mathbb{R} \subseteq \mathbb{C}$ is not discrete. ◁

Example 1.14. Let $K = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. The two embeddings $K \hookrightarrow \mathbb{C}$ are

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

These embeddings are self-conjugate so the map $K \hookrightarrow K_{\mathbb{R}} = \mathbb{R}^2$ is given by $\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha))$. Note that $\mathbb{Z}[\sqrt{2}]$ is not discrete in $\mathbb{R}$ but considering $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}^2$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ is discrete.

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

We can picture this embedding as a lattice in $\mathbb{R}^2$ generated by vectors $\langle 1, -1 \rangle$ and $\langle \sqrt{2}, -\sqrt{2} \rangle$. ◁

This last example is not an aberration.

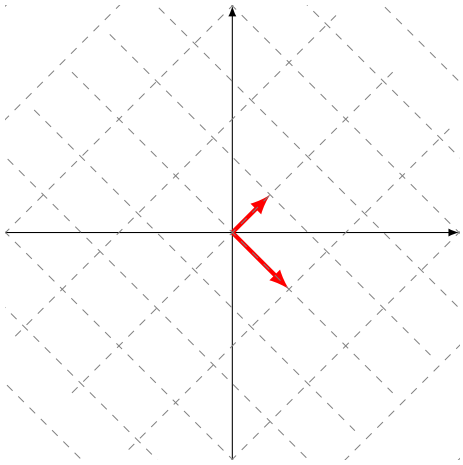


Figure 1: The lattice for $\mathbb{Z}[\sqrt{2}]$ generated by $\langle 1, 1\rangle$ and $\langle \sqrt{2}, -\sqrt{2}\rangle$.

Proposition 1.7. *Under the inclusion $\iota : K \hookrightarrow K_{\mathbb{R}}$, $\iota(\mathcal{O}_K)$ is a discrete subgroup of the $\mathbb{R}$-vector space $K_{\mathbb{R}}$; that is, all its points are isolated.*

Proof. Take $r > 0$. It suffices to show there are only finitely many $\alpha \in \mathcal{O}_K$ with $|\sigma(\alpha)| \leq r$ for all $\sigma : K \hookrightarrow \mathbb{C}$. Suppose $\alpha \in \mathcal{O}_K$ has this property. Then

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

as $\alpha \in \mathcal{O}_K$. The coefficients of the polynomial on the left are bounded, by the assumption that $|\sigma(\alpha)| \leq r$, in terms of r and the degree n. 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. □

While the next proposition is not directly related to the topics at hand, it will be useful later.

Proposition 1.8. *Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is a free $\mathbb{Z}$-module of rank at most n. Then any $\mathbb{Z}$-basis of H is linearly independent over $\mathbb{R}$.*

Proof. Let $V := \operatorname{span}_{\mathbb{R}} H$. Choose a basis for V in H. We may assume $\mathbb{Z}^r \subseteq H \subseteq \mathbb{R}^r$, where $r = \dim_{\mathbb{R}} V \leq n$. Replacing $\mathbb{R}^n$ by V if necessary, we may assume $\mathbb{Z}^n \subseteq H \subseteq \mathbb{R}^n$.

Now every coset of $H/\mathbb{Z}^n$ has a representative with $(a_1, \ldots, a_n) \in \mathbb{R}^n$ with $0 \leq a_i < 1$ (simply by rounding down each component and subtracting off a vector consisting of these numbers). Since H is discrete, there are only finitely many such representatives. Hence, the 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, i.e $H \cong \mathbb{Z}^n$. □

We can then obtain one of our long term goals, describing $(\mathcal{O}_K, +)$.

Proposition 1.9. *Let $K/\mathbb{Q}$ be a number field. Then $\mathcal{O}_K \cong \mathbb{Z}^n$ as an additive abelian group.*

Proof. By Proposition **??**, we know that $\mathcal{O}_K \cong \iota(\mathcal{O}_K) \subseteq K_{\mathbb{R}} \cong \mathbb{R}^n$. Therefore, $\mathcal{O}_K \cong \mathbb{Z}^r$, where $r \leq n$. Now take a basis $\{x_1, \ldots, x_n\}$ of K over $\mathbb{Q}$. After multiplication by some integer $m \geq 1$, i.e. clearing denominators (this does not affect linear independence), we may assume that $x_i \in \mathcal{O}_K$. Then $x_1, \ldots, x_n$ are linearly independent elements in $(\mathcal{O}_K, +)$. Therefore, $r \geq n$. But then we must have $r = n$. Hence, $\mathcal{O}_K \cong \mathbb{Z}^n$ as an additive abelian group. □

In general, how does one compute $\mathcal{O}_K$? We know how to compute $\mathcal{O}_K$ for quadratic extensions but very little else. We will introduce a 'good guess' for the ring of integers (this will be an order). For instance, if $K = \mathbb{Q}(\sqrt[3]{2})$, one would 'guess' $\mathcal{O}_K \stackrel{?}{=} \mathbb{Z}[\sqrt[3]{2}]$. The theory of discriminants will then allow us to check and adjust our guess, allowing us to work our way to the true ring of integers.

Definition (Order)**.** Let K be a number field. An order of K is a subring $R \subseteq K$ that is isomorphic as an additive group to $\mathbb{Z}^n$, where $n = [K : \mathbb{Q}]$.

Example 1.15. If $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathbb{Z}[\sqrt[3]{2}]$ is an order of K. ◁

Example 1.16. By Proposition **??**, $\mathcal{O}_K$ is always an order of K. ◁

Indeed, $\mathcal{O}_K$ is the maximal order of K. One can define $\mathcal{O}_K$ to be the maximal order of K. However, it does take a bit of work to then show it is equivalent to our definition.

Lemma 1.1. *For any order $R \subseteq K$, $R \subseteq \mathcal{O}_K$, i.e. $\mathcal{O}_K$ is the maximal order of K.*

Proof. Take $\alpha \in R$. Then $\alpha R \subseteq R$. Note that R is an order, i.e. a finitely generated $\mathbb{Z}$-submodule of K. But then by Propostion **??**, we know that $\alpha \in \mathcal{O}_K$. □

Now we have a symmetric (non-degenerate) $\mathbb{Q}$-bilinear pairing on K:

$$\begin{aligned} \langle\ ,\ \rangle &\longrightarrow \mathbb{Q} \\ (\alpha, \beta) &\longmapsto Tr_{K/\mathbb{Q}}(\alpha\beta) \end{aligned}$$

For any order R, $\langle\ ,\ \rangle : R \times R \to \mathbb{Z}$ since $(\alpha, \beta) \mapsto Tr_{K/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}$ by Corollary **??**.

Remark. This induces a pairing on $K \otimes_{\mathbb{Q}} \mathbb{R} \cong K_{\mathbb{R}}$ and gives it a Euclidean structure, i.e. a standard inner product on $\mathbb{R}^n$.

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

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

where $a_i, b_i \in \mathbb{Z}$. Expanding using linearity,

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

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

$$\operatorname{disc}(x_1, \ldots, x_n) := \det \left(Tr_{K/\mathbb{Q}}(x_i x_j) \right)_{i,j}$$

Note that the discriminant takes values in $\mathbb{Z}$. But how does this depend on the choice of basis? If one chose another basis of R, say $\{y_1, \ldots, y_n\}$, write

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

for some $B_{ij} \in \mathbb{Z}$. Define the matrix $B = (B_{ij})_{ij}$. The matrix B is invertible, i.e. $B \in \mathrm{GL}_n(\mathbb{Z})$ and clearly symmetric. It is routine to verify that

$$\left(Tr_{K/\mathbb{Q}}(y_i y_j) \right)_{ij} = B \left(Tr_{K/\mathbb{Q}}(x_i x_j) \right)_{ij} B^T$$

Then taking determinants, we have

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

but since $B \in \mathrm{GL}(\mathbb{Z})$, $\det(B) = \pm 1$. Therefore, the discriminant is independent of the choice of basis.

Definition (Discriminant (Order))**.** The discriminant of an order R is $\operatorname{disc}(R) := \operatorname{disc}(x_1, \ldots, x_n)$, where $\{x_1, \ldots, x_n\}$ is a basis of R.

We can now make our previous 'guess-and-check' notion for calculating $\mathcal{O}_K$ a bit more precise. For an order $R \subseteq \mathcal{O}_K$, $\operatorname{disc}(R) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K : R]^2$ (as we shall show). Then to find $\mathcal{O}_K$:

1. Guess an order R.

2. Compute $\mathrm{disc}(R)$, which gives a finite number of possibilities for $[\mathcal{O}_K : R]$.

3. Observe $R \subseteq \mathcal{O}_K \subseteq \frac{1}{m}R$. Find representatives for the cosets and determine which are algebraic integers.

Proposition 1.10. *For an order $R \subseteq K$, $\mathrm{disc}(R) \neq 0$.*

Proof. Suppose $0 \neq \alpha \in R$. Then $Tr_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = [K : \mathbb{Q}] \neq 0$. There is some $m \geq 1$ such that $m\alpha^{-1} \in R$. Then $\langle \alpha, \beta \rangle = m[K : \mathbb{Q}] \neq 0$ since $\langle\ ,\ \rangle$ is non-degenerate. □

1.6 Discriminants

Definition (Discriminant (Number Field))**.** If K is a number field, then we define $\mathrm{disc}(K) := \mathrm{disc}(\mathcal{O}_K)$.

Remark. There are many notations for what we have denoted as $\mathrm{disc}(K)$: $d_K, D_K, \Delta_K, \ldots$

Before we prove a useful lemma relating $\mathrm{disc}(R)$ and $\mathrm{disc}(\mathcal{O}_K)$, we shall remind the reader of Smith Normal Form.

Theorem 1.2 (Smith Normal Form)**.** *Let $B \in M_n(\mathbb{Z})$ be of rank r. There exists matrices $P, Q \in \mathrm{GL}(\mathbb{Z})$ such that*

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

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

Remark. One only need the entries of the matrix be in a PID and the matrix need not be square. One defines $d_i = \mathrm{div}_i(A)/\ \mathrm{div}_{i-1}(A)$, where div_i is the ith determinant divisor, i.e. the gcd of all the $i \times i$ minors of A and $d_0(A) := 1$.

Exercise: Prove the classification of finitely generated abelian groups using the Smith Normal Form.

Lemma 1.2. *Let $R \subseteq K$ be an order. Then* $\mathrm{disc}(R) = \mathrm{disc}(\mathcal{O}_K)[\mathcal{O}_K : R]^2$.

Proof. Write $\mathcal{O}_K = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n$ and let $R \subseteq \mathcal{O}_K$ be an order. Write $R = \mathbb{Z}y_1 \oplus \cdots \oplus \mathbb{Z}y_n$. For each of the y_i's, write

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

Define $B := (B_{ij})_{ij}$. We know that $B \in \mathrm{GL}_n(\mathbb{Z})$. Observe that $[\mathcal{O}_K \colon R] = [\mathbb{Z}^n \colon B(\mathbb{Z}^n)]$. By some previous remarks,

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

Therefore, $\operatorname{disc}(R) = \det(B)^2 \operatorname{disc}(\mathcal{O}_K)$. It remains to show that $\det(B) = \pm[\mathcal{O}_K \colon R]$. Without loss of generality, assume that B is of the form

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

with $d_i \geq 1$ and $\det B \neq 0$. [Using Smith Normal Form, we replace B by PBQ. This does not change $[\mathbb{Z}^n \colon B(\mathbb{Z}^n)]$ or $\pm \det(B)$ since P, Q are invertible integer matrices. Then $\det(P), \det(Q) \in \{\pm 1\}$.] Now $\det(B) = d_1 d_2 \cdots d_n$. Therefore,

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

and

$$\mathbb{Z}^n / B(\mathbb{Z}^n) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z},$$

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

Example 1.17. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. Now $R = \mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ is an order of K. Furthermore,

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

So $4d = \operatorname{disc}(R) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K \colon R]^2$. Since d is squarefree, this implies that $[\mathcal{O}_K \colon R] \in \{1, 2\}$; that is, $\mathcal{O}_K = R$ or is index 2 larger, i.e.

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

Now $R/\frac{1}{2}R$ has coset representatives $1, \frac{1}{2}, \frac{\sqrt{d}}{2}$, and $\frac{1+\sqrt{d}}{2}$. One need only check which of these are algebraic integers. It is routine to check that 1 is an algebraic integer, $\frac{1}{2}, \frac{\sqrt{d}}{2}$ are not algebraic integers, and $\frac{1+\sqrt{d}}{2}$ is sometimes an algebraic integer (if and only if $d \equiv 1 \mod 4$). Therefore,

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

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

◁

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

Lemma 1.3. *Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the complex embeddings of K into $\mathbb{C}$. Then for $x_1, \ldots, x_n \in \mathcal{O}_K$,*

$$\operatorname{disc}(x_1, \ldots, x_n) = \Big(\det\left(\sigma_i(x_j)\right)_{i,j}\Big)^2 = \left[\det\begin{pmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \cdots & \sigma_n(x_n) \end{pmatrix}\right]^2$$

Proof. Recall $Tr_{K/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x)$. Let $A := (\sigma_i(x_j))_{ij}$. Then we have

$$\begin{aligned} \operatorname{disc}(x_1, \ldots, x_n) &= \det\Big(Tr_{K/\mathbb{Q}}(x_i x_j)\Big)_{i,j} \\ &= \det\left(\sum_{k=1}^n \sigma_k(x_i)\sigma_k(x_j)\right) \\ &= \det\left(\sum_{k=1}^n \sigma_k(x_i x_j)\right) \\ &= \det(A^T A) \\ &= [\det(A)]^2. \end{aligned}$$

□

Example 1.18. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer. Consider $R = \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Q}(\sqrt{d}) = K$. The two complex embeddings of K into $\mathbb{C}$ are

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

Then by Lemma **??**

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

◁

The term 'discriminant' will already be familiar to the reader from the discriminant of a polynomial.

Definition (Discriminant (Polynomial))**.** If $f(x) \in \mathbb{Q}[x]$ is a monic polynomial of degree $n \geq 1$, the discriminant of f is

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

where $\alpha_1, \ldots, \alpha_n$ are the roots of f in $\mathbb{C}$.

It is worth noting that $\operatorname{disc}(f) \in \mathbb{Q}$ and if $f \in \mathbb{Z}[x]$ then $\operatorname{disc}(f) \in \mathbb{Z}$. Note also that if the polynomial is not monic, one can always divide by the leading coefficient and use the fact that if $\alpha \in \mathbb{Q}$, then $\operatorname{disc}(\alpha x) = \alpha^n \operatorname{disc}(x)$, where $n = [K : \mathbb{Q}]$.

Example 1.19. Here are some discriminants of several specific polynomials:

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

◁

We shall connect the discriminant of a number field with that of the discriminant of a polynomial.

Lemma 1.4. *If $\alpha \in \mathcal{O}_K$ is such that $K = \mathbb{Q}(\alpha)$ (so that $\mathbb{Z}[\alpha]$ 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 $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the complex embeddings of K into $\mathbb{C}$. The roots of $p_\alpha(x)$ are $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. Write $\alpha_i = \sigma_i(\alpha)$. The order $\mathbb{Z}[\alpha]$ has a integral $\mathbb{Z}$-basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Therefore,

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

□

Example 1.20. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 + x + 1$. Observe that $f(x)$ is irreducible and then $[K : \mathbb{Q}] = 3$. Now $\mathbb{Z}[\alpha]$ is an order of K with

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

But $\operatorname{disc}(\mathbb{Z}[\alpha]) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$. Since 31 is prime, we must have $[\mathcal{O}_K : \mathbb{Z}[\alpha] = 1$ which implies that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(K) = -31$. ◁

Example 1.21. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - x^2 - 2x - 8$. Consider the order $\mathbb{Z}[\alpha]$ of K.

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

Then $[\mathcal{O}_K : \mathbb{Z}[\alpha]] \in \{1, 2\}$. Therefore,

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

The group $\frac{1}{2}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha$ has coset representatives $\frac{a}{2} + \frac{b}{2}\alpha + \frac{c}{2}\alpha^2$, where $a, b, c \in \{0, 1\}$. We need only check which of these eight elements are algebraic integers. Let $\theta := \frac{\alpha + \alpha^2}{2}$. Now K has $\mathbb{Q}$-basis $\{1, \alpha, \alpha^2\}$ and θ acts on this by

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

Therefore, θ is a root of

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

But then $\theta \in \mathcal{O}_K$. Therefore, $\mathcal{O}_K = \mathbb{Z}1 \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\frac{\alpha+\alpha^2}{2} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\theta$. Note that $\mathcal{O}_K \neq \mathbb{Z}[\beta]$ for any $\beta \in \mathcal{O}_K$ — a result due to Dedekind. ◁

Example 1.22. In the previous example, we saw that for $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = x^3 - x^2 - 2x - 8$, $\mathcal{O}_K \neq \mathbb{Z}[\beta]$ for any $\beta \in \mathcal{O}_K$. This is not the only example. For example, if $K = \mathbb{Q}(\sqrt[3]{19})$, then $\mathcal{O}_K \neq \mathbb{Z}[\sqrt[3]{19}]$ but rather $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega + \mathbb{Z}\frac{1+\omega+\omega^2}{3}$, where $\omega = \sqrt[3]{19}$. ◁

We have seen how the discriminant relates to $\mathcal{O}_K$. We shall now see how the discriminant relates to the norm.

Lemma 1.5. *Let $K = \mathbb{Q}(\alpha)$ be a number field, where $\alpha \in \mathcal{O}_K$. If $f \in \mathbb{Z}[x]$ is the minimal polynomial of α over $\mathbb{Q}$, then*

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

In particular, $\operatorname{disc}(\mathbb{Z}[\alpha]) \in \mathbb{Q}$.

Proof. The first equality was Lemma **??**. For the second equality, let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the complex embeddings of K into $\mathbb{C}$. By rearranging terms,

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

However, we know $f = \prod_i (x - \sigma_i(\alpha))$. Using the product rule, this gives

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

But then $f'(\sigma_j(\alpha)) = \prod_{i \neq j}(\sigma_j(\alpha) - \sigma_i(\alpha))$ since all but one term vanishes. Using this in the above along with the fact that the σ_i fix $\mathbb{Q}$ (hence fix the coefficients of f'), we have

$$\begin{aligned} (-1)^{\binom{n}{2}} \prod_j \prod_{i \neq j} (\sigma_j(\alpha) - \sigma_i(\alpha)) &= (-1)^{\frac{n(n-1)}{2}} \prod_j f'(\sigma_j(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_j \sigma_j(f'(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha)) \end{aligned}$$

□

Example 1.23 (pth Cyclotomic Field)**.** Fix an odd prime p. Let $\zeta \neq 1$ be a pth root of unity, i.e. $\zeta^p = 1$. Let $K = \mathbb{Q}(\zeta)$ be the pth cyclotomic field. Define

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

Observe that $f(\zeta) = 0$ and that f is irreducible (examine $f(x+1)$, use Eisenstein's criterion, then invoke Gauß' lemma). In particular, $[K\colon \mathbb{Q}] = p - 1$. Now what is $\mathcal{O}_K$. We have the 'obvious guess' of the order $\mathbb{Z}[\zeta]$. We need to check this guess. We know $\operatorname{disc}(\mathbb{Z}[\zeta]) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{K/\mathbb{Q}}(f'(\zeta))$. But what is $f'(\zeta)$? We first calculate $f'(x)$, then evaluate at ζ:

$$\begin{aligned} (x-1)f(x) &= x^p - 1 \\ f(x) + (x-1)f'(x) &= px^{p-1} \\ f'(\zeta) &= \frac{p\,\zeta^{p-1}}{\zeta - 1} \end{aligned}$$

Note that $[K\colon \mathbb{Q}] = \phi(p) = p - 1$ and $\zeta \in \mathcal{O}_K^\times$. Let $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of K into $\mathbb{C}$. Then noting that $p - 1$ is even and $f(x) = \prod_i (x - \sigma_i(\zeta))$, we have

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

We know $(\zeta - 1)f'(\zeta) = p\zeta^{p-1}$. Taking norms gives

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

Therefore, $\operatorname{disc}(\mathbb{Z}[\zeta]) = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2} = (-1)^{\frac{p-1}{2}} p^{p-2}$, since p is odd. Note that we lose nothing by assuming that p is odd: if $p = 2$, then $\mathbb{Q}(\zeta) = \mathbb{Q}$. Then if $\mathbb{Z}[\zeta] \subsetneq \mathcal{O}_K$, it

must be that $[\mathcal{O}_K : \mathbb{Z}[\zeta]] = p^e$ for some $e \geq 1$. After possibly multiplying by a power of p, we know there is a $\alpha \in \mathcal{O}_K$ such that $\alpha \notin \mathbb{Z}[\zeta]$ and $p\alpha \in \mathbb{Z}[\zeta]$. We know $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$. Then α can be written

$$\alpha = \frac{a_0}{p} + \frac{a_1}{p}(\zeta - 1) + \cdots + \frac{a_{p-2}}{p}(\zeta - 1)^{p-2},$$

where $a_i \in \mathbb{Z}$ with not all a_i divisible by p. Subtracting multiples of p from those terms divisible by p, we may assume a_i is not divisible by p for $0 \leq i \leq p-2$. Hence, we can write

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

where $p \nmid a_i$. Multiplying by $\frac{p}{(\zeta-1)^{i+1}}$, we have

$$\frac{p\alpha}{(\zeta-1)^{i+1}} = \frac{a_1}{\zeta - 1} + \underbrace{a_{i+1} + a_{i+2}(\zeta - 1) + \cdots + a_{p-2}(\zeta - 1)^{p-2-(i+1)}}_{\in \mathbb{Z}[\zeta]}$$

Now $N_{K/\mathbb{Q}}(\frac{a_i}{\zeta-1}) = \frac{a_i^{p-1}}{p} \notin \mathbb{Z}$ as $p \nmid a_i$. But then $\frac{a_i}{\zeta-1} \notin \mathcal{O}_K$. But then using the above equality, this shows $\frac{p}{(\zeta-1)^{i+1}}\alpha \notin \mathcal{O}_K$. But as $\alpha \in \mathcal{O}_K$, this shows $\frac{p}{(\zeta-1)^{i+1}} \notin \mathcal{O}_K$. Therefore, $\frac{p}{(\zeta-1)^{i+1}} \notin \mathbb{Z}[\zeta]$. On the other hand,

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

Using the fact that $\zeta^i - 1 = (\zeta - 1)(1 + \zeta + \cdots + \zeta^{i-1})$, this shows that $(\zeta - 1)^{p-1} \mid p$ in $\mathbb{Z}[\zeta]$. But as $i + 1 \leq p - 1$, this contradicts the fact that $\frac{p}{(\zeta-1)^{i+1}} \notin \mathbb{Z}[\zeta]$. Therefore, we know

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}[\zeta] \\ \operatorname{disc} \mathcal{O}_K &= (-1)^{\frac{p-1}{2}} p^{p-2} \end{aligned}$$

Note that $\frac{p}{(\zeta-1)^{p-1}} \in \mathbb{Z}[\zeta]$ and $N_{K/\mathbb{Q}}(\frac{p}{(\zeta-1)^{p-1}}) = \frac{p^{p-1}}{p^{p-1}} = 1$ so that $p = u(\zeta - 1)^{p-1}$ for some $u \in \mathbb{Z}[\zeta]^\times$. ◁

Remark. Choose $m \geq 1$ and let ζ_m be the primitive mth root of unity. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ and $\operatorname{disc} \mathcal{O}_K \mid m^{\phi(m)}$.

2 Unique Factorization and Ramification in $\mathcal{O}_K$

2.1 Prime Ideals in $\mathcal{O}_K$

Let $K/\mathbb{Q}$ be a number field of degree n.

Proposition 2.1. *If $I \subseteq \mathcal{O}_K$ is a nonzero ideal, then $\mathcal{O}_K/I$ is a finite ring.*

Proof. Take $0 \neq \alpha \in I$. Since$\alpha\mathcal{O}_K \subseteq I$, we have a surjective map of rings

$$\mathcal{O}_K/\alpha\mathcal{O}_K \longrightarrow\!\!\!\!\!\rightarrow \mathcal{O}_K/I$$

It suffices to show that $\mathcal{O}_K/\alpha\mathcal{O}_K$ is finite. Then without loss of generality, we may assume $I = \alpha\mathcal{O}_K$. Consider the multiplication by α map: $\mu_\alpha : \mathcal{O}_K \to \mathcal{O}_K$, $x \mapsto \alpha x$. Choosing an integral basis for $\mathcal{O}_K$, we can write $\mathcal{O}_K \cong \mathbb{Z}^n$ as an abelian group. Then μ_α can be written as a matrix $B \in M_n(\mathbb{Z})$. Observe

$$\#\mathcal{O}_K/\alpha\mathcal{O}_K = [\mathcal{O}_K \colon \alpha\mathcal{O}_K] = [\mathcal{O}_K \colon \mu_\alpha(\mathcal{O}_K)] = [\mathbb{Z}^n \colon B(\mathbb{Z}^n)]$$

Note also that $\det B = \det(\mu_\alpha) = N_{K/\mathbb{Q}}(\alpha) \neq 0$. Using the Smith Normal Form, we may write

$$B' := PBQ = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix},$$

where $P, Q \in \mathrm{GL}_n(\mathbb{Z})$ and $d_i \geq 1$. But then

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

□

Remark. In Proposition **??**, we actually showed that $\#\mathcal{O}_K/\alpha\mathcal{O}_K = |N_{K/\mathbb{Q}}(\alpha)|$.

Corollary 2.1. *If $I \subseteq \mathcal{O}_K$ is a prime ideal, then $\mathcal{O}_K/I$ is a field.*

Proof. By Proposition **??**, we know that $\mathcal{O}_K/I$ is finite. But I is a prime ideal so that $\mathcal{O}_K/I$ is a finite integral domain, hence a field. □

Proposition 2.2. *All nonzero prime ideals in $\mathcal{O}_K$ are maximal.*

Proof. If I is a nonzero prime ideal in $\mathcal{O}_K$, then we know $\mathcal{O}_K/I$ is a field. But then I must be maximal. □

Definition (Norm (Ideal))**.** For a nonzero ideal $I \subseteq \mathcal{O}_K$, we define the norm of I to be $N(I) = \#(\mathcal{O}_K/I)$.

This definition replicates the traditional case: if $I = (\alpha) = \alpha\mathcal{O}_K$, then $N(I) = \#(\mathcal{O}_K/I) = \#(\mathcal{O}_K/\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$. Moreover, observe that there are finitely many ideals of a given norm: if $N(I) = m$, then $I \subseteq \mathcal{O}_K$ is of index m, i.e. $m\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$. But then $m\mathcal{O}_K \subseteq \mathcal{O}_K$ is of index m. Since $\mathcal{O}_K \cong \mathbb{Z}^n$, we know $\mathcal{O}_K/m\mathcal{O}_K \cong \mathbb{Z}^n/m\mathbb{Z}^n$ as abelian groups. Then there can be only finitely many such ideals.

Furthermore, if I is a nonzero ideal of $\mathcal{O}_K$, then $I \cong \mathbb{Z}^n$ as additive groups. In particular, $\mathcal{O}_K$ is noetherian: all ideals of $\mathcal{O}_K$ are finitely generated $\mathcal{O}_K$-modules. [In fact, we have the stronger result that all ideals of $\mathcal{O}_K$ are finitely generated abelian groups.]

2.2 Factoring in $\mathcal{O}_K$

The goal for constructing $\mathcal{O}_K$ was to mimic $\mathbb{Z} \subseteq \mathbb{Q}$ but instead for a generally number field $K/\mathbb{Q}$. Thus far, we have seen $\mathcal{O}_K$ is a useful ring that does much of what we want. However, one of the vital properties of $\mathbb{Z}$, the unique factorization of elements into products of primes, does not generally hold for $\mathcal{O}_K$.

Example 2.1. Let $K = \mathbb{Q}(\sqrt{-5})$ so that $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$. We first show that $\mathcal{O}_K^\times = \{\pm 1\}$. Suppose that $\alpha \in \mathcal{O}_K^\times$, where $\alpha = a + b\sqrt{-5}$. We know α is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. But then $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2 = \pm 1$. Therefore, $b = 0$ so $a \in \{\pm 1\}$ forcing $\mathcal{O}_K^\times = \{\pm 1\}$. Now observe

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

We claim these are two distinct factorizations of 6 into irreducibles in $\mathcal{O}_K$. To see $1 + \sqrt{-5}$ is irreducible, suppose $1 + \sqrt{-5} = \alpha\beta$, where $\alpha, \beta \in \mathcal{O}_K$ are not units. Then

$$N_{K/\mathbb{Q}}(1 + \sqrt{-5}) = N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$$
$$6 = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$$

But $N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta) \in \mathbb{Z}$ since $\alpha, \beta \in \mathcal{O}_K$. Since we assumed α, β were not units, $|N_{K/\mathbb{Q}}(\alpha)| \neq 1$. It must be then that $N_{K/\mathbb{Q}}(\alpha) \in \{2, 3\}$. But neither $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2 = 2$ nor $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2 = 3$ have integer pairs of solutions. Therefore, one of $N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta)$ is ± 1 so that one of α, β must be a unit. Then $1 + \sqrt{-5}$ is irreducible. This works the same for showing 2, 3, and $1 - \sqrt{-5}$ are irreducible. Furthermore since $\mathcal{O}_K^\times = \{\pm 1\}$, it is clear that none of 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are associates. But then $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is two distinct factorization of 6 into irreducibles in $\mathcal{O}_K$. Hence, unique factorization fails for $\mathcal{O}_K$. ◁

The previous example shows that unique factorization in $\mathcal{O}_K$ fails for elements. However, we can recover unique factorization if instead we work on the level of ideals in $\mathcal{O}_K$ instead. We are going to see that all ideals in $\mathcal{O}_K$ factor into products of prime ideals in $\mathcal{O}_K$. Before proving the theorem, let us see an example of this type of factorization.

