Number Theory
Teorija števil

Daniel Smertnig

Summer Semester 2024

February 8, 2025

Contents

Preface

These are lecture notes for a first master level course in number theory, taught at the Faculty of Mathematics and Physics at the University of Ljubljana in the summer term 2024. The material is largely standard for such a course.

In the first chapter, the prime number theorem is proved, following the proof of Newman as presented by Zagier [Zag97]. The main reference for this chapter is [Koc00, Chapter 1.7 and 1.8].

After this taste of analytic number theory, the remaining material is on algebraic number theory. Chapter 2 follows the book by Marcus [Mar18], whereas the remaining chapters are more in line with the presentation of Neukirch [Neu99]. As in the book by Marcus, the local theory is (unfortunately) omitted, but quadratic and cyclotomic fields are developed throughout as examples. As an illustration of the theory, three proofs of quadratic reciprocity are given (first using Gauss sums, then by relating the decomposition of primes in quadratic and cyclotomic fields, and finally, as a slight variation on the second proof, using Frobenius elements).

The notes assume robust familiarity with undergraduate algebra, but no course on the master level is a prerequisite, in particular, no commutative algebra course is required. The first chapter requires complex analysis (up to contour integration). Familiarity with infinite products is not assumed, the few necessary results are discussed in an appendix. It is helpful to be familiar with field theory and Galois theory, however the necessary statements are recalled when needed (only separable extensions appear). The Structure Theorem on Finitely Generated Abelian Groups is used without proof, but stated in such a way that it may be used as a black box (Theorem 2.41).

Notation

In these notes $\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of all nonnegative integers, and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We write $\mathbb{P} = \{2, 3, 5, \dots\} \subseteq \mathbb{N}$ for the set of all prime numbers. The symbols $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ denote the complex numbers, real numbers, rational numbers, and integers, respectively. We write $\mathbb{R}_{\ge 0}$ for the nonnegative reals, and $\mathbb{R}_{>0}$ for the positive reals (with analogous notation applied to other sets).

Rings are always commutative and unital. Ring homomorphisms are assumed to preserve the multiplicative identity. A domain is a (nonzero) ring in which 0 is the only zero-divisor. For a ring R, we denote by $R^\times$ the group of units (i.e., the group of invertible elements) and by $R^\bullet$ the submonoid of non-zero-divisors. A ring R is a domain if and only if $R^\bullet = R \setminus \{0\}$.

Two functions f, $g\colon (a, \infty) \to \mathbb{R}$ are asymptotically equivalent, denoted by $f \sim g$ if

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

By $\log(x)$ we denote the natural logarithm. By $\operatorname{Log}(z)$ we denote the principal branch of the logarithm, defined on $\mathbb{C} \setminus \mathbb{R}_{\le 0}$.

Chapter 1

Distribution of Prime Numbers

This chapter largely follows [Koc00, Chapters 1.7, 1.8]. The proof of the prime number theorem is essentially the "short" proof of Newman, as presented by Zagier [Zag97].

By the *Fundamental Theorem of Arithmetic*, every natural number can be written as a product of prime numbers, and this factorization is unique up to the order of the factors. Everyone has surely seen a proof that there are infinitely many prime numbers (most probably a version of Euclid's proof). The following strengthening was found by Euler.

Theorem 1.1.

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty. \tag{1.1}$$

Exercise 1.2. *Prove Theorem 1.1. You may proceed along the following intermediate steps.*

(1) *For every* $m \geq 0$,

$$P(x) \coloneqq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(1 - \frac{1}{p}\right)^{-1} > \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^m}\right),$$

and if $2^m > x$, *then*

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^m}\right) > \sum_{n \leq x} \frac{1}{n}.$$

Conclude $\lim_{x \to \infty} P(x) = \infty$.

(2) *Using the Taylor series of* $\log(1-t)$,

$$-\log(1-t) - t < \frac{1}{2} \frac{t^2}{1-t} \quad \text{for } 0 < t < 1.$$

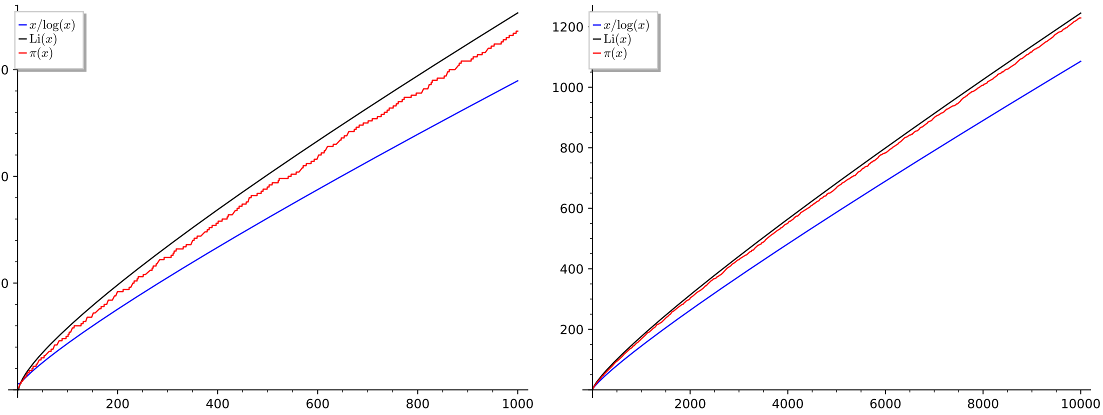

Figure 1.1: Prime counting function $\pi(x)$ for $x \leq 1000$ und for $x \leq 10000$. Here $\mathrm{Li}(x) = \int_2^x 1/\log(t)\,dt$ is the logarithmic integral. While $\mathrm{Li}(x) \sim x/\log(x) \sim \pi(x)$, the logarithmic integral provides a better approximation of $\pi(x)$ than $x/\log(x)$.

(3) *With* $S(x) \coloneqq \sum_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{1}{p}$, *estimate*

$$\log P(x) - S(x) < \sum_{n=2}^{\infty} \frac{1}{2}\frac{1}{n(n-1)} = \frac{1}{2}.$$

Equation (1.1) tells us more about the number of primes than just their infinitude: since the series $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges, there must be “more” primes than square numbers. To make this more precise, we define the prime counting function π.

Definition 1.3 (Prime Counting Function). *For* $x \in \mathbb{R}$, *let*

$$\pi(x) \coloneqq |\{\, p \in \mathbb{P} : p \leq x \,\}|.$$

This function encodes the distribution of prime numbers. The exact distribution of prime numbers is a notoriously difficult topic with many basic questions still open (e.g., the twin prime conjecture). However, asymptotically, we have the following.

Theorem 1.4 (Prime Number Theorem, PNT).

$$\pi(x) \sim \frac{x}{\log(x)}. \tag{1.2}$$

Versions of the prime number theorem were first conjectured at the end of the 18th century. A proof attempt of P. Chebyshev (1848 and 1850) yielded that there are constants c, $C > 0$, such that

$$c\,\frac{x}{\log(x)} \leq \pi(x) \leq C\,\frac{x}{\log(x)}.$$

However, the first proofs of the PNT were only published in 1896, independently by J. Hadamard and C. J. de la Vallée Poussin. Most proofs use some amount of complex analysis. The proof presented here is due to Newman and is fairly simple while simultaneously only using basic complex analysis.

1.1 The Riemann Zeta Function

We first introduce the Riemann zeta function and its Euler product.

Theorem 1.5. *Fix $\sigma \in \mathbb{R}_{>1}$. Then, for all $s \in \mathbb{C}$ with $\operatorname{Re}(s) \geq \sigma$,*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \tag{1.3}$$

converges uniformly and absolutely.

Proof. We first check that the series as well as the infinite product converge uniformly and absolutely on the stated region, and then that they are equal.

Recall that exponentiation by a complex number is defined as $n^s = \exp(s \log(n))$. Hence $|n^s| = n^{\operatorname{Re}(s)} > n^{\sigma}$. Thus

$$\sum_{n=1}^{\infty} \left| \frac{1}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}},$$

and because of $\sigma > 1$, the series on the right side converges. Therefore $\sum_{n=1}^{\infty} n^{-s}$ converges uniformly and absolutely on $\operatorname{Re}(s) \geq \sigma$. In particular, the induced function is holomorphic (Theorem A.8).

Substituting the geometric series, the product is of the form

$$\prod_{p \in \mathbb{P}} \left(1 + \sum_{k \geq 1} \frac{1}{p^{sk}}\right).$$

Noting that $\sum_{p \in \mathbb{P}} \left| \sum_{k \geq 1} p^{-sk} \right| \leq \sum_{p \in \mathbb{P}} \sum_{k \geq 1} p^{-\sigma k}$ is dominated by $\sum_{n \geq 1} n^{-\sigma}$, this product converges uniformly and absolutely on $\operatorname{Re}(s) \geq \sigma$ (Lemma A.7).

By the fundamental theorem of arithmetic, every $n \in \mathbb{N}$ has a unique representation as a product of primes $p \leq x$. Using the geometric series expansion

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - p^{-s}} = \prod_{p \leq x} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right),$$

we therefore get $(x > 1)$

$$\left| \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - p^{-s}} - \sum_{n \leq x} \frac{1}{n^s} \right| \leq \sum_{n \geq x} |n^{-s}| \leq \sum_{n \geq x} n^{-\sigma},$$

and hence

$$\lim_{x\to\infty}\left|\prod_{\substack{p\in\mathbb{P}\\ p\leq x}}\frac{1}{1-p^{-s}}-\sum_{n\leq x}\frac{1}{n^s}\right|=0.$$

□

Definition 1.6. *For $s\in\mathbb{C}$ with $\mathrm{Re}(s)>1$, the Riemann zeta function is defined by*

$$\zeta(s):=\sum_{n=1}^{\infty}\frac{1}{n^s}. \tag{1.4}$$

The product representation in Equation (1.3) is called the Euler product representation of $\zeta(s)$.

Lemma 1.7. *For all $s\in\mathbb{C}$ with $\mathrm{Re}(s)>1$, we have $\zeta(s)\neq 0$.*

Proof. This is immediate from the convergence of the Euler product. □

Note that there is a subtlety here: convergence of an infinite product requires the partial products, by definition, to converge to a *nonzero* value, and this is indeed ensured by the convergence criterion we have used in Theorem 1.5.

Remark 1.8. While the series in Equation (1.4) diverges for $s=1$, it is possible to extend ζ to a meromorphic function on $\mathbb{C}$ having only a single (simple) pole at $s=1$ with residue 1. On possibility to do so, is to prove a functional equation, such as the reflection functional equation

$$\zeta(1-s)=(2\pi)^{-s}2\cos\left(\frac{\pi}{2}s\right)\Gamma(s)\zeta(s),$$

where $\Gamma(s)$ is the gamma function.