Example 2.2. Let $K = \mathbb{Q}(\sqrt{-5})$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We claim $\mathfrak{p} = (2, 1+\sqrt{-5}) = 2\mathcal{O}_K + (1+\sqrt{-5})\mathcal{O}_K \subseteq \mathcal{O}_K$ is a prime ideal. This follows from the fact that

$$\mathcal{O}_K/\mathfrak{p} = \frac{\mathbb{Z}[\sqrt{-5}]}{(2, 1+\sqrt{-5})} = \mathbb{Z}/2\mathbb{Z}$$

is an integral domain. Now

$$\begin{aligned}\mathfrak{p}^2 &= (2, 1+\sqrt{-5})(2, 1+\sqrt{-5}) \\ &= (4, 2(1+\sqrt{-5}), (1+\sqrt{-5})^2) \\ &= (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})\end{aligned}$$

But then $\mathfrak{p}^2$ contains $(2+2\sqrt{-5}) - (-4+2\sqrt{-5}) = 6$ and hence then contains $6-4=2$. But then all the generators of $\mathfrak{p}^2$ are multiples of $2 \in \mathfrak{p}^2$ so that $\mathfrak{p}^2 = (2)$. Note that while $\mathfrak{p}^2$ is principal, $\mathfrak{p}$ itself cannot be principle for then 2 would a factorization, contradicting its irreducibility.

Now let $\mathfrak{q}_1 = (3, 1+\sqrt{-5})$ and $\mathfrak{q}_2 = (3, 1-\sqrt{-5})$ be ideals of $\mathcal{O}_K$. As above, one can check that these ideals are prime. Further,

$$\mathfrak{q}_1\mathfrak{q}_2 = (9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6) = (3),$$

since $9-6 = 3 \in \mathfrak{q}_1\mathfrak{q}_2$ and all the generators of $\mathfrak{q}_1\mathfrak{q}_2$ are multiples of 3. But then

$$(6) = (2)(3) = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2$$

is a factorization of $(6) = 6\mathcal{O}_K$ into prime ideals. But from Example **??**, we knew $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Assuming unique factorization, the factorization for (6) should then give factorizations for $(1+\sqrt{-5})$ and $(1-\sqrt{-5})$. Observe

$$\mathfrak{p}\mathfrak{q}_1 = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5})$$

so that $(3+3\sqrt{-5}) - (2+2\sqrt{-5}) = 1+\sqrt{-5} \in \mathfrak{p}\mathfrak{q}_1$. Therefore, $\mathfrak{p}\mathfrak{q}_1 = (1+\sqrt{-5})$. Similarly, we have $\mathfrak{p}\mathfrak{q}_2 = (1-\sqrt{-5})$. ◁

Notice in the previous example, unique factorization failed for the element 6 but held for the ideal (6). Since we can recover unique factorization into prime ideals in $\mathcal{O}_K$, it will be necessary to study the structure of prime ideals in $\mathcal{O}_K$.

Remark. Unique factorization fails for every order $R \subsetneq \mathcal{O}_K \subseteq K$.

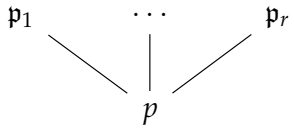
Take $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ to be a prime ideal. Note that $\mathfrak{p} \cap \mathbb{Z} = (p)$, where p is prime. We know that $\mathfrak{p}$ is maximal so that $\mathcal{O}_K/\mathfrak{p}$ is a field. Recall that if K is a field, char K is the cardinality of the kernel of the unique map $\mathbb{Z} \to K$ (if the kernel is infinite, we define char $K := 0$). It must be that $\mathcal{O}_K/\mathfrak{p} = p$, where P is prime. The ideal $p\mathcal{O}_K$ must factor into a product of prime ideals in $\mathcal{O}_K$, say $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ for distinct prime ideals $\mathfrak{p}_i$ and $e_i \geq 1$.

Definition ((Un)Ramified)**.** Let p be prime. If $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ is factorization of the ideal $p\mathcal{O}_K$ into distinct primes $\mathfrak{p}_i$ and $e_i \geq 1$, we say that p is ramified in K if $e_i > 1$ for some i and unramified in K if $e_i < 1$ for all i.

We shall eventually show that p is ramified in K if and only if p divides disc K. Hence, there are only finitely many ramified primes in K. Now $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ so that $\mathfrak{p} \supseteq p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Recall the following result:

Lemma 2.1. *Let $\mathfrak{p}$ be a prime ideal of R and I, J be ideals of R. If $\mathfrak{p} \subseteq IJ$, then $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$.*

The the lemma, we know $\mathfrak{p} \subseteq \mathfrak{p}_i$ for some i. However, $\mathfrak{p}_i$ is maximal forcing $\mathfrak{p} = \mathfrak{p}_i$. Therefore, $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ appears in the factorization of $p\mathcal{O}_K$, where $p = \text{char } \mathcal{O}_K/\mathfrak{p}$. Then the primes $\mathfrak{p}_i$ 'lie over' p.



We shall now see how to factor $p\mathcal{O}_K$ for 'most' primes p. Suppose $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. By maximality for $i \neq j$, $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathcal{O}_K$. [If this were not the case, there would be a maximal ideal $\mathfrak{q}$ such that $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} \subseteq \mathfrak{q}$. But then $\mathfrak{p}_i^{e_i}, \mathfrak{p}_j^{e_j} \subseteq \mathfrak{q}$ and then $\mathfrak{p}_i, \mathfrak{p}_j \subseteq \mathfrak{q}$. Since $\mathfrak{p}_i, \mathfrak{p}_j$ are maximal, $\mathfrak{p}_i = \mathfrak{q} = \mathfrak{p}_j$.] Recall the Chinese Remainder Theorem:

Theorem 2.1 (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 $\phi : R \to R/I_1 \oplus \cdots R/I_m$ given by $r \mapsto to(r + I_1, \ldots, r + I_m)$ is surjective with kernel $I_1 \cap \cdots \cap I_m = I_1 \cdots I_m$.*

The Chinese Remainder Theorem gives

$$p\mathcal{O}_K \cong \prod_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}_i^{e_i} = \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$$

Now let K be a number field and $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ an order. Define $g(x) \in \mathbb{Z}[x]$ to be the minimal polynomial of α. Take $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ (this is 1 if $\mathcal{O}_K = \mathbb{Z}[\alpha]$). Define also $\overline{g} := g \mod p$, the polynomial obtained by reducing the coefficients of $g(x) \mod p$. Then we have $\overline{g} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$ with the $\overline{g}_i \in \mathbb{F}_p[x]$ distinct, monic, irreducible, and $e_i \geq 1$. For each i, choose a lift $g_i \in \mathbb{Z}[x]$ with $g_i \mod p = \overline{g}_i$. Note that one can choose g_i to be monic with the same degree as g_i, say f_i. Define the ideal $\mathfrak{p}_i := (p, g_i(\alpha))$.

Proposition 2.3. *The ideal $\mathfrak{p} = (p, g_i(\alpha)) \subseteq \mathcal{O}_K$ is prime and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Moreover, $[\mathcal{O}_K/\mathfrak{p}_i \colon \mathbb{F}_p] = f_i$.*

Proof. From the fact that $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$, we have a map $\phi : \mathbb{Z}[\alpha]/(p) \to \mathcal{O}_K/(p)$. We claim this map is an isomorphism. Both have cardinality p^n:

$$\begin{aligned} \mathcal{O}_K &\cong \mathbb{Z}^n & \mathbb{Z}[\alpha] &\cong \mathbb{Z}^n \\ \mathcal{O}_K/p\mathcal{O}_K &\cong \mathbb{Z}^n/p\mathbb{Z}^n & \mathbb{Z}[\alpha]/(p) &\cong \mathbb{Z}^n/p\mathbb{Z}^n \end{aligned}$$

Now $\#\operatorname{coker}\phi$ divides p^n and $[\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$ but p^n and $[\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$ are relatively prime by assumption.This forces $\operatorname{coker}\phi$ to be trivial so that ϕ is surjective. But then ϕ is a surjective map between finite sets of the same cardinality. Therefore, ϕ is an isomorphism.

We have isomorphisms

$$\begin{aligned} \mathcal{O}_K \Big/ p\mathcal{O}_K &\cong \mathcal{O}_K \Big/ \mathfrak{p}_i \\ &\cong \mathbb{Z}[x] \Big/ (p, g(x)) \\ &\cong \mathbb{F}_p[x] \Big/ (\overline{g}) \\ &\overset{\text{C.R.T.}}{\cong} \prod_i \mathbb{F}_p[x] \Big/ (\overline{g}_i^{e_i}) \end{aligned}$$

The homomorphisms $\mathcal{O}_K \twoheadrightarrow \mathbb{F}_p[x] \,/\, (\overline{g}_i^{e_i})$ have kernel $I_i = (p, g_i(\alpha)^{e_i})$ (the ambivalence in choice of lift is absorbed by p). Hence, $\mathcal{O}_K \,/\, I_i \cong \mathbb{F}_p[x] \,/\, (\overline{g}_i^{e_i})$. Therefore, the map

$$\mathcal{O}_K \longrightarrow\!\!\!\!\!\rightarrow \textstyle\prod_{i=1}^r \mathcal{O}_K \,/\, I_i = \mathcal{O}_K \,/\, I_1 \times \cdots \times \mathcal{O}_K \,/\, I_r$$

has kernel $p\mathcal{O}_K$. But by the Chinese Remainder Theorem, the kernel is $I_1 \cap \cdots \cap I_r = I_1 \cdots I_r$. Therefore, $p\mathcal{O}_K = I_1 \cdots I_r$. It is routine to verify that $I_i = \mathfrak{p}_i^{e_i}$. Finally,

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

□

Remark. The degree of the extension restricts possible factorizations in that

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

In fact, this is true for all p.

Example 2.3. Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer, and choose an odd prime p. Let $\alpha = \sqrt{d}$ and $g(x) = x^2 - d$. Note that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, since $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is 1 or 2. Since $\sum_{i=1}^{r} e_i f_i = 2$, we have a limited number of possibilities for the factorization of $p\mathcal{O}_K$:

r	e_i	f_i	$p\mathcal{O}_K$	$\mathcal{O}_K \,/\, \mathfrak{p}_i$
2	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathbb{F}_p$
1	2	1	$\mathfrak{p}^2$	$\mathbb{F}_p$
1	1	2	$\mathfrak{p}$	$\mathbb{F}_{p^2}$

In the first case, we say, '$\mathfrak{p}$ splits in K'. In the second case, we say, '$\mathfrak{p}$ ramifies in K'. In the third case, we say, '$\mathfrak{p}$ is inert in K'. But given an odd prime p, can we say which case will occur? The possibilities are characterized by the possible factorizations of $x^2 - d \bmod p$:

(i) p splits in K if and only if $p \nmid d$ and d is a square mod p

(ii) p ramifies in K if and only if $p \mid d$

(iii) p is inert in K if and only if $p \nmid d$ and d is not a square mod p

If $p = 2$, there are fewer possibilities: if $d \not\equiv 1 \mod 4$, then there was no reason for the exclusion and it ramifies as above. If $d \equiv 1 \mod 4$, take $\alpha = \frac{1+\sqrt{d}}{2}$ and $g(x) = x^2 - x + \frac{1-d}{4}$. A routine calculation shows that it depends on if $d \equiv 1 \mod 8$. ◁

Remark. In Example **??**, quadratic reciprocity will describe all three cases, depending only on the value p modulo $4d$. This will be proven later.

Example 2.4. Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = \sqrt[3]{2}$. Let $g(x) = x^3 - 2$. Then

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

Hence, 5 and 31 split while 7 is inert in K. ◁

2.3 Fractional Ideals

In order describe unique factorization of ideals into prime ideals, we will need to extend our notion of an ideal.

Definition (Fractional Ideal)**.** A fractional ideal of K is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.

Note that a fractional ideal I must also be itself finitely generated as $\mathcal{O}_K$ is noetherian. The next lemma will demonstrate the reason for the name; fractional ideals are ideals of $\mathcal{O}_K$ after 'clearing denominators'.

Lemma 2.2. *Let I be a nonzero $\mathcal{O}_K$-submodule of K. The following are equivalent:*

(i) *I is a fractional ideal*

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

(iii) *$dI \subseteq \mathcal{O}_K$ for some $0 \neq d \in \mathcal{O}_K$*

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

Proof.
$(i) \to (ii)$: Suppose $I = \mathcal{O}_K x_1 + \cdots + \mathcal{O}_K x_r$, where $x_i \in K$. Then there exists $d_i \geq 1$ such that $d_i x_i \in \mathcal{O}_K$. Let $d = \prod d_i$. Then $dI \subseteq \mathcal{O}_K$.

$(ii) \to (iii)$: This is clear as $d \in \mathcal{O}_K$.

$(iii) \to (iv)$: Define $J := dI$. Then $I = d^{-1}J$.

$(iv) \to (i)$: I is a finitely generated $\mathcal{O}_K$-submodule of K as ideals of $\mathcal{O}_K$ are finitely generated. □

Given two fractional ideals I, J of K, there is another fractional ideal, IJ. If I, J, and K are fractional ideals, a few easy properties follow:

- $IJ = JI$
- $I(JK) = (IJ)K$
- $I\mathcal{O}_K = \mathcal{O}_K = I$ (I is an O_K-module)

Definition (Fractional Ideals)**.** Let $\mathcal{J}_K$ be the set of fractional ideals of K.

We shall see that $\mathcal{J}_K$ is an abelian group under multiplication with identity $\mathcal{O}_K$. The last point above shows that the identity exists. We now need to establish the existence of inverses.

Definition (Principal Fractional Ideals)**.** Let $\mathcal{B}_K \subseteq \mathcal{J}_K$ be the set of group of principal fractional ideals, i.e. $x\mathcal{O}_K$ with $x \in K^\times$.

$\mathcal{B}_K$ is clearly a group with identity $\mathcal{O}_K$ and if $x\mathcal{O}_K \in \mathcal{B}_K$ the inverse is $x^{-1}\mathcal{O}_K$. Moreover, $\mathcal{B}_K \subseteq \mathcal{J}_K$. Once we have established $\mathcal{J}_K$ is a group, we shall define the ideal class group:

Definition (Ideal Class Group)**.** The ideal class group of K is

$$\mathrm{C}\ell_K := \mathcal{J}_K \Big/ \mathcal{B}_K$$

We shall see that $\mathrm{C}\ell_K$ is in fact finite.

Example 2.5. $\mathrm{C}\ell_{\mathbb{Q}(\sqrt{-5})} \cong \mathbb{Z} \,/\, 2\mathbb{Z}$ ◁

For now, we continue to show that $\mathcal{J}_K$ is an group under multiplication. We first define a candidate for inverses. For $I \in \mathcal{J}_K$, define

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

Note that $\widetilde{I}$ is a fractional ideal: fix $0 \neq \alpha \in I$. Then $\alpha\widetilde{I} \subseteq \mathcal{O}_K$. By Proposition **??**, $\widetilde{I}$ is a finitely generated $\mathcal{O}_K$-module.

Lemma 2.3. *If $J \in \mathcal{J}_K$ satisfies $IJ = \mathcal{O}_K$, then $\widetilde{I} = J$.*

Proof. If $I\widetilde{I} = \mathcal{O}_K$, then $J \subseteq \widetilde{I}$. Multiplication by I gives

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

Hence, $I\widetilde{I} = O_K$. Then

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

□

So if an inverse for $I \in \mathcal{J}_K$ exists, it must be $\widetilde{I}$.

Lemma 2.4. *Every nonzero ideal of $\mathcal{O}_K$ contains a product of nonzero prime ideals.*

Proof. Suppose this were not the case. The set of all ideals not containing a product of nonzero prime ideals must have a maximal element with respect to inclusion, say I. Now I itself cannot be prime. Therefore, there are $a, b \in \mathcal{O}_K$ such that $ab \in I$ and $a \notin I$, $b \notin I$. Then the ideals $\langle a \rangle + I$ and $\langle b \rangle + I$ are strictly larger than I. But then they must contain a product of nonzero primes

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

But then

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

But then I contains a product of ideals, a contradiction. Then the set of ideals not containing a product of nonzero prime ideals must be empty. □

Example 2.6. Let $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ with ideals $\mathfrak{q} = (3, 1+\sqrt{-5})$ and $\mathfrak{q}' = (3, 1-\sqrt{-5})$. We saw $\mathfrak{q}\mathfrak{q}' = (3)$, so $\mathfrak{q}(\frac{1}{3}\mathfrak{q}') = \mathcal{O}_K$. Then

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

◁

We shall now see that prime ideals are invertible.

Proposition 2.4. *If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a nonzero prime ideal, then $\mathfrak{p}\widetilde{\mathfrak{p}} = \mathcal{O}_K$.*

Proof. First, we need to show that $\widetilde{p} \supsetneq \mathcal{O}_K$. We know that $\widetilde{p} \supseteq \mathcal{O}_K$. Choose a nonzero $a \in \mathfrak{p}$. Then $\mathfrak{p} \supseteq (a)$. By Lemma **??**, (a) contains a product of prime ideals, say $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. But then

$$\mathfrak{p} \supseteq (a) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

Assume that $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ is a minimal product of primes, i.e. r is the smallest integer such that a product of prime ideals is contained in (a). Since $\mathfrak{p}$ is prime, $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i. But then $\mathfrak{p} = \mathfrak{p}_i$ since all primes in $\mathcal{O}_K$ are maximal.

If $r = 1$, then $\mathfrak{p} \supseteq (a) \supseteq \mathfrak{p}_1$. Hence, $\mathfrak{p} = (a)$ is a principal ideal with 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 $r \geq 2$, without loss of generality, assume that $\mathfrak{p} = \mathfrak{p}_1$. Then

$$(a) \supseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$$

and $(a) \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$ by the minimality of r. Let $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin (a)$. Define $x = \frac{b}{a} \in K^\times$. Then $x \notin \mathcal{O}_K$ and we claim $x \in \widetilde{\mathfrak{p}}$, which would show that $\widetilde{\mathfrak{p}} \neq \mathcal{O}_K$. We have

$$b \subseteq \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a) = a\mathcal{O}_K.$$

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

Now fix $x \in \widetilde{\mathfrak{p}} \setminus \mathcal{O}_K$. Then $x\mathfrak{p} \subseteq \mathcal{O}_K$ which implies $\mathfrak{p} + x\mathfrak{p} \subseteq \mathcal{O}_K$. Since $\mathfrak{p}$ is a maximal ideal, either $\mathfrak{p} + x\mathfrak{p} = \mathfrak{p}$ or $\mathfrak{p} + x\mathfrak{p} = \mathcal{O}_K$.

If $\mathfrak{p} + x\mathfrak{p} = \mathfrak{p}$, then $x\mathfrak{p} \subseteq \mathfrak{p}$. Now $\mathfrak{p} \neq 0$ is a finitely generated $\mathbb{Z}$-submodule of K, which implies that $x \in \mathcal{O}_K$ by Proposition **??**. Since $x \notin \mathcal{O}_K$, this is a contradiction. [This is where we have made use of the fact that the ring of algebraic integers instead of a general order.] Then $\mathfrak{p} + x\mathfrak{p} = \mathcal{O}_K$. Hence, $\mathfrak{p}(\mathcal{O}_K + x\mathcal{O}_K) = \mathcal{O}_K$. By Lemma **??**, $\mathcal{O}_K + x\mathcal{O}_K = \widetilde{\mathfrak{p}}$ since it is an inverse to $\mathfrak{p}$. □

Corollary 2.2. *If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$.*

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

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

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

Proof.

(i) Multiplication by $\widetilde{p}$.

(ii) If $\mathfrak{p} \supseteq I$, then defining $J = \widetilde{p}I \subseteq \mathcal{O}_K$ to see $I = \mathfrak{p}J$. Conversely, if $I = \mathfrak{p}J$ so that $\mathfrak{p} \supseteq I$.

(iii) Assume to the contrary that $\mathfrak{p}I = I$. Then $I = \mathfrak{p}I = \mathfrak{p}^2 I = \cdots = \mathfrak{p}^n I \subseteq \mathfrak{p}^n$. Since $\#(\mathcal{O}_K/I)$ is finite, $\mathfrak{p}^{n+1} = \mathfrak{p}^n$ for n sufficiently large. Multiplication by $\widetilde{\mathfrak{p}}^n$, we obtain $\mathfrak{p} = \mathcal{O}_K$, a contradiction. □

We are now in a position to prove unique factorization in $\mathcal{O}_K$.

Theorem 2.2. *Every nonzero ideal in $\mathcal{O}_K$ factors uniquely, up to reordering, into a product of prime ideals of $\mathcal{O}_K$.*

Proof. Let $I \subsetneq \mathcal{O}_K$ be a nonzero proper ideal. By Lemma **??**, I contains a product of nonzero prime ideals:

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

We proceed by induction on r. If $r = 1$, then $I \supseteq \mathfrak{p}_1$. Therefore, $I = \mathfrak{p}_1$ by maximality. If $r > 1$, write $I \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}_{r+1}$. Choose a maximal ideal $\mathfrak{p} \supseteq I$, so $\mathfrak{p} = \mathfrak{p}_i$ for some i. Without loss of generality, assume that $\mathfrak{p} = \mathfrak{p}_{r+1}$. Multiplying by $\widetilde{\mathfrak{p}}$, we have

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

By induction, we factor $\widetilde{p}I = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ into a product of primes. Multiplication by $\mathfrak{p}$, we have $I = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_s$. This concludes the proof of existence.

To prove uniqueness, suppose that

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

with $\mathfrak{p}_i$, $\mathfrak{q}_i$ nonzero prime ideals and $r \leq s$. We know that $\mathfrak{p}_1 = \mathfrak{q}_i$ for some i. Without loss of generality, assume $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplication by $\widetilde{\mathfrak{p}}_1$ gives $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Continuing in this fashion, we have $\mathfrak{p}_i = \mathfrak{q}_i$ for $1 \leq i \leq r$ and $\mathcal{O}_K = \mathfrak{q}_{r+1} \cdots \mathfrak{q}_s$, a contradiction unless $r = s$. □

Corollary 2.3. *$\mathcal{J}_K$ is a group.*

Proof. It remains only to check that every element of $\mathcal{J}_K$ has an inverse. Suppose $I \in \mathcal{J}_K$. Then $dI \subseteq \mathcal{O}_K$ for some $d \geq 1$ and that $dI = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Then $I = \frac{1}{d}\mathfrak{p}_1 \cdots \mathfrak{p}_r$, which has inverse $d\widetilde{\mathfrak{p}}_1 \cdots \widetilde{\mathfrak{p}}_r$. □

Since we now know $\mathcal{J}_K$ is a group, we shall write $I^{-1} := \widetilde{I}$ from now on. Every ideal $I \in \mathcal{J}_K$ has a unique factorization $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_\mathfrak{p}}$, where the product is taken over all nonzero primes $\mathfrak{p}$, $e_\mathfrak{p} \in \mathbb{Z}$, and $e_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p}$. How different is the multiplication of fractional ideals than from ordinary multiplication in K? The subgroup $\mathcal{B}_K \subseteq \mathcal{J}_K$ has multiplication which behaves much like the multiplication in $K^\times$. The class group of K, $C\ell_K = \mathcal{J}_K/\mathcal{B}_K$, measures this difference. As stated before, $C\ell_K$ is a finite abelian group, as we shall see.

Example 2.7. We shall find all integer pair of solutions to $y^2 = x^3 - 5$. We shall use the fact that $C\ell_{\mathbb{Q}(\sqrt{-5})} \cong \mathbb{Z}/2\mathbb{Z}$. We know if $K = \mathbb{Q}(\sqrt{-5})$ that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Fix solution pair (x, y). Over $\mathcal{O}_K$, we may factor as

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

We claim that the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime.

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

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

which implies $x \in \mathfrak{p}$. Now $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, where $p = \text{char}\ (\mathcal{O}_K/\mathfrak{p})$. Since $x \in \mathbb{Z}$, we know $x \in \mathfrak{p} \cap \mathbb{Z}$ so that $x \in 2\mathbb{Z}$ or $x \in 5\mathbb{Z}$. Then either $2 \mid x$ or $5 \mid x$. But since $y^2 = x^3 - 5$, neither $y^2 = -5 \mod 4$ nor $y^2 = -5 \mod 25$ have solutions, a contradiction. Then the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime.

Factor the ideal generated by x into primes (noting that x cannot be 0):

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

Then in particular,

$$\prod_{i=1}^{r} \mathfrak{p}_i^{3e_i} = (y + \sqrt{-5})(y - \sqrt{-5})$$

Since the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime, we must have

$$(y + \sqrt{-5}) = \prod_{i \in \mathfrak{I}} \mathfrak{p}_i^{3e_i},$$

where $\mathcal{I} \subseteq \{1, \dots, r\}$. Rewrite this as

$$(y + \sqrt{-5}) = I^3$$

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

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

for some $a, b \in \mathbb{Z}$. Noting the units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, we then have

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

Without loss of generality, we assume the unit above is 1 (as -1 is a cube). Hence, $y + \sqrt{-5} = (a + b\sqrt{-5})^3$. Then

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

Relating real and imaginary parts, we have the following system of equations:

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

Using the second equation, $1 = b(3a^2 - 5b^2)$ so that $b \in \{\pm 1\}$ (as $b \in \mathbb{Z}$). But then $1 = \pm(3a^2 - 5)$ which implies $3a^2 = 5 \pm 1$, neither of which have integer solutions. But then the equation $y^2 = x^3 - 5$ has no integer solutions. ◁

2.4 Ramification

Definition (Ramification)**.** Let p be a prime. Factor $p\mathcal{O}_K$ as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are distinct prime ideals and $e \geq 1$. We call e_i the ramification index of $\mathfrak{p}$ over $\mathfrak{p}$. Further, we say $\mathfrak{p}$ is ramified in K if $e_i > 1$ for some i and otherwise say that $\mathfrak{p}$ is unramified.

Definition (Inertia Degree)**.** Let p be a prime. Factor $p\mathcal{O}_K$ as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are distinct prime ideals and $e \geq 1$. The inertia degree of $\mathfrak{p}_i$ over $\mathfrak{p}$ is $f_i := [\mathcal{O}_K/\mathfrak{p}_i \colon \mathbb{F}_p]$.

Theorem 2.3. *Let p be a prime. Factor $p\mathcal{O}_K$ as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are distinct prime ideals and $e \geq 1$. 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, $r \leq [K \colon \mathbb{Q}]$.

Proof. See page **??**. □

Remark. It is true that $r = [K\colon \mathbb{Q}]$ for infinitely many primes p.

Example 2.8. Suppose that $[K\colon \mathbb{Q}] = 3$ and p is unramified in K. Then $e_i = 1$ for all i. Then there are 3 possibilities:

(i) $r = 3$: $f_1 = f_2 = f_3 = 1$

(ii) $r = 2$: $f_1 = 1$, $f_2 = 2$

(iii) $r = 1$: $f_1 = 3$

It is possible for only a few of these cases to occur. For example in $K = \mathbb{Q}(\sqrt[3]{2})$, each of these cases occurs. However 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 $N(I) := \#(\mathcal{O}_K/I)$.

Proposition 2.5. *If I, J are ideals of $\mathcal{O}_K$, then $N(IJ) = N(I)N(J)$. In particular, if $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ for distinct primes p_i, then $N(I) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$.*

Proof. It suffices to only check the last statement. For $i \neq j$, $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathcal{O}_K$ by maximality. Then by the Chinese Remainder Theorem,

$$\mathcal{O}_K/I = \mathcal{O}_K/\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}.$$

Hence, $N(I) = \prod_i N(\mathfrak{p}_i^{e_i})$. It only remains to show that for a prime $\mathfrak{p}$, $N(\mathfrak{p}^i) = N(\mathfrak{p})^i$. Consider the chain

$$\mathcal{O}_K \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \cdots \supseteq \mathfrak{p}^i.$$

Then

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

where we define $\mathfrak{p}^0 = \mathcal{O}_K$. Then we only need show $\#(\mathfrak{p}^{i-1}/\mathfrak{p}^i) = N(\mathfrak{p})$.

If $\mathfrak{p}^{i-1}/\mathfrak{p}^i = 0$ for some i, then $\mathfrak{p}^{i-1} = \mathfrak{p}^i$ so that $\mathfrak{p}^i = \mathcal{O}_K$, a contradiction. Therefore, $\mathfrak{p}^{i-1}/\mathfrak{p}^i \neq 0$ for all i. Choose then $0 \neq x \in \mathfrak{p}^{i-1}/\mathfrak{p}^i$. Define a homomorphism of $\mathcal{O}_K$-modules $\phi : \mathcal{O}_K \to \mathfrak{p}^{i-1}/\mathfrak{p}^i$ via $b \mapsto bx$. If ϕ were not surjective, then we have $0 \subsetneq \operatorname{im}\phi \subsetneq \mathfrak{p}^{i-1}/\mathfrak{p}^i$. But then there is a $\mathcal{O}_K$-submodule J of M with $\mathfrak{p}^i \subseteq J \subseteq \mathfrak{p}^{i-1}$.Hence, $\mathfrak{p} \subsetneq (\mathfrak{p}^{i-1})^{-1}J \subsetneq \mathcal{O}_K$, contradicting the maximality of $\mathfrak{p}$. Therefore, ϕ is a surjective map. But then $\phi : \mathcal{O}_K \twoheadrightarrow \mathfrak{p}^{i-1}/\mathfrak{p}^i \neq 0$. The kernel of ϕ contains $\mathfrak{p}$, so there is a surjection

$$\mathcal{O}_K \,/\, \mathfrak{p} \longrightarrow\!\!\!\!\!\rightarrow \mathfrak{p}^{i-1} \,/\, \mathfrak{p}^i.$$

But $\mathcal{O}_K/\mathfrak{p}$ is a field which forces $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{i-1}/\mathfrak{p}^i$. Therefore, $N(\mathfrak{p}) = \#(\mathfrak{p}^{i-1}/\mathfrak{p}^i)$. □

We can now prove Theorem **??**.

Theorem ??. *Let p be a prime. Factor $p\mathcal{O}_K$ as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the $\mathfrak{p}_i$ are distinct prime ideals and $e \geq 1$. 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, $r \leq [K\colon \mathbb{Q}]$.

Proof. We compute $N(p\mathcal{O}_K)$ in two different ways. If $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. By Proposition **??** implies

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

Moreover,

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

But then

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

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:

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

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

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

so that $\sum_{i=1}^{r} e_i f_i = n$, as desired. □

Some facts we shall not prove that are useful nonetheless:

Remark.

(i) Given two number fields K_1, K_2 with relatively prime discriminant, $K_1 \cap K_2 = \mathbb{Q}$.

(ii) 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 $p \notin S$.

The first is not too hard to show while the second is a much harder theorem. What we shall prove is that p ramifies in K if and only if p divides the discriminant of K. Hence, there are only finitely many primes p which ramify in K. In order to prove this, we will have to extend our notion of discriminant.

Definition (Discriminant)**.** Suppose $A \subseteq B$, where B is a free A-module of rank n. Choose an A-basis $x_1, \ldots, x_n$ of B, define the discriminant of B over A as

$$\mathrm{disc}_A(B) := \mathrm{disc}(x_1, \ldots, x_n) = \det(Tr_{B/A}(x_i x_j)) \in A,$$

where $Tr_{B/A}(x)$ is the trace of the A-linear map $B \to B$ given by $b \mapsto xb$.

If one chose another A-basis $y_1, \ldots, y_n$, then

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

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, $\det(C) \in A^\times$. Then $\mathrm{disc}(y_1, \ldots, y_n)$ and $\mathrm{disc}(x_1, \ldots, x_n)$ differ by the square of a unit in A. Then $\mathrm{disc}_A(B)$ is well defined up to an element of $(A^\times)^2$ and defines a coset $\mathrm{disc}(x_1, \ldots, x_n) \cdot (A^\times)^2$.

Proposition 2.6. *For $A \subseteq B_1$ and $A \subseteq B_2$,*

$$\mathrm{disc}_A(B_1 \times B_2) = \mathrm{disc}_A(B_1)\,\mathrm{disc}_A(B_2).$$

Before proving our desired theorem, a lemma.

Lemma 2.5. *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 $x_1, \ldots, x_n$ of $B = \mathcal{O}_K/\mathfrak{p}^e$ over $\mathbb{F}_p$ with $x_1^2 = 0$. [We may choose x_1 this was because

$$x_i \in \mathfrak{p}^{e-1} \Big/ \mathfrak{p}^e \Longrightarrow x_1^2 \in (\mathfrak{p}^{e-1})^2 \subseteq \mathfrak{p}^e,$$

the last inclusion holding since $e \geq 2$.] Define a linear map $B \to B$ via $b \mapsto x_1 x_j b$. This map can be represented by an $n \times n$ matrix M in $\mathbb{F}_p$ with $M^2 = 0$ (since $x_1^2 = 0$). Now

$$Tr_{B/\mathbb{F}_p}(x_1 x_j) = \mathrm{tr}(M) = 0$$

since the eigenvalues of M are all zero. Then

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

since the first row is zero. Hence,

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

If $e = 1$, we want to show that $\operatorname{disc}(\mathcal{O}_K/\mathfrak{p}^e) \neq 0$. We show, in fact, for a finite field extension L/K of separable fields, $\operatorname{disc}(L/K) \neq 0$. The separable assumption gives $L = K(\alpha)$ 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 $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \overline{K}$ are the K-embeddings of L into an algebraic closure $\overline{K}$ of K. The product on the right size is nonzero and will be nonzero up to a unit squared. Hence, $\operatorname{disc}_K(L) \neq 0$. □

We are now in a position to prove our theorem.

Theorem 2.4. *A prime p is ramified in K if and only if p divides the discriminant of K. In particular, there are only finitely many primes p which ramify in K.*

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

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

This class represents an element of the coset $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/p\mathcal{O}_K)$. So $p \mid \operatorname{disc} K$ if and only if $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/p\mathcal{O}_K) = 0$. But then by Lemma **??**, p ramifies in K if and only if $p \mid \operatorname{disc} K$. Since $\operatorname{disc} K \in \mathbb{Z}$, there are finitely many primes dividing it. Hence, there are finitely many primes which ramify in K. □

3 Dedekind Domains & DVRs

3.1 Dedekind Domains

Though we have been working with the ring of integers of a number field, factorization of ideals into prime ideals holds in a more general setting — in Dedekind domains.

Definition (Integrally Closed)**.** A ring R is integrally closed if for each monic $f(x) \in R[x]$ with root $\alpha \in K$, where $K = \operatorname{Frac} R$, then $\alpha \in R$.

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

(i) R is noetherian

(ii) R is integrally closed

(iii) every nonzero prime ideal in R is maximal

(iv) there is at least one nonzero prime ideal

Remark. The last condition for a Dedekind domain is to exclude fields from being Dedekind domains.

Example 3.1. If K is a number field, then $\mathcal{O}_K$ is a Dedekind domain. Indeed, we know that $\mathcal{O}_K$ is noetherian and every nonzero prime ideal in $\mathcal{O}_K$ is maximal. To see that $\mathcal{O}_K$ is integrally closed, take any $\alpha \in K$ such that $f(\alpha) = 0$ with monic $f \in \mathcal{O}_K[x]$. 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 $\alpha M \subseteq M$ so that $\alpha \in \mathcal{O}_K$ by Proposition **??**. Finally, $\mathcal{O}_K$ contains a nonzero prime ideal. ◁

Though we shall not prove it, factorization in Dedekind domains holds just as in $\mathcal{O}_K$.

Theorem 3.1. *Let R be an integral domain. Then R is a Dedekind domain if and only if every nonzero ideal has a unique factorization into prime ideals.*

The proof that Dedekind domains have unique factorization is as in Theorem **??**, with minor changes.

Example 3.2.

(i) Any PID is a Dedekind domain.

(ii) $R = \mathbb{C}[x, y]/(y^2 - x^3 - 1)$ is a Dedekind domain, but it is not a PID. The nonzero prime ideals are $(x - a, y - b)$ with $b^2 = a^3 + 1$ for $a, b \in \mathbb{C}$.

(iii) If C is a nonsingular affine curve over any field k, then its coordinate ring $k[C]$ is a Dedekind domain. ◁

Remark. For any Dedekind domain R, we may also define the ideal class group $\mathrm{C}\ell_R$, 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 $y^2 = x^3 - 1$, then $\mathrm{C}\ell_R \cong \mathbb{R}^2/\mathbb{Z}^2$.

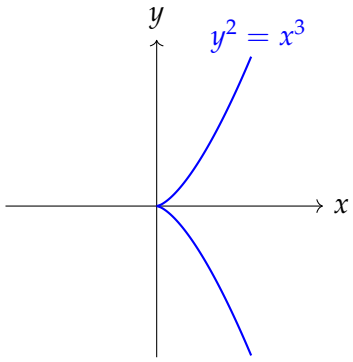
Definition (Integral Closure)**.** Let R be a ring with fraction field K. Let L be a finite field extension of K. The integral closure of R in L is the ring

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

Proposition 3.1. *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.*

$$\begin{array}{ccc} L & \supseteq & S \\ | & & | \\ K & \supseteq & R \end{array}$$

Example 3.3. Let $R = \mathbb{C}[x,y]/(y^2 - x^3)$. This is not a Dedekind domain as it is not integrally closed. Indeed, the curve $y^2 - x^3 = 0$ is singular at the origin.



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

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

$$t^2 = \frac{y^2}{x^2} = \frac{x^3}{x^2} = x$$
$$t^3 = \frac{y^3}{x^3} = \frac{y^3}{y^2} = y$$

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

3.2 Discrete Valuation Rings

Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. For $x \in K^\times$, 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 $\mathfrak{p}$. By definition, we declare $\nu_\mathfrak{p}(0) := \infty$.

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

Proposition 3.2. *The valuation $\nu_\mathfrak{p}$ satisfies the following properties:*

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

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

Definition (Integral at $\mathfrak{p}$)**.** Define $\mathcal{O}_\mathfrak{p} := \{x \in K \colon \nu_\mathfrak{p}(x) \geq 0\}$. 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 3.1. *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. Let I be a nonzero ideal of $\mathcal{O}_\mathfrak{p}$. 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 $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ 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 $\nu_\mathfrak{p}(x) = 0$, implying $\nu_\mathfrak{p}(x^{-1}) = -\nu_\mathfrak{p}(x) = 0$ so $x^{-1} \in \mathcal{O}_\mathfrak{p}$ as well. Therefore, $\pi^{-n}I = \mathcal{O}_\mathfrak{p}$ and then $I = \pi^n\mathcal{O}_p>$ □

Definition (Discrete Valuation Ring)**.** A discrete valuation ring (DVR) is a local PID, i.e. a PID with a unique maximal ideal.

Lemma **??** shows that $\mathcal{O}_\mathfrak{p}$ is a DVR.

Lemma 3.2.

$$\mathcal{O}_p = \left\{ \frac{a}{b} \colon a \in \mathcal{O}_K, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}$$

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

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

since $b \notin \mathfrak{p}$ (when we factor $b\mathcal{O}_K$, $\mathfrak{p}$ does not 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 $\mathfrak{p}$ does not divide J. Essentially, we factored $\alpha\mathcal{O}_K$ into primes and collected all primes with positive exponent into I and collected all primes with negative exponents into J^{-1}. We may assume $\mathfrak{p}$ does not divide J since $\nu_\mathfrak{p}(\alpha) \geq 0$.

The prime ideal $\mathfrak{p}$ does not divide J if and only if $J \not\subseteq \mathfrak{p}$. We may choose $b \in J \setminus \mathfrak{p}$. Then

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

Notice $bJ^{-1} \subseteq \mathcal{O}_K$, since $JJ^{-1} = \mathcal{O}_K$. Hence, $I(bJ^{-1}) \subseteq I$. Write $b\alpha = a \in I$. Then $\alpha = \frac{a}{b}$. 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. $\mathcal{O}_\mathfrak{p}$ is the localization of $\mathcal{O}_K$ at $\mathfrak{p}$. To show that $\mathcal{O}_\mathfrak{p}$ is a DVR, we could have (instead of defining $\nu_\mathfrak{p}$) noted that $\mathcal{O}_\mathfrak{p}$ is necessarily local and demonstrated that it was a PID.

Theorem 3.2. *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 another proof that $\mathcal{O}_K$ is a Dedekind domain, although the proof is a bit more roundabout.

3.3 Extension of Number Fields

Thus far, we have been working with an extension $K/\mathbb{Q}$. However, much of the work done thus far equally applies to an extension of number fields L/K. So suppose L/K is an extension of number fields and $\mathfrak{p} \in \mathcal{O}_K$ be a nonzero 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

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

Theorem 3.3. $\displaystyle\sum_{\mathfrak{q}|\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p}) f(\mathfrak{q}/\mathfrak{p}) = [L \colon K]$

Proof. We compute $N(\mathfrak{p}\mathcal{O}_L)$ in two ways. First,

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

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 $\mathcal{O}_L \cong \mathcal{O}_K^{[L\colon K]}$. Therefore,

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

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

If $\mathcal{O}_L$ is not free over $\mathcal{O}_K$, we need to localize. We have $\mathcal{O}_K \subseteq \mathcal{O}_L$. Localizing, we obtain $(\mathcal{O}_K)_\mathfrak{p}$ and $(\mathcal{O}_L)_\mathfrak{p}$. We know $(\mathcal{O}_K)_\mathfrak{p}$ is a PID and that $(\mathcal{O}_L)_\mathfrak{p}$ is a finitely generated $(\mathcal{O}_K)_\mathfrak{p}$-module. Therefore, $(\mathcal{O}_L)_\mathfrak{p}$ is a free $(\mathcal{O}_K)_\mathfrak{p}$-module (there is no torsion as we are in characteristic 0). But we have isomorphisms $\mathcal{O}_K/\mathfrak{p} \cong (\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong (\mathcal{O}_L)_\mathfrak{p}/\mathfrak{p}(\mathcal{O}_L)_\mathfrak{p}$. Then

$$\dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L \Big/ \mathfrak{p}\mathcal{O}_L = \dim_{(\mathcal{O}_K)_\mathfrak{p}/\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}} (\mathcal{O}_L)_\mathfrak{p} \Big/ \mathfrak{p}(\mathcal{O}_L)_\mathfrak{p} = [L\colon K].$$

Therefore, $\#(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L) = N(\mathfrak{p})$. □

These results also extend to towers of number fields:

$$\begin{array}{cc} M & \mathfrak{Q} \\ | & \cup \\ L & \mathfrak{P} \\ | & \cup \\ K & \mathfrak{p} \end{array}$$

where $\mathfrak{Q}$, $\mathfrak{P}$, and $\mathfrak{p}$ are prime ideals in $\mathcal{O}_M$, $\mathcal{O}_L$, and $\mathcal{O}_K$, respectively.

Proposition 3.3. *In the scenario above, we have*

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

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

Proof.

(a)

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

By unique factorization, the exponents must be the same.

(b) This follows from the fact that degrees of field extensions are multiplicative:

$$\begin{array}{c} \mathcal{O}_M \,/\, \mathfrak{Q} \\ | \\ \mathcal{O}_L \,/\, \mathfrak{P} \\ | \\ \mathcal{O}_K \,/\, \mathfrak{p} \end{array}$$

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

□

Example 3.4. Let X and Y be compact Riemann surfaces with a non-constant holomorphic map $\phi : Y \to X$. Let $\mathcal{M}_X$ and $\mathcal{M}_Y$ be the field of meromorphic functions on X and Y, respectively. The map ϕ induces an inclusion $\phi^* : \mathcal{M}_X \hookrightarrow \mathcal{M}_Y$ given by $f \mapsto f \circ \phi$. Let n be the degree of the extension $\mathcal{M}_Y/\mathcal{M}_X$, called the degree of ϕ.

Fix a point $p \in X$ and let $\mathcal{O}_p = \{f \in \mathcal{M}_X \colon f \text{ holomorphic at } p\}$. It is routine to verify that $\mathcal{O}_p$ is a ring. In fact, $\mathcal{O}_p$ is a DVR with maximal ideal $\mathfrak{p} = \{f \in \mathcal{O}_p \colon f(p) = 0\}$, i.e. those holomorphic functions vanishing at p. Let B be the integral closure of $\mathcal{O}_\mathfrak{p}$ in $\mathcal{M}_Y$. Now B is a Dedekind domain. We have

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

where the $\mathfrak{P}_i$ are distinct prime ideals with $f_i = [B/\mathfrak{P}_i \colon \mathcal{O}_p/\mathfrak{p}] = [\mathbb{C} \colon \mathbb{C}] = 1$. Furthermore, if $\phi^{-1}(\{p\}) = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$, then $\mathcal{O}_{\mathfrak{P}_i} = B_{\mathfrak{P}_i}$. Geometrically considering p as a divisor, $\phi^{-1}(p) = \sum_{i=1}^{r} e_i \mathfrak{P}_i$ with degree $\sum_{i=1}^{r} e_i = n$. ◁

4 Geometry of Numbers

4.1 Minkowski Theory

Definition (Euclidean Space)**.** A Euclidean space is a finite dimensional real inner product space $\langle \cdot\,, \cdot \rangle : V \times V \to \mathbb{R}$.

Example 4.1. The pair $(\mathbb{R}^n, \cdot)$, where $\cdot$ is the usual dot product, is a Euclidean space. ◁

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

Example 4.2. Both $\mathbb{Z} \subseteq \mathbb{C}$ and $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ are discrete. ◁

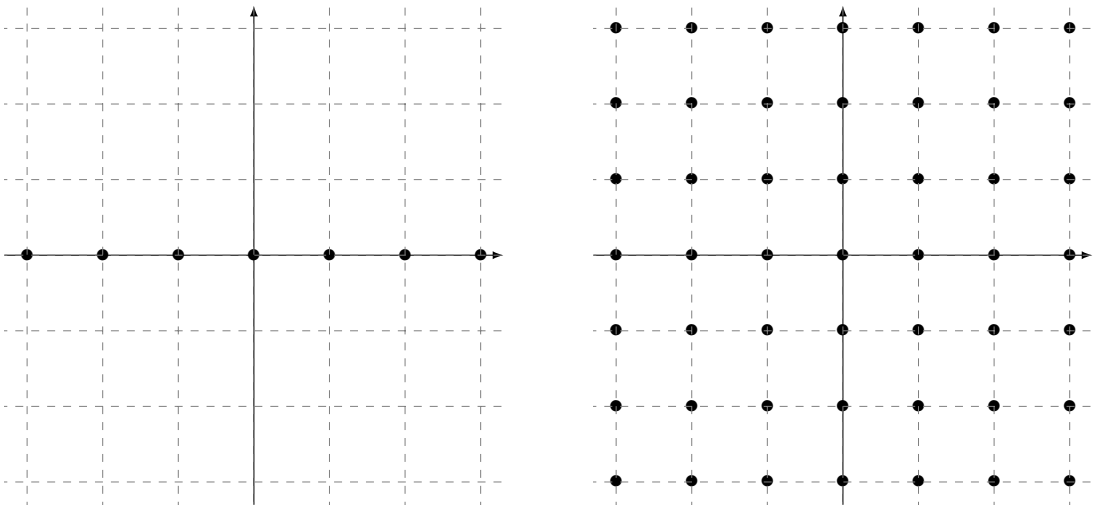


Figure 2: The lattice for $\mathbb{Z} \subseteq \mathbb{C}$ (left) and $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ (right).

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

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

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

Remark. What we here refer to as a lattice is sometimes referred to as a complete or full lattice.

On V, we have a volume measure on V — the Haar measure μ: $\mu(\{x_1e_1 + \cdots + x_ne_n \colon 0 \leq x_i < 1\}) = 1$, where $e_1, \ldots, e_n$ is an orthonormal basis.

Definition (Fundamental Domain)**.** Let $\Lambda \subseteq V$ be a lattice with $\Lambda = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \cdots \mathbb{Z}v_n$. A fundamental domain for Λ is

$$\mathcal{F} := \{x_1v_1 + \cdots + x_nv_n \colon 0 \leq x_i < 1\}.$$

Example 4.3. A fundamental domain for the lattice in $\mathbb{R}^2$ generated by the vectors $\langle 1, 1\rangle$ and $\langle \sqrt{2}, -\sqrt{2}\rangle$ is the region shaded in the Figure **??** below.

Note that we have

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

The Haar measure on V assigns volume 1 to the fundamental domain and we say that

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

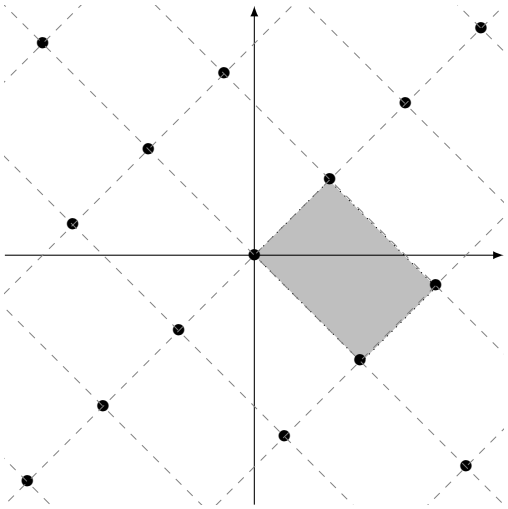


Figure 3: The fundamental domain of $\mathbb{Z}[\sqrt{2}]$ generated by $\langle 1, 1\rangle$ and $\langle \sqrt{2}, -\sqrt{2}\rangle$.

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

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 $\operatorname{vol}(\mathcal{F}) = |\det A|$ (the absolute value removes sign issues that could arise). The matrix $B := B_{ij} = (\langle v_i, v_n\rangle)_{i,j}$ satisfies $B = AA^T$, and $\operatorname{covol}(\Lambda) = \operatorname{vol}(\mathcal{F}) = |\det((\langle v_i, v_j\rangle)_{i,j})|^{1/2} = \sqrt{|\det B|}$.

Remark. The quotient map $V \to V/\Lambda$ gives a way of relating volume and covolume. The space V/Λ is compact and has Haar measure $\overline{\mu}$ — the one induced from μ on V.

$$\operatorname{vol}(V/\Lambda) = \overline{\mu}(V/\Lambda) = \mu(\mathcal{F}) = \operatorname{covol}(\Lambda)$$

4.2 Lattices from $\mathcal{O}_K$

Let K be a number field of degree n. Let $\sigma : K \hookrightarrow \mathbb{C}$ be a complex embedding of K to $\mathbb{C}$. Recall that we have a map

$$K_{\mathbb{R}} := \{(a_\sigma) \in \prod_{\sigma} \mathbb{C} : \overline{a_\sigma} = a_{\overline{\sigma}} \text{ for all } \sigma : K \hookrightarrow \mathbb{C}\},$$

where σ runs over all complex embeddings $\sigma : K \hookrightarrow \mathbb{C}$ and $\overline{\sigma}$ is the complex conjugate embedding of σ given by $\mathrm{conj} \circ \sigma$ with conj being complex conjugation. Now $K_{\mathbb{R}}$ is a real

vector space of dimension n. There is a map

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

that induces an isomorphism of $\mathbb{R}$-algebras $K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}}$. We have seen that $\Lambda := i(\mathcal{O}_K)$ is a lattice in $K_{\mathbb{R}}$: $\mathcal{O}_K \cong \mathbb{Z}^n \subseteq K \cong \mathbb{Q}^n$ as additive abelian groups.

$$\begin{array}{ccc} \mathcal{O}_K & \cong & \mathbb{Z}^n \\ \cap & & \cap \\ K & \cong & \mathbb{Q}^n \end{array}$$

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 symmetric, positive definite, bilinear pairing

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

where

$$Tr_{K/\mathbb{Q}}(\alpha\beta) = \sum_{\sigma : K \hookrightarrow \mathbb{C}} \sigma(\alpha)\sigma(\beta).$$

Define a pairing $\langle\ ,\ \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ by

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

The image of this pairing is indeed in $\mathbb{R}$ as

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

The pairing is clearly bilinear and symmetric. It only remains to show that the pairing is positive definite but this is clear as $\langle i(\alpha), i(\beta)\rangle = Tr_{K/\mathbb{Q}}(\alpha\beta)$ for $\alpha, \beta \in K$.

Now let r be the number of embeddings $\sigma : K \hookrightarrow \mathbb{R}$ (the real embeddings) and let s be the number of complex conjugate pairs of embeddings $\sigma : K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$ (the complex embeddings). Since K has degree n, $n = r + 2s$. Order the embeddings as follows:

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

Then we have $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{R}^{2s} \cong \mathbb{R}^n$ using the isomorphism

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

We have an inner product on the left hand side given by

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

This forces us into the following choice for an inner product on $\mathbb{R}^n$:

$$\begin{aligned}\mathbb{R}^n \times \mathbb{R}^n &\longrightarrow \mathbb{R} \\ \langle x, y \rangle &\longmapsto \sum_{i=1}^{r} x_i y_i + 2 \sum_{i=r+1}^{r+s???} x_i y_i\end{aligned}$$

What then 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 $i(\mathcal{O}_K)$. The covolume is then

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

Thus, we have proved the following:

Proposition 4.1. *$i(\mathcal{O}_K)$ is a lattice in $(K_{\mathbb{R}}, \langle \cdot\,, \cdot \rangle)$ with covolume $\sqrt{\operatorname{disc} K}$.*

4.3 Minkowski's Theorem

Our goal in this section will be to prove a fundamental theorem in the geometry of numbers — Minkowski's Theorem. Before stating the theorem, we will need some definitions.

Definition (Symmetric)**.** A subspace $X \subseteq V$ of a Euclidean space is symmetric if $x \in X$ implies that $-x \in X$.

Definition (Convex)**.** A subspace $X \subseteq V$ of a Euclidean space is convex if for all $x, y \in X$, we have $t + x(1-t)y \in X$ for all $0 \leq t \leq 1$.

With sufficient vocabulary, we are now in a position to proceed to the theorem.

Lemma 4.1. *If* $\operatorname{vol} X > \operatorname{covol} \Lambda$*, then there are two distinct points* $x, y \in X$ *such that* $x - y \in \Lambda$*.*

Proof. Consider the quotient map $\phi : V \to V/\Lambda$. If $\phi|_X$ is injective, then $\operatorname{vol}(X) = \mu(X) = \overline{\mu}(X)$. But then $\operatorname{vol} X \leq \overline{\mu}(V/\Lambda) = \operatorname{covol} \Lambda$. But this contradicts the assumption. Therefore, $\phi|_X$ cannot be injective. There then exist distinct $x, y \in X$ such that $\phi(x) = \phi(y)$, i.e. $\phi(x - y) = 0$. But then $x - y \in \Lambda$. In particular since $x \neq y$, $x - y \in \Lambda \setminus \{0\}$. □

Theorem 4.1 (Minkowski's Theorem)**.** *Let* Λ *be a lattice in a Euclidean space* V *of dimension. Let* X *be a measurable subset of* V *that is symmetric and convex. Assume on of the following:*

(i) $\operatorname{vol} X > 2^n \operatorname{covol} \Lambda$

(ii) $\operatorname{vol} X \geq 2^n \operatorname{covol} \Lambda$ *and* X *compact*

Then X *contains a nonzero element of* Λ*.*

Proof. Assume that (i) holds. Define $X' = \frac{1}{2}X$. By assumption,

$$\operatorname{vol} X' = \frac{1}{2^n} \operatorname{vol} X > \operatorname{covol} \Lambda.$$

By Lemma **??**, there exists distinct $x, y \in X'$ such that $x - y \in \Lambda \setminus \{0\}$. We claim that $x - y \in X$. Note that $2x, 2y \in 2X' = X$. As $2y \in X$ and X is symmetric, we have $-2y \in X$. Therefore,

$$\begin{aligned} x - y &= \frac{1}{2}(2x - 2y) \\ &= \frac{1}{2} \underbrace{\left(\underbrace{2x}_{\in X} + \underbrace{(-2y)}_{\in X} \right)}_{\in X} \end{aligned}$$

where $2x + (-2y) \in X$ by convexity (use $t = 1/2$ in $(1-t)2x + t(-2y)$).

Now assume (ii) holds. Choose $\epsilon > 0$ and consider $(1+\epsilon)X$. We have

$$\operatorname{vol}((1+\epsilon)X) > 2^n \operatorname{covol}(\Lambda).$$

By (i), $(1+\epsilon)X$ contains a nonzero lattice point. For any ϵ' with $0 < \epsilon' < \epsilon$, using convexity and the fact that $0 \in X$ (being symmetric and convex), that $(1+\epsilon')X \subseteq (1+\epsilon)X$. But then

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

is the intersection of compact and nonempty sets, and the intersections are therefore nonempty. So there exists $\lambda \in \Lambda \setminus \{0\}$ such that $\lambda \in (1+\epsilon)X$ for all $\epsilon > 0$. But then $\lambda \in X$ as X is compact (so that X is closed). □

Remark. Note that in (ii) above, compactness is required. If $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$, then

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

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

There are other interesting and surprising uses for this theorem. We see at least one such example here.

Theorem 4.2 (Lagrange)**.** *All positive integers are the sum of four squares.*

Lemma 4.2. *If every prime is the sum of four squares, then every positive integer is the sum of four squares.*

Proof. Let $\mathbb{H}$ be the ring of quaternions. Take $\alpha = a + bi + cj + dk$, where $a, b, c, d \in \mathbb{Z}$. The conjugate of α is $\overline{\alpha} := a - bi - cj - dk$. We have $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$. This defines a norm

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

For $\alpha, \beta \in \mathbb{H}$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$. Now $N(\alpha\beta)$ is the sum of four squares and $N(\alpha)N(\beta)$ are each the sum of four squares. Then if $n \in \mathbb{Z}$ (viewing $\mathbb{Z} \subseteq \mathbb{H}$ via $\mathbb{Z}1 \subseteq \mathbb{H}$), write $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$N(n) = N(p_1^{e_1} \cdots p_r^{e_r}) = N(p_1)^{e_1} \cdots N(p_r)^{e_r}.$$

Now an integer is the sum of four squares if and only if it is the norm of an 'integer quaternion'. Therefore since $N(p_1^{e_1} \cdots p_r^{e_r})$ is a sum of four squares and by assumption $N(p_i)$ is known to exist for all p_i prime, we can find a representation for n as a sum of four squares. □

Lemma 4.3. *For any odd prime p, there exists $r, s \in \mathbb{Z}$ such that $r^2 + s^2 + 1^2 \equiv 0 \mod p$.*

Proof. The multiplicative group $(\mathbb{F}_p^\times)^2$ is cyclic of order $\frac{p-1}{2}$. There are $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ possible residues for r^2 modulo p. Similarly, there are $\frac{p+1}{2}$ possible residues fro $-1 - s^2$ modulo p. However, observe

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

Therefore by the Pigeonhole Principle, there must be $r, s \in \mathbb{F}_p$ such that $r^2 = -1 - s^2$. □

Theorem ?? (Lagrange)**.** *All positive integers are the sum of four squares.*

Proof. By Lemma **??**, it suffices to prove the theorem for the positive prime integers. The case where $p = 2$ is simple: $2 = 1^1 + 1^2 + 0^2 + 0^2$. Now let p be an odd prime. By Lemma **??**, choose $r, s \in \mathbb{Z}$ such that $r^2 + s^2 + q \equiv 0 \mod p$. 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 $\operatorname{covol}\Lambda = |\det A| \operatorname{covol}(\mathbb{Z}^4) = p^2$.