The functional equation shows that $\zeta(s)$ has simple zeros at $-2k$ with $k\geq 1$. These are the *trivial zeros* of $\zeta(s)$. Riemann showed that all other zeros are in the *critical strip* defined by $0<\mathrm{Re}(s)<1$ (and that there are indeed infinitely many non-trivial zeros). The famous *Riemann hypothesis* states that all non-trivial zeros are on the critical strip $\mathrm{Re}(s)=1/2$. While the conjecture was already formulated by Riemann in 1859, it remains open. It is one of the most notorious open problems in number theory (and pure mathematics) and is also one of the Millenium Prize Problems. For the prime number theorem, it will suffice to show that ζ has no zero s with $\mathrm{Re}(s)=1$, but better knowledge of the zeros can be used to derive error bounds.

We do not pursue the full analytic continuation of $\zeta(s)$ here, and instead only extend it to $\mathrm{Re}(s)>0$ with $s=1$.

Proposition 1.9. $\zeta(s)-\frac{1}{s-1}$ *has a holomorphic continuation to $s\in\mathbb{C}$ with $\mathrm{Re}(s)>0$.*

Proof. For $\mathrm{Re}(s)>1$,

$$\zeta(s)-\frac{1}{s-1}=\sum_{n=1}^{\infty}n^{-s}-\int_1^{\infty}x^{-s}\,dx=\sum_{n=1}^{\infty}\left(n^{-s}+\int_n^{n+1}x^{-s}\,dx\right)=\sum_{n=1}^{\infty}\int_n^{n+1}n^{-s}-x^{-s}\,dx. \tag{1.5}$$

Let $I_n(s) \coloneqq \int_n^{n+1} n^{-s} - x^{-s}\,dx$.

For $\mathrm{Re}(s) \geq 0$, we can estimate (for $n \leq x \leq n+1$),

$$|n^{-s} - x^{-s}| = \left| \int_n^x s u^{-s-1}\,du \right| \leq \frac{|s|}{n^{\mathrm{Re}(s)+1}}.$$

Fix $s_0 \in \mathbb{C}$ with $\mathrm{Re}(s_0) > 0$. Taking $\varepsilon \leq \mathrm{Re}(s_0)/2$, for all $s \in \mathbb{C}$ with $|s - s_0| < \varepsilon$, we can bound $|n^{-s} - x^{-s}| \leq (|s_0| + \varepsilon)/n^{\sigma+1}$ with $\sigma = \mathrm{Re}(s_0) - \varepsilon > 0$. Then

$$|I_n(s)| \leq \frac{|s_0| + \varepsilon}{n^{\sigma+1}} \qquad \text{and} \qquad \sum_{n=1}^{\infty} |I_n(s)| \leq \big(|s_0| + \varepsilon\big) \sum_{n=1}^{\infty} n^{-\sigma-1} < \infty.$$

We conclude that the series on the right side of Equation (1.5) converges uniformly in the open disc $|s - s_0| < \varepsilon$. Since each $I_n(s)$ is holomorphic in s, the series defines a function that is holomorphic in s (Theorem A.8). □

Lemma 1.10. *For all $s \in \mathbb{C} \setminus \{1\}$ with $\mathrm{Re}(s) > 0$, it holds that $\overline{\zeta(\overline{s})} = \zeta(s)$.*

Proof. For $\mathrm{Re}(s) > 1$ this follows from $\zeta(\overline{s}) = \sum_{n=1}^{\infty} n^{-\overline{s}} = \overline{\sum_{n=1}^{\infty} n^{-s}}$. Now both $s \mapsto \zeta(s)$ and $s \mapsto \overline{\zeta(\overline{s})}$ are meromorphic on $\mathrm{Re}(s) > 0$, and so must coincide (away from their pole $s = 1$). □

1.2 Proof of the Prime Number Theorem

Aside from $\zeta(s)$ we need two more auxiliary functions,

$$\phi(s) \coloneqq \sum_{p \in \mathbb{P}} \frac{\log(p)}{p^s} \qquad \text{and} \qquad \vartheta(x) \coloneqq \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \log(p).$$

One should think of ϑ as a log-weighted version of $\pi(x)$. The relevance of ϕ will be that $\phi(s)/s$ will turn out to be the Laplace transform of $\vartheta(e^t)$. The strategy is to show $\vartheta(x) \sim x$, from which one can then deduce Theorem 1.4 with some comparatively straightforward estimates.

Proposition 1.11. *The series $\sum_{p \in \mathbb{P}} \frac{\log(p)}{p^s}$ converges uniformly and absolutely for $\mathrm{Re}(s) \geq \sigma > 1$, and therefore $\phi(s)$ is holomorphic on the domain $\mathrm{Re}(s) > 1$.*

Proof (Sketch). The proof is similar to Theorem 1.5. With $\mathrm{Re}(s) \geq \sigma > 1$ and $0 < \varepsilon < \sigma - 1$,

$$\sum_{p \in \mathbb{P}} \left| \frac{\log(p)}{p^s} \right| \leq \sum_{p \in \mathbb{P}} \frac{\log(p)}{p^{\sigma}} \leq \sum_{n=1}^{\infty} \frac{\log(n)}{n^{\varepsilon}} \frac{1}{n^{\sigma - \varepsilon}}.$$

Convergence of the right side is ensured by $\sigma - \varepsilon > 1$ together with $\lim_{n\to\infty} \frac{\log(n)}{n^{\varepsilon}} = 0$. □

For meromorphic f one can consider the logarithmic derivative f'/f. It has the property of transforming poles and zeros of f into simple poles of f'/f and is particularly useful when f

is defined by an infinite product (Proposition A.9). More specifically, about the poles of f'/f we can say the following. Suppose that $f\colon U \to \mathbb{C}$ is meromorphic, with a root of order $\mu > 0$ at $z_0 \in U$. Looking at the Taylor series expansion, we have $f(z) = a_\mu(z - z_0)^\mu + \dots$ with $a_\mu \neq 0$ in a neighborhood of z_0. Since $f'(z) = \mu a_\mu (z - z_0)^{\mu-1} + \dots$, we see that the logarithmic derivative

$$f'(z)/f(z) = \mu(z - z_0)^{-1} + \cdots,$$

has a simple pole with residue μ at z_0. Similarly, if f has a pole of order μ at z_0, then we look at the Laurent series expansion $f = a_{-\mu}(z - z_0)^{-\mu} + \cdots$ to see that f'/f has a simple pole with residue $-\mu$. If f has neither a pole nor a zero at z_0, then f'/f is holomorphic at z_0.

As for $\zeta(s)$, we can extend $\phi(s)$ meromorphically to a larger domain.

Proposition 1.12. *The function $\phi(s)$ has a meromorphic continuation to the domain* $\mathrm{Re}(s) > 1/2$*, with simple poles at $s = 1$ and at the zeros of $\zeta(s)$, but no other poles.*

Proof. Computing the logarithmic derivative of the Euler product formula for $\zeta(s)$ gives (using Proposition A.9), for $\mathrm{Re}(s) > 1$,

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p\in\mathbb{P}} -\frac{(-1)(1-p^{-s})^{-2}(-p^{-s})(-\log(p))}{(1-p^{-s})^{-1}} = \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s - 1} = \phi(s) + \sum_{p\in\mathbb{P}} \frac{\log(p)}{p^s(p^s-1)}, \tag{1.6}$$

(using $\frac{1}{p^s-1} = \frac{1}{p^s} - \frac{1}{p^s(p^s-1)}$ in the last step). Now the series on the right converges uniformly and absolutely on the region $\mathrm{Re}(s) \geq \sigma'$ for all $\sigma' > \frac{1}{2}$. Because $\zeta'(s)/\zeta(s)$ is meromorphic in that region, it follows that $\phi(s)$ must also be meromorphic on $\mathrm{Re}(s) > 1/2$. □

The following extension of Lemma 1.7 is a crucial step in the proof of the prime number theorem. It was first established by de la Vallée Poussin in 1896.

Theorem 1.13. *For all $s \in \mathbb{C}$ with* $\mathrm{Re}(s) = 1$*, it holds that $\zeta(s) \neq 0$.*

Proof. Suppose that $s = 1 + ib$ with $0 \neq b \in \mathbb{R}$ is a zero of ζ of order μ. Let $\nu \geq 0$ be the order of vanishing of ζ at $1 + 2ib$ (that is, $\nu = 0$ if there is no zero of ζ at $1 + 2ib$ and $\nu > 0$ is the order of the root otherwise). By Lemma 1.10 the roots are symmetric with respect to reflection around the real axis. Having expressed the logarithmic derivative of ζ as a sum of ϕ and a holomorphic function in Equation (1.6), we get

$$\lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon) = 1, \quad \lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon \pm ib) = -\mu, \quad \lim_{\varepsilon\to 0} \varepsilon\phi(1+\varepsilon \pm 2ib) = -\nu.$$

Substituting into the definition of ϕ and using the binomial formula gives

$$\begin{aligned}\sum_{r=-2}^{2}\binom{4}{2+r}\phi(1+\varepsilon+irb) &= \sum_{p\in\mathbb{P}}\log(p)\left(\binom{4}{0}p^{-1-\varepsilon\pm 2ib}+\binom{4}{1}p^{-1-\varepsilon\pm ib}+\binom{4}{2}p^{-1-\varepsilon}\right)\\ &= \sum_{p\in\mathbb{P}}\frac{\log(p)}{p^{1+\varepsilon}}\left(\binom{4}{0}p^{\pm 2ib}+\binom{4}{1}p^{\pm ib}+\binom{4}{2}\right) = \sum_{p\in\mathbb{P}}\frac{\log(p)}{p^{1+\varepsilon}}(p^{ib/2}+p^{-ib/2})^4\\ &= \sum_{p\in\mathbb{P}}\frac{\log(p)}{p^{1+\varepsilon}}(2\operatorname{Re}(p^{ib/2}))^4 \geq 0.\end{aligned}$$

Multiplying by $\varepsilon > 0$ and taking the limit $\varepsilon \to 0$, we get

$$-2\nu - 8\mu + 6 \geq 0,$$

but because of ν, $\mu \in \mathbb{Z}_{\geq 0}$, this is only possible if $\mu = 0$. □

The previous theorem together with Equation (1.6) implies that $\phi(z+1)$ is meromorphic in $\operatorname{Re}(z) \geq 0$, with a unique simple pole with residue 1 at $z = 0$. Thus

$$g(z) = \frac{\phi(z+1)}{z+1} - \frac{1}{z} \tag{1.7}$$

is holomorphic for $\operatorname{Re}(z) \geq 0$. We can moreover express g in terms of an integral involving ϑ. To do so, we should first recognize that ϑ has at most linear growth.