We claim that if $\lambda \in \Lambda$, then $\|\lambda\|^2 \equiv 0 \mod p$. If

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

then

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

Now choosing $X = \{v \in \mathbb{R}^4 \colon \|v\| < 2p\}$, then observe Minkowski's Theorem applies to X as

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

But then $\lambda \in \Lambda \setminus \{0\} \in X$. But $0 < \|\lambda\|^2 < 2p$ and $\|\lambda\|^2 \in \mathbb{Z}$ is divisible by p. Therefore, $\|\lambda\|^2 = p$ so that p is a sum of four squares as

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

□

4.4 Finiteness of $\mathrm{C}\ell_K$

We now come to our most important application of Minkowski's Theorem: the finiteness of the class group for number fields. Before proving the theorem, we will state the result and explore a few examples.

Theorem 4.3. *Let $K/\mathbb{Q}$ be a number field of degree n. Let r be the number of real embeddings $\rho : K \hookrightarrow \mathbb{C}$ and s be the number of complex conjugate embeddings $\sigma : K \hookrightarrow \mathbb{C}$, $\sigma(K) \not\subseteq \mathbb{R}$. Let I be a nonzero ideal of $\mathcal{O}_K$. Then I contains a nonzero element α with*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} |\operatorname{disc} K|^{1/2} N(I)$$

Remark. Observe that given a fixed K,

$$M_K := \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} |\operatorname{disc} K|^{1/2}$$

is a constant, not depending on I. This is called the Minkowski bound for the field K, which we shall denote M_K.

One interpretation of the theorem would be that for $\alpha \in I$, noting $\alpha\mathcal{O}_K \subseteq I$, that

$$[I \colon \alpha\mathcal{O}_K] = \frac{[\mathcal{O}_K \colon \alpha\mathcal{O}_K]}{[\mathcal{O}_K \colon I]} = \frac{N(\alpha\mathcal{O}_K)}{N(I)} = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(I)} \leq \left(\frac{\pi}{4}\right)^s \frac{n!}{n} |\operatorname{disc} K|^{1/2}.$$

This upper bound depends only on the field K and not on I nor on α. So in a sense, principal ideals and ideals generally are 'close to each other' — in the sense that the index $[I \colon \alpha\mathcal{O}_K]$ is bounded. However, note that α depends on I in Theorem **??**. If we were free to choose $\alpha \in I$, we could make $[I \colon \alpha\mathcal{O}_K]$ arbitrarily large by scaling α by an integer to make $|N_{K/\mathbb{Q}}(\alpha)|$ arbitrarily large. One final use of the theorem, as we shall see, is that $\mathrm{C}\ell_K$ is generated by equivalence classes of prime ideals less than M_K, see Corollary **??**.

Example 4.4. Let $K = \mathbb{Q}(i)$. For this field, we have $r = 0$ and $s = 1$ so

$$M_K = \left(\frac{\pi}{4}\right)^1 \frac{2!}{2} |-4|^{1/2} = \frac{4}{\pi} < 2.$$

Therefore, every element of $\mathrm{C}\ell_K$ contains an ideal of norm 1. But then we have $\mathrm{C}\ell_K = \{[\mathcal{O}_K]\} = 1$. Since $\mathcal{O}_K = \mathbb{Z}[i]$, this implies that $\mathbb{Z}[i]$ is a PID. ◁

Example 4.5. Let $K = \mathbb{Q}(\sqrt{-5})$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. For this field, $r = 0$ and $s = 1$ so that

$$M_K = \left(\frac{\pi}{4}\right)^1 \frac{2!}{2} |-20|^{1/2} \approx 2.8$$

We have seen previously that $\mathcal{O}_K$ is not a PID (as it is not a UFD, see Example **??**). To calculate $\mathrm{C}\ell_K$, we need only calculate the ideals of norm at most 2. The only ideal of norm 1

is $\mathcal{O}_K$. In Example **??**, we have seen $2\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle$. Hence, $\mathfrak{p}$ has norm 2. But then we must have $\mathrm{C}\ell_K = \{[\mathcal{O}_K], [\mathfrak{p}]\} \cong \mathbb{Z}/2\mathbb{Z}$. 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 $|N_{K/\mathbb{Q}}(\alpha)| = N(\mathfrak{p}) = 2$. But if $\alpha = a + b\sqrt{-5}$, then $N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2$, which can never be 2 for $a, b \in \mathbb{Z}$. ◁

Example 4.6. Let $K = \mathbb{Q}(\sqrt{-26})$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-26}]$. Routine calculation verifies that $n = 2$, $r = 0$, $s = 1$, and $\operatorname{disc} K = -104$. Then we have

$$M_K = \left(\frac{\pi}{4}\right)^1 \frac{2!}{2}|-104|^{1/2} \approx 6.49.$$

Therefore, $\mathrm{C}\ell_K$ is generated by classes of prime ideals, $[\mathfrak{p}]$, with $N(\mathfrak{p}) \leq 6 < 6.49$. In particular, $N(\mathfrak{p}) \in \{1, 2, 3, 4, 5\}$. The rest is computation by cases:

- If $N(\mathfrak{p}) = 1$, then $\mathfrak{p} = \mathcal{O}_K$.
- If $N(\mathfrak{p}) = 2$, as $x^2 + 26 \equiv x^2 \mod 2$, we have $(2) = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 = (2, \sqrt{-26})$.
- If $N(\mathfrak{p}) = 3$, as $x^2 + 26 \equiv x^2 - 1 \equiv (x-1)(x+1) \mod 3$, we have $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, where $\mathfrak{p}_3 = (3, \sqrt{-26}+1)$ and $\mathfrak{p}_3' = (3, \sqrt{-26}-1)$.
- If $N(\mathfrak{p}) = 5$, as $x^2 + 26 \equiv x^2 + 1 \equiv (x+2)(x+3) \mod 5$, we have $(5) = \mathfrak{p}_5\mathfrak{p}_5'$, where $\mathfrak{p}_5 = (5, \sqrt{-26}+2)$ and $\mathfrak{p}_5' = (5, \sqrt{-26}+3)$.

The relations $\mathfrak{p}_3\mathfrak{p}_3' = (3)$ and $\mathfrak{p}_5\mathfrak{p}_5' = (5)$ give the following relations in the class group: $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$ and $[\mathfrak{p}_5'] = [\mathfrak{p}_5]^{-1}$. For $\alpha = a + b\sqrt{-26} \in \mathcal{O}_K$, we have $|N_{K/\mathbb{Q}}(\alpha)| = a^2 + 26b^2$. Since $a^2 + 26b^2$ is never 2, 3, or 5, it cannot be that any $\mathfrak{p}_2$, $\mathfrak{p}_3$, or $\mathfrak{p}_5$ are principal. Therefore, $\mathrm{C}\ell_K$ is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, and $[\mathfrak{p}_5]$. It only remains to find relations between these generators.

If $\alpha = 2 + \sqrt{-26}$, we have $N_{K/\mathbb{Q}}(\alpha) = 30 = 2 \cdot 3 \cdot 5$. We have $\alpha = 2 + \sqrt{-26} \in \mathfrak{p}_2$ but $\alpha = 3 + (\sqrt{-26} - 1) \in \mathfrak{p}_3'$ and $\alpha = 2 + \sqrt{-26} \in \mathfrak{p}_5$. Therefore, $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3'\mathfrak{p}_5$. This shows in $\mathrm{C}\ell_K$, we have $1 = [\mathfrak{p}_2][\mathfrak{p}_3'][\mathfrak{p}_5]$ so that $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3']^{-1} = [\mathfrak{p}_2][\mathfrak{p}_3]$ so that we may eliminate $[\mathfrak{p}_5]$ from the list of generators.

As we know that $\mathfrak{p}_2$ is not principal and $(2) = \mathfrak{p}_2^2$, $[\mathfrak{p}_2]$ has order 2, i.e. $[\mathfrak{p}_2]^2 = 1$. We claim that $[\mathfrak{p}_3]$ has order 3. Let $\alpha = 1 + \sqrt{-26}$. Routine computation verifies $N_{K/\mathbb{Q}}(\alpha) = 27$. Write $(\alpha) = \mathfrak{p}_3^a(\mathfrak{p}_3')^b$. The left side has norm 27 and the right side has norm 3^{a+b}. Then we must have $a + b = 3$. If $a, b \geq 1$, then $\alpha \in \mathfrak{p}_3\mathfrak{p}_3' = (3)$. But as $\alpha/3 \notin \mathcal{O}_K$, this is a contradiction. But as $\mathfrak{p}_3$ is not principal, we must have $[\mathfrak{p}_3]^3 = 1$. Therefore,

$$\mathrm{C}\ell_K \cong \mathbb{Z}\Big/2\mathbb{Z} \oplus \mathbb{Z}\Big/3\mathbb{Z} \cong \mathbb{Z}\Big/6\mathbb{Z}.$$

In fact, $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3]$ is a generator for $\mathrm{C}\ell_K$, as one can verify. ◁

Theorem ??. *Let $K/\mathbb{Q}$ be a number field of degree n. Let r be the number of real embeddings $\rho : K \hookrightarrow \mathbb{C}$ and s be the number of complex conjugate embeddings $\sigma : K \hookrightarrow \mathbb{C}$, $\sigma(K) \not\subseteq \mathbb{R}$. Let I be a nonzero ideal of $\mathcal{O}_K$. Then I contains a nonzero element α with*

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} |\operatorname{disc} K|^{1/2} N(I)$$

Proof. Consider the embedding $\iota : \mathcal{O}_K \hookrightarrow K_{\mathbb{R}} \cong \mathbb{R}^n$ given by

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

Recall that $\mathbb{R}^n$ has an inner product given by the pairing

$$\langle x, y \rangle = \sum_{i=1}^{n} e_i x_i y_i,$$

where $e_i = 1$ for $1 \leq i \leq r$ and $e_i = 2$ for $r+1 \leq i \leq r+s$. Furthermore, $\iota(\mathcal{O}_K)$ is a lattice of covolume $\sqrt{|\operatorname{disc} K|}$. Then if $0 \neq I \subseteq \mathcal{O}_K$ is an ideal, $\iota(I) \subseteq \mathbb{R}^n$ is also a lattice of covolume $N(I)\sqrt{|\operatorname{disc} K|}$.

Let $\alpha \in I$. Then

$$|N_{K/\mathbb{Q}}(\alpha)| = \left|\prod_\sigma \sigma(\alpha)\right| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \prod_{i=r+1}^{r+s} |\sigma_i(\alpha)|^2.$$

By the AM-GM 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

$$X_t := \left\{ x \in \mathbb{R}^n : \sum_{i=1}^{r} |x_i| + 2\sum_{i=r+1}^{r+s} \sqrt{x_i^2 + x_{i+s}^2} \leq t \right\}.$$

If $\iota(\alpha) \in X_t$, then $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{t^n}{n^n}$. It is routine to verify that $X_t \subseteq \mathbb{R}^n$ is compact, symmetric, and convex. Therefore, Minkowski's Theorem (Theorem **??**) applies. If $\operatorname{vol}(X_t) \geq 2^n \operatorname{covol}(\iota(I)) = 2^n\sqrt{|\operatorname{disc} K|}\ N(I)$, then there exists a nonzero element in $\iota(I) \cap X_t$. In particular, there exists $0 \neq \alpha \in I$ with

$$\operatorname{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}.$$

It is routine to show that $\operatorname{vol}(X_t) = 2^r\pi^s\frac{t^n}{n!}$. Choose then $t > 0$ such that $2^r\pi^s\frac{t^n}{n!} = 2^n\sqrt{|\operatorname{disc} K|}\ N(I)$. Then as $r + 2s = n$, we have

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

□

Remark. In the proof of Theorem **??**, while it may be more straightforward to choose

$$X_t := \left\{ x \in \mathbb{R}^n \colon \prod_{i=1}^{r} |x_i| \prod_{i=r+1}^{r+s} (x_i^2 + y_{i+s})^2 \leq t \right\},$$

by using the idea from $N_{K/\mathbb{Q}}(\alpha)$, this region is not necessarily convex or compact. If $r = 2$ and $s = 0$, then using X_t as above, we have $X_t = \{(x, y) \in \mathbb{R}^2 \colon |xy| \leq t\}$, which is

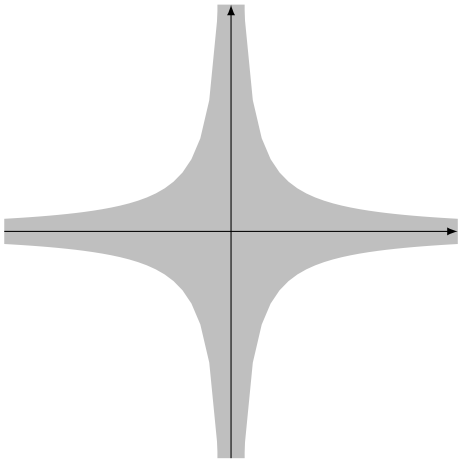


Figure 4: The region $X_t = \{(x, y) \in \mathbb{R}^2 \colon |xy| \leq t\}$.

Corollary 4.1. *Every class in $C\ell_K$ contains an integral ideal of norm at most $\left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} |\operatorname{disc} K|^{1/2}$. In particular, $C\ell_K$ is finite.*

Proof. Take $\kappa \in C\ell_K$. Choose an integral ideal I such that $[I] = \kappa^{-1}$. By Theorem **??**, there is a nonzero $\alpha \in I$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq M_K N(I).$$

Let $J = \alpha I^{-1} \subseteq \mathcal{O}_K$. By construction, $[J] = [I^{-1}] = [I]^{-1} = \kappa$ as these classes are equal up to a prime ideal. However,

$$N(J)N(I) = N(JI) = N(\alpha \mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)| \leq M_K N(I),$$

so that $N(J) \leq M_K$. Therefore as there are only finitely many ideals of $\mathcal{O}_K$ with a given norm, $C\ell_K$ is finite. □

Corollary 4.2. *$C\ell_K$ is generated by equivalence classes of prime ideals with norm at most $\left(\frac{\pi}{4}\right)^s \frac{n!}{n} |\operatorname{disc} K|^{1/2}$.*

Proof. (Sketch) Write $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Then $[I] = [\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_r]^{e_r}$ in $C\ell_K$. However, $N(I) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r}$. The result then follows from Corollary **??**. □

4.5 Discriminant Bounds

Now given a fixed discriminant D, how many number fields K are there such that $\operatorname{disc} K = D$? It turns out $\#\{K/\mathbb{Q} \colon [K \colon \mathbb{Q}] < \infty, \operatorname{disc} K = d\}$ is finite.

Proposition 4.2. *For any integer d, there are only finitely many $n \geq 1$ for which there is a number field $K/\mathbb{Q}$ of degree n and discriminant d.*

By Corollary **??**, every class of $C\ell_K$ contains an integral ideal of norm at most $M_K := \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} |\operatorname{disc} K|^{1/2}$. Since the norm of an ideal is at least 1, we have a lower bound for M_K:

$$1 \leq \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n} |\operatorname{disc} K|^{1/2} =: M_K$$

But then for $\operatorname{disc} K$, we have

$$\sqrt{|\operatorname{disc} K|} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}.$$

We can obtain a slightly weaker inequality by using $\frac{\pi}{4} < 1$ and $s \leq \frac{n}{2}$. Then we have

$$|\operatorname{disc} K|^{1/2} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}.$$

If $a_n = \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}$, then

$$\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2} \left(1 + \frac{1}{n}\right)^n \xrightarrow{n \to \infty} e\sqrt{\frac{\pi}{4}}$$

□

If $K \neq \mathbb{Q}$, i.e. $[K \colon \mathbb{Q}] > 1$, then we have

$$\sqrt{|\operatorname{disc} K|} \geq \left(\frac{\pi}{4}\right)^{2/2} \frac{2^2}{2!} = \frac{\pi}{2} > 1.$$

Hermit then used this fact to show the following:

Theorem 4.4 (Hermite)**.** *For any number field $K \neq \mathbb{Q}$, $\operatorname{disc} K \neq \pm 1$. In particular, there is a prime p that ramifies in K.*

As an interesting application of this, which is otherwise difficult to prove, we have the following:

Proposition 4.3. *Let K, L be number fields such that* $\gcd(\operatorname{disc} K, \operatorname{disc} L) = 1$. *Then* $K \cap L = \mathbb{Q}$.

Proof. Define $E := K \cap L$ and suppose that p ramifies in E. Then p must ramify in both K and L. The ramification degree of $\mathfrak{p}$ over p must be greater than 1 so that

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p) > 1.$$

Now $\mathfrak{P}$ ramifies in K so that $p \mid \operatorname{disc} K$. Similarly, $p \mid \operatorname{disc} L$. But then $\gcd(\operatorname{disc} K, \operatorname{disc} L) > 1$, a contradiction. Therefore, no prime ramifies in E. By Theorem **??**, it must be that $E = \mathbb{Q}$. □

One can use this idea to prove interesting results for the composite of fields.

Proposition 4.4. *Let K, L be number fields such that* $\gcd(\operatorname{disc} K, \operatorname{disc} L) = 1$. *Then if $F = KL$,*

(i) $\mathcal{O}_F = \mathcal{O}_K \mathcal{O}_L$

(ii) if $\{x_i\}$ is an integral basis of K and $\{y_j\}$ is an integral basis for L, then $\{x_i y_j\}$ is a basis for F

(iii) $\operatorname{disc} F = (\operatorname{disc} K)^{[L:\mathbb{Q}]} (\operatorname{disc} L)^{[K:\mathbb{Q}]}$

Theorem 4.5. *For $d \in \mathbb{Z}$, there are only finitely many number fields, up to isomorphism, with discriminant d.*

Proof. It suffices to consider number fields K with a fixed degree n as

$$|\operatorname{disc} K|^{1/2} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!}$$

so that for sufficiently large n, the inequality fails. Fix a number field K of degree $n > 1$ (the case where $n = 1$ is trivial) and let $d = \operatorname{disc} K$. Consider $\iota : \mathcal{O}_K \hookrightarrow \mathbb{R}^n$. Let $\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$ be the r real embeddings of K into $\mathbb{R}$ and let $\sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \dots, \overline{\sigma_{r+s}} : K \hookrightarrow \mathbb{C}$ be the $2s$ complex embeddings of K into $\mathbb{C}$. The map $\iota : \mathcal{O}_K \to \mathbb{R}^n$ can be given by

$$\iota(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Im}(\sigma_{r+1}(\alpha)), \dots, \operatorname{Im}(\sigma_{r+s}(\alpha)), \operatorname{Re}(\sigma_{r+1}(\alpha)), \dots, \operatorname{Re}(\sigma_{r+s}(\alpha))).$$

Fix a constant $C > 0$ and define

$$X := \{x \in \mathbb{R}^n : |x_1| \leq C, |x_i| \leq \frac{1}{2} \text{ for } i \geq 2\}.$$

Because X is a hypercube, it is clear that X is compact, symmetric, and convex. For some constant r_n, depending on n, we have $\operatorname{vol} X \gg r_n C$. Take C sufficiently large (recalling this depends on n and d) so that $\operatorname{vol} X \geq 2^n \operatorname{covol}(\iota(\mathcal{O}_K)) = 2^n |\operatorname{disc} K|^{1/2} = 2^n \sqrt{|d|}$.

Minkowski's Theorem (Theorem **??**) says there exists a nonzero $\alpha \in \mathcal{O}_K$ such that $\iota(\alpha) \in X$. For real σ_i, $|\sigma_i(\alpha)| \leq \frac{1}{2} < 1$ while for complex σ_i, $|\sigma_i(\alpha)| \leq \sqrt{(1/2)^2 + (1/2)^2} < 1$. Therefore, $|\sigma_i(\alpha)| < 1$ for $i \geq 2$. But then $|\sigma_1(\alpha)| > 1$ since

$$1 \leq |N_{K/\mathbb{Q}}(\alpha)| = \prod_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(\alpha)|.$$

and $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ so that all $|\sigma(\alpha)|$ cannot be less than 1.

We claim that $K = \mathbb{Q}(\alpha)$: if p_α is the minimal polynomial of α, then

$$\prod_{\sigma: K \hookrightarrow \mathbb{C}} (x - \sigma(\alpha)) = p_\alpha(x)^{[K:\, \mathbb{Q}(\alpha)]}.$$

We show that $\sigma_1(\alpha) \neq \sigma(\alpha)$ for $\sigma \neq \sigma_1$. This will show that $\sigma_1(\alpha)$ is a root of multiplicity 1, forcing the exponent to be 1. This will show that $[K\colon \mathbb{Q}(\alpha)] = 1$, forcing $K = \mathbb{Q}(\alpha)$. For $\sigma \notin \{\sigma_1, \overline{\sigma_1}\}$, $|\sigma(\alpha)| < 1$. But then $\sigma(\alpha) \neq \sigma_1(\alpha)$ as $|\sigma_1(\alpha)| > 1$. Furthermore, $\sigma_1(\alpha) \neq \overline{\sigma_1(\alpha)}$ as $|\operatorname{Re}(\sigma_1(\alpha))| < \frac{1}{2}$. But then $\operatorname{Im}(\sigma_1(\alpha)) \neq 0$ as $|\sigma_1(\alpha)| > 1$.

Now $|\sigma(\alpha)|$ is bounded by some constant (depending only on n and d for all $\sigma : K \hookrightarrow \mathbb{C}$). Therefore, the coefficients of p_α are bounded in terms of n and d. Then there are finitely many possible p_α since $p_\alpha \in \mathbb{Z}[x]$. Then there are only finitely many $K = \mathbb{Q}(\alpha)$, up to isomorphism. □

Example 4.7. For number fields to be isomorphic, it is necessary that they have the same discriminant. However, this is not sufficient. 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 $p_\beta(x) = x^4 - 24$. Define $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$. We have $\operatorname{disc} K = \operatorname{disc} L = -2^{11} \cdot 3^3$. To tell that the fields are distinct, we examine how primes factor in K and in L. In $\mathcal{O}_K$, $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ while in $\mathcal{O}_L$, $5\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$. Therefore, K and L are not isomorphic. ◁

5 Units in $\mathcal{O}_K$

5.1 Roots of Unity

Fix a number field K of degree n with r real embeddings and s pairs of complex embeddings, i.e. $2s$ total complex embeddings. We now work on addressing the following question: what are the units of the number ring $\mathcal{O}_K$?

Consider the map

$$\begin{aligned} \phi : K^\times &\longrightarrow \mathfrak{I}_K \\ \alpha &\longmapsto \alpha\mathcal{O}_K \end{aligned}$$

where $\mathfrak{I}_K$ is the group of fractional ideals of $\mathcal{O}_K$ which, by the factorization of ideals in $\mathcal{O}_K$ into prime ideals, is the free abelian group on the prime ideals of $\mathcal{O}_K$ The cokernel of ϕ is the class group:

$$\operatorname{coker}\phi = \mathfrak{I}_K \Big/ \operatorname{im}\phi = \mathfrak{I}_K \Big/ \mathfrak{P}_L = \mathrm{C}\ell_K$$

But what is the kernel of ϕ? If $\alpha\mathcal{O}_K = \mathcal{O}_K$ as fractional ideals, then $1 \in \alpha\mathcal{O}_K$. But then there is some $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. Therefore, $\ker\phi = \mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$.

Definition (Roots of Unity)**.** 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 $\phi : \mathcal{O}_K^\times \to \mathbb{R}^{r+s}$ by

$$\alpha \mapsto (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \ldots, 2\log|\sigma_{r+s}(\alpha)|)$$

Proposition 5.1. *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 S of $\alpha \in \mathcal{O}_K^\times$ such that $-C \leq \log|\sigma_i(\alpha)| \leq C$ for all $1 \leq i \leq r+s$. We claim that S is a finite set. If $\alpha \in S$, then $|\sigma_i(\alpha)| \leq e^C$ for all i. Since $i : \mathcal{O}_K \to \mathbb{R}^n$ has a discrete image, there are only finitely many $\alpha \in \mathcal{O}_K$ with $|\sigma(\alpha)| \leq e^C$ for all $\sigma : K \hookrightarrow \mathbb{C}$. Hence, S is finite.

Since C is arbitrary and S is finite, $\psi(\mathcal{O}_K^\times)$ is discrete. Moreover, $\ker\psi \subseteq S$ for any C. Since S is finite, $\ker\psi$ is a finite subgroup of $\mathcal{O}_K^\times$. Hence, $|ker\psi \subseteq \mu_K$. Now let $\zeta \in \mu_K$ be such that $\zeta^m = 1$. Then for any embedding $\sigma : K \hookrightarrow \mathbb{C}$, $|\sigma(\zeta)^m| = 1$, so $|\sigma(\zeta)| = 1$ and $\zeta \in \ker\psi$. Hence, $\mu_K \subseteq \ker\psi$. But then $\mu_K = \ker\psi$. □

5.2 Dirichlet's Unit Theorem

We hope to prove Dirichlet's Unit Theorem:

Theorem 5.1 (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 a finitely generated abelian group with rank $r+s-1$ and $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K are the roots of unity in $\mathcal{O}_K$.*

That is, 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 $\alpha = \zeta \cdot \mu_1^{n_1} \cdots \mu_{r+s-1}^{n_{r+s-1}}$.

Fix a number field K of degree n with r real embeddings and $2s$ complex embeddings, i.e. s pairs of complex conjugate pairs of embeddings. We wish to study $\mathcal{O}_K^\times$. Recall that $\mathfrak{I}_K$ is the group of fractional ideals of $\mathcal{O}_K$; that is, $\mathfrak{I}$ is the free abelian group generated by the prime ideals of $\mathcal{O}_K$. Consider the map $\phi : K^\times \to \mathfrak{I}_K$ given by $\alpha \mapsto \alpha\mathcal{O}_K$. The cokernel of ϕ is precisely the class group:

$$\operatorname{coker}\phi = \mathfrak{I}_K \Big/ \operatorname{im}\phi = \mathfrak{I} \Big/ \mathfrak{P}(K) = \mathrm{C}\ell_K.$$

That is, ϕ is 'not far' from being surjective. What is the kernel of ϕ? We have $\ker \phi = \mathcal{O}_K^\times$: if $\alpha\mathcal{O}_K = \mathcal{O}_K$ as fractional ideals, then $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$.

Definition (Roots of Unity)**.** Let μ_K be the torsion subgroup of $\mathcal{O}_K^\times$; that is, μ_K is the (finite) group of $\alpha \in \mathcal{O}_K^\times$ such that $\alpha^n = 1$ for some $n > 0$ (along with the identity). We call μ_K the roots of unity of $\mathcal{O}_K$.

Define a homomorphism $\psi : \mathcal{O}_K^\times \to \mathbb{R}^{r+s}$ by

$$\alpha \mapsto (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \dots, 2\log|\sigma_{r+s}(\alpha)|).$$

This is a homomorphism as σ and $|\cdot|$ respect multiplication and the logarithm turns multiplication to addition.

Proposition 5.2. *$\phi(\mathcal{O}_K^\times)$ is discrete in $\mathbb{R}^{r+s}$. The kernel of ψ is the finite group μ_K.*

Proof. Fix $C \geq 1$. Consider the set $S = \{\alpha \in \mathcal{O}_K^\times : \log|\sigma_i(\alpha)| \leq C \forall 1 \leq i \leq r+s\}$. We claim that S is finite: if $\alpha \in S$, then $|\sigma_i(\alpha)| \leq e^C$ for all $1 \leq i \leq r+s$. Since $\iota : \mathcal{O}_K \to \mathbb{R}^n$ has discrete image, there are only finitely many $\alpha \in \mathcal{O}_K$ with $|\sigma(\alpha)| \leq e^C$ for all $\sigma : K \hookrightarrow \mathbb{C}$. Hence, S is finite. Now C was arbitrary and S was finite, this shows $\psi(\mathcal{O}_K^\times)$ is discrete.

Now $\ker\psi \subseteq S$ for any C. As S is finite, $\ker\psi$ is a finite subgroup of $\mathcal{O}_K^\times$. But then $\ker\psi \subseteq \mu_K$. Let $\zeta \in \mu_J$ such that $\zeta^n = 1$. For any embedding $\sigma : K \hookrightarrow \mathbb{C}$, $|\sigma(\zeta)|^m = 1$. But then $|\sigma(\zeta)| = 1$ and $\zeta \in \ker\psi$. Therefore, $\mu_K \subseteq \ker\psi$ and hence $\mu_K = \ker\psi$. □

Before proving Dirichlet's Unit Theorem make a definition, and prove a useful lemma. Define

$$V := \left\{ x \in \mathbb{R}^{r+s} \;\middle|\; \sum_{i=1}^{r+s} x_i = 0 \right\}$$

Note that V is an $\mathbb{R}$-vector space of dimension $r+s-1$. We claim that $\psi(\mathcal{O}_K^\times) \subseteq V$. If $\alpha \in \mathcal{O}_K^\times$, then

$$1 = |N_{K/\mathbb{Q}}(\alpha)| = \prod_\sigma |\sigma(\alpha)| = \prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{i=1}^{r+s} |\sigma_i(\alpha)|^2.$$

Taking logarithms, we have

$$0 = \sum_{i=1}^{r} \log|\sigma_i(\alpha)| + 2\sum_{i=1}^{r+s} \log|\sigma_i(\alpha)|.$$

But then $\psi(\alpha) \in V$. By the discreteness of $\psi(\mathcal{O}_K^\times)$,

$$\mathcal{O}_K^\times \Big/ \mu_K \cong \psi(\mathcal{O}_K^\times).$$

Dirichlet's Unit Theorem is equivalent to the claim that $\psi(\mathcal{O}_K^\times)$ is a lattice in V. This leads to the regulator of a number field.