Lemma 1.14. *For all $x \in \mathbb{R}_{\geq 0}$ it holds that $\vartheta(x) \leq 4x$.*

Proof. First, let $n \in \mathbb{N}$. Then $\exp(\vartheta(2n)-\vartheta(n)) = \prod_{n<p\leq 2n} p$. Every prime of the product divides $(2n)!$, but none of them divides $n!$, therefore

$$\prod_{n<p\leq 2n} p \leq \frac{(2n)!}{n!\cdot n!} = \binom{2n}{n}.$$

Using the binomial formula,

$$\exp(\vartheta(2n)-\vartheta(n)) \leq \binom{2n}{n} \leq (1+1)^{2n} \leq 2^{2n},$$

and hence $\vartheta(2n) - \vartheta(n) \leq 2n\log(2)$. Taking an arbitrary $x \in \mathbb{R}_{\geq 0}$ and $2n-2 < x \leq 2n$ (so that $n-1 < x/2 \leq n$), we get

$$\vartheta(x) - \vartheta(x/2) \leq \vartheta(2n) - \vartheta(n-1) \leq \vartheta(2n) - \vartheta(n) + \log(n) \leq 2n\log(2) + \log(n) \leq 3n \leq 2x.$$

Now, using $2 = 1/(1-2^{-1}) = \sum_{n=0}^{\infty} 2^{-n}$,

$$4x = \sum_{n=0}^{\infty}\frac{2x}{2^n} \geq \sum_{n=0}^{\infty}\left(\vartheta(x/2^n) - \vartheta(x/2^{n+1})\right) = \vartheta(x),$$

where the last equality follows from the observation that the series is a (finite) telescope sum.□

Lemma 1.15. *For* $\mathrm{Re}(z) > 0$,

$$g(z) = \int_0^\infty (\vartheta(e^t)e^{-t} - 1)e^{-zt}\,dt.$$

Proof. This will follow from recognizing $\phi(s)/s$ as the Laplace transform of $\vartheta(e^t)$ and then making some substitutions. So, first, if we enumerate the primes by $p_1 < p_2 < \dots$ and set $p_0 = 1$, we find (for $\mathrm{Re}(s) > 1$)

$$\begin{aligned}\phi(s) &= \sum_{j=0}^\infty \frac{\log(p_j)}{p_j^s} = \sum_{j=0}^\infty \frac{\vartheta(p_j) - \vartheta(p_{j-1})}{p_j^s} = \sum_{j=0}^\infty \vartheta(p_j)\Big(\frac{1}{p_j^s} - \frac{1}{p_{j+1}^s}\Big) = \sum_{j=1}^\infty \vartheta(p_j) s \int_{p_j}^{p_{j+1}} \frac{1}{x^{s+1}}\,dx \\ &= \sum_{j=0}^\infty s \int_{p_j}^{p_{j+1}} \frac{\vartheta(x)}{x^{s+1}}\,dx = s\int_1^\infty \frac{\vartheta(x)}{x^{s+1}}\,dx = s\int_0^\infty \frac{\vartheta(e^t)}{e^{(s+1)t}}e^t\,dt = s\int_0^\infty \vartheta(e^t)e^{-st}\,dt,\end{aligned}$$

Now, for $\mathrm{Re}(z) > 0$,

$$g(z) = \frac{\phi(z+1)}{z+1} - \frac{1}{z} = \int_0^\infty \vartheta(e^t)e^{-(z+1)t}\,dt - \int_0^\infty e^{-zt}\,dt = \int_0^\infty f(t)e^{-zt}\,dt,$$

with $f(t) = \vartheta(e^t)e^{-t} - 1$. □

We seek to apply the following theorem (whose proof we postpone for the moment) to our situation.

Theorem 1.16 ("Analytic Theorem"). *Let* $f\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ *be bounded and locally integrable. Suppose that*

$$g(z) := \int_0^\infty f(t)e^{-zt}\,dt \qquad (\mathrm{Re}(z) > 0)$$

extends holomorphically to $\mathrm{Re}(z) \geq 0$. *Then* $\int_0^\infty f(t)\,dt$ *exists and equals* $g(0)$.

Under the given conditions, it can be shown with some basic complex analysis that the integral (which is really the Laplace transform of f) converges for $\mathrm{Re}(z) > 0$ and defines a holomorphic function (see Proposition A.3). The theorem says that if we can extend the region of holomorphicity of the function $g(z)$ a little bit, namely to $\mathrm{Re}(z) = 0$ (where the function would then *not* be defined by this particular integral in general), we can still compute the value at 0 by "naively" plugging in 0 into the integral.

In our case we will use $f(t) = \vartheta(e^t)e^{-t} - 1$; its boundedness follows from Lemma 1.14.

Putting this together allows us to observe the following.

Theorem 1.17. *The limit*

$$\lim_{T\to\infty} \int_1^T \frac{\vartheta(x) - x}{x^2}\,dx$$

exists and equals $g(0)$.

Proof. We make a substitution $x = e^t$, and get

$$\int_1^{e^T} \frac{\vartheta(x) - x}{x^2}\, dx = \int_0^T \vartheta(e^t)e^{-t} - 1\, dt.$$

Now $f(t) = \vartheta(e^t)e^{-t} - 1$ is bounded by Lemma 1.14. Thanks to Lemma 1.15 we can apply Theorem 1.16 with $g(z) = \phi(z+1)/(z+1) - 1/z$, which shows the claim. □

Theorem 1.18. *It holds that $\vartheta(x) \sim x$ for $x \to \infty$.*

Proof. Suppose this is not the case. Then there exists some $\lambda > 1$ such that $\vartheta(x) \geq \lambda x$ for arbitrarily large x, or there exists $\lambda < 1$ such that $\vartheta(x) \leq \lambda x$ for arbitrarily large x.

First consider the case where $\vartheta(x) > \lambda x$ for arbitrarily large x (with $\lambda > 1$). Since $\vartheta(x)$ is non-decreasing, for such x,

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2}\, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^{\lambda} \frac{\lambda - y}{y^2}\, dy = c_\lambda,$$

for some constant $c_\lambda > 0$ that depends on λ but not on x. This contradicts the convergence of the improper integral (Theorem 1.17).

If $\vartheta(x) < \lambda x$ for arbitrarily large x (with $\lambda < 1$), then similarly

$$\int_{\lambda x}^{x} \frac{\vartheta(t) - t}{t^2}\, dt \leq \int_{\lambda x}^{x} \frac{\lambda x - t}{t^2}\, dt = \int_{\lambda}^{1} \frac{\lambda - y}{y^2}\, dy = c'_\lambda < 0,$$

again contradicting the convergence in Theorem 1.17. □

Proof (Proof of the Prime Number Theorem, Theorem 1.4). For $x > 0$ and $\varepsilon > 0$ we estimate

$$\vartheta(x) = \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \log(p) \leq \pi(x)\log(x), \quad \text{and}$$
$$\vartheta(x) \geq \sum_{\substack{p \in \mathbb{P} \\ x^{1-\varepsilon} \leq p \leq x}} \log(p) \geq \sum_{\substack{p \in \mathbb{P} \\ x^{1-\varepsilon} \leq p \leq x}} (1-\varepsilon)\log(x) \geq (1-\varepsilon)\log(x)\big(\pi(x) - x^{1-\varepsilon}\big).$$

Therefore

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x)\log(x)}{x} \leq \frac{\vartheta(x)}{(1-\varepsilon)x} + \frac{\log(x)}{x^{\varepsilon}}.$$

Then

$$1 \leq \limsup_{x\to\infty} \frac{\pi(x)\log(x)}{x} \leq \frac{1}{1-\varepsilon},$$

and

$$1 \leq \liminf_{x\to\infty} \frac{\pi(x)\log(x)}{x} \leq \frac{1}{1-\varepsilon},$$

Since this is true for arbitrarily small ε, we obtain $\lim_{x\to\infty} \pi(x)/(x\log(x)) = 1$. □

We still have to prove the Analytic Theorem.

Proof (Proof of Theorem 1.16). For $T > 0$, define

$$g_T(z) \coloneqq \int_0^T f(t) e^{-zt}\, dt.$$

This function is holomorphic on all of $\mathbb{C}$.[1] We have to show $\lim_{T\to\infty} g_T(0) = g(0)$. To do so, we use Cauchy's integral formula to express $g(0) - g_T(0)$ as a contour integral, and then show that this integral goes to 0 for $T \to \infty$.

Fix a radius $R > 0$ (we will later consider $R \to \infty$) and consider the semicircle of radius R in the positive half-plane. Since $g(z)$ is holomorphic in the half-plane $\mathrm{Re}(z) \geq 0$, it is in particular holomorphic on the vertical line segment $z = yi$ with $y \in [-R, R]$. Using that g is analytic on this line segment and the line segment is compact, we can find a $\delta > 0$ (depending on R), so that $g(z)$ (and therefore $g(z) - g_T(z)$) is still analytic in the closed set

$$S = \{\, z \in \mathbb{C} : |z| \leq R,\ \mathrm{Re}(z) \geq -\delta \,\}.$$

Applying Cauchy's integral formula (Theorem A.1) to the boundary C of S and the function $(g(z) - g_T(z)) \exp(zT)(1 + z^2/R^2)$,

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_C \underbrace{(g(z) - g_T(z)) \exp(zT)\Big(1 + \frac{z^2}{R^2}\Big)\frac{1}{z}}_{I(z)}\, dz.$$

We estimate the integral, by splitting C into three parts

$$\begin{aligned} C_1 &\coloneqq \{\, z \in \mathbb{C} : |z| = R,\ \mathrm{Re}(z) \geq 0 \,\}, \\ C_2 &\coloneqq \{\, z \in \mathbb{C} : |z| = R,\ -\delta \leq \mathrm{Re}(z) \leq 0 \,\}, \text{and} \\ C_3 &\coloneqq \{\, z \in \mathbb{C} : |z| \leq R,\ \mathrm{Re}(z) = -\delta \,\}. \end{aligned}$$

We first deal with C_1. By boundedness of f, there exists $B \coloneqq \max\{\, |f(t)| : t \in \mathbb{R}_{\geq 0} \,\}$. For $\mathrm{Re}(z) > 0$, then

$$|g(z) - g_T(z)| \leq \left| \int_T^\infty f(t) e^{-zt}\, dt \right| \leq B \int_T^\infty |e^{-zt}|\, dt = B \frac{e^{-\mathrm{Re}(z)T}}{\mathrm{Re}(z)},$$

and so

$$|I(z)| \leq \frac{B}{\mathrm{Re}(z)} \frac{1}{R} \left| \frac{R}{z} + \frac{z}{R} \right| = \frac{B}{\mathrm{Re}(z)} \frac{1}{R} \frac{2\,\mathrm{Re}(z)}{R} = \frac{2B}{R^2},$$

[1] E.g., using Moreara's Theorem. One can exchange the line integral and the integral because the integral of the absolute values is finite, because the integrand is bounded on compact sets. The argument is similar to Proposition A.3, but even easier because here T is finite.

where we used $\overline{z/R} = (z/R)^{-1}$ because $R = |z|$. Since the semicircle C_1 has arc length πR, we get

$$\frac{1}{2\pi}\int_{C_1} |I(z)|\,dz \le B/R.$$

On C_2 and C_3, we will bound the integral for $g_T(z)$ and $g(z)$ separately.

We first deal with g_T and consider the paths C_2 and C_3 together. Since g_T is holomorphic on all of $\mathbb{C}$, we can change the integration path to be over the entire semicircle $-C_1$ in the negative half-plane, without affecting the value of the integral. We then estimate $g_T(z)$ (using $\mathrm{Re}(z) < 0$):

$$|g_T(z)| \le \int_0^T |f(t)e^{-zt}|\,dt \le B\int_0^T e^{-\mathrm{Re}(z)t}\,dt = \frac{B}{\mathrm{Re}(z)}(1 - e^{-\mathrm{Re}(z)T}) \le \frac{Be^{-\mathrm{Re}(z)T}}{|\mathrm{Re}(z)|}.$$

This is the same bound we obtained for $|g(z) - g_T(z)|$ on C_1 before. Hence we can bound

$$\frac{1}{2\pi}\int_{-C_1} \left| g_T(z)\exp(zT)\Big(1 + \frac{z^2}{R^2}\Big)\frac{1}{z}\right| dz \le B/R$$

in the same way as in the case of C_1.

For the integral with $g(z)$, we can bound $\left|g(z)(1 + z^2/R^2)\frac{1}{z}\right| \le M$ on $C_2 \cup C_3$ with some $M \ge 0$ (because the function is holomorphic, in particular continuous, there). Then we get $\left|g(z)(1 + z^2/R^2)\frac{1}{z}\right|\exp(zT) \to 0$ for all $\mathrm{Re}(z) \le 0$ and $T \to \infty$. Thus

$$\frac{1}{2\pi}\int_{C_2\cup C_3} \left| g(z)\Big(1 + \frac{z^2}{R^2}\Big)\frac{1}{z}\exp(zT)\right| dz \to 0 \qquad \text{for } T \to \infty,$$

(which is justified by, say, monotone convergence).

Putting everything together, have shown $\limsup_{T\to\infty}|g(0) - g_T(0)| \le 2B/R$. Since R is arbitrary, we get $\lim_{T\to\infty}|g(0) - g_T(0)| = 0$. □

Chapter 2

Algebraic Integers

2.1 Motivating Examples

Sums of squares and the Gaussian integers. Which natural numbers n can be represented as sums of two squares $n = a^2 + b^2$ with $a, b \in \mathbb{N}_0$? E.g. $1 = 1^2 + 0^2$, $2 = 1^2 + 1^2$, but for 3 this is not possible, whereas again $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, for 6, 7, it is again impossible, while $8 = 2^2 + 2^2$, $9 = 3^2 + 0^2$, ...

Allowing ourselves to use the imaginary unit $i^2 = -1$, we see

$$n = a^2 + b^2 = (a + ib)(a - ib),$$

and so the problem reduces to a question about factorizations in the ring of Gaussian integers

$$\mathbb{Z}[i] = \{\, a + bi : a, b \in \mathbb{Z} \,\} \subseteq \mathbb{C}.$$

This ring is very well-behaved from the point of view of factorizations.

Definition 2.1. *A domain R is Euclidean if there is a map $\delta\colon R \smallsetminus \{0\} \to \mathbb{N}_0$ with the following property: for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.*

Proposition 2.2. *$\mathbb{Z}[i]$ is an Euclidean domain with respect to the* Norm $\mathsf{N}(a + bi) = |a + ib|^2 = a^2 + b^2$.

Proof. See also the exercises or [Bre19, Theorem 5.71].

Suppose $\alpha = a + bi$ and $\beta = c + di \in \mathbb{Z}[i]$ with $\beta \neq 0$. The element β has an inverse in the field $\mathbb{Q}(i)$, and we get $\alpha\beta^{-1} = \gamma$ with $\gamma = x + yi$ and some $x, y \in \mathbb{Q}$. Looking at the complex plane, the set (lattice) $\mathbb{Z}[i]$ consists of all points with integral coordinates. Since the unit square has diameter $\sqrt{2}$, any point in $\mathbb{C}$ is at a Euclidean distance at most $\sqrt{2}/2$ from a point of $\mathbb{Z}[i]$.

Picking the point $\gamma' = x' + y'i \in \mathbb{Z}[i]$ that is closest to γ, we must therefore have

$$\mathsf{N}(\gamma - \gamma') = |\gamma - \gamma'|^2 \le (\sqrt{2}/2)^2 < 1.$$

But then

$$\alpha = \beta\gamma = \beta\gamma' + \beta(\gamma - \gamma'),$$

with $\beta(\gamma - \gamma') \in \mathbb{Z}[i]$ and $\mathsf{N}(\beta(\gamma - \gamma')) < \mathsf{N}(\beta)$. □

In particular, the domain $\mathbb{Z}[i]$ is a *principal ideal domain*: every ideal I of $\mathbb{Z}[i]$ is of the form $I = (\alpha)$ with $\alpha \in I$ (to see this, take α an element of minimal norm in I; then using the Euclidean property, every other element of I is a multiple of α). Therefore $\mathbb{Z}[i]$ is a *unique factorization domain* (in short *UFD*, also called a *factorial domain*): every nonzero non-unit element $\alpha \in \mathbb{Z}[i]$ can be written as a product of the form $\alpha = \pi_1 \cdots \pi_n$ with $\pi_1, \dots, \pi_n$ prime elements [1]. Further, this factorization is unique up to permutation and associativity of the factors: recall that α, β are associated (written $\alpha \simeq \beta$) if and only if there exists a unit $\varepsilon \in \mathbb{Z}[i]$ such that $\alpha = \beta\varepsilon$ (equivalently, the principal ideals generated by these elements are equal, that is $(\alpha) = (\beta)$). Then, if also $\alpha = \pi_1' \cdots \pi_m'$ with prime elements $\pi_1', \dots, \pi_m'$, then $m = n$, and, after a possible reindexing, $\pi_j' \simeq \pi_j$ for all $1 \le j \le n$. See [Bre19, Chapter 5.3] for details.

Thus, the ring $\mathbb{Z}[i]$ looks in many aspects quite similar to $\mathbb{Z}$. Understanding which elements of $\mathbb{N}$ are sums of two squares amounts to understanding the image of the norm function on $\mathbb{Z}[i]$, so let us take a closer look.

Lemma 2.3. *Let* $\mathsf{N}\colon \mathbb{Z}[i] \to \mathbb{N}_0$, $a + bi \mapsto a^2 + b^2$ *(with* $a, b \in \mathbb{Z}$*). Let* $\alpha, \beta \in \mathbb{Z}[i]$.

(1) $\mathsf{N}(\alpha) = 0$ *if and only if* $\alpha = 0$.

(2) $\mathsf{N}(\alpha\beta) = \mathsf{N}(\alpha)\,\mathsf{N}(\beta)$. *That is, the map* N *is a homomorphism of multiplicative monoids* $\mathbb{Z}[i] \to \mathbb{N}_0$ *and, when restricted, of* $\mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$.

(3) $\alpha \in \mathbb{Z}[i]^\times$ *if and only if* $\mathsf{N}(\alpha) = 1$. *In particular,* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Proof. First observe that N is indeed well-defined: if $\alpha \in \mathbb{Z}[i]$, then the representation $\alpha = a + bi$ with $a, b \in \mathbb{Z}$ is unique by linear independence of $(1, i)$ over $\mathbb{Z}$ (indeed, 1 and i are even linearly independent over $\mathbb{R}$). Moreover, the expression $a^2 + b^2$ is always nonnegative for $a, b \in \mathbb{Z}$.

(1) Clear.

(2) Note that $\mathsf{N}(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = \mathsf{N}(\alpha)\,\mathsf{N}(\beta)$.

(3) The necessity of $\mathsf{N}(\alpha) = 1$ is a consequence of $\mathbb{N}^\times = \{1\}$ and (2). Explicitly, if $\alpha \in \mathbb{Z}[i]^\times$, then there exists $\alpha^{-1} \in \mathbb{Z}[i]$ such that $\alpha^{-1}\alpha = 1$. But then $\mathsf{N}(\alpha), \mathsf{N}(\alpha^{-1}) \in \mathbb{N}_0$ and $\mathsf{N}(\alpha)\,\mathsf{N}(\alpha^{-1}) = 1$, which is only possible for $\mathsf{N}(\alpha) = \mathsf{N}(\alpha^{-1}) = 1$.

[1] Recall that a nonzero non-unit π of a domain R is a *prime element* if $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$. A nonzero non-unit π is *irreducible* if every representation $\pi = \alpha\beta$ implies that α or β is a unit. Prime elements are always irreducible. In a UFD all irreducible elements are prime. More specifically, if R is a domain in which every nonzero non-unit is a product of irreducible elements (e.g., a noetherian domain), then R is a UFD *if and only if* all irreducible elements are prime.

For sufficiency, we can simply observe that the only solutions to $\mathsf{N}(a+bi)=1$ are given by ± 1 and $\pm i$, each of which is obviously a unit in $\mathbb{Z}[i]$.

There is another way that is more conceptually insightful for later generalizations: Note $\mathsf{N}(\alpha)=\alpha\overline{\alpha}$ (complex conjugation). If $\mathsf{N}(\alpha)\in\mathbb{N}^\times=\{1\}$, we can simply divide by $\mathsf{N}(\alpha)$, to get $\alpha(\overline{\alpha}\,\mathsf{N}(\alpha)^{-1})=1$, and hence, that α is a unit. □

The multiplicativity of the norm function immediately implies: if m and n are sums of two squares, then so is mn. Indeed, we can even explicitly expand the absolute values in (2) to get the identity

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

This suggests to first consider prime numbers that are representable as sums of two squares. (Together with unique factorization in $\mathbb{Z}[i]$, this will later turn out to be sufficient to also understand the composite case.)

Theorem 2.4 (Fermat). *Let $p\in\mathbb{P}$ be an odd prime. Then there exist a, $b\in\mathbb{Z}$ such that $p=a^2+b^2$ if and only if $p\equiv 1 \mod 4$.*

Proof. First suppose $p\equiv 3 \mod 4$. If $a\in\mathbb{Z}$ then $a^2\equiv 0,1 \mod 4$. Hence $a^2+b^2\not\equiv 3 \mod 4$, and p cannot be represented as sum of two squares ("there is a congruence obstruction modulo 4").