Definition (Regulator)**.** Given a number field K, the regular of K is

$$\mathrm{Reg}_K := \frac{\mathrm{covol}(\psi(\mathcal{O}_K^\times))}{\sqrt{r+s}}$$

Alternatively, consider the $(r+s-1)\times(r+s)$ matrix $M = (e_j \log|\sigma_j(u_i)|)$, where $u_1, \dots, u_{r+s-1}$ is a basis for $\mathcal{O}_K^\times/\mu_k$ as an $\mathcal{O}_K^\times$-module. Then $\pm\,\mathrm{Reg}_K$ is the determinant of the matrix M after removing a column, say M'. Then $\mathrm{Reg}_K = |\det M'|$.

Remark. The regulator is a real positive number. The denominator $\sqrt{r+s}$ is merely a 'normalization' factor.

It is often useful to know the regulator of a field K. Indeed, if $\mu_K, \alpha_1, \dots, \alpha_{r+s-1}$ generate a subgroup $H \leq \mathcal{O}_K^\times$ of rank $r+s-1$ then

$$\frac{\mathrm{covol}(\psi(H))}{\mathrm{covol}(\psi(\mathcal{O}_K^\times))} = [\mathcal{O}_K^\times : H].$$

The denominator we obtain from the regulator after 'normalization'. Therefore, if we know the index and the regulator, we can find $\mathrm{covol}(\psi(H))$ and use this to to find H. In any case, we are now in a position to prove Dirichlet's Unit Theorem.

Theorem ?? (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 a finitely generated abelian group with rank $r+s-1$ and $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K are the roots of unity in $\mathcal{O}_K$.*

Proof. Consider the case $r+s-1=0$. In this case, $\psi(\mathcal{O}_K^\times) \subseteq K$ and $\dim_{\mathbb{R}} V = r+s-1 = 0$. Therefore, $\psi(\mathcal{O}_K^\times) = 0$.

Now assume that $r+s-1 > 0$. Assume to the contrary that $\psi(\mathcal{O}_K^\times)$ has rank less than $r+s-1$. Then there is a nonzero $\mathbb{R}$-linear map $f : V \to \mathbb{R}$ with $f(\psi(\mathcal{O}_K^\times)) = 0$. [Since $\psi(\mathcal{O}_K^\times)$ has rank less than $r+s-1$, there are some defining equations. These are then in the kernel] There are unique $c_i \in \mathbb{R}$ such that for all $v \in V \subseteq \mathbb{R}^{r+s}$, $f(v) = c_1 v_1 + \cdots + c_{r+s-1} v_{r+s-1}$. Note that we do not require v_{r+s} since $\sum_i v_i = 0$. Using $\phi(\mathcal{O}_K^\times) \subseteq V$, we can extend f to an $\mathbb{R}$-linear map $f : \mathbb{R}^{r+s} \to \mathbb{R}$.

Define

$$A := \sqrt{|\operatorname{disc} K|}\left(\frac{2}{\pi}\right)^s > 0,$$

which depends only on the number field K. We want to construct a sequence $\alpha_1, \alpha_2, \dots$ of nonzero elements of $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha_i)| \leq A$, and the values $f(\psi(\alpha_i))$ are distinct. Assuming such a sequence exists, then $N_{K/\mathbb{Q}}(\alpha_i\mathcal{O}_K)|N_{K/\mathbb{Q}}(\alpha_i)| \leq A$. 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 $f(\psi(\alpha_n)) \neq f(\psi(\alpha_m))$ (this is the Pigeonhole Principle). Define $\beta = \alpha_n \alpha_m^{-1} \in K^\times$. Then $\beta \mathcal{O}_K = \mathcal{O}_K$ so that $\beta \in \mathcal{O}_K^\times$. On the other hand,

$$f(\psi(\beta)) = f(\psi(\alpha_n)) - f(\psi(\alpha_m)) \neq 0,$$

contradicting the choice of f such that $f(\psi(\mathcal{O}_K^\times)) = 0$ as $\beta \in \mathcal{O}_K^\times$.

We need now only prove the existence of such a sequence. Recall we have an embedding $\iota : \mathcal{O}_K \hookrightarrow \mathbb{R}^n$ such that $\iota(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ with covolume $\sqrt{|\operatorname{disc} K|}$. Define

$$X := \left\{ x \in \mathbb{R}^n \colon |x_i| \leq b_i \text{ for } 1 \leq i \leq r, x_i^2 + x_{i+s}^2 \leq b_i^2 \text{ for } r+1 \leq i \leq r+s \right\}$$

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 $\iota(\alpha) \in X$, 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, convex, and

$$\operatorname{vol} X = \prod_{i=1}^{r} (2b_i) \cdot \prod_{i=r+1}^{r+s} (\pi b_i^2) \cdot 2^s = 2^{r+s} \pi^s A = 2^n \sqrt{|\operatorname{disc} K|} = 2^n \operatorname{covol}(\iota(\mathcal{O}_K)).$$

So by Minkowski's Theorem, there is some $\alpha \in \mathcal{O}_K \setminus \{0\}$ such that $\iota(\alpha) \in X$. Therefore, $|N_{K/\mathbb{Q}}(\alpha)| \leq A$. By varying the b_i, we can find α with $f(\psi(\alpha)) \in \mathbb{R}$ arbitrarily large. This will complete the proof.

We claim that for $1 \leq i \leq r+s$, $b_i / A \leq |\sigma_i(\alpha)| \leq b_i$. We know that $|\sigma_i(\alpha)| \leq b_i$ by the construction of α. For the lower bound, we have

$$\begin{aligned} 1 \leq |N_{K/\mathbb{Q}}(\alpha)| &= |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)| \left(|\sigma_{r+1}(\alpha)| \cdots |\sigma_{r+s}(\alpha)| \right)^2 \\ &\leq |\sigma_i(\alpha)| \, \frac{b_1 \cdots b_r (b_{r+1} \cdots b_{r+s})}{b_i} = |\sigma_i(\alpha)| \, \frac{A}{b_i}, \end{aligned}$$

i.e. $|\sigma_i(\alpha)|$ is 'roughly' b_i. Evaluating $f(v) = \sum_{i=1}^{r+s-1} c_i v_i$ at $\psi(\alpha)$ yields

$$f(\psi(\alpha)) = \sum_{i=1}^{r+s-1} c_i e_i \log |\sigma_i(\alpha)|.$$

Approximating $|\sigma_i(\alpha)|$ by b_i,

$$\begin{aligned} \left| f(\psi(\alpha)) - \sum_{i=1}^{r+s-1} c_i e_i \log b_i \right| &\leq 2 \sum_{i=1}^{r+s-1} |c_i| \, |\log |\sigma_i(\alpha)| - \log b_i| \\ &\leq 2 \sum_{i=1}^{r+s-1} |c_i| \log(|\sigma_i(\alpha)| / b_i) \\ &\leq 2 \sum_{i=1}^{r+s-1} |c_i| \log A, \end{aligned}$$

where the last inequality follows from the remarks above. The bound $2\sum_{i=1}^{r+s-1}|c_i|\log A$ depends only on the number field K. Rearranging,

$$f(\psi(\alpha)) \geq \sum_{i=1}^{r+s-1} c_i e_i \log b_i - 2\sum_{i=1}^{r+s-1} |c_i| \log A.$$

The c_i are not all zero since $f \neq 0$. Therefore, there exist $b_1, \ldots, b_{r+s-1}$ 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 not present in the sum, we can choose $b_1, \ldots, \hat{b_i}, \ldots, b_{r+s-1}$, where b_i is excluded from this list, such that $b_1 \ldots b_r (b_{r+1} \cdots b_{r+s})^2 = A$. □

5.3 Examples of Dirichlet's Unit Theorem

Example 5.1. If $K = \mathbb{Q}$, then $r = 1$ and $s = 0$ so that $r + s - 1 = 0$. Therefore, $\mathcal{O}_{\mathbb{Q}}^{\times} = \mathbb{Z}^{\times} = \{\pm 1\}$. ◁

Example 5.2. Let $d > 1$ be a squarefree integer. If $K = \mathbb{Q}(\sqrt{d})$, then $r = 2$ and $s = 0$ so that $r + s - 1 = 1$. Then $\mathcal{O}_K^{\times} \cong \mu_K \times \mathbb{Z}$. Since $K \subseteq \mathbb{R}$ and the only real roots of unit are ± 1, $\mu_K = \{\pm 1\}$. Under the isomorphism $\mathcal{O}_K \cong \mu_K \times \mathbb{Z}$, there is $\epsilon \in \mathcal{O}_K^{\times}$ such that $\mathcal{O}_K^{\times} = \{\pm \epsilon^n : n \in \mathbb{Z}\}$. If we choose $\epsilon > 1$, this fundamental unit of this ring of integers. As a few examples:

d	ϵ	$N_{K/\mathbb{Q}}(\epsilon)$
2	$1 + \sqrt{2}$	-1
10	$3 + \sqrt{10}$	-1
93	$\frac{29 + 3\sqrt{93}}{2}$	-1
94	$2143295 + 221064\sqrt{94}$	-1

◁

Example 5.3. Let $d < 0$ be a squarefree integer. If $K = \mathbb{Q}(\sqrt{d})$, then $r = 0$ and $s = 1$ so that $r + s - 1 = 0$. In this case, $\mathcal{O}_K^{\times} = \mu_K$. We can be even more explicit: if $d \not\equiv 1 \mod 4$, take $\alpha = a + b\sqrt{d} \in \mathcal{O}_K \setminus \{0\}$. Then 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 $(a, b) = (\pm 1, 0)$ for $d \neq -1$ and $(a, b) = (0, \pm 1)$ if $d = -1$. Hence, $\alpha = \pm 1$ if $d \neq -1$ and $\alpha = \pm i$ if $d = -1$. Thus, we have

found

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1\}, & d \neq -1, -3 \\ \{\pm i\}, & d = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\}, & d = -3 \end{cases}$$

◁

Example 5.4. If $K = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, where $\zeta = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity. We have $[K\colon \mathbb{Q}] = 6$. Furthermore, we have $\mathcal{O}_K = \mathbb{Z}[\epsilon]$. There are no real embeddings, i.e. $r = 0$, and six complex embeddings, i.e. $s = 3$. Then we have $r + s - 1 = 2$. Then we have $\mu_K = \mu_6 = \{\pm 1, \pm\zeta, \pm\zeta^2\}$. Therefore, $\mathcal{O}_K^\times = \mu_6\langle\epsilon, \bar{\epsilon}\rangle$, where the fundamental unit is

$$\epsilon = \frac{-1 + 2\sqrt[3]{2} + (\sqrt[3]{2})^2}{3} + \frac{1 - \sqrt[3]{2} + (\sqrt[3]{2})^2}{2}\,\zeta$$

◁

Example 5.5. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $r = 4$ and $s = 0$ so taht $r + s - 1 = 3$. The roots of unity of $\mathcal{O}_K$ is $\mu_K = \{\pm 1\}$ with fundamental units

$$\begin{aligned} u_1 &= 1 + \sqrt{2} \\ u_2 &= \sqrt{2} + \sqrt{3} \\ u_3 &= \frac{\sqrt{2} + \sqrt{6}}{2} \end{aligned}$$

Verifying that these are units and linearly independent is fairly routine. However, showing that they do indeed generate $\mathcal{O}_K$ is not so trivial. ◁

Example 5.6. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $p_\alpha(x) = x^3 - 3x + 1$. We have $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Now $p_\alpha(x)$ has three real roots so that $r = 3$ and $s = 0$. Therefore, $\mathcal{O}_K^\times$ has rank $r + s - 1 = 2$. In fact, $\mathcal{O}_K^\times = \pm\langle u_1, u_1\rangle$, 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 u in terms of the generators u_1, u_2? Compute the image of u, u_1, u_2 under the map $\psi : \mathcal{O}_K^\times \to \mathbb{R}^3$ given by $\alpha \mapsto (\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|, \log|\sigma_3(\alpha)|)$. We have

$$\begin{aligned} \psi(u) &= (-1.0395\ldots, 4.4346\ldots, -3.3950\ldots) \\ \psi(u_1) &= (-0.4266\ldots, -0.6309\ldots, 1.0575\ldots) \\ \psi(u_2) &= (-0.6309\ldots, 1.0575\ldots, -0.4266\ldots) \end{aligned}$$

Since $u = \pm u_1^m u_2^n$ for unique $m, n \in \mathbb{Z}$ and ψ is a homomorphism, we may write $\psi(u) = m\psi(u_1) + n\psi(u_2)$. A numerical calculation shows $(m, n) \approx (-2.0002\ldots, 3.0001\ldots)$. So we expect $u = \pm u_1^{-2} u_2^3$. A routine calculation verifies that $u = \pm u_1^{-2} u_2^3$. ◁

Moreover for any order $R \subseteq K$, we have $R^\times \cong \mu_R \times \mathbb{Z}^{r+s-1}$. Dirichlet proved this for $R = \mathbb{Z}[\alpha]$, i.e. monogenic orders.

Proposition 5.3. *For any order $R \subseteq K$, $R^\times \cong \mu_R \times \mathbb{Z}^{r+s-1}$, where μ_R is the set of roots of unity in R.*

Proof. Let $N = [\mathcal{O}_K : R]$. Note that $N\mathcal{O}_K \subseteq R \subseteq \mathcal{O}_K$. We want to show that $[\mathcal{O}_K^\times : R^\times]$ is finite. Consider the map $\phi : \mathcal{O}_K^\times \to (\mathcal{O}_K/N\mathcal{O}_K)^\times$. We want to show $\ker\phi = R^\times$. This would prove finite index.

Choose $\alpha \in \mathcal{O}_K^\times$. There exists $n \in \mathbb{N}$ such that $\alpha^n \equiv 1 \mod N\mathcal{O}_K$. We have $\alpha^{-1} \equiv 1 \mod N\mathcal{O}_K$. But then both $\alpha - 1$ and $\alpha^{-1} - 1$ are in $N\mathcal{O}_K \subseteq R$. But then $\alpha, \alpha^{-1} \in R$ so that $\alpha \in R^\times$. Therefore, $[\mathcal{O}_K^\times : R^\times]$ divides $\#(\mathcal{O}_K/N\mathcal{O}_K)^\times$. Since $\#(\mathcal{O}_K/N\mathcal{O}_K)^\times$ is finite, this proves finiteness. Furthermore by Theorem **??**, $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r + s - 1$. But then $R^\times$ must too be a finitely generated abelian group of rank $r + s - 1$. □

5.4 Pell's Equation

One example of the power of Dirichlet's Unit Theorem deserves special attention: the Pell equation. [One might recall this from Example **??** and Example **??**.]

Fix $d > 0$ a squarefree integer. What are the solutions $(x, y) \in \mathbb{Z}^2$ to the Pell equation $x^2 - dy^2 = 1$? We can rephrase this question as follows: what elements $a + b\sqrt{d} \in K := \mathbb{Q}(\sqrt{d})$ of the order $R = \mathbb{Z}[\sqrt{d}]$ with $N_{K/\mathbb{Q}}(a + b\sqrt{d}) = 1$? This set is in bijection with the set of solutions of Pell's equation $G := \{(a, b) \in \mathbb{Z}^2 : a^2 - db^2 = 1\}$. We know by Proposition **??** that $R^\times \cong \mu_R \times \mathbb{Z}$. In this case, G is index 1 (all units have norm 1) or 2 (there is a unit of norm -1) in $R^\times$. Therefore, $G = \pm\langle u \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Example 5.7. If $d = 10$, we have the equation $x^2 - 10y^2 = 1$. The fundamental unit of $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ is $\epsilon = 3 + \sqrt{10}$. The norm of this fundamental unit is $N_{K/\mathbb{Q}}(\epsilon) = -1$. A few possible solutions are:

n	$(\epsilon^2)^n$	Solution
1	$19 + 6\sqrt{10}$	(19,6)
2	$721 + 228\sqrt{10}$	(721,228)
3	$27379 + 8658\sqrt{10}$	(27379,8658)

In fact, these are all the solutions in the positive integers. ◁

Example 5.8. Recall Example **??**. We want to find a solution (x, y) in positive integers to $x^2 - 1141y^2 = 1$. Let $K = \mathbb{Q}(\sqrt{1141}) \subseteq \mathbb{R}$. The corresponding ring of integers is

$\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{1141}}{2}$ as $1141 \equiv 1 \mod 4$. Then

$$\mathcal{O}_K = Z[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha = \left\{ \frac{a + b\sqrt{1141}}{2} \;\middle|\; a, b \in \mathbb{Z}, a \equiv b \mod 2 \right\}$$

We want to describe $\mathcal{O}_K^\times$ and $R^\times$. Note that $r = 2$ and $s = 0$ so that $r + s - 1 = 1$. Dirichlet's Unit Theorem, Theorem **??**, gives $\mathcal{O}_K^\times = \pm\langle u \rangle$ for some unique fundamental unit $u > 1$ in $\mathcal{O}_K^\times$. The problem then reduces down to finding u.

For $\beta \in K^\times$, $\beta\mathcal{O}_K = \mathcal{O}_K$ if and only if $\beta \in \mathcal{O}_K^\times$. We wish to find α, β such that $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$, implying $\alpha\beta^{-1} \in \mathcal{O}_K^\times$. As $x^2 - x - 285 \equiv x^2 - x \equiv x(x-1) \mod 3$, factor $3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$, where $\mathfrak{p}_3 = (3, \alpha)$ and $p_3' = (3, \alpha - 1)$. Similarly, $x^2 - x - 285 \equiv x(x-1) \mod 5$ so that we factor $5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'$, where $\mathfrak{p}_5 = (5, \alpha)$ and $\mathfrak{p}_5' = (5, \alpha - 1)$. Finally, factor

$$\begin{aligned} 15 - \alpha &= \frac{29 - \sqrt{1141}}{2} \\ 15 + \alpha &= \frac{31 + \sqrt{1141}}{2} \\ 21 - \alpha &= \frac{41 - \sqrt{1141}}{2} \end{aligned}$$

The norms suggest the factorizations as these only involve 3 and 5 — three ideals, two relations. We have $N_{K/\mathbb{Q}}(15 - \alpha) = -75 = -3 \cdot 5^2$. Note that $15 - \alpha \in \mathfrak{p}_3$, $15 - \alpha \in \mathfrak{p}_5$, and $15 - \alpha \notin \mathfrak{p}_5'$. For the last, note that if $15 - \alpha \in \mathfrak{p}_5\mathfrak{p}_5' = (5)$, then $\frac{15-\alpha}{5} \in \mathcal{O}_K$, a contradiction. Then we have factored $(15 - \alpha) = \mathfrak{p}_3\mathfrak{p}_5^2$. Similarly, we can factor

$$\begin{aligned} (15 - \alpha) &= \mathfrak{p}_3\mathfrak{p}_5^2 \\ (15 + \alpha) &= \mathfrak{p}_3^2\mathfrak{p}_5 \\ (21 - \alpha) &= \mathfrak{p}_3^3\mathfrak{p}_5 \end{aligned}$$

Multiplying the last equation by $\mathfrak{p}_5^2$ on the right and dividing by (5), we have an equation in fraction ideals

$$\left(\frac{21 - \alpha}{5}\right) = \mathfrak{p}_3^2\mathfrak{p}_5^{-1}.$$

To obtain a unit, observe

$$(15 - \alpha)^a(15 + \alpha)^b \left(\frac{21 - \alpha}{5}\right)^c = (\mathfrak{p}_3^2\mathfrak{p}_5^2)^a(\mathfrak{p}_3^2\mathfrak{p}_5)^b(\mathfrak{p}_3^3\mathfrak{p}_5^{-1})^c = \mathfrak{p}_3^{a+2b+3c}\mathfrak{p}_5^{2a+b-c}$$

To find a unit in $\mathcal{O}_K$, we need question when this ideal is $\mathcal{O}_K$. This occurs when both exponents vanish, i.e. for $a = \frac{5}{3}c$ and $b = -\frac{7}{3}c$ with c free. Choosing $c = 3$, we have

$(a,b,c) = (-5,7,-3)$. Then

$$\begin{aligned}\epsilon &= -(15-\alpha)^{-5}(15+\alpha)^7\left(\frac{21-\alpha}{5}\right)^{-3}\\ &= 618715978 + 37751109\,\alpha\end{aligned}$$

is a unit in $\mathcal{O}_K$ (which is not ± 1). In fact, ϵ is the fundamental unit of $\mathcal{O}_K^\times$. Now we wanted solutions of $x^2 - 1141y^2 = 1$. Hence, we were searching for units in $R = \mathbb{Z}[\sqrt{1141}] \neq \mathcal{O}_K$. In particular, $\epsilon \notin R$. However, $\epsilon^3 \in R^\times$. In fact, $R^\times = \pm\langle\epsilon^3\rangle$. This gives a solution (x_0, y_0), where

$$\begin{aligned}x_0 &= 1036782394157223963237125215\\ y_0 &= 30693385322765657197397208\end{aligned}$$

Moreover, this is the smallest possible positive pair of solutions. ◁

6 Factoring in Galois Extensions

6.1 Overview of Galois Theory

Let K be a field, which for simplicity we assume has characteristic 0 or is finite. [This assumption is to force K to be perfect so that finite extensions L/K are separable.] Let L/K be a finite extension of fields. Define $\mathrm{Aut}(L/K)$ to be the group (under function composition) of field automorphisms of L fixing K element-wise, i.e. if σ is an automorphism of L, then $\sigma|_K = 1_K$. For $H \leq \mathrm{Aut}(L/K)$, denote by L^H the field (the reader should check this) of $x \in L$ such that $\sigma(x) = x$ for all $\sigma \in H$. In particular, $K \subseteq L^H \subseteq L$. Observe taking subgroups of $H \leq \mathrm{Aut}(L/K)$ and finding L^H is a way of producing fields.

Example 6.1. Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree. We know that $\mathrm{Aut}(L/K) = \{1, \tau\}$, where τ is conjugation of $\sqrt{d}$, i.e. $1(a + b\sqrt{d}) = a + b\sqrt{d}$ and $\tau(a + b\sqrt{d}) = a - b\sqrt{d}$. Then $L^{\mathrm{Aut}(L/K)} = \mathbb{Q}$. ◁

Example 6.2. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. If $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$, then $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2$. However, $x^3 - 2$ has only one root in $L \subseteq \mathbb{R}$. Therefore, $\mathrm{Aut}(L/\mathbb{Q}) = \{1\}$. ◁

Non-Example 6.1. Consider $K = \mathbb{F}_p(t)$ and choose a root u of the irreducible polynomial $x^p + t \in K[x]$. Let $L = K(u) = \mathbb{F}_p(u)$. We have $(x+u)^p = x^p + u^p = x^p + t$ is totally reducible. But then L/K is a splitting field but $\mathrm{Aut}(L/K) = 1$ as there is only one root so the automorphism is forced: $u \mapsto u$. ◁

Since the definition of a Galois extension involves the size of $\mathrm{Aut}(L/K)$, we remind the reader that the cardinality of $\mathrm{Aut}(L/K)$ is bounded by the degree of the extension.

Proposition 6.1. $\#\operatorname{Aut}(L/K) \leq [L\colon K]$

Proof. Let $L = K(\alpha)$. We have assumed K has characteristic 0 or is finite so that the extension L/K is separable. Let $f(x) \in K[x]$ be the minimal polynomial of α. Each $\sigma \in \operatorname{Aut}(L/K)$ is determined by $\sigma(\alpha)$ and $\sigma(\alpha)$ is also a root of $f(x)$ (apply σ to $f(x)$ and use the fact that the coefficients are in K: $\sigma(f(\alpha)) = f(\sigma(\alpha))$). Therefore,

$$\#\operatorname{Aut}(L/K) \leq \#\{a \in L\colon f(a) = 0\} \leq \deg f = [L\colon K]. \qquad \square$$

Definition (Galois Extension)**.** We say that an extension L/K is Galois if it is a separable extension and any of the following equivalent conditions hold:

(i) $\#\operatorname{Aut}(L/K) = [L\colon K]$

(ii) $L^{\operatorname{Aut}(L/K)} = K$

(iii) L is the splitting field of some (irreducible) polynomial, i.e. $L = K(\alpha_1, \ldots, \alpha_n)$ with $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$.

Definition (Galois Group)**.** If L/K is Galois, then the Galois group of L/K is $\operatorname{Gal}(L/K) := \operatorname{Aut}(L/K)$.

Theorem 6.1 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite Galois extension. There is an inclusion reversing bijection*

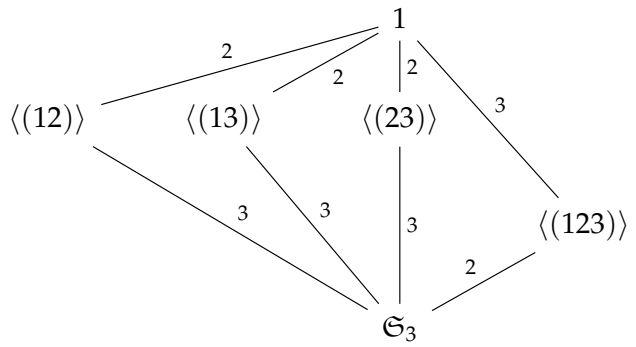
$$\left\{\begin{matrix}\textit{Subgroups of} \\ \operatorname{Gal}(L/K).\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\textit{Subfields} \\ K \subseteq F \subseteq L.\end{matrix}\right\}$$

where the coorespondences are given by $H \mapsto L^H$ and $F \mapsto \operatorname{Aut}(L/F =: \operatorname{Gal}(L/F)$, respectively.

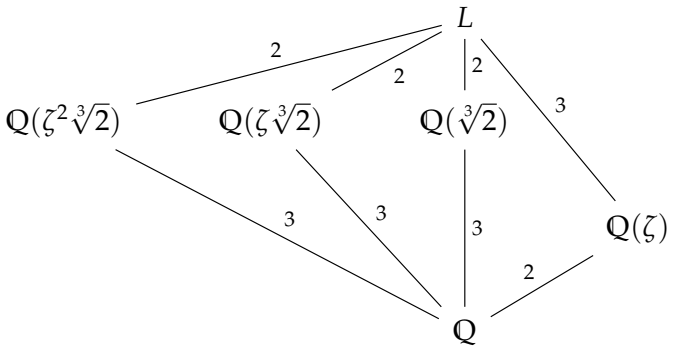
An amazing result to come out of the Fundamental Theorem of Galois Theory is the fact that there must be finitely many intermediate fields between L and K (since these correspond to subgroups of a finite group). While it is possible to prove this without Galois Theory, it is not a simple matter.

Example 6.3. Let $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$, where ζ is a primitive cube root of unity. Then L is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$, which has roots $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \zeta\sqrt[3]{2}$, and $\alpha_3 = \zeta^2\sqrt[3]{2}$. There is an injective group homomorphism $\phi : \operatorname{Gal}(L/\mathbb{Q}) \hookrightarrow \mathfrak{S}_3$, the symmetric group on '3 letters', such that $\sigma_{\alpha_i} = \alpha_{\phi(\sigma)_i}$ for all $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$ with $i = 1, 2, 3$. Since $\#\operatorname{Gal}(L/\mathbb{Q}) = [L\colon \mathbb{Q}] = 6$ and $|\mathfrak{S}_3| = 6$, this map must then be an isomorphism. The lattice of subgroups

of $\mathfrak{S}_3$ is



By the Fundamental Theorem of Galois Theory, we get a corresponding lattice for subfields $K \subseteq F \subseteq L$. Notice the lattice is the 'upside-down' version of the group lattice with the same extension degrees.



◁

Example 6.4 (Frobenius)**.** Let p be a prime. Consider the field extension $\mathbb{F}_p \leq \mathbb{F}_{p^n}$. This is a separable extension as $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$. In fact, the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group of order n generated by the Frobenius homomorphism: $\mathrm{Frob}_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ given by $x \mapsto x^p$. It is clear that Frob_p generates as Frob_p has order the smallest integer d such that $\mathrm{Frob}_p^d(x) = x^{p^d} = x$ for all $x \in \mathbb{F}_{p^n}$ so that $d = n$. The intermediate fields $\mathbb{F}_p \subseteq F \subseteq \mathbb{F}_{p^n}$ are the subgroups of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ which are the cyclic groups of order d for $d \mid n$. ◁

Example 6.5 (Cyclotomic Extensions)**.** Let $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. The extension $L/\mathbb{Q}$ is Galois as the roots of $x^n - 1$ are ζ_n^i with $0 \leq i < n$. The minimal polynomial of ζ_n is

$$\Phi_n(x) = \prod_{\substack{i=1 \\ \gcd(i,m)=1}}^{n} (x - \zeta_n^i) \in \mathbb{Z}[x]$$

The degree of $\Phi_n(x)$ is $\phi(n)$, where $\phi(n)$ is the Euler totient function: $\phi(r) = \#C_r$, where $C_r := \{i \colon 1 \leq i < r, \gcd(i,r) = 1\}$.