Now let $p\equiv 1 \mod 4$. To see that p is a sum of two squares, it suffices to show that p is not a prime element in $\mathbb{Z}[i]$. Indeed, then $p=\alpha\beta$ with non-units α, $\beta\in\mathbb{Z}[i]$, and, taking norms, $p^2=\mathsf{N}(\alpha)\,\mathsf{N}(\beta)$ shows $\mathsf{N}(\alpha)=p=\mathsf{N}(\beta)$.

So let us show that p is not a prime element. Because $p\equiv 1 \mod 4$, we claim that there exists $b\in\mathbb{Z}$ such that $b^2\equiv -1 \mod p$. An easy way to see this is the following: for all $a\not\equiv 0 \mod p$, we have $a^{p-1}\equiv 1 \mod p$ (little Fermat). Therefore the polynomial $X^{p-1}-1$ has $p-1$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$, and since $X^{p-1}-1=(X^{(p-1)/2}-1)(X^{(p-1)/2}+1)$, there exists $a\in\mathbb{Z}$ such that $a^{(p-1)/2}\equiv -1 \mod p$. Taking $b:=a^{(p-1)/4}$, which is possible because $4\mid p-1$, we have $b^2\equiv -1 \mod p$.

So p divides $b^2+1=(b+i)(b-i)$. But $\frac{b}{p}\pm\frac{1}{p}i\notin\mathbb{Z}[i]$. Thus p divides neither of the two factors and hence cannot be prime. □

Let us also make explicit note of the following property, that we proved in the course of the previous proof (and that you have probably seen before, in an elementary number theory course).

Lemma 2.5. *Let $p\in\mathbb{P}$. Then -1 is a square modulo p if and only if $p\equiv 1 \mod 4$ or $p=2$.*

Proposition 2.6. *Up to associativity, the following are the prime elements of $\mathbb{Z}[i]$.*

(1) $\pi=1+i$.

(2) $\pi=a+bi$ *with* $a^2+b^2=p\in\mathbb{P}$, $p\equiv 1 \mod 4$, *and* $0<|b|<a$.

(3) $\pi=p\in\mathbb{P}$ *with* $p\equiv 3 \mod 4$.

Proof. We first check that the listed elements are prime elements. Clearly if $\mathsf{N}(\pi) \in \mathbb{P}$, then π is irreducible (and hence prime) in $\mathbb{Z}[i]$. This shows that the elements $1 + i$ and $a + bi$ with $a^2 + b^2 \in \mathbb{P}$ are prime elements. Note that $a^2 \equiv 0, 1 \mod 4$ for all $a \in \mathbb{Z}$. Let $p \in \mathbb{P}$ with $p \equiv 3 \mod 4$. If p is not irreducible, then $p = \alpha\beta$ with α, $\beta \in \mathbb{Z}[i]$ non-units. Hence $\mathsf{N}(\alpha)\,\mathsf{N}(\beta) = p^2$ implies $\mathsf{N}(\alpha) = p$. But if $\alpha = a + bi$, this means $a^2 + b^2 \equiv 3 \mod 4$, which is impossible. So p is irreducible in $\mathbb{Z}[i]$.

We now check that none of the stated elements are associated. Associated elements must have the same norm (because all units have norm 1), so we only need to consider $\pi = a + bi$ with $a^2 + b^2 = p \equiv 1 \mod 4$ and $0 < |b| < a$. Then π has exactly three other associates: $-\alpha$ is not on the list (because $-a < 0$), and neither are $\pm i\alpha$ (because $|b| < |a|$).

It remains to check that every prime element of $\mathbb{Z}[i]$ is associated with one of the listed ones. Let $\pi \in \mathbb{Z}[i]$ be prime. Then $\mathsf{N}(\pi) = \pi\overline{\pi} = p_1 \cdots p_k$ with prime numbers $p_1, \ldots, p_k$. Hence $\pi \mid p_j$ for some j. Setting $p \coloneqq p_j$, we must have $\mathsf{N}(\pi) = p$ or $\mathsf{N}(\pi) = p^2$.

First suppose $\mathsf{N}(\pi) = p$. Then $\pi = a + bi$ with $a^2 + b^2 = p$. Hence $p \not\equiv 3 \mod 4$. If $p \equiv 1 \mod 4$, then multiplying by one of -1, $\pm i$ if necessary, we can ensure the remaining constraints in (2). Otherwise $p = 2$. But this is only possible for $\pi = \pm 1 \pm i$, all of which are associated with $1 + i$.

Now suppose $\mathsf{N}(\pi) = p^2$. Then $\mathsf{N}(p/\pi) = 1$, and hence p and π are associated. We can rule out $p \equiv 1 \mod 4$, because in that case p is not irreducible (by the argument in Theorem 2.4). For the same reason we can rule out $p = 2$, as $2 = (1 + i)(1 - i)$ is not prime. Thus $p \equiv 3 \mod 4$, and we are in case (3). □

We now completely understand the factorization of prime numbers (of $\mathbb{Z}$) in the larger ring $\mathbb{Z}[i]$. Up to units, we have

$$\begin{cases} 2 = (-i) \cdot (1 + i)^2, & \\ p & \text{remains prime if } p \equiv 3 \mod 4, \\ p = \pi\overline{\pi} & \text{for any } \pi \in \mathbb{Z}[i] \text{ with } \mathsf{N}(\pi) = p \text{ if } p \equiv 1 \mod 4. \end{cases}$$

Theorem 2.7. *A natural number $n \in \mathbb{N}$ is a sum of two squares if and only if every prime divisor $p \equiv 3 \mod 4$ of n has even multiplicity in n.*

Proof. First suppose

$$n = 2^e p_1^{e_1} \cdots p_s^{e_s} q_1^{2f_1} \cdots q_t^{2f_t}$$

with distinct primes $p_j \equiv 1 \mod 4$, $q_j \equiv 3 \mod 4$ and e, e_j, $f_j \in \mathbb{N}_0$. Then each of 2, p_j, and q_j^2 is a sum of two squares. Therefore, so is their product, by multiplicativity of the norm.

Now suppose $n = a^2 + b^2$ with a, $b \in \mathbb{Z}$. Set $\alpha = a + bi \in \mathbb{Z}[i]$. Write $n = 2^e p_1^{e_1} \cdots p_s^{e_s} q_1^{f_1} \cdots q_t^{f_t}$ with prime numbers $p_j \equiv 1 \mod 4$ and $q_j \equiv 3 \mod 4$ (pairwise distinct). We claim that the exponents

f_j are even. Factoring α into primes in $\mathbb{Z}[i]$, we can write

$$\alpha = (1+i)^{e'} \pi_1 \cdots \pi_k r_1 \cdots r_l,$$

where $N(\pi_j) \equiv 1 \mod 4$, and $r_j \in \mathbb{P}$ are primes with $r_j \equiv 3 \mod 4$. Comparing

$$n = \mathsf{N}(\alpha) = \alpha\overline{\alpha} = 2^{e'} \pi_1 \overline{\pi_1} \cdots \pi_k \overline{\pi_k} r_1^2 \cdots r_l^2,$$

it follows that $q_1^{f_1} \cdots q_t^{f_t} = r_1^2 \cdots r_l^2$, from which the claim follows. □

Remark 2.8. (1) The observation that an odd prime p is expressible as a sum of two squares if and only if $p \equiv 1 \mod 4$ is usually attributed to Fermat, although it seems that the first published version (including the composite case) is in fact due to Albert Girard (published 1625). The first proof was published by Euler (1752 and 1755) using *infinite descent.* There are many different proofs of this fact, not all of them exploit the structure of $\mathbb{Z}[i]$.

(2) Legendre showed (in 1797/1798) that n is a sum of three squares unless it is of the form $n = 4^a(8b+7)$ with a, $b \in \mathbb{N}_0$. In the ternary case, unfortunately, there is no good norm that can be exploited. Lagrange showed that *every* natural number is a sum of four squares. Here one can again exploit the norm function on the quaternions (a noncommutative ring) to reduce the problem to expressing every prime as sum of four squares.

The ring $\mathbb{Z}[i]$ plays in the field $\mathbb{Q}(i) = \{ a + bi : a, b \in \mathbb{Q} \}$ a similar role as $\mathbb{Z}$ plays in $\mathbb{Q}$. To this end let us observe one final property, regarding the dependence on the generator i. Clearly we have $\mathbb{Q}(i) = \mathbb{Q}(i+1) = \mathbb{Q}(2i)$. But whereas $\mathbb{Z}[i] = \mathbb{Z}[1+i]$ obviously $\mathbb{Z}[2i] \subsetneq \mathbb{Z}[i]$. Nevertheless the ring $\mathbb{Z}[i]$ plays a distinguished role.

Proposition 2.9. *Let $\alpha \in \mathbb{Q}(i)$. Then $\alpha \in \mathbb{Z}[i]$ if and only if there exist c, $d \in \mathbb{Z}$ such that α is a root of*

$$X^2 + cX + d$$

Proof. First suppose $\alpha = a + bi$ with a, $b \in \mathbb{Z}$. Then $\overline{\alpha} = a - bi$, and so α is a root of the polynomial

$$(X - \alpha)(X - \overline{\alpha}) = X^2 + (-2a)X + (a^2 + b^2) \in \mathbb{Z}[X].$$

Now let $\alpha = a + bi$ with a, $b \in \mathbb{Q}$ and suppose that α is the root of a polynomial

$$X^2 + cX + d,$$

with c, $d \in \mathbb{Z}$. First, suppose $b = 0$. Let $a = m/n$ with $n \in \mathbb{N}$, $m \in \mathbb{Z}$ and $\gcd(m,n) = 1$. Then $m^2 + cmn + dn^2 = 0$. Therefore $n \mid m^2$, and this is only possible if $n = 1$.

Now suppose $b \neq 0$. Then $a - bi$ must also be a root of the polynomial. Hence $c = -2a$ and $d = a^2 + b^2$. From $a^2 \in \frac{1}{4}\mathbb{Z}$, we get $b^2 \in \frac{1}{4}\mathbb{Z}$, and hence $2b \in \mathbb{Z}$. Substituting, we find $(2a)^2 + (2b)^2 \equiv 0$

mod 4. Because squares are 0 or 1 modulo 4, this is only possible if $(2a)^2 \equiv (2b)^2 \equiv 0 \mod 4$, hence $a, b \in \mathbb{Z}$. □

Special cases of Fermat's Last Theorem and Cyclotomic Fields. Consider the Diophantine equation

$$X^n + Y^n = Z^n \qquad \text{for } n \geq 2.$$

A solution $(x, y, z) \in \mathbb{Z}^3$ is *non-trivial* if $xyz \neq 0$. A solution for $n = 2$ is known as a Pythagorean triple, as these solutions correspond to right triangles with integral side lengths. There are infinitely many primitive solutions (that is, with $\gcd(x, y, z) = 1$), and they can again be described by working in $\mathbb{Z}[i]$ (see the exercise class). "Fermat's Last Theorem" famously asserts that there are no non-trivial solutions for $n \geq 3$. A proof of this theorem was first found by Andrew Wiles (announced in 1993, but there was a flaw that Wiles fixed together with his student Robert Taylor, and the proof was completed in 1995). A proof is far beyond our scope, but we can sketch an earlier approach, due to Kummer, that resolves the question for a few particular exponents.