For $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, σ is determined entirely by its action on ζ_n: $\sigma(\zeta_n) = \zeta_n^a$ for $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$. There is an injective homomorphism

$$\Psi : \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

given by $\sigma(\zeta_n) = \zeta_n^{\Psi(\sigma)}$ for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Since both groups have the same cardinality, this is an isomorphism. ◁

6.2 Splitting in Galois Extensions

Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L.K)$. For $\alpha \in L$, recall we have maps:

$$Tr_{L/K}(\alpha) = \sum_{g \in G} \sigma(\alpha)$$
$$N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Proposition 6.2. *Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. For any $\sigma \in G$, $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.*

Proof. If $\alpha \in L$, the minimal polynomial of $\sigma(\alpha)$ is the same as the minimal polynomial of α:

$$\sigma(p_\alpha(x)) = p_\alpha(\sigma(x)) = p_{\sigma(\alpha)}(x).$$

□

By the Proposition, there is a well-defined action of G on $\mathcal{O}_L$: if $\sigma \in G$ and $I \subseteq \mathcal{O}_L$ is an ideal, then $\sigma(I) \subseteq \sigma(\mathcal{O}_L) = \mathcal{O}_L$ is also an ideal. Then we have an isomorphism of rings

$$\mathcal{O}_L \,/\, I \longrightarrow \mathcal{O}_L \,/\, \sigma(I)$$
$$x + I \longmapsto \sigma(x) + \sigma(I)$$

In particular, if $\mathfrak{P} \subseteq \mathcal{O}_L$ is a prime ideal, then $\sigma(\mathfrak{P}) \subseteq \mathcal{O}_L$ is a prime ideal. Choose any nonzero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ and $\sigma \in G$. As $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ and $\mathfrak{p} \subseteq K$ is fixed, we have $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$. On the other hand, $\sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{\mathfrak{P}} \sigma(\mathfrak{P})^{e(\mathfrak{P}/\mathfrak{p})}$, where $\sigma(\mathfrak{P})$ is still prime. Therefore, $\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}} \sigma(\mathfrak{P})^{e(\mathfrak{P}/\mathfrak{p})}$. By unique factorization, the Galois group G acts on the set of primes diving $\mathfrak{p}$: $\{\mathfrak{P} \subseteq \mathcal{O}_L \colon \mathfrak{P} \mid \mathfrak{p}\}$. Furthermore, $e(\sigma(\mathfrak{P})/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ (by unique factorization) and $f(\sigma(\mathfrak{P})/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$ (by the isomorphism of rings above). This proves the following:

Proposition 6.3. *Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. If $\mathfrak{p} \subseteq \mathcal{O}_K$ is a nonzero prime and $\mathfrak{P} \subseteq \mathcal{O}_L$ with $\mathfrak{P} \mid \mathfrak{p}$, then*

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{P}} \sigma(\mathfrak{P})^{e(\mathfrak{P}/\mathfrak{p})}$$
$$e(\sigma(\mathfrak{P})/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$$
$$f(\sigma(\mathfrak{P})/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$$

The Galois group even acts transitively on the set of prime ideals of $\mathcal{O}_L$ dividing $\mathfrak{p}$.

Proposition 6.4. *Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime ideal. Then G acts transitively on the set of prime ideals of $\mathcal{O}_L$ dividing $\mathfrak{p}$.*

Proof. Suppose to the contrary that this were not the case. Then there are two primes $\mathfrak{P}, \mathfrak{P}'$ in two different Galois orbits. By the Chinese Remainder Theorem, there exists $x \in \mathcal{O}_L$ with $x \in \mathfrak{P}$ and $x \notin \sigma(\mathfrak{P}')$ for all $\sigma \in G$. Then

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) = x \prod_{\substack{\sigma \in G \\ \sigma \neq 1}} \sigma(x) \in \mathfrak{P}$$

since $x \in \mathfrak{P}$. But then we must have

$$\prod_{\sigma \in G} \sigma(x) = N_{L/K}(x) \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \subseteq \mathfrak{P}'.$$

As $\mathfrak{P}'$ is prime, $\sigma(x) \in \mathfrak{P}'$ for some $\sigma \in G$. But then $x \in \sigma^{-1}(\mathfrak{P}')$, a contradiction. □

Combining Proposition **??** and Proposition **??**, we can now characterize factoring in Galois extensions.

Theorem 6.2 (efg-Theorem)**.** *Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. For any nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$, we have $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$, where the $\mathfrak{P}_i \subseteq \mathcal{O}_L$ are distinct prime ideals dividing $\mathfrak{p}$ and $e \geq 1$ is unique. Furthermore, $f = f(\mathfrak{P}_i/\mathfrak{p})$ is independent of the choice of $\mathfrak{P}_i$. Finally,*

$$[L\colon K] = \sum_{\mathfrak{P}\mid\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = \sum_{\mathfrak{P}\mid\mathfrak{p}} ef = efg.$$

Remark. Note that while e, f, g do not depend on the choice of $\mathfrak{P}$, they do depend on the choice of $\mathfrak{p}$. One can indicate this by writing $e_\mathfrak{p}$, $f_\mathfrak{p}$, and $g_\mathfrak{p}$, respectively.

Definition (Decomposition Group)**.** Let L/K be a finite Galois extension of number fields, and let $G = \mathrm{Gal}(L/K)$. Choose a nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$ and fix a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ dividing $\mathfrak{p}$. Define the decomposition group of $\mathfrak{P}$ to be the subgroup of G, $D_\mathfrak{P}$, fixing $\mathfrak{P}$, i.e.

$$D_\mathfrak{P} := \{\sigma \in G\colon \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

It is routine to verify that there is a bijection

$$G \,/\, D_{\mathfrak{P}} \xrightarrow{\sim} \{\mathfrak{P}' \colon \mathfrak{P}' \mid \mathfrak{p}\}$$
$$\sigma \longmapsto \sigma(\mathfrak{P})$$

By Theorem **??**, we know that $\#\{\mathfrak{P}' \colon \mathfrak{P}' \mid \mathfrak{p}\} = g$. Then

$$g = \left| G \Big/ D_{\mathfrak{P}} \right| = \frac{|G|}{|D_{\mathfrak{P}}|} = \frac{[L \colon K]}{|D_{\mathfrak{P}}|} = \frac{efg}{|D_{\mathfrak{P}}|}.$$

Therefore, $|D_{\mathfrak{P}}| = ef$. Choose now $\sigma \in D_{\mathfrak{P}}$. We have an isomorphism

$$\mathbb{F}_P := \mathcal{O}_L \,/\, \mathfrak{P} \xrightarrow{\sim} \mathcal{O}_L \,/\, \mathfrak{P} =: \mathbb{F}_{\mathfrak{P}}$$
$$x + \mathfrak{P} \longmapsto \sigma(x) + \sigma(\mathfrak{P}) = \sigma(x) + \mathfrak{P}$$

Therefore, σ induces an automorphism of $\mathbb{F}_{\mathfrak{P}}$ that fixes $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$. This induces a group homomorphism $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. The group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is cyclic of order $f(\mathfrak{P}/\mathfrak{p}) = f_{\mathfrak{p}}$, generated by $x \mapsto x^{N(\mathfrak{p})}$, where $N(\mathfrak{p}) = \#\mathbb{F}_{\mathfrak{p}}$.

Lemma 6.1. *The map $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is surjective.*

Proof. Using the Chinese Remainder Theorem, choose $\alpha \in \mathcal{O}_L$ such that $\mathbb{F}_{\mathfrak{p}}(\overline{\alpha}) = \mathbb{F}_{\mathfrak{P}}$, where $\overline{\alpha} := \alpha \mod \mathfrak{P}$, and $\alpha \in \mathfrak{P}'$ for $\mathfrak{P}' \mid \mathfrak{p}$ with $\mathfrak{P}' \neq \mathfrak{P}$. For $\sigma \in G \setminus D_{\mathfrak{P}}$, $\sigma(\mathfrak{P}) \neq \mathfrak{P}$. Hence, $\alpha \in \sigma(\mathfrak{P})$. Define

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

Reducing mod $\mathfrak{P}$, we have $f(x) \equiv x^{|G \setminus D_{\mathfrak{P}}|}\, h(x) \mod \mathfrak{P}$, where $h(x) \in \mathbb{F}_{\mathfrak{p}}[x]$. Observe that $\overline{\alpha}$ is a root of $h(x)$ and all the terms in $h(x)$ come from $\sigma \in D_{\mathfrak{P}}$. Then $x - \alpha$ is a root of $f(x)$ so that $x - \overline{\alpha}$ is a linear factor of $h(x)$ not generated by $x^{|G \setminus D_{\mathfrak{P}}|}$. Choose $\tau \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. Now τ is completely determined by $\tau(\overline{\alpha})$. But $\overline{\alpha}$ is a root of $h(x) \in \mathbb{F}_{\mathfrak{p}}[x]$ so that $\tau(\overline{\alpha})$ is a root of $h(x)$. Then $\tau(\overline{\alpha}) = \sigma(\alpha) \mod \mathfrak{P}$ for some $\sigma \in D_{\mathfrak{P}}$. Therefore, $\phi(\sigma) = \tau$. □

Since $\#D_{\mathfrak{P}} = ef$ and $\#\,\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) = f$, we must have $\#\ker\phi = e$.

Definition (Inertia Group)**.** The kernel of $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is called the inertia group of $\mathfrak{P}/\mathfrak{p}$ and is denoted $I_{\mathfrak{P}}$.

There is a short exact sequence of groups

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow D_{\mathfrak{P}} \xrightarrow{\phi} \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 1.$$

This gives a chain of subgroups of G and an associated tower of number fields and ideals:

$$\begin{array}{ccc}
1 & L & \mathfrak{P} \\
\Big| e & \Big| e & \cup \\
I_{\mathfrak{P}} & L^{I_{\mathfrak{P}}} & \mathfrak{P}_I := \mathfrak{P} \cap \mathcal{O}_{L^{I_{\mathfrak{P}}}} \\
\Big| f & \Big| f & \cup \\
D_{\mathfrak{P}} & L^{D_{\mathfrak{P}}} & \mathfrak{P}_D := \mathfrak{P} \cap \mathcal{O}_{L^{D_{\mathfrak{P}}}} \\
\Big| g & \Big| g & \cup \\
G & K = L^G & \mathfrak{p}
\end{array}$$

Definition (Inertia Field)**.** The field $L^{I_{\mathfrak{P}}}$ is called the inertia field at $\mathfrak{P}$.

Definition (Decomposition Field)**.** The field $L^{D_{\mathfrak{P}}}$ is called the decomposition field at $\mathfrak{P}$.

In fact, the splitting of primes in this tower has 'nice' behavior:

Proposition 6.5. *In the tower above, there is unique splitting behavior:*

- *In the extension $L^{D_{\mathfrak{P}}}/K$, 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. For some i, $\ell_i = \mathfrak{P}_D$.*
- *In the extension $L^{I_{\mathfrak{P}}}/L^{D_{\mathfrak{P}}}$, $\mathfrak{P}_D\mathcal{O}_{L^{I_{\mathfrak{P}}}} = \mathfrak{P}_I$ such that $e(\mathfrak{P}_I/\mathfrak{P}_D) = 1$ and $f(\mathfrak{P}_I/\mathfrak{P}_D) = f$.*
- *In the extension $L/L^{I_{\mathfrak{P}}}$, $\mathfrak{P}_I\mathcal{O}_L = \mathfrak{P}^e$, where $e(\mathfrak{P}/\mathfrak{P}_I) = e$ and $f(\mathfrak{P}/\mathfrak{P}_I) = 1$.*

Furthermore, $L^{D_{\mathfrak{P}}}/L$ is Galois with Galois group $D_{\mathfrak{P}}$.

6.3 Frobenius & Quadratic Reciprocity

Fix a Galois extension L/K with Galois group G. Fix a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ that is unramified in L. Choose a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ dividing $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified, $e_{\mathfrak{p}} = e(\mathfrak{P}/\mathfrak{p}) = 1$ so that $I_{\mathfrak{P}} = 1$. Then there is an isomorphism $D_{\mathfrak{P}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ since both are cyclic of order $f_{\mathfrak{p}}$. Then $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is generated by Frobenius: $x \mapsto x^{N(\mathfrak{p})}$. Pulling back to $D_{\mathfrak{P}}$, we obtain an element we call $\mathrm{Frob}_{\mathfrak{P}} \in D_{\mathfrak{P}} \subseteq G$ ($\mathrm{Frob}_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$ for all $x \in \mathcal{O}_L$).

Definition (Frobenius)**.** Under the isomorphism described above, the pullback of a generator of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is called $\mathrm{Frob}_{\mathcal{B}} : \mathbb{F}_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{P}}$ given by $x \mapsto x^{N(\mathfrak{p})}$.

So given a local object (a prime ideal), we obtain a global object, L (an element of the Galois group).

Remark. What we have called $\mathrm{Frob}_{\mathfrak{P}}$ is also denoted $\mathrm{Frob}_{\mathfrak{P},L/K}$, $(\mathfrak{P}, L/K)$, $\left(\frac{L/K}{\mathfrak{P}}\right)$.

Lemma 6.2. *For $\tau \in G$, $\mathrm{Frob}_{\tau(\mathfrak{P})} = \tau \,\mathrm{Frob}_{\mathfrak{P}}\, \tau^{-1}$.*

Proof. Observe that $\mathrm{Frob}_{\mathfrak{P}}(\tau^{-1}x) \equiv \tau^{-1}(x)^{N(\mathfrak{p})} \mod \mathfrak{P}$ and $\tau \,\mathrm{Frob}_{\mathfrak{P}}(\tau^{-1}x) \equiv x^{N(\mathfrak{p})} \mod \tau(\mathfrak{P})$. Applying τ, we obtain the result. □

By Lemma **??**, the conjugacy class of a prime ideal of $\mathrm{Frob}_{\mathfrak{P}}$ in G is well defined for any $\mathfrak{P} \mid \mathfrak{p}$.

Definition. For $\mathfrak{p} \subseteq \mathcal{O}_K$, $\mathrm{Frob}_{\mathfrak{p}}$ is the conjugacy class in G of $\mathrm{Frob}_{\mathfrak{P}}$ for any $\mathfrak{P} \subseteq \mathcal{O}_K$ with $\mathfrak{P} \mid \mathfrak{p}$.

Example 6.6. Let $L = \mathbb{Q}(\sqrt{d})$, where $1 \neq d \in \mathbb{Z}$ is squarefree. Then $[L\colon \mathbb{Q}] = 2$ and $L/\mathbb{Q}$ is Galois because L is the splitting field of $x^2 - d$. Define $G := \mathrm{Gal}(L/\mathbb{Q})$ and observe $G \cong \{\pm 1\}$. Choose a prime p with $p \nmid 2d$. Then p is unramified in L. Since G is abelian (so conjugacy classes are singleton sets and can then be identified with elements), Frob_p is an element of G. When is Frob_p trivial?

If $x^2 - d \mod p$ splits, then $f_p = 1$. If $x^2 - d \mod p$ is irreducible, then $f_p = 2$. Since G 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 $\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}$, where the map is $\mathrm{Frob}_p \mapsto \left(\frac{d}{p}\right)$. ◁

Definition (Legendre Symbol)**.** Fix an odd prime p. The Legendre symbol of an integer d is

$$\left(\frac{d}{p}\right) := \begin{cases} +1, & \text{if } d \text{ is a nonzero square mod } p, \\ -1, & \text{if } d \text{ is not a square mod } p, \\ 0, & \text{if } d \equiv 0 \mod p \end{cases}$$

Proposition 6.6.

(i) $\left(\frac{a}{p}\right)$ *depends only on the value of* $a \mod p$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iii) $\#\{a \in \mathbb{Z}/p\mathbb{Z}\colon a^2 \equiv d \mod p\} = 1 + \left(\frac{d}{p}\right)$

The multiplicative property of the Legendre symbol arises from the isomorphism $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \{\pm 1\}$ given by $a \mapsto \left(\frac{a}{p}\right)$. Since the Legendre symbol is multiplicative, it

is only necessary to understand $\left(\frac{-1}{p}\right)$ and $\left(\frac{l}{p}\right)$ for $l \neq p$ prime. As special cases of the Legendre symbol, we have the following:

Proposition 6.7.

(i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv 3 \mod 4 \end{cases}$

(ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & \text{if } p \equiv \pm 1 \mod 8, \\ -1, & \text{if } p \equiv \pm 3 \mod 8 \end{cases}$

The proof of (i) above will come in Example **??**. For part (ii), observe that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$. In fact, $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$. There is an extension of fields

$$\begin{array}{c} \mathbb{Q}(\zeta_8) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ |_2 \\ \mathbb{Q} \end{array}$$

However, $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$ is not a cyclic group and contains three subgroups of index 2. To prove the result, one must show that $\mathbb{Q}(\zeta 2)$ corresponds to the subgroup $\{\pm 1\} \subseteq (\mathbb{Z}/8\mathbb{Z})^\times$.

Proposition **??** combined with deep result of Gauss (conjectured by Euler and Legendre), called quadratic reciprocity, will allow one to calculate all Legendre symbols. The goal of this section will be to prove quadratic reciprocity.

Theorem ?? (Quadratic Reciprocity)**.** *For distinct odd primes p and l, we have*

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

That is,

$$\left(\frac{p}{l}\right) = \begin{cases} \left(\frac{l}{p}\right), & p \equiv 1 \text{ or } l \equiv 1 \mod 4 \\ -\left(\frac{l}{p}\right), & p \equiv l \equiv 3 \mod 4. \end{cases}$$

This is a truly deep and remarkable theorem since a priori there should be no relationship between integers modulo p and integers modulo l. The following examples illustrate the ease with which one can compute Legendre symbols using quadratic reciprocity. Moreover, we can answer questions about splitting of primes in number fields.

Example 6.7. Is 3 a square modulo $p = 144169$? Note that $p = 144169 \equiv 1 \mod 4$ and $144169 \equiv 1 \mod 3$. Therefore, we have

$$\left(\frac{3}{144169}\right) = \left(\frac{144169}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Therefore, 3 is a square modulo 144169. ◁

Example 6.8. Is 31 a square modulo 103? Note that $31 \equiv 103 \equiv 3 \mod 4$. Then

$$\left(\frac{31}{103}\right) = -\left(\frac{103}{31}\right) = -\left(\frac{10}{31}\right) = -\left(\frac{2}{31}\right)\left(\frac{5}{31}\right) = -\left(\frac{5}{31}\right) = -\left(\frac{31}{5}\right) = -\left(\frac{1}{5}\right) = -1.$$

Therefore, 31 is not a square modulo 103. ◁

Example 6.9. Recall the situation in Example **??**. We have that p splits in L if and only if $x^2 - d \mod p$ has two distinct roots if and only if $\left(\frac{d}{p}\right) = 1$. ◁

Example 6.10. For what primes p, $p \neq 2, 5$, does p split in $K = \mathbb{Q}(\sqrt{5})$? This happens precisely when $\left(\frac{5}{p}\right) = 1$. Now

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1, & p \equiv 1 \text{ or } 4 \mod 5 \\ -1, & p \equiv 2 \text{ or } 3 \mod 5. \end{cases}$$

Therefore, p splits in K if and only if $p \equiv \pm 1 \mod 5$. ◁

Now let L/K be a Galois extension of number fields with Galois group $\mathfrak{G} = \mathrm{Gal}(L/K)$. Given a nonzero $\mathfrak{p} \subseteq \mathcal{O}_K$ unramified in L, there is a unique $\mathrm{Frob}_{\mathfrak{P}} \in \mathfrak{G}$, where $\mathfrak{P} \mid \mathfrak{p}$, with $\mathrm{Frob}_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}$ and $\mathrm{Frob}_{\mathfrak{P}}$ induces the automorphism $x \mapsto x^{N(\mathfrak{p})}$ on $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$. Equivalently, there is a unique $\mathrm{Frob}_{\mathfrak{P}} \in \mathfrak{G}$ such that $\mathrm{Frob}_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$ for all $x \in \mathcal{O}_L$. Note that $\mathrm{Frob}_{\mathfrak{P}} \in \mathfrak{G}$ has order $f_{\mathfrak{p}} := f(\mathfrak{P}/\mathfrak{p})$. The conjugacy class $\mathrm{Frob}_{\mathfrak{P}}$ in $\mathfrak{G}$ is denoted by $\mathrm{Frob}_{\mathfrak{p}}$ and does not depend on $\mathfrak{P} \mid \mathfrak{p}$. If $\mathfrak{G}$ is abelian, then the conjugacy class is trivial so that $\mathrm{Frob}_{\mathfrak{p}} \in \mathfrak{G}$ is a well defined element in $\mathfrak{G}$.

Example 6.11. Fix an integer $n \geq 2$. Let $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. There is an isomorphism

$$\Psi : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

such that $\sigma(\zeta_n) = \zeta_n^{\Psi(\sigma)}$ for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Take a prime $p \nmid n$ so that it is unramified in L. Choose $\mathfrak{P} \mid \mathfrak{p}$ with $\mathfrak{P} \subseteq \mathcal{O}_L$. Now $\mathrm{Frob}_{\mathfrak{P}}(\zeta_n) \equiv \zeta_n^p \mod \mathfrak{P}$. As p does not divide n, $x^n - 1$ is separable modulo p, and ζ_n^p and $\mathrm{Frob}_{\mathfrak{P}}(\zeta_n)$ are roots of $x^n - 1$. However, these

are equivalent modulo $\mathfrak{P}$ so that $\mathrm{Frob}_{\mathfrak{P}}(\zeta_n) = \zeta_n^p$. Since the Galois group is abelian, we can write $\mathrm{Frob}_p = \mathrm{Frob}_{\mathfrak{P}}$. The isomorphism is given by

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \xrightarrow{\Psi} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \mathrm{Frob}_p & \longmapsto & p \end{array}$$

◁

Example 6.12. Choose $n = 4$ in Example **??**. The 4th root of unity is denoted i and we have $L = \mathbb{Q}(i)$. Choosing an odd prime p

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) & \xrightarrow{\Psi} & (\mathbb{Z}/4\mathbb{Z})^\times \\ \mathrm{Frob}_p & \longmapsto & p \mod 4 \end{array}$$

Note 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 $\mathrm{Frob}_p = 1 \in \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ if and only if $p \equiv 1 \mod 4$. We know also that p splits in $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ if and only if $\left(\frac{-1}{p}\right) = 1$. Putting these two different answers together, we obtain Proposition **??**. ◁

Theorem 6.3 (Quadratic Reciprocity)**.** *For distinct odd primes p and l, we have*

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

Proof. Fix an odd prime l and set $L = \mathbb{Q}(\zeta_l)$. Then via Ψ, we have $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/l\mathbb{Z})^\times = \mathbb{F}_l^\times$. Let $K/\mathbb{Q}$ be the subfield of L corresponding to $(\mathbb{F}_l^\times)^2$, i.e. the subfield fixed by $\Psi^{-1}((\mathbb{F}_l^\times)^2)$. Now K is a quadratic extension of $\mathbb{Q}$.

$$\begin{array}{cc} L & 1 \\ | & | \\ K & (\mathbb{F}_l^\times)^2 \\ |2 & |2 \\ \mathbb{Q} & \mathbb{F}_l^\times \end{array}$$

We claim $K = \mathbb{Q}(\sqrt{l^*})$, where

$$l^* = (-1)^{\frac{l-1}{2}} l = \begin{cases} l, & \text{if } l \equiv 1 \mod 4 \\ -l, & \text{if } l \equiv 3 \mod 4 \end{cases}$$

Clearly, L is unramified at all primes $p \neq l$ and $\operatorname{disc} L = \pm l^n$ for some n. Therefore, K is also unramified at $p \neq l$ so that $\operatorname{disc} K = \pm l$. Then if $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree.

$$\operatorname{disc} K = \begin{cases} d, & \text{if } d \equiv 1 \mod 4 \\ 4d, & \text{if } d \not\equiv 1 \mod 4 \end{cases}$$

Then we must choose d such that $d = \pm l$ and $d \equiv 1 \mod 4$. Hence, $K = \mathbb{Q}(\sqrt{l^*})$.

Now choose a prime p such that $p \nmid 2l$. We find two different necessary and sufficient conditions for a prime p to split in K. Comparing the results will result in the theorem.

Now we know p splits in K if and only if $\left(\frac{l^*}{p}\right) = 1$. On the other hand, choosing a prime $\mathfrak{P}$ of $\mathcal{O}_L$ dividing p. We have $\operatorname{Frob}_{\mathfrak{P}} \in \operatorname{Gal}(L/\mathbb{Q})$. For $x \in \mathcal{O}_K$, $\operatorname{Frob}_{\mathfrak{P}}(x) - x^p \in \mathfrak{P}$. Therefore as $\operatorname{Frob}_{\mathfrak{P}}|_K \in \operatorname{Gal}(K.\mathbb{Q})$, $\operatorname{Frob}_{\mathfrak{P}}(x) - x^p \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then we have $\operatorname{Frob}_{\mathfrak{P}}|_K = \operatorname{Frob}_{\mathfrak{p}}$. But 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 $\operatorname{Frob}_{\mathfrak{P}}$ fixes K as $\operatorname{Frob}_{\mathfrak{P}}|_K = \operatorname{Frob}_{\mathfrak{p}}$. However, this happens if and only if $\Psi(\operatorname{Frob}_{\mathfrak{P}}) \in (\mathbb{F}_l^\times)^2$. Since the Galois group is abelian, it suffices to show that $\Psi(\operatorname{Frob}_p) \in (\mathbb{F}_l^\times)^2$. However by Example **??**, $\Psi(\operatorname{Frob}_p) \in (\mathbb{F}_l^\times)^2$ if and only if $p \mod l \in (\mathbb{F}_l^\times)^2$ if and only if $\left(\frac{p}{l}\right) = 1$.

Combining these results, we obtain $\left(\frac{l^*}{p}\right) = 1$ if and only if p splits in K if and only if $\left(\frac{p}{l}\right) = 1$. But then $\left(\frac{l^*}{p}\right) = \left(\frac{p}{l}\right)$. Therefore,

$$\begin{aligned} \left(\frac{l^*}{p}\right) &= \left(\frac{(-1)^{l-1}2l}{p}\right) \\ &= \left(\frac{-1}{p}\right)^{\frac{l-1}{2}} \left(\frac{l}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\frac{l-1}{2}} \left(\frac{l}{p}\right) \end{aligned}$$

□

6.4 Chebotarev Density Theorem

Now let L/K be a finite Galois extension of number fields. Set $G = \operatorname{Gal}(L/K)$ and choose a nonzero prime $\mathfrak{p} \subseteq \mathcal{O}_K$ which is unramified in L. Choose a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ with $\mathfrak{P} \mid \mathfrak{p}$. We know there exists a unique $\operatorname{Frob}_{\mathfrak{P}} \in G$ such that $\operatorname{Frob}_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$ for all $x \in \mathcal{O}_L$. Furthermore, $\operatorname{Frob}_{\mathfrak{P}}$ has order $f_{\mathfrak{p}} = f(\mathfrak{P}/\mathfrak{p})$. Denote by $\operatorname{Frob}_{\mathfrak{p}}$ the conjugacy class of $\operatorname{Frob}_{\mathfrak{P}}$ in G. Fix a separable monic $h \in \mathcal{O}_K[x]$ whose splitting field is L, i.e. $L = K(\alpha_1, \ldots, \alpha_n)$, where $h(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Note that the α_i are distinct. The Galois

Table 1: Splitting Proportions

$f_1, \dots, f_r$	(1,1,1,1)	(1,1,2)	(1,3)	(2,2)	(4)
Number Occurences	55338	0	443017	166222	0
Proportion	0.083268	0	0.666615	0.250116	0

group of L/K acts on this set of roots of h by permutation. Then there is an injective homomorphism

$$\Psi : G \hookrightarrow \mathfrak{S}_n,$$

where for $\sigma \in G$, we have $\sigma(\alpha_i) = \alpha_{\Psi(\sigma)(i)}$. Take a prime $\mathfrak{p}$ not dividing $\operatorname{disc} h$. We have $h \equiv h_1 \cdots h_r \mod p$ for distinct $h_i \in \mathbb{F}_p[x]$ monic and irreducible. Set $f_i = \deg h_i$ — noting that $\sum_i f_i = n$.

Theorem 6.4. *For a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ dividing $\mathfrak{p}$, $\Psi(\mathrm{Frob}_{\mathfrak{P}}) \in \mathfrak{S}_n$ is a permutation of cycle type $(f_1, \dots, f_r)$.*

Proof. Define $\overline{\alpha_i} = \alpha_i \mod \mathfrak{P}$. There is a bijection between $\{\alpha_1, \dots, \alpha_n\}$ and $\{\overline{\alpha}_1, \dots, \overline{\alpha}_n\}$ given by $\alpha \mapsto \alpha \mod \mathfrak{P}$. Since $\mathfrak{p}$ does not divide $\operatorname{disc} h$ so that h is separable modulo $\mathfrak{p}$. The action of $\mathrm{Frob}_{\mathfrak{P}}$ corresponds to the action of $\mathrm{Frob} : \mathbb{F}_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{P}}$ given by $x \mapsto x^{N(\mathfrak{p})}$, where $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) = \langle \mathrm{Frob} \rangle$. An orbit of Frob on $\{\overline{\alpha}_1, \dots, \overline{\alpha}_n\}$ corresponds to the roots of an $h_i \in \mathbb{F}_{\mathfrak{p}}[x]$. □

Example 6.13. Let $L/\mathbb{Q}$ be the splitting field for $h(x) = x^4 + x + 5$. Note that $\operatorname{disc} h = 31973$ is prime. We factor $h \mod p$ for prime p:

- $p = 2, 3$: h is irreducible. Hence, $\Psi(\mathrm{Frob}_2), \Psi(\mathrm{Frob}_3) \in \mathfrak{S}_4$ are 4-cycles.
- $p = 5$: $h \equiv x(x+1)(x^2 + 4x + 1) \mod 5$, so $\Psi(\mathrm{Frob}_5) \in \mathfrak{S}_4$ is a 2-cycle.
- $p = 7$: $h \equiv (x+6)(x^3 + x^2 + x + 2) \mod 7$, so $\Psi(\mathrm{Frob}_7) \in \mathfrak{S}_4$ is a 3-cycle.