First, while there are solutions for $n = 2$, one can use this to show that there are no non-trivial solutions for $n = 4$ (see the exercise class). However, then there are no solutions for any $n = 4m$ with $m \geq 1$. It therefore suffices to rule out non-trivial solutions for $n = p$ an odd prime.

First note that, cancelling common factors, one can always assume that at most one of the components of a solution is divisible by p. (If two are, then so is the third, giving a common factor.) We restrict to the special case of solutions (x, y, z) with $p \nmid xyz$, and can also assume $\gcd(x, y, z) = 1$. Then the equation already implies $\gcd(x, y) = \gcd(y, z) = \gcd(x, z) = 1$.

We factor the left side of $X^p + Y^p = Z^p$: observe that the roots of $T^p - 1$ are precisely the p-th roots of unity. Hence we can write

$$T^p - 1 = (T - 1)(T - \zeta) \dots (T - \zeta^{p-1}) \tag{2.1}$$

where ζ is a p-th root of unity, that is $\zeta^p = 1$ but $\zeta \neq 1$ (e.g., to pick a specific ζ, we may take $\zeta = e^{2\pi i/p} \in \mathbb{C}$). Substituting $T = -X/Y$ and multiplying by Y^p leads to

$$X^p + Y^p = \prod_{i=0}^{p-1} (X + \zeta^i Y) = Z^p. \tag{2.2}$$

Thus we are naturally led to consider the equation in the subring $\mathbb{Z}[\zeta]$ of the *cyclotomic field* $\mathbb{Q}(\zeta)$. We forego a detailed analysis of $\mathbb{Z}[\zeta]$, analogous to what we did for $\mathbb{Z}[i]$, at this point, and just note that not all of these rings are UFDs anymore ($p = 23$ provides the first counterexample).

Suppose that $x^p + y^p = z^p$ with $p \nmid xyz$ and $\gcd(x, y, z) = 1$. For $p = 3$ we note $x^3 \equiv \pm 1 \mod 9$, so there is a congruence obstruction modulo 9. We can assume $p \geq 5$.

One can show the following.

Lemma 2.10. (1) *If $\mathbb{Z}[\zeta]$ is a UFD, then $x + \zeta y = \varepsilon \alpha^p$ for some unit $\varepsilon \in \mathbb{Z}[\zeta]^\times$ and $\alpha \in \mathbb{Z}[\zeta]$.*

(2) *One has* $x \equiv y \mod p$ *in* (1).

Proof. (1) Since $\mathbb{Z}[\zeta]$ is a UFD, it suffices to show: if a prime π divides $x + \zeta y$, then it does so with multiplicity a multiple of p. Suppose π is a prime element dividing $x + \zeta y$. By (2.2), the element π divides z^p. Since π is prime, it divides z, and therefore it must divide z^p with some multiplicity ep. If we can show that π does not divide any $x + \zeta^i y$ with $i = 0$ or $2 \leq i \leq p-1$, we will be done by unique factorization in $\mathbb{Z}[\zeta]$. Suppose that π divides some other factor $x + \zeta^i y$. Then $\pi \mid (x + \zeta^i y) - (x + \zeta y) = y(\zeta^i - \zeta) = y\zeta(\zeta^{i-1} - 1)$. Substituting $T = 1$ into

$$(T - \zeta)\dots(T - \zeta^{p-1}) = \frac{T^p - 1}{T - 1} = \sum_{i=0}^{p-1} T^i,$$

gives $p = \prod_{j=1}^{p-1}(\zeta^j - 1)$. It follows that $\pi \mid py$. Now π divides py and z. However, py and z are coprime integers, so there exist $a, b \in \mathbb{Z}$ with $apy + bz = 1$. Then $\pi \mid 1$, a contradiction.

(2) We skip the proof of this. It is less relevant to our motivation and needs a lemma of Kummer about units in cyclotomic fields, but for the proof of this lemma, we should first develop some more theory. We refer to [Mar18, Exercise 16–28] for a sketch. □

Swapping (x, y, z) for $(x, -z, -y)$ one also gets $x \equiv -z \mod p$. Then

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \mod p.$$

Hence $3x^p \equiv 0 \mod p$. Because of $p \nmid 3$ and $p \nmid x$, this is a contradiction.

Unique factorization was used to obtain $x + \zeta y = \varepsilon\alpha^p$. However, this argument can be saved in a larger number of cases: it as *always* the case that in $\mathbb{Z}[\zeta]$ every nonzero *ideal* is (uniquely) a product of *prime ideals*. This insight is due to Dedekind and will be one of the main results on rings of algebraic integers. Now one can show $(x + \zeta y) = I^p$ for some ideal I, even if $\mathbb{Z}[\zeta]$ is not a UFD. Clearly, the ideal I^p is principal. To recover the argument (in special cases) we would like to deduce that I itself is principal.

We now sketch a key invariant in algebraic number theory: if I, J are nonzero ideals of $\mathbb{Z}[\zeta]$ one can define an equivalence relation by $I \sim J$ if and only if there exists $\beta \in \mathbb{Q}(\zeta)$ such that $I = \beta J$ (in fact, this is equivalent to $I \cong J$ as ideals). Denoting by $[I]$ the class of an ideal, one obtains a multiplication $[I][J] \coloneqq [IJ]$. We will show that in this way the set of ideal classes is a *finite abelian group*, called the (*ideal*) *class group*. Its order h is the *class number*. The trivial class $[R]$ (the neutral element) consists of the principal ideals. We therefore have

$$[R] = [I^p] = [I]^p.$$

If $p \nmid h$, then p is coprime to the order of $[I]$, and hence $\operatorname{ord}([I]) = \operatorname{ord}([I^p])$, and so also $[I]$ is principal. Such a prime is *regular* and in this case Kummer's argument works. The prime $p = 23$ is regular, but unfortunately, there exist irregular primes (e.g. $p = 37$). In fact, one knows that there are infinitely many irregular primes, but it is not known if there are infinitely many regular primes.

2.2 Number Fields and their Rings of Integers

Definition 2.11. *A number field is a subfield K of $\mathbb{C}$ having finite degree over $\mathbb{Q}$. Elements of a number field are called algebraic numbers.*

More explicitly: $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ is a field. Therefore K is a $\mathbb{Q}$-vector space, and we require the degree $[K:\mathbb{Q}] \coloneqq \dim_{\mathbb{Q}} K$ to be finite. Then we have the following.

- K is algebraic (over $\mathbb{Q}$), that is, every $\alpha \in K$ is the root of some nonzero (monic) polynomial $f \in \mathbb{Q}[X]$ [Bre19, Lemma 7.32]. Thus actually $K \subseteq \overline{\mathbb{Q}}$. Moreover, every $\alpha \in K$ is the root of a unique monic polynomial of minimal degree, the minimal polynomial of α, denoted by $m_\alpha \in \mathbb{Q}[X]$. The degree of α is defined as $\deg m_\alpha$. If $f \in \mathbb{Q}[X]$ with $f(\alpha) = 0$, then m_α divides f.
- Because $\mathbb{Q}$ is a perfect field, all field extensions are separable. In particular, by the primitive element theorem [Bre19, Theorem 7.127], there always exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.
- If $K = \mathbb{Q}(\alpha)$ and α has minimal polynomial m_α of degree d, then $1, \alpha, \ldots, \alpha^{d-1}$ form a $\mathbb{Q}$-basis of K. Thus $[K:\mathbb{Q}] = \deg m_\alpha$ and

$$K = \{\, a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} : a_0, a_1, \ldots, a_{d-1} \in \mathbb{Q} \,\} \cong \mathbb{Q}[X]/(m_\alpha).$$

- Suppose $K = \mathbb{Q}(\alpha)$ with m_α the minimal polynomial of α. Over $\mathbb{C}$ (more specifically, already over $\overline{\mathbb{Q}}$) we may factor

$$m_\alpha = (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_d),$$

  with $\alpha_1 = \alpha$. Because m_α is irreducible, it is coprime to the formal derivative m_α' and therefore has no repeated roots, that is, the α_i are pairwise distinct. By standard facts from field theory, the field K has precisely d embeddings into $\mathbb{C}$, one for each root, mapping $\alpha \mapsto \alpha_i$. The α_i are the algebraic conjugates of α.

Observe that the algebraic numbers are exactly the elements of $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. In particular, they form a field.

Example. (1) The number $\sqrt{2}$ has minimal polynomial $X^2 - 2$ with roots $\pm\sqrt{2}$. The quadratic field $\mathbb{Q}(\sqrt{2})$ has two embeddings into $\mathbb{C}$, given by $a + \sqrt{2}b \mapsto a \pm \sqrt{2}b$. Note that these map $\mathbb{Q}(\sqrt{2})$ to itself, and hence are automorphisms of the field.

(2) The minimal polynomial of $\sqrt[3]{2}$ is $X^3 - 2$. It has the three distinct roots $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2}$ where $\zeta = e^{2\pi i/3}$. Because $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, only the identity is an automorphism of the field, the other two embeddings do not have their image in $\mathbb{Q}(\sqrt[3]{2})$. This can be rectified by

working in a bigger number field (the *normal closure*), in this example the field $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ of degree 6. □

Definition 2.13. *An algebraic integer is an algebraic number that is the root of a monic polynomial $f \in \mathbb{Z}[X]$.*

The following crucial fact on factorizations of polynomials in $\mathbb{Z}[X]$ is a standard fact [Bre19, Theorem 5.8], (essentially Gauss's Lemma, [Bre19, Lemma 5.7]). Since will be a crucial fact for us, we give a short proof anyway.

Lemma 2.14. *Let $f \in \mathbb{Z}[X]$ be monic and suppose $f = gh$ with monic g, $h \in \mathbb{Q}[X]$, then g, $h \in \mathbb{Z}[X]$.*

Proof. Let d, $e \in \mathbb{N}$ be minimal such that dg, $eh \in \mathbb{Z}[X]$. If $p \in \mathbb{P}$ divides dg, then $p \mid d$ because g is monic. But then $(d/p)g \in \mathbb{Z}[X]$, contradicting the minimality of d, and so we see that the coefficients of dg must be coprime. The same is true for eh. Now we show $de = 1$. Suppose not, and let $p \in \mathbb{P}$ with $p \mid de$. Then $p \mid def$ but $p \nmid dg$ and $p \nmid eh$. In $\mathbb{Z}/p\mathbb{Z}[X] \cong \mathbb{Z}[X]/p\mathbb{Z}[X]$ we get

$$\overline{0} = \overline{def} = \overline{dg} \cdot \overline{eh}.$$

But $\mathbb{Z}/p\mathbb{Z}[X]$ is a domain and so $p \mid dg$ or $p \mid eh$, a contradiction. □

Lemma 2.15. *An algebraic number α is an algebraic integer if and only if the minimal polynomial satisfies $m_\alpha \in \mathbb{Z}[X]$.*

Proof. If $m_\alpha \in \mathbb{Z}[X]$, then α is an algebraic integer by definition. Conversely, suppose α is an algebraic integer and let $f \in \mathbb{Z}[X]$ be a monic polynomial with $f(\alpha) = 0$. Then $f = gm_\alpha$ for some monic $g \in \mathbb{Q}[X]$. Lemma 2.14 yields $m_\alpha \in \mathbb{Z}[X]$. □

Proposition 2.16. *Let K be a number field and $\alpha \in K$. The following statements are equivalent.*

(a) *α is an algebraic integer.*

(b) *The additive group of the ring $\mathbb{Z}[\alpha] \subseteq K$ is finitely generated.*

(c) *α is contained in some subring R of K with $(R, +)$ a finitely generated group.*

(d) *There exists some nonzero finitely generated subgroup $(A, +) \subseteq (K, +)$ such that $\alpha A \subseteq A$.*

Proof. (a) ⇒ (b) If $\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha_1 + a_0$ with $a_i \in \mathbb{Z}$, then $\mathbb{Z}[\alpha]$ is generated by 1, α, …, α^{n-1} as additive group.

(b) ⇒ (c) Take $R = \mathbb{Z}[\alpha]$.

(c) ⇒ (d) Take $A = R$.

(d) ⇒ (a) Let $A = \langle \beta_1, \ldots, \beta_n \rangle_{\mathbb{Z}}$. For each $1 \le i \le n$, let c_{i1}, …, $c_{in} \in \mathbb{Z}$ be such that

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

Let $C = (c_{ij})_{i,j} \in M_n(\mathbb{Z})$ and $\mathbf{v} = (\beta_1, \dots, \beta_n)^T$. Then $\alpha\mathbf{v} = C\mathbf{v}$ and so $(\alpha I - C)\mathbf{v} = 0$. Because $\mathbf{v} \neq 0$, this means $\det(\alpha I - C) = 0$, and expanding the determinant gives the desired monic polynomial. □

Corollary 2.17. *The algebraic integers of a number field form a subring.*

Proof. Clearly every $a \in \mathbb{Z}$ is an algebraic integer. It therefore suffices to show: if α, β are algebraic integers, then so are $\alpha\beta$ and $\alpha + \beta$.

Let $\mathbb{Z}[\alpha] = \langle \alpha_1, \dots, \alpha_m \rangle_{\mathbb{Z}}$ and $\mathbb{Z}[\beta] = \langle \beta_1, \dots, \beta_n \rangle_{\mathbb{Z}}$ with α_i, $\beta_j \in K$. Using distributivity, we immediately see $\mathbb{Z}[\alpha, \beta] = \langle \alpha_i \beta_j : 1 \leq i \leq m, 1 \leq j \leq n \rangle_{\mathbb{Z}}$. Since $\alpha + \beta$ and $\alpha\beta$ are contained in $\mathbb{Z}[\alpha, \beta]$, the previous lemma implies the claim. □

Definition 2.18. *The* ring of integers *of a number field K is the ring of all algebraic integers in K. It is denoted by $\mathcal{O}_K$.*

Rings of integers of number fields are also known as the maximal order or principal order in the number field; less commonly they are called number rings. One can also consider the set $\overline{\mathbb{Z}}$ of all algebraic integers in $\overline{\mathbb{Q}}$. By the same argument $\overline{\mathbb{Z}}$ is a ring, and $\overline{\mathbb{Z}} \cap K = \mathcal{O}_K$.

Example. We have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ and $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ by Proposition 2.9.

In $\mathbb{Q}(\sqrt{5})$, we have $\mathbb{Z}[\sqrt{5}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. We have $\mathbb{Z}[\sqrt{5}] = \langle 1, \sqrt{5} \rangle$. However, also

$$\alpha = \frac{1 + \sqrt{5}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})},$$

because $\alpha^2 - \alpha - 1 = 0$. □

Remark 2.20 (Generalizations in commutative algebra). Let $R \subseteq S$ be rings. An element $s \in S$ is integral over R if is the root of a monic polynomial $f \in R[X]$. One can generalize the previous results to show that the set of all elements in S that are integral over R form a subring of S. This subring is called the integral closure of R in S. Thus $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

Quadratic Fields.

Exercise 2.21. *A number field of degree 2 is called a* quadratic field. *Show the following.*

(1) *Every quadratic number field is of the form $\mathbb{Q}(\sqrt{d})$ with d a squarefree integer.*

(2) *If d, d' are two squarefree integers and $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}(\sqrt{d'})$, then $d = d'$.*

Proposition 2.22. *Let $d \in \mathbb{Z}$ be squarefree and $K = \mathbb{Q}(\sqrt{d})$.*

(1) *If $d \equiv 2, 3 \mod 4$, then*

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \{\, a + b\sqrt{d} : a, b \in \mathbb{Z} \,\}.$$

(2) *If* $d \equiv 1 \mod 4$, *then*

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z},\ a \equiv b \mod 2\right\}.$$

Proof. Let $\alpha = \frac{a+b\sqrt{d}}{2}$ with a, $b \in \mathbb{Q}$. Since $\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$, the case $b = 0$ is trivial. Suppose $b \neq 0$. Then $\alpha' = \frac{a-b\sqrt{d}}{2}$ is the unique algebraic conjugate of α (other than α itself), that is,

$$m_\alpha = (X-\alpha)(X-\alpha') = X^2 - aX + \frac{a^2-db^2}{4}. \tag{2.3}$$

Thus $\alpha \in \mathcal{O}_K$ if and only if $a \in \mathbb{Z}$ and $a^2 - db^2 \in 4\mathbb{Z}$. If $a \in \mathbb{Z}$, then $a^2 - db^2 \in \mathbb{Z}$ implies also $db^2 \in \mathbb{Z}$. Since d is squarefree, this is only possible if $b \in \mathbb{Z}$.

Now consider the case $d \equiv 2, 3 \mod 4$. For $x \in \mathbb{Z}$, recall $x^2 \equiv 0 \mod 4$ if x is even, and $x^2 \equiv 1 \mod 4$ if x is odd. Thus $a^2 - db^2 \equiv 0 \mod 4$ holds if and only if a, b are both even. Thus $\mathcal{O}_K = \langle 1, \sqrt{d}\rangle_{\mathbb{Z}}$. The equality $\mathbb{Z}[\sqrt{d}] = \langle 1, \sqrt{d}\rangle_{\mathbb{Z}}$ is immediate.

Now consider $d \equiv 1 \mod 4$. Here $a^2 - db^2 \equiv a^2 - b^2 \equiv 0 \mod 4$ is possible if a, b are either both even or both odd, that is, if $a \equiv b \mod 2$. Hence

$$\mathcal{O}_K = \left\{\frac{a+b\sqrt{d}}{2} : a, b \in \mathbb{Z},\ a \equiv b \mod 2\right\}.$$

Because the stated set contains $\frac{1+\sqrt{d}}{2}$ and is a ring, we obtain $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathcal{O}_K$. For the converse inclusion, let $\alpha = \frac{a+b\sqrt{d}}{2}$ with $a \equiv b \mod 2$. Then $a = 2a' + \epsilon$ and $b = 2b' + \epsilon$ with a', $b' \in \mathbb{Z}$ and $\epsilon \in \{0, 1\}$. Hence

$$\alpha = a' + b'\sqrt{d} + \epsilon\frac{1+\sqrt{d}}{2}.$$

To see $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, we just have to show $\sqrt{d} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. But

$$\sqrt{d} = 2\,\frac{1+\sqrt{d}}{2} - 1.$$

□

Cyclotomic Fields. An element $\zeta \in \mathbb{C}$ is a n-th root of unity ($n \geq 1$) if $\zeta^n = 1$. It is a primitive n-th root of unity if $\zeta^m \neq 1$ for all $m \mid n$ with $m \neq n$. The n-th roots of unity in $\mathbb{C}$ are given by $e^{k2\pi i/n}$ with $0 \leq k \leq n-1$. Such a root is primitive if and only if $\gcd(k, n) = 1$. We write $\mu_n(\mathbb{C})$ for the set of all n-th roots of unity in $\mathbb{C}$, and $\mu_n^*(\mathbb{C})$ for the set of primitive n-th roots of unity.

Definition 2.23. *Let ζ_n be a primitive n-th root of unity. The field $\mathbb{Q}(\zeta_n) = \mathbb{Q}(e^{2\pi i/n})$ is the n-th cyclotomic field.*

Note that $\mathbb{Q} = \mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2)$ because $\zeta_1 = 1$ and $\zeta_2 = -1 \in \mathbb{Q}$. If n is odd, then $-\zeta_n$ is a primitive $2n$-th root of unity. Thus $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ for odd n.

The primitive n-th roots of unity are roots of $X^n - 1$ but not of $X^m - 1$ for any $m \mid n$ with $m \neq n$. It follows that all the conjugates of ζ_n are primitive n-th roots, that is, of the form ζ_n^k with $\gcd(k, n) = 1$. Nontrivially, the converse holds as well.

Proposition 2.24. *Let $\zeta = \zeta_n$ be a primitive n-th root of unity. If $k \geq 1$ with $\gcd(k, n) = 1$, then ζ and ζ^k are algebraic conjugates.*

Proof. The algebraic conjugacy relation (having the same minimal polynomial) is an equivalence relation, in particular, it is transitive. Therefore it suffices to show the claim for $k = p \in \mathbb{P}$. The general case follows by successfully applied the prime case to a prime factorization of k.