Therefore, $\Psi : \mathrm{Gal}(L/\mathbb{Q}) \to \mathfrak{S}_4$ must be an isomorphism as $\mathfrak{S}_4$ has no proper subgroups containing elements of order 3 and 4. ◁

Example 6.14. Let $L/\mathbb{Q}$ be the splitting field of $h(x) = x^4 + 8x + 12$. The discriminant of h is $\operatorname{disc} h = 2^{12} \cdot 3^4$. We can factor h modulo p for p not dividing 6. Order the sequence $f_1, \dots, f_r$ to be increasing. Table **??** shows how many times each cycle type occurs as well as its proportion of the total for primes $5 \leq p \leq 10,000,000$. Observe only odd cycle types occur in the table. Observe also $0.083268 \approx \frac{1}{12}$, $0.666615 \approx 23$, and $0.250116 \approx \frac{1}{4}$. Finally, these fractions have common denominator 12. One could then conjecture $\Psi(\mathrm{Gal}(L/\mathbb{Q})) \subseteq \mathcal{A}_4 \subseteq \mathfrak{S}_4$. To make this rigorous, first note that

$$2^{12} \cdot 3^4 = \operatorname{disc} h = \prod_{1 \leq i < j \leq 4} (\alpha_i - \alpha_j)^2,$$

where h has roots $\alpha_1, \ldots, \alpha_4$. Furthermore, we have

$$\delta := \prod_{1 \le i < j \le 4} (\alpha_i - \alpha_j) = 2^6 \cdot 3^2 \in \mathbb{Q}^\times.$$

Then 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 $\mathrm{sgn} : \mathfrak{S}_4 \to \{\pm 1\}$ is the map to the sign of the permutation. This homomorphism has kernel $\mathcal{A}_4$. Cancelling δ on both sides of the equation gives $\mathrm{sgn}(\Psi(\sigma)) = 1$. Therefore, $\Psi(\mathrm{Gal}(L/\mathbb{Q})) \subseteq \mathcal{A}_4$. As $\Psi(\mathrm{Gal}(L/\mathbb{Q}))$ contains elements of order 2 and 3, we must have $\Psi(\mathrm{Gal}(L/\mathbb{Q})) = \mathcal{A}_4$. But then $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathcal{A}_4$. ◁

The 'nice' distribution in Table **??** in Example **??** is not an accident but an example of a general phenomenon.

Definition (Density)**.** For a set S of prime ideals of $\mathcal{O}_K$, define the density of S

$$\delta(S) := \lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in S \colon N(\mathfrak{p}) \le x\}}{\#\{\mathfrak{p} \colon N(\mathfrak{p}) \le x\}},$$

whenever this limit exists.

We now have sufficient vocabulary to state the main theorem of this section.

Theorem 6.5 (Chebotarev Density Theorem)**.** *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 S_C be the set of $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathfrak{p}$ is unramified in L and $\mathrm{Frob}_\mathfrak{p} \subseteq C$.*

$$S_C := \{\mathfrak{p} \subseteq \mathcal{O}_K \colon \mathfrak{p} \text{ unramified in } L, \mathrm{Frob}_\mathfrak{p} \subseteq C\}.$$

Then the density of S_C is the ratio of the sizes of C to G: $\delta(S_C) = \dfrac{\#C}{\#G}$.

We shall not prove the theorem since this veers into many analytic techniques which will not be otherwise relevant for our purposes. However, we shall address a few examples.

Example 6.15. For $n \ge 2$ and $a \in \mathbb{Z}$ relatively prime to n.

$$\begin{aligned} \Phi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\xrightarrow{\Psi} (\mathbb{Z}/n\mathbb{Z})^\times \\ \mathrm{Frob}_p &\longmapsto \mathfrak{p} \mod n \end{aligned}$$

Let $C = \Phi^{-1}([a])$ and $S_C = \{p\colon p \nmid, \mathrm{Frob}_p \in \Phi^{-1}([a])\}$. By the Chebotarev Density Theorem,

$$\delta(S_C) = \frac{1}{\#(\mathbb{Z}/n\mathbb{Z})} = \frac{1}{\phi(n)},$$

where ϕ is the Euler totient function. Furthermore, $S_C = \{p\colon p \equiv a \mod n\}$. This gives a theorem of Dirichlet: the density of primes p congruent to a modulo m is $1/\phi(n)$ (see Proposition **??**). ◁

Proposition 6.8 (Dirichlet)**.** *Let $n \geq 2$. The set of primes $p \equiv a \mod n$ has density $1/\phi(n)$, where ϕ is the Euler totient function. In particular, there are infinitely many such p.*

This is a common application of Chebotarev: guaranteeing the existence of a prime with certain properties.

Example 6.16. Let L/K be a Galois extension with Galois group G. Let S be the set of primes $\mathfrak{p} \subseteq \mathcal{O}_K$ that splits completely in L, i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r$, wher $e e(\mathfrak{q}_i/\mathfrak{p}) = 1$ and $f(\mathfrak{q}_i/\mathfrak{p}) = 1$. In this case, $r = [L\colon K]$. Choosing $C = \{1\}$, by the Chebotarev Density Theorem,

$$\delta(S) = \frac{1}{\#G} = \frac{1}{[L\colon K]}.$$

◁

Proposition 6.9. *Let L/K and M/K be Galois extensions. Denote by $S_{L/K}$ the set of primes of K that split completely in L and mutatis mutandis for $S_{M/K}$. Then $L \subseteq M$ if and only if $S_{L/K} \supseteq S_{M/K}$.*

Proof. (Sketch): If $L \subseteq M$, then $S_{L/K} \supseteq S_{M/K}$. Conversely, consider

$$\begin{aligned} \mathrm{Gal}(LM/K) &\hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K) \\ \sigma &\longmapsto (\sigma|_L, \sigma|_M) \end{aligned}$$

Furthermore, $\mathrm{Frob}_\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p} \times \mathrm{Frob}_\mathfrak{p}$. Then $S_{LM/K} = S_{L/K} \cap S_{M/K}$. By assumption, $S_{L/K} \supseteq S_{M/K}$, so $S_{LM/K} = S_{M/K}$. Therefore,

$$\frac{1}{[LM\colon K]} = \delta(S_{LM/K}) = \delta(S_{M/K}) = \frac{1}{[M\colon K]}.$$

But then $[LM\colon K] = [M\colon K]$ so that $LM = M$. This shows $L \subseteq M$. □

Before moving to more analytic topics in Algebraic Number Theory, we give some foreshadowing to Class Field Theory. Let L/K be a Galois extension with $G = \mathrm{Gal}(L/K)$ abelian. Let S denote teh finite set of primes of $\mathcal{O}_K$ containing those that ramify in L. Let

$\mathfrak{I}_K^S \subseteq \mathfrak{I}_K$ denote the group generated by $\mathfrak{p} \notin S$. Define a homomorphism $\theta : \mathfrak{I}_K^S \to G$ by $\mathfrak{p} \mapsto \mathrm{Frob}_\mathfrak{p}$ (noting that invertible fractional ideals are an abelian group generated by the $\mathfrak{p}$'s so it is sufficient to define the map there). The Chebotarev Density Theorem says that this map is surjective. Then we have $\mathfrak{I}_K^S / \ker\phi \cong G$. Now $\ker\theta$ determines L (the idea being $\mathfrak{p} \notin S$ and $\mathfrak{p}$ splits completely in L if and only if $\mathfrak{p} \in \ker\theta$). The problem (one of the problems of Class Field Theory) is to describe the finite index subgroups of $\mathrm{C}\ell_K^S$ that correspond to L/K abelian Galois extensions.

7 Dedekind Zeta Function

7.1 Calculating $\mathrm{C}\ell_K$ and $\mathcal{O}_K^\times$

Since this section will pull together much of the theory and notation developed thus far, we begin by reminding the reader of the notation as well as establishing two new notational conveniences: ω_K, h_K.

Let $K/\mathbb{Q}$ be a number field. Then define…

- $n = [K\colon \mathbb{Q}]$
- r, the number of real embeddings $\sigma : K \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$
- s, the number of complex conjugate pairs of embeddings, $\sigma : K \hookrightarrow \mathbb{C}$, $\sigma(K) \not\subseteq \mathbb{R}$
- $\mathrm{disc}\, K \in \mathbb{Z}$, the discriminant of K
- $\mathcal{O}_K^\times$, the group of units of $\mathcal{O}_K$ (which will be of rank $r + s - 1$)
- $\phi : \mathcal{O}_K^\times \to V := \{x \in \mathbb{R}^{r+s}\colon \sum_i x_i = 0\}$ given by $\alpha \mapsto (e_i \log|\sigma_i(\alpha)|)_i$, where $e_i = 1$ for $1 \le i \le r$ and $e_i = 2$ for $r+1 \le i \le r+s$
- $\mathrm{Reg}_K := \frac{1}{\sqrt{r+s}} \mathrm{covol}(\phi(\mathcal{O}_K^\times)) > 0$, the regulator of K
- $\omega_K := \#\mu_K \in \mathbb{Z}^+$, the group of roots of unity in K
- $h_K := \#\mathrm{C}\ell_K \in \mathbb{Z}^+$, where $\mathrm{C}\ell_K$ is the class group of K (which will be a finite abelian group)

Up to this point, we have computed some elementary examples of $\mathrm{C}\ell_K$ and $\mathcal{O}_K^\times$. But we have yet to give an effective algorithm for computing these in general. Assuming one can numerically compute $h_K \mathrm{Reg}_K$, we give an "effective" algorithm to calculate both $\mathrm{C}\ell_K$ and $\mathcal{O}_K^\times$ (modulo some terms 'many', 'guess', and 'enough', which we shall leave ill defined for our purpose). One can then use $\mathrm{C}\ell_K$ and $\mathcal{O}_K^\times$ to compute h_K and Reg_K exactly. However, we shall describe in later sections a method of computing $h_K \cdot \mathrm{Reg}_K$ so that this algorithm

will not be circular. Strangely enough, it is simpler to compute $h_K \cdot \mathrm{Reg}_K$ than either h_K or Reg_K individually. In any case, the algorithm is as follows:

1. Compute primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ with $N(\mathfrak{p}_i) \leq M_K$, where M_K is the Minkowski constant for K.

2. Find 'many' factorizations $\alpha_i \mathcal{O}_K = \mathfrak{p}_1^{a_{i,1}} \cdots \mathfrak{p}_m^{a_{i,m}}$ with $1 \leq i \leq M$ (the number of factorizations found) and $\alpha_i \in K$.

3. Define a 'guess' for O_K: $C := \mathbb{Z}^m / \langle \{(a_{i,1}, \ldots, a_{i,m}) \colon 1 \leq i \leq M\} \rangle$ (being sure to find 'enough' relations so that C is finite). Now $C \twoheadrightarrow \mathrm{C}\ell_K$ under the map $e_i \mapsto [\mathfrak{p}_i]$, where e_i is the ith standard basis vector. Note then $(a_{i,1}, \ldots, a_{i,m}) \mapsto [\mathfrak{p}_1]^{a_{i,1}} \cdots [\mathfrak{p}_m]^{a_{i,m}} = [\alpha \mathcal{O}_K] = 1$. The map is surjective since $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ generate $\mathrm{C}\ell_K$. This map will be an isomorphism if we have found 'enough factorizations to find all the relations in $\mathrm{C}\ell_K$.

4. Take $(b_1, \ldots, b_M) \in \mathbb{Z}^M$ such that $\sum_{i=1}^M a_{i,j} b_i = 0$ for all $1 \leq j \leq M$. This says that $\prod_{i=1}^M (\alpha_i \mathcal{O}_K)^{b_i} = \prod_{i=1}^M \alpha_i^{b_i} \mathcal{O}_K = \mathcal{O}_K$ (collecting the exponent of $[\mathfrak{p}_i]$, one finds the total is zero). Then $\prod_{i=1}^M \alpha_i^{b_i} \in \mathcal{O}_K^\times$. Let $U \subseteq \mathcal{O}_K^\times$ be the group generated by these units (being sure one has found enough so that U has rank $r + s - 1$) along with μ_K. We will have $U = \mathcal{O}_K^\times$ for 'enough' factorizations.

5. Now $\frac{\#C}{\#\mathrm{C}\ell_K}$ is a positive integer. We have $\frac{\mathrm{covol}(\phi(U))}{\mathrm{covol}(\phi(\mathcal{O}_K^\times))} = [\phi(\mathcal{O}_K^\times) \colon \phi(U)] = [\mathcal{O}_K^\times \colon U]$ (as both contain the roots of unity). But

$$\underbrace{\frac{\#C}{\sqrt{r+s}} \, \mathrm{covol}(\phi(U))}_{\text{Computable}} = \underbrace{\frac{\#C}{\#\mathrm{C}\ell_K} \cdot [\mathcal{O}_K^\times \colon U]}_{\text{“}\in \mathbb{Z}^+\text{”}} \cdot \underbrace{h_K \, \mathrm{Reg}_K}_{\text{Known}}.$$

   By assumption, $h_K \, \mathrm{Reg}_K$ is known. The number $\frac{\#C}{\sqrt{r+s}} \, \mathrm{covol}(\phi(U))$ is effectively computable. Finally, $\frac{\#C}{\#\mathrm{C}\ell_K} \cdot [\mathcal{O}_K^\times \colon U] \in \mathbb{Z}^+$ theoretically. However in practice, we will know this only as an approximation in $\mathbb{R}^+$. Once this number is 'numerically 1', $\#C = \#\mathrm{C}\ell_K$ and $[\mathcal{O}_K^\times \colon U] = 1$. Then $C \twoheadrightarrow \mathrm{C}\ell_K$ is a surjective map between finite groups of the same size so that it is an isomorphism. We have also clearly calculated the unit group.

7.2 Counting Ideals

While the above algorithm was useful, it rested on the assumption that one could calculate $h_K \, \mathrm{Reg}_K$. It remains to show that one can effectively compute $h_K \, \mathrm{Reg}_K$. We calculate this by counting ideals.

Definition. Let $x \in \mathbb{R}$. Define

$$\mathcal{A}(x) := \#\{0 \neq I \subseteq \mathcal{O}_K \colon N(I) \leq\}.$$

For $x \leq 0$, $\mathcal{A}(x) = 0$ and $\mathcal{A}(x)$ is finite for $x \in \mathbb{R}$ as there are only finitely many ideals of a given norm. A natural question to ask is how does $\mathcal{A}(x)$ grow with x? This leads to the class number.

Theorem 7.1 (Analytic Class Number)**.** *There exists a constant κ, called the class number, such that $\mathcal{A}(x) \sim \kappa x$ as $x \to \infty$. Moreover,*

$$\kappa = \frac{2^r (2\pi)^s h_K \operatorname{Reg}_K}{\omega_K |\operatorname{disc} K|^{1/2}}.$$

Proof (Sketch). Fix $C \in \mathrm{C}\ell_K$ and define

$$\mathcal{A}(x, C) := \#\left\{I \subseteq \mathcal{O}_K \colon N(I) \leq x, [I] = C\right\}.$$

Note that $\mathcal{A}(x) = \sum_{C \in \mathrm{C}\ell_K} \mathcal{A}(x, C)$. It suffices to prove

$$\mathcal{A}(x, C) \sim \frac{2^r (2\pi)^s \operatorname{Reg}_K}{\omega_K |\operatorname{disc} K|^{1/2}}$$

since there are h_K such $\mathcal{A}(x, C)$ in total. We shall prove the theorem in the case where $K/\mathbb{Q}$ is quadratic. The general case works the same but merely involves (extreme) 'bookkeeping'.

Fix an ideal J with $[J] = C^{-1}$. For I with $[I] = C$ and $N(I) \leq x$, we have $IJ = (\alpha)$ for some $\alpha \in J$ and

$$|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha \mathcal{O}_K) = N(IJ) = N(I)N(J) \leq xN(J).$$

Conversely, choose $0 \neq \alpha \in J$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq xN(J)$. Then $(\alpha) \subseteq J$, which implies $I := (\alpha)J^{-1}$ is an ideal with

$$N(I) = \frac{|N_{K/\mathbb{Q}}(\alpha)|}{N(J)} \leq \frac{xN(J)}{N(J)} = x.$$

Therefore, this shows

$$\mathcal{A}(x, C) = \#\left\{(\alpha) \colon 0 \neq \alpha \in J, N_{K/\mathbb{Q}}(\alpha) \leq xN(J).\right\}.$$

It remains to count $\alpha \in J$, which leads to lattices. [Note, we count up to units since if u is a unit, $(u\alpha) = (\alpha)$.]

Case 1, $K/\mathbb{Q}$ imaginary quadratic: We have $\mathcal{O}_K^\times = \mu_K$ and $\mathcal{A}(x, C) = \#(J \cap D_x)$, where

$$D_x = \left\{z \in \mathbb{C} \colon 0 \leq \operatorname{Arg}(z) < \frac{2\pi}{\omega_K}, z\bar{z} \leq xN(J)\right\}.$$

The set D_x simply induces rotation on nonzero elements. Note that any principal ideal of $\mathcal{O}_K$ has a unique, nonzero generator α with $0 \leq \operatorname{Arg}(\alpha) < 2\pi/\omega_K$ and norm $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} > 0$.

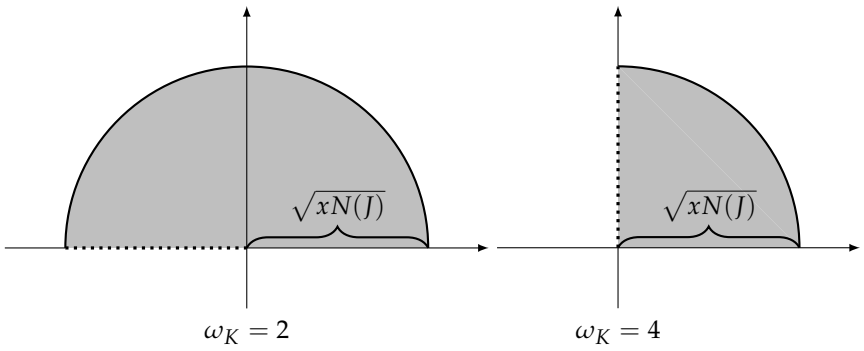


Figure 5: The region D_x for $\omega_K = 2$ (left) and $\omega_K = 4$ (right).

Then as x tends to infinity,

$$\mathcal{A}(x, C) \sim \frac{\operatorname{Area}(D_x)}{\operatorname{covol} J} = \frac{\dfrac{\pi\sqrt{xN(J)}^2}{\omega_K}}{|\operatorname{disc} K|^{1/2} \cdot N(J)/2} = \frac{2\pi}{\omega_K |\operatorname{disc} K|^{1/2}}\, x$$

Case 2, $K/\mathbb{Q}$ real quadratic: Let $K \subseteq \mathbb{R}$ be a real quadratic field and let $\tau : K \hookrightarrow \mathbb{R}$ be the non-identity embedding. By Dirichlet's Unit Theorem, we may write $\mathcal{O}_K^\times = \pm\langle\epsilon\rangle$, choosing $\epsilon > 1$ to be the fundamental unit. Let $\phi : K^\times \overset{1\times\tau}{\hookrightarrow} \mathbb{R}^\times \times \mathbb{R}^\times \to \mathbb{R}^2$, where the final map is $(a, b) \mapsto (\log|a|, \log|b|)$. Then we have $\phi(\mathcal{O}_K^\times) = \mathbb{Z}(\log\epsilon, -\log\epsilon)$. However, $(1, 1)$ and $(\log\epsilon, -\log\epsilon)$ are linearly independent over $\mathbb{R}$. But then

$$(\log|a|, \log|b|) = \frac{\log|a| + \log|b|}{2}(1, 1) + \frac{\log|a| - \log|b|}{2\log\epsilon}(\log\epsilon, -\log\epsilon).$$

For nonzero $\alpha \in \mathcal{O}_K$, there exists a unique $n \in \mathbb{Z}$ such that $\phi(\alpha\epsilon^n) = c_1(1, 1) + c_2(\log\epsilon, -\log\epsilon)$ with $c_i \in \mathbb{R}$ and $0 \leq c_2 < 1$. Set $\mathcal{A}(x, C) = \#(J \cap D_x)$, where

$$D_x = \left\{(a, b) \in \mathbb{R}^2 \colon |ab| \leq xN(J), 0 \leq \frac{\log|a| + \log|b|}{2\log\epsilon} < 1, a > 0, b \neq 0\right\}$$

Set $r = xN(J)$. Then we can rewrite this as

$$D_x = \left\{(a, b) \in \mathbb{R}^2 \colon |ab| \leq r, 1 \leq \frac{a}{|b|} < \epsilon^2, a > 0, b \neq 0\right\}$$

This region is plotted in Figure **??** below.

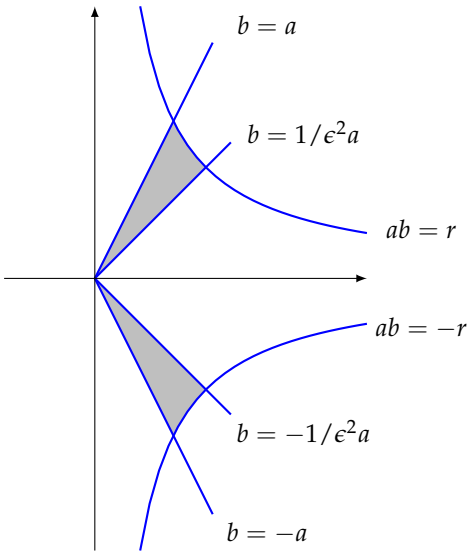


Figure 6: The region D_x for a real quadratic field.

We need now calculate $\dfrac{\text{Area}(D_x)}{\text{covol}\, J}$, which comes down to computing $\text{Area}(D_x)$. It is sufficient to calculate the area of the upper shaded region. This is

$$\begin{aligned}
\text{Area}(D_x) &= 2\left[\int_0^{\sqrt{r}} \left(a - \frac{a}{\epsilon^2}\right)\, da + \int_{\sqrt{r}}^{\epsilon\sqrt{r}} \left(\frac{r}{a} - \frac{a}{\epsilon^2}\right)\, da\right] \\
&= 2\left[\left(1 - \frac{1}{\epsilon^2}\right)\cdot \frac{a^2}{2}\Big|_{a=0}^{a=\sqrt{r}} + \left(r\ln|a| - \frac{a^2}{2\epsilon^2}\right)\Big|_{a=\sqrt{r}}^{\epsilon\sqrt{r}}\right] \\
&= 2\left[\left(1 - \frac{1}{\epsilon^2}\right)\cdot \frac{r}{2} + \left(r\ln(\epsilon\sqrt{r}) - \frac{\epsilon^2 r}{2\epsilon^2}\right) - \left(r\ln\sqrt{r} - \frac{r^2}{2\epsilon^2}\right)\right] \\
&= 2\left[\frac{r}{2} - \frac{r}{2\epsilon^2} + r\ln(\epsilon\sqrt{r}) - \frac{r}{2} - r\ln\sqrt{r} + \frac{r^2}{2\epsilon^2}\right] \\
&= 2\left[r\ln(\epsilon\sqrt{r}) - r\ln\sqrt{r}\right] \\
&= 2\left[r\ln\epsilon + r\ln\sqrt{r} - r\ln\sqrt{r}\right] \\
&= 2r\ln\epsilon
\end{aligned}$$

Then letting x tend to infinity, we have

$$\mathcal{A}(x, C) \sim \frac{\text{Area}(D_x)}{\text{covol}\, J} = \frac{2r\log\epsilon}{|\operatorname{disc} K|^{1/2} N(J)} = \frac{2xN(J)\log\epsilon}{|\operatorname{disc} K|^{1/2} N(J)} = \frac{2\log\epsilon}{|\operatorname{disc} K|^{1/2}}\, x.$$

□

Remark. Since $\mathcal{A}(x)$ is effectively computable, this gives a numerical approach to compute (really estimate) $h_K \operatorname{Reg}_K$. In fact examining the proof closer, one could use the methods of the proof to show $\mathcal{A}(x) = \kappa x + O(x^{1-[K\colon \mathbb{Q}]^{-1}})$. The idea is that $Nx = \#(\mathbb{Z}^2 \cap D_x)$, where

$$D_x = \{(a, b) \in \mathbb{R}^2 \colon \sqrt{a^2 + b^2} \leq x\}.$$

But

$$\pi(x-1)^2 = \text{area } D_{x-1} \leq Nx \leq \text{area } D_{x+1} = \pi(x+1)^2$$

so that $Nx = \pi x^2 + O(x)$.

Example 7.1. If $K = \mathbb{Q}$, then $\mathcal{A}(x) = \#\{n \leq x\} = 1 \cdot x + o(x)$, i.e. $\mathcal{A}(x) \sim 1 \cdot x$. We have $r = 1$, $s = 0$, $h_K = 1$, $\operatorname{Reg}_K = 1$, $\omega_K = 1$, and $\operatorname{disc} K = 1$. Then

$$\kappa = \frac{2 \cdot 1 \cdot 1 \cdot 1}{2 \cdot 1} = 1.$$

◁

7.3 Dedekind Zeta Function

We attach a function to the various counts made in the previous section, called the Dedekind Zeta function.

Definition (Dedekind Zeta Function)**.** Let K be a number field. For $n \geq 1$, define $a_n := \#\{I \subseteq \mathcal{O}_K \colon N(I) = n\}$. The Dedekind Zeta function of K is

$$\zeta_K(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Since we will often deal with products of series, we remind the reader of a few useful lemmas.

Lemma 7.1 (Partial Summation)**.** *Let $\{a_i\}_{i \in \mathbb{N}}$ be a sequence of complex numbers. Let $f : [1, \infty) \to \mathbb{C}$ be a C^1 function. Define*

$$\mathcal{A}(x) = \sum_{n \geq x} a_n.$$

Then

$$\sum_{n \leq x} a_n f(n) = A(x)f(x) - \int_1^x A(t)f'(t)\, dt$$

Proof (Sketch). Take $x \geq 1$ an integer.

$$\begin{aligned}\int_1^x A(t)f'(t)\,dt &= \sum_{n\leq x-1}\int_n^{n+1} A(t)f'(t)\,dt \\ &= \sum_{n\leq x-1} A(n)\int_n^{n+1} f'(t)\,dt \\ &= \sum_{n\leq x} A(n)(f(n+1)-f(n))\end{aligned}$$

The rest is a matter of distributing the summation and re-indexing. □

Lemma 7.2. *Fix a formal Dirichlet series* $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ *with* $a_n \in \mathbb{C}$. *Set* $\mathcal{A}(x) = \sum_{n\leq x} a_n$. *Suppose* $\mathcal{A}(x) = O(x^\delta)$ *for some* $\delta > 0$. *Then* $\sum \frac{a_n}{n^s}$ *converges absolutely for* $\mathrm{Re}(s) > \delta$ *and*

$$\sum_{n=1}^{\infty}\frac{a_n}{n^s} = s\int_1^{\infty}\frac{\mathcal{A}(t)}{t^{s+1}}\,dt.$$

In particular, $\sum \frac{a_n}{n^s}$ *is holomorphic for* $\mathrm{Re}(s) > \delta$.

Proof. Let $f(n) = n^{-s}$. Now

$$\begin{aligned}f(x) &= x^{-s} = e^{-s\log x} \\ f'(x) &= e^{-s\log x}\left(-\frac{s}{x}\right) = \frac{-s}{x^{s+1}}\end{aligned}$$

Using Lemma **??**, we have

$$\sum_{n\leq x} a_n n^{-s} = \underbrace{\frac{\mathcal{A}(x)}{x^s}}_{\substack{\to 0\\ x\to\infty}} + s\int_1^x \frac{\mathcal{A}(t)}{t^{s+1}}\,dt$$

Now the quantity on the left tends to 0 as x tends to infinity ($\mathrm{Re}(s) > \delta$ and $A(x) = O(x^\delta)$) while for the integral on the right we have

$$s\int_1^x \frac{\mathcal{A}(t)}{t^{s+1}}\,dt = O\left(\int_1^x \frac{dt}{t^{\mathrm{Re}(s)-\delta+1}}\right) = O(1) \text{ if } \mathrm{Re}(s) > \delta.$$

□

Example 7.2. Consider $\zeta(s) = \zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, the ordinary Riemann zeta function. Now taking $\mathrm{Re}(s) > 1$, $A(x) = \sum_{n \le x} 1 = \lfloor x \rfloor$ and $\delta = 1$ in Lemma **??**, we have

$$\begin{aligned}\zeta(s) = \zeta_{\mathbb{Q}}(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= s \int_1^{\infty} \frac{\lfloor t \rfloor}{t^{s+1}}\, dt + s \int_1^{\infty} \frac{\lfloor t \rfloor - t}{t^{s+1}}\, dt \\ &= \frac{s}{s-1} + s \int_1^{\infty} \frac{\lfloor t \rfloor - t}{t^{s+1}}\, dt\end{aligned}$$

However, $\lfloor t \rfloor - t = O(1)$ and the integral on the right then converges for $\mathrm{Re}(s) > 0$. Therefore, $\zeta(s)$ has a unique analytic continuation to $\mathrm{Re}(s) > 0$ except for at the simple pole at $s = 1$ with residue 1. ◁

Remark. In fact, $\zeta(s)$ and $\zeta_K(s)$ extend to holomorphic functions on $\mathbb{C} \setminus \{1\}$.

Example 7.3. Let $a_n = \#\{I \subseteq \mathcal{O}_K \colon N(I) = n\}$. Now $\mathcal{A}(x) = \sum_{n \le x} a_n \sim \kappa x$ so that $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges absolutely for $\mathrm{Re}(s) > 1$. Note that $\kappa\zeta(s)$ is defined for $\mathrm{Re}(s) > 0$ with $s \neq 1$. Consider

$$\zeta_K(s) - \kappa\zeta(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s},$$

where $b_n = a_n - \kappa$.

$$\mathcal{B}(x) := \sum_{n \le x} b_n = \sum_{n \le x} (a_n - \kappa \lfloor x \rfloor) = \mathcal{A}(x) - \kappa x + O(1) = O(x^{1 - [K\colon \mathbb{Q}]^{-1}})$$

This shows that $\sum_{n=1}^{\infty} \frac{b_n}{n^s}$ converges for $\mathrm{Re}\, s > 1 - [K\colon \mathbb{Q}]^{-1}$. But then $\zeta_K(s)$ has an analytic continuation for $\mathrm{Re}(s) > 1 - [K\colon \mathbb{Q}]^{-1}$ except at $s = 1$. ◁

Now denote by r_1 the number of real embeddings for K and r_2 the number of complex conjugate pairs of embeddings for K, where K is a number field.

Theorem 7.2 (Analytic Class Number Formula)**.**

$$res_{s=1}\zeta_K(s) = \lim_{s \to 1}(s-1)\zeta_K(s) = \kappa = \frac{2^{r_1}(2\pi)^{r_2} h_k \,\mathrm{Reg}_K}{\omega_K |\operatorname{disc} K|^{1/2}}$$

Other than being fascinating in its own right, Theorem **??** gives us a method of calculating κ. But this in turn allows us to calculate $h_K \,\mathrm{Reg}_K$ so that the methods of Section **??** apply. Therefore, Theorem **??** gives us an algorithmic way of finding $\mathrm{C}\ell_K$ and $\mathcal{O}_K^{\times}$.

Furthermore, there is an interesting relationship between ζ_K and the primes.

Theorem 7.3 (Euler Product)**.** *For* $\operatorname{Re} s > 1$,

$$\zeta_K(s) = \prod_{\substack{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prime}}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

Proof (Sketch). Fix a nonzero prime $\mathfrak{p}$. Using Geometric Series and the multiplicative property of the norm, we have

$$\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{i=1}^{\infty} \frac{1}{N(\mathfrak{p})^{is}} = \sum_{i=0}^{\infty} \frac{1}{N(\mathfrak{p}^i)^s}.$$

But then we have

$$\prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq x}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq x}} \sum_{i=0}^{\infty} \frac{1}{N(\mathfrak{p}^i)^s} = \sum_{I \in \mathcal{I}} \frac{1}{N(I)^s} = \sum_{I \in \mathcal{I}} \frac{1}{N(I)^s}.$$

where $\mathcal{I}$ is the set of ideals $I \subseteq \mathcal{O}_K$ whose prime factors have norm at most x. Note that we have made use of the unique factorization of ideals in $\mathcal{O}_K$. Finally,

$$\left| \zeta_K(s) - \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \leq x}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \right| = \left| \sum_{I \notin \mathcal{I}} \frac{1}{N(I)^{\operatorname{Re}(s)}} \right| \leq \sum_{N(I) > x} \frac{1}{N(I)^{\operatorname{Re} s}}$$

But the rightmost sum tends to 0 since $\zeta_K(\operatorname{Re}(s))$ converges. □

For the moment, let us focus on the case where $K/\mathbb{Q}$ is quadratic. Choose a prime p.

$$\prod_{\mathfrak{p} \mid p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \begin{cases} (1 - 1 \,/\, p^s)^{-2}, & p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \\ (1 - 1 \,/\, p^{2s})^{-1} = (1 - 1/p^s)^{-1}(1 - 1/p^s)^{-1}, & p\mathcal{O}_K = \mathfrak{p} \\ (1 - 1 \,/\, p^s)^{-1}, & p\mathcal{O}_K = \mathfrak{p}^2 \end{cases}$$

This leads to the following definition.

Definition (Dirichlet L-function)**.**

$$L(s, \chi) := \frac{\zeta_K(s)}{\zeta(s)} = \prod_p \left(1 - \frac{\chi(\mathfrak{p})}{p^s}\right)^{-1},$$

where

$$\chi(p) = \begin{cases} 1, & p \text{ splits in } K \\ -1, & p \text{ inert in } K \\ 0, & p \text{ ramifies in } K \end{cases}$$

Since we have defined χ on the primes, we can extend χ to a map $\chi : \mathbb{N} \to \{-1, 0, +1\}$ multiplicatively.

Definition (L-series)**.**

$$L(s, x) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Again denote by r_1 to be the number of real embeddings of K and by r_2 to be the number of complex conjugate pairs of embeddings of K, where $K/\mathbb{Q}$ is a number field. Observe that

$$L(1, x) = \frac{2^{r_1}(2\pi)^{r_2} h_k \operatorname{Reg}_K}{\omega_K |\operatorname{disc} K|^{1/2}} = \kappa.$$

In particular, we have

$$h_K \operatorname{Reg}_K = \frac{\omega_K |\operatorname{disc} K|^{1/2}}{2^{r_1}(2\pi)^{r_2}} L(1, x).$$

Dirichlet was able to give some closed forms for h_K.

Theorem 7.4 (Dirchlet)**.**

$$h_k = \begin{cases} \dfrac{\omega_K}{2|\operatorname{disc} K|} \left| \displaystyle\sum_{\substack{1 \le j \le |\operatorname{disc} K|/2 \\ (j, \operatorname{disc} K) = 1}} \chi(j)\, j \right|, & \operatorname{disc} K < 0 \\ \dfrac{1}{\log \epsilon} \left| \displaystyle\sum_{\substack{1 \le j \le |\operatorname{disc} K|/2 \\ (j, \operatorname{disc} K) = 1}} \chi(j) \log \left| \sin\left(\frac{\pi j}{|\operatorname{disc} K|}\right) \right| \right|, & \operatorname{disc} K > 0 \end{cases}$$

where $|ep$ is the fundamental unit.

Example 7.4. Let $K = \mathbb{Q}(\sqrt{5})$. We have $\operatorname{disc} K = 5$ and $h_K = 1$. Then

$$\log \epsilon = \left| \log \sin \frac{\pi}{5} - \log \sin \frac{2\pi}{5} \right| = \log \left(\frac{\sin \frac{2\pi}{5}}{\sin \frac{\pi}{5}} \right)$$

Therefore, the fundamental unit is $\epsilon = \dfrac{\sin(\pi/5)}{\sin(2\pi/5)}$. ◁

Example 7.5. Let $K = \mathbb{Q}(\sqrt{-5})$. The formula gives $h_K = 2$. ◁

In the case of quadratics, there are also useful non-closed forms which converges much quicker. Set $d = \operatorname{disc} K$. If $d < 0$,

$$h_K = \sum_{n=1}^{\infty} \chi(n) \left(\operatorname{erfc}\left(n\sqrt{\frac{\pi}{|d|}} \right) + \frac{\sqrt{d}}{\pi n} e^{-\frac{\pi n^2}{|d|}} \right)$$

whereas if $d > 0$

$$h_K \log \epsilon = \frac{1}{2} \sum_{n=1}^{\infty} \chi(n) \left(\frac{\sqrt{|d|}}{n} \operatorname{erfc}\left(n\sqrt{\frac{\pi}{|d|}} + E_1\left(\frac{\pi n^2}{|d|} \right) \right) \right),$$

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 7.6. Let $K = \mathbb{Q}(\sqrt{94})$. We have $\operatorname{disc} K = 4 \cdot 94$. It is also routine to verify that $h_K = 1$. Now $\operatorname{Reg}_K = \log \epsilon = h_K \log \epsilon = 15.271002103$.

$$\epsilon = e^{15.271002103} = 4286589.9999997667\ldots$$

What is the minimal polynomial of ϵ? There are two possibilities:

$$(x - \epsilon)(x - \epsilon^{-1}) \text{ if } N_{K/\mathbb{Q}}(\epsilon) = 1$$
$$(x - \epsilon)(x + \epsilon^{-1}) \text{ if } N_{K/\mathbb{Q}}(\epsilon) = -1$$

The first is $x^2 - 4286590.000\ldots x + 1$ while the second is $x^2 - 4286589.9999953\ldots x + 1 \notin \mathbb{Z}[x]$. Therefore, the minimal polynomial for ϵ is $(x - \epsilon)(x - \epsilon^{-1})$. This allows one to calculate ϵ directly using the quadratic formula. One then finds

$$\epsilon = 2143295 + 221064\sqrt{94}.$$

◁

8 Local Fields

8.1 $\mathfrak{p}$-adic Fields

Definition (Topological Field)**.** A topological field is a field K with a topology such that $+, -, \cdot : K \to K$ and $(\cdot)^{-1} : K^{\times} \to K^{\times}$ are continuous.

Example 8.1. Both $\mathbb{R}$ and $\mathbb{C}$, under their usual topology, are topological fields. ◁

Definition (Local Field)**.** 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.

Now let us see this explicitly in the context of Algebraic Number Theory. Let K be a number field. The fractional ideal generated by $x \in K^\times$ factors uniquely as

$$x\mathcal{O}_K = \prod_{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K} \mathfrak{p}^{\nu_\mathfrak{p}(x)},$$

where $\nu_\mathfrak{p}(x) \in \mathbb{Z}$. Fix $\mathfrak{p}$ and set $\nu_\mathfrak{p}(0) = +\infty$. Define $|\cdot|_\mathfrak{p} : K \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ via $x \mapsto N(\mathfrak{p})^{-\nu_\mathfrak{p}(x)}$.

Definition (Absolute Value)**.** An absolute value on an integral domain R is a function $|\cdot| : R \to \mathbb{R}$ satisfying for all $x, y \in R$,

- $|x| \geq 0$
- $|x| = 0$ if and only if $x = 0$
- $|xy| = |x|\,|y|$
- $|x + y| \leq |x| + |y|$

Example 8.2. The function constructed above, $|\cdot|_\mathfrak{p} : K \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ via $x \mapsto N(\mathfrak{p})^{-\nu_\mathfrak{p}(x)}$, is an absolute value on K. In fact, we have a stronger triangle inequality:

$$|x + y|_\mathfrak{p} \leq \max\{|x|_\mathfrak{p}, |y|_\mathfrak{p}\}.$$

A usual thing about absolute values is that they give norms which can then be used to give a metric: if $\|\cdot\|$ is a norm then $d(x, y) = \|x - y\|$ is a metric. In particular, $|\cdot|_\mathfrak{p}$ induces a topology.

Definition ($\mathfrak{p}$-adic Topology)**.** Let K be a number field and $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$. Define the topology induced by the norm $|\cdot|_\mathfrak{p}$ is called the $\mathfrak{p}$-adic topology.

Remark. Note that in the trivial number field case $K = \mathbb{Q}$, the topology given by the norm $|\cdot|_\mathfrak{p}$ is *not* the usual topology on $\mathbb{Q}$. In particular in this new topology, all triangles are isosceles and the intersection of open balls $B_\epsilon(x) = \{y \in K \colon |x - y|_\mathfrak{p} < \epsilon\}$ is either empty or is one of the open neighborhoods, i.e. one contains the other.

Now that we have a metric topology, we may complete the space so that all Cauchy sequences converge. Let $\widehat{K}$ be the completion of K with respect to the $\mathfrak{p}$-adic topology. [Recall the completion of a metric space is the set of equivalence classes of Cauchy sequences in the metric space.] 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. 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 $|\cdot|_\mathfrak{p}$. The space $K_\mathfrak{p}$ is called the $\mathfrak{p}$-adic completion of K.

Much to the hopes and dreams of all Calculus students, here the Divergence Test become the 'Convergence Test', i.e.

Proposition 8.1. *The series* $\sum_{n=1}^{\infty} a_n$ *converges if and only if* $a_n \to 0$ *as* $n \to \infty$.

Proof (Sketch):

$$\left| \sum_{n=m}^{N} a_n \right| \leq \max\{|a_n| : m \leq n \leq N\}$$

□

Example 8.3. Consider the 2-adic topology on $\mathbb{Q}$, denoted $\mathbb{Q}_2$. In the field $\mathbb{Q}_2$, the sequence

$$a_n = 1 + 2 + 2^2 + \cdots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$$

converges to -1 as $n \to \infty$. ◁

Example 8.4. For $n \geq 0$, consider the rational number

$$\binom{1/2}{n} = \frac{\frac{1}{2}(\frac{1}{2} - 1)(\frac{1}{2} - 2) \cdots (\frac{1}{2} - n + 1)}{n!}.$$

We claim that the denominator is a power of 2: take any odd prime p, it suffices to show that

$$\left| \binom{1/2}{n} \right| \leq 1 \Leftrightarrow \nu_\mathfrak{p}\left(\binom{1/2}{n} \right) \geq 9.$$

Define $f : \mathbb{Q}_p \to \mathbb{Q}_p$ via

$$f(x) = \binom{x}{n} = \frac{x(x-1)(x-2) \cdots (x-n+1)}{n!}.$$

Note that f is continuous. Now

$$\binom{\frac{p^m+1}{2}}{n} = f\left(\frac{p^n + 1}{2} \right) \overset{m \to \infty}{\longrightarrow} f\left(\frac{0+1}{2} \right) = \binom{1/2}{n}.$$

On the left side, we have $\binom{\frac{p^m+1}{2}}{n} \in \mathbb{Z}$. Therefore as $\left| \frac{p^m+1}{2} \right|_\mathfrak{p} \leq 1$ for $m \geq 1$, we have $\left| \binom{1/2}{n} \right|_\mathfrak{p} \leq 1$. ◁

Example 8.5. Consider the field $\mathbb{Q}_5$. Define

$$\alpha = \frac{1}{2}\sum_{n=0}^{\infty}(-1)^n\binom{1/2}{n}5^n.$$

We first need check that α is well defined: the individual terms tend to 0 as

$$\left|(-1)^n\binom{1/2}{n}\right|_5 \leq 1,$$

and as in the previous example $|5^n|_5 = 5^{-n} \to 0$ as $n \to \infty$. For real $|x| < 1$,

$$\sqrt{1+x} = \sum_{n=0}^{\infty}\binom{1/2}{n}x^n.$$

But then we have an equality of formal power series

$$1 + x = \left(\sum_{n=0}^{\infty}\binom{1/2}{n}x^n\right)^2.$$

Setting $x = -5$,

$$-4 = \left(\sum_{n=0}^{\infty}\binom{1/2}{n}(-5)^n\right)^2 \in \mathbb{Q}_5.$$

Therefore, $\alpha^2 = -1$. In particular, $\mathbb{Q}_5$ contains a fourth root of unity.

Now that our fields possess a notion of metric, we may define the ring of integers in terms of this metric.

Definition (Ring of $\mathfrak{p}$-adic Integers)**.** The subring $K_\mathfrak{p}$

$$\mathcal{O}_\mathfrak{p} := \{x \in K_\mathfrak{p} \colon |x|_\mathfrak{p} \leq 1\}$$

is called the ring of $\mathfrak{p}$-adic integers. In the case where $K = \mathbb{Q}$, we denote $\mathcal{O}_\mathfrak{p}$ by $\mathbb{Z}_p$.

It is routine to verify that $\mathcal{O}_\mathfrak{p}$ is indeed a subring of $K_\mathfrak{p}$.

Proposition 8.2. *$\mathcal{O}_\mathfrak{p}$ is a DVR.*

Proof (Sketch): The function $\nu_\mathfrak{p} : K^\times \to \mathbb{Z} \subseteq \mathbb{R}$ is continuous with respect to $|\cdot|_\mathfrak{p}$, and extends uniquely to a continuous map $\nu_\mathfrak{p} : K_\mathfrak{p}^\times \to \mathbb{Z} \subseteq \mathbb{R}$. Choose $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Note that $\nu_\mathfrak{p}(\pi) = 1$. Let $\mathcal{O}_\mathfrak{p}^\times = \{x \in K_\mathfrak{p} \colon |x|_\mathfrak{p} = 1\}$. For $x \in \mathcal{O}_p^\times$, $|x^{-1}|_\mathfrak{p} = |x|_\mathfrak{p}^{-1}$ and 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 $a\pi^{-\nu_\mathfrak{p}(a)} \in \mathcal{O}_p^\times$. 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, i.e. a local PID. Therefore, $\mathcal{O}_\mathfrak{p}$ is a DVR. □

Remark. We can relate $\mathcal{O}_\mathfrak{p}$ to the DVR $\mathcal{O}_K$ via the isomorphism

$$\mathcal{O}_K \Big/ \mathfrak{p} \xrightarrow{\sim} \mathcal{O}_\mathfrak{p} \Big/ \mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \Big/ \pi\mathcal{O}_\mathfrak{p}.$$

Note that the left side is a finite field so that $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is a finite field also.

Parallel to the ordinary number field case, given an element of $K_\mathfrak{p}$, we may multiply by a sufficiently large power of $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ to obtain an element of $\mathcal{O}_\mathfrak{p}$. Therefore to understand the elements of $K_\mathfrak{p}$, one need only understand the elements 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 $\nu_\mathfrak{p}(\pi) = 1$.

Theorem 8.1. *Any $x \in \mathcal{O}_\mathfrak{p}$ can be written uniquely as $\sum_{n=0}^{\infty} a_n \pi^n$, where $a_i \in S$. Conversely, any such series converges to an element of $\mathcal{O}_\mathfrak{p}$.*

Proof (Sketch): Let $x \in \mathcal{O}_\mathfrak{p}$. We make use of the fact that

$$\mathcal{O}_K \Big/ \mathfrak{p} \xrightarrow{\sim} \mathcal{O}_\mathfrak{p} \Big/ \mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \Big/ \pi\mathcal{O}_\mathfrak{p}.$$

Now $x \equiv a_0 \mod \mathfrak{p}\mathcal{O}_\mathfrak{p}$ for a unique $a_0 \in S$. But then $\frac{x-a_0}{\pi} \in \mathcal{O}_\mathfrak{p}$. Then we have $\frac{x-a_0}{\pi} \equiv a_1 \mod \mathfrak{p}\mathcal{O}_\mathfrak{p}$ for a unique $a_1 \in S$. Then as before, $\frac{x-(a_0+a_1\pi)}{\pi^2} \in \mathcal{O}_\mathfrak{p}$. Repeating this process, we find $x - (a_0 + a_1\pi + \cdots + a_n\pi^n) \in \pi^{n+1}\mathcal{O}_\mathfrak{p}$, where $a_i \in S$ are unique. Finally,

$$\left| x - \sum_{i=0}^{n} a_i \pi^i \right|_\mathfrak{p} \leq |\pi|_\mathfrak{p}^{n+1} = \left(\frac{1}{N(\mathfrak{p})} \right)^{n+1} \xrightarrow{n\to\infty} 0.$$

□

Proposition 8.3. *The space $\mathcal{O}_\mathfrak{p}$ is compact.*

Proof (Sketch): Since $K_\mathfrak{p}$ is a metric space, it suffices to prove that $\mathcal{O}_\mathfrak{p}$ is sequentially compact. Consider any sequence $(x_n)_{n\in\mathbb{N}}$ in $\mathcal{O}_\mathfrak{p}$. Write each x_i as $x_i = \sum_{n=0}^{\infty} a_{n_i} \pi^n$ for $a_{n,i} \in S$. There are infinitely many x_n with the same $a_{0,i}$ as S is finite. For such x_n, there are infinitely many with the same $a_{1,i} \in S$. Continuing in this fashion, we obtain a convergence subsequence in $\mathcal{O}_\mathfrak{p}$. □

Note that 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.

8.2 Extensions of $\mathbb{Q}_p$

Fix a prime p, and let $K/\mathbb{Q}_p$ be a finite field extension. Let B be the integral closure of $\mathbb{Z}_p$ in K.

$$\begin{array}{ccc} K & \supseteq & B \\ | & & | \\ \mathbb{Q}_p & \supseteq & \mathbb{Z}_p \end{array}$$

We know that integral closure of Dedekind domains are Dedekind so that B is Dedekind. But then pB factors uniquely, say $pB = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. In fact, there is a single prime so that $pB = \mathfrak{P}^e$. Then $[K\colon \mathbb{Q}_p] = ef$, where $f = [B/\mathfrak{p}\colon \mathbb{Z}_p/(p)]$. Furthermore, we have valuations

$$\nu_\mathfrak{p} : K^\times \to \mathbb{Z}$$
$$\nu_\mathfrak{p} : \mathbb{Q}_p^\times \to \mathbb{Z}$$

such that $\nu_\mathfrak{p}|_{\mathbb{Q}_p^\times} = e\nu_\mathfrak{p}$.

Proposition 8.4. *The p-adic absolute value $|\cdot|_p$ extends uniquely to K.*

Corollary 8.1. *The p-adic absolute value extends uniquely to $\overline{\mathbb{Q}}_p = \overline{K}$.*

Proof. Choose $\sigma : K(\alpha, \beta) \hookrightarrow \overline{K}$ that fixes $K(\beta)$. It suffices to show that $\sigma(\alpha) = \alpha$. As $\beta = \sigma(\beta)$, we have

$$|\sigma(\alpha) - \beta|_p = |\sigma(\alpha) - \sigma(\beta)|_p = |\sigma(\alpha - \beta)|_p.$$

Now $|\sigma(\cdot)|_p$ is an absolute value on $K(\alpha, \beta)$ which extends the absolute value $|\cdot|_p$ on $\mathbb{Q}_p$. By Proposition **??**, this extension is unique. Therefore, $|\sigma(\cdot)|_p = |\cdot|_p$. Observe that

$$|\sigma(\alpha) - \beta|_p = |\sigma(\alpha) - \sigma(\beta)|_p = |\sigma(\alpha - \beta)|_p = |\alpha - \beta|_p.$$

Therefore,

$$\begin{aligned} |\sigma(\alpha) - \alpha|_p &= |\sigma(\alpha) - \beta + \beta - \alpha|_p \\ &\leq \max\{|\sigma(\alpha) - \beta|_p, |\beta - \alpha|_p\} \\ &= |\sigma(\alpha) - \beta|_p. \end{aligned}$$

As $|\sigma(\alpha) - \beta| < |\sigma(\alpha) - \alpha|$ for $\sigma(\alpha) \neq \alpha$, we must have $\sigma(\alpha) = \alpha$. □

Krasner's Lemma is an amazing result that links the analytic properties of local fields with algebraic properties of the field. For instance, consider the following result:

Proposition 8.5. *Fix a monic, irreducible polynomial $f(x) \in K[x]$ of degree n. For any $g(x) \in K[x]$ of degree n "sufficiently close" (with respect to $|\cdot|_p$) to $f(x)$, $g(x)$ is irreducible and for any root $\alpha \in \overline{K}$ of f, there is a root $\beta \in \overline{K}$ of g such that $K(\alpha) = K(\beta)$.*

From this, we are able to obtain the following:

Proposition 8.6. *There is a number field L and a prime $\mathfrak{p} \subseteq \mathcal{O}_L$ dividing p such that $K = L_{\mathfrak{p}}$.*

Proof (Sketch): Using the Primitive Element Theorem, $K = \mathbb{Q}_p(\alpha)$. Let $f(x) \in \mathbb{Q}_p[x]$ be the minimal polynomial of α over $\mathbb{Q}_p$. Take $g(x) \in \mathbb{Q}[x]$ "sufficiently close" to $f(x)$. By Proposition **??** since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, there is a root $\beta \in \overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}}_p$ of $g(x)$ such that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Take $L = \mathbb{Q}(\beta)$. □

Theorem 8.2. *The local fields K of characteristic zero are (up to isomorphism)*

(i) finite extensions $K/\mathbb{Q}_p$

(ii) $\mathbb{R}$ or $\mathbb{C}$

The local fields K of positive characteristic are (up to isomorphism) $\mathbb{F}_q((x))$ for q a prime power.

If B is the integral closure of $\mathbb{Z}_p$ in $K/\mathbb{Q}_p$, then $B = \mathcal{O}_{\mathfrak{p}}$ for a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_L$, where $K = L_{\mathfrak{p}}$.

Lemma 8.1 (Hensel's Lemma)**.** *Let $f(x) \in B[x] = \mathcal{O}_p[x]$ be a monic polynomial and $\overline{f}(x) \in \mathbb{F}_p[x]$ be its reduction mod $\mathfrak{p}$. If $a \in \mathbb{F}_p$ is a simple root of $\overline{f}$, then there is a unique $\alpha \in \mathcal{O}_{\mathfrak{p}}$ with $\alpha \equiv a \mod \mathfrak{p}$ such that α is a root of $f(x)$.*

Proof (Sketch): Suppose $\alpha_n \in \mathcal{O}_{\mathfrak{p}}$ is such that $\alpha_n \equiv a \mod \mathfrak{p}$ and $f(\alpha_n) \equiv 0 \mod \mathfrak{p}^n$ (note that this is true if $n = 0$). Take $\pi \in \mathcal{O}_{\mathfrak{p}}$ with $\nu_{\mathfrak{p}}(\pi) = 1$. We want to solve

$$0 \equiv f(\alpha_n + b\pi^n) \equiv f(\alpha_n) + f'(\alpha_n)b\pi^n \mod \mathfrak{p}^{n+1}$$

Equivalently, we want to solve

$$f'(\alpha_n)b \equiv -\frac{f(\alpha_n)}{\pi^n} \mod \mathfrak{p}.$$

We know that $f'(\alpha_n)b \equiv f'(a)b \mod \mathfrak{p}$ and $f'(a)b \not\equiv \mod \mathfrak{p}$ as a is a simple root. But then we may solve the previous equation for $b \in \mathcal{O}_{\mathfrak{p}}$. Then $\alpha_{n+1} = \alpha_n + b\pi^n$. The sequence $(\alpha_n)_{n\in\mathbb{N}}$ converges to a root. □

Note that the proof of Hensel's Lemma even gives an algorithm for finding a root! Now let $K/\mathbb{Q}_p$ be a finite extension of fields with ring of $\mathfrak{p}$-adic integers $\mathcal{O}_{\mathfrak{p}} \subseteq K$. We have a field extension

$$\begin{array}{c} \mathcal{O}_{\mathfrak{p}}/\mathfrak{p} \\ \Big| f \\ \mathbb{Z}_p/(p) \cong \mathbb{F}_p \end{array}$$

where $f = [\mathcal{O}_\mathfrak{p} \colon \mathbb{Z}_p/(p)]$. But 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 over $\mathbb{F}_p$, Hensel's Lemma gives that $x^{p^f} - x$ is separable in $\mathcal{O}_\mathfrak{p}[x]$. But then K contains $p^f - 1$ roots of unity. Note that this was 'difficult' to show in the Number Field case whereas in the local field case we essentially get roots of unity "for free" by Hensel's Lemma.

Let $\mu_{p^f-1} \subseteq K$ denote the roots of unity in K. We have a tower of field extensions

$$\begin{array}{c} K \\ \Big| e \\ \mathbb{Q}_p(\mu_{p^f-1}) \\ \Big| f \\ \mathbb{Q}_p \end{array}$$

The extension $K/\mathbb{Q}_p(\mu_{p^f-1})$ is totally ramified, but the extension $\mathbb{Q}_p(\mu_{p^f-1})/\mathbb{Q}_p$ is unramified.

Proposition 8.7. *Fix a prime p and integer $n \geq 1$. There are only finitely many extensions, up to isomorphism, $K/\mathbb{Q}_p$ of degree n.*

Proof (Sketch): Any extension $K/\mathbb{Q}_p$ is a totally ramified extension of the intermediate field $\mathbb{Q}_p(\mu_{p^f-1})$ of degree e. Note that both f and e divide n. Set $F := \mathbb{Q}_p(\mu_{p^f-1})$. We need only show that there are only finitely many totally ramified extensions K/F of degree e.

Choose a uniformizer $\pi \in K$ with $\nu_K(\pi) = 1$. The minimal polynomial of π over F is Eisenstein at $\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}$. By Proposition **??**, 'small' change in the coefficients of this minimal polynomial does not change the field extension. This gives an open cover of the compact set $\mathfrak{p}^{e-1}(\mathfrak{p} - \mathfrak{p}^2)$. There is then a finite subcovering so that K can be obtained from one of these finitely many Eisenstein polynomials. □

This even gives information about number fields.

Theorem 8.3. *Let K be a number field, S a finite set of primes of $\mathcal{O}_K$, and $n \geq 1$ an integer. There are only finitely many extensions L/K of degree n unramified at all primes $\mathfrak{p} \notin \mathcal{O}_K$.*

Proof (Sketch): Consider the case $K = \mathbb{Q}$. We know there are only finitely many extensions $L/\mathbb{Q}$ of degree n with given discriminant $\operatorname{disc} L$. The prime divisors of $\operatorname{disc} L$ are the ramified primes of the extension $L/\mathbb{Q}$. We may bound the powers of $\operatorname{disc} L$ occurring by using the finiteness of the number of extensions of $\mathbb{Q}_p$ from Proposition **??**. □

8.3 Class Field Theory