The polynomial $X^n - 1$ has ζ and ζ^p as roots. Let $m_a \in \mathbb{Z}[X]$ the minimal polynomial of ζ. Then $X^n - 1 = gm_\zeta$ with a monic $g \in \mathbb{Q}[X]$. From Lemma 2.14, we get $g \in \mathbb{Z}[X]$. We have $0 = g(\zeta^p)m_\zeta(\zeta^p)$, and need to show $m_\zeta(\zeta^p) = 0$. Suppose not; then $g(\zeta^p) = 0$. Hence ζ is a root of $g(X^p)$ and therefore $g(X^p) = hm_\zeta$ with $h \in \mathbb{Q}[X]$. Again by Lemma 2.14, we have $h \in \mathbb{Z}[X]$. We reduce modulo $p\mathbb{Z}[X]$ (because of $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong \mathbb{Z}/p\mathbb{Z}[X]$, this works coefficient-wise), to find

$$\overline{g}(X^p) = \overline{g}(X)^p \in \mathbb{Z}/p\mathbb{Z}[X].$$

Therefore $\overline{m_\zeta}(X)$ divides $\overline{g}(X)^p$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Because $\mathbb{Z}/p\mathbb{Z}[X]$ is Euclidean (hence a UFD), the polynomials $\overline{g}(X)$ and $\overline{m_\zeta}(X)$ have a non-constant common factor $\overline{h} \in \mathbb{Z}/p\mathbb{Z}[X]$. From

$$X^n - \overline{1} = \overline{g}(X^p)\,\overline{m_\zeta}(X) = \overline{g}(X)^p\,\overline{m_\zeta}(X),$$

it follows that $\overline{h}^2$ divides $\overline{f} \coloneqq X^n - \overline{1}$. Therefore $\overline{f}$ and $\overline{f}'$ (the formal derivative) have a common factor $\overline{h}$. However $\overline{f}' = \overline{n}X^{n-1} \neq 0$ (because $\gcd(n, p) = 1$ it holds that $\overline{n} \neq 0$), and hence $\overline{f}$, $\overline{f}'$ are coprime, a contradiction. □

Recall that

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, \overline{a} \in \mathbb{Z}/n\mathbb{Z} : 0 \leq a \leq n-1,\ \gcd(a, n) = 1 \,\}.$$

The Euler ϕ-function $\phi\colon \mathbb{N} \to \mathbb{N}$ is defined by $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. If $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of n, with pairwise distinct prime numbers p_i, then an application of the Chinese Remainder Theorem together with an easy combinatorial argument gives the formula

$$\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1).$$

In particular, $\phi(p) = p - 1$ for all primes p, consistent with the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field.

Note that the previous proposition showed that the minimal polynomial of $\zeta \in \mu_n^*(\mathbb{C})$ is

$$\Phi_n = \prod_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} (X - \zeta^k) \in \mathbb{Z}[X].$$

These are known as the cyclotomic polynomials. For $n = p \in \mathbb{P}$ it is possible to show directly that they are irreducible.

Exercise 2.25. *Let $p \in \mathbb{P}$. Show that*

$$f = \frac{X^p - 1}{X - 1} \in \mathbb{Z}[X]$$

is irreducible. To do so, note that it suffices to show that $f(X+1)$ is irreducible, because $X \mapsto X+1$ induces a ring automorphism of $\mathbb{Z}[X]$. Then use the binomial formula to show that $f(X+1)$ is irreducible by the Eisenstein criterion.

Proposition 2.26. *Let $\zeta = \zeta_n$ be an n-th primitive root of unity. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, and*

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \quad \bar{i} \mapsto \sigma_i,$$

with $\sigma_i(\zeta) = \zeta^i$ is a group isomorphism. In particular $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$. [2]

Proof. The pairwise distinct conjugates of ζ are ζ^k with $\gcd(k, n) = 1$ and $1 \le k \le n-1$. Since there are precisely $\phi(n)$ of them by Proposition 2.24, the minimal polynomial of ζ has degree $\phi(n)$. Hence $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.

An embedding of $\mathbb{Q}(\zeta)$ into $\mathbb{C}$ is uniquely determined by the image of ζ. The possible images of ζ are precisely its conjugates, and all of these are in $\mathbb{Q}(\zeta)$. Thus the automorphisms are of the form $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\sigma_i(\zeta) = \zeta^i$ and $\gcd(i, n) = 1$. Two such automorphisms are the same if and only if $\zeta^i = \zeta^j$, that is, if and only if $\zeta^{i-j} = 1$, which in turn is equivalent to $i \equiv j \mod n$. Thus we have the claimed bijection $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. To verify that it is a group homomorphism, note

$$\sigma_i \circ \sigma_j(\zeta) = \sigma_i(\zeta^j) = \zeta^{ij} = \sigma_{ij}(\zeta),$$

and $\overline{ij} = \bar{i}\,\bar{j} \in \mathbb{Z}/n\mathbb{Z}$. □

Corollary 2.27. *Let $\zeta = \zeta_n$ be a primitive n-th root of unity ($n \ge 1$). If n is even, then the roots of unity in $\mathbb{Q}(\zeta)$ are precisely the n-th roots of unity. If n is odd, then they are the $2n$-th roots of unity.*

Proof. If n is odd then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$, so it suffices to consider the case where n is even. Suppose that there is a primitive k-th root of unity ω with $k \nmid n$. Let $d = \gcd(k, n)$. Then the multiplicative order of ω^d is $k/\gcd(k, n)$, which is coprime to n. Replacing ω by ω^d and k by $k/\gcd(k, n)$, we can therefore without loss of generality assume $\gcd(k, n) = 1$. We claim that $\omega\zeta$ is a primitive root of unity of order kn. Clearly $(\omega\zeta)^{kn} = 1$. Suppose $(\omega\zeta)^m = 1$ for some $m \in \mathbb{N}$.

[2] That is, $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}]$. Equivalently, every field homomorphism $\varphi\colon \mathbb{Q}(\zeta) \to \mathbb{C}$ is actually an automorphism of $\mathbb{Q}(\zeta)$.

Then $1 = (\omega\zeta)^{mk} = \omega^{mk}\zeta^{mk} = \zeta^{mk}$, so $n \mid mk$, and hence $n \mid m$, because $\gcd(n,k) = 1$. Similarly $1 = \omega^{mn}$, so $k \mid mn$, and hence $k \mid m$. Again by coprimality of k and n, we have $kn \mid m$. Thus the multiplicative order of $\omega\zeta$ is m. [3]

This implies that $\mathbb{Q}(\zeta_{kn}) \subseteq \mathbb{Q}(\zeta_n)$. Because degrees of field extensions are multiplicative on towers [Bre19, Theorem 7.29], we find $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_{kn})][\mathbb{Q}(\zeta_{kn}) : \mathbb{Q}]$, and hence $\phi(kn) \mid \phi(n)$. Coprimality of k and n implies $\phi(kn) = \phi(k)\phi(n)$, so this is only possible if $\phi(k) = 1$, hence $k \in \{1,2\}$. This contradicts $k \nmid n$. □

Corollary 2.28. *There is a bijection*

$$\{\, m \in \mathbb{N} : m \text{ even} \,\} \Leftrightarrow \{\, \text{Cyclotomic fields (up to isomorphism)} \,\},$$

given by $m \mapsto \mathbb{Q}(e^{2\pi i/m})$.

Proof. Every cyclotomic field can be obtained in this way, because $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m})$ for odd m. If m, n are distinct even numbers, then Corollary 2.27 shows that the two fields contain different roots of 1, and are therefore non-isomorphic. □

2.3 Trace, Norm, and Discriminant

Let $K \subseteq L$ be number fields (the most important case will be the *absolute* case $K = \mathbb{Q}$, but it is useful to also have the *relative* version where $K \neq \mathbb{Q}$). We write $\mathrm{Hom}_K(L,\mathbb{C})$ for the embeddings of L into $\mathbb{C}$ that fix K pointwise. Then

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

and every $\varphi \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ has precisely $[L : K]$ distinct extensions to embeddings $\widetilde{\varphi} \in \mathrm{Hom}_{\mathbb{Q}}(L,\mathbb{C})$ with $\widetilde{\varphi}|_K = \varphi$ [Bre19, Theorem 7.128]. The elements of $\mathrm{Hom}_K(L,\mathbb{C})$ arise as the $[L : K]$ extensions of the identity. Writing $L = K(\alpha)$, as before (for $K = \mathbb{Q}$) they are obtained by mapping α to the distinct roots of the minimal polynomial of α over K.

Example. Let $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\sqrt[3]{2})(\zeta)$ with $\zeta = e^{2\pi i/3}$. Then

$$\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) = \left\{ \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \sqrt[3]{2} \mapsto \zeta\sqrt[3]{2},\ \sqrt[3]{2} \mapsto \zeta^2\sqrt[3]{2} \right\},$$

and

$$\mathrm{Hom}_K(L,\mathbb{C}) = \left\{ \zeta \mapsto \zeta,\ \zeta \mapsto \zeta^2 \right\},$$

with each of them mapping $\sqrt[3]{2}$ to itself. On the other hand, $\mathrm{Hom}_{\mathbb{Q}}(L,\mathbb{C})$ has six elements as we also have three choices for the image of $\sqrt[3]{2}$. □

[3] The proof amounts to the following: if a, b are *commuting* elements of a group of finite order k and m, then ab has order $\mathrm{lcm}(k,m)$.

Definition 2.30. *Let $K \subseteq L$ be number fields. Let $\operatorname{Hom}_K(L,\mathbb{C}) = \{\sigma_1,\dots,\sigma_n\}$. For $\alpha \in L$, we define the (relative) trace and (relative) norm as*

$$\mathsf{T}_K^L(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \quad \textit{and} \quad \mathsf{N}_K^L(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

In case $K = \mathbb{Q}$ we just write T^L and N^L and call it the (absolute) trace and (absolute) norm. We even abbreviate to T and N if the field L is clear from the context.

The following basic properties are immediate.

Lemma 2.31. *Let α, $\beta \in L$ and $c \in K$. Let $\mathsf{T} = \mathsf{T}_K^L$ and $\mathsf{N} = \mathsf{N}_K^L$.*

(1) $\mathsf{T}(\alpha+\beta) = \mathsf{T}(\alpha) + \mathsf{T}(\beta)$, $\mathsf{T}(c\alpha) = c\,\mathsf{T}(\alpha)$, $\mathsf{T}(c) = nc$.

(2) $\mathsf{N}(\alpha\beta) = \mathsf{N}(\alpha)\,\mathsf{N}(\beta)$, $\mathsf{N}(c\alpha) = c^n\,\mathsf{N}(\alpha)$, $\mathsf{N}(c) = c^n$.

Further, $\mathsf{N}(\alpha) = 0$ if and only if $\alpha = 0$.

By relating norm and trace to coefficients of a minimal polynomial, we can see that they actually take values in the ground field.

Proposition 2.32. *Let $K \subseteq L$ be number fields with $n = [L:K]$. Let $\mathsf{T} = \mathsf{T}_K^L$ and $\mathsf{N} = \mathsf{N}_K^L$. Let $\alpha \in L$, and let*

$$f = X^d + a_{d-1}X^{d-1} + \dots + a_0 \in K[X]$$

be the minimal polynomial of α over K. Then $\mathsf{T}(\alpha) = -\frac{n}{d}a_{d-1}$ and $\mathsf{N}(\alpha) = (-1)^n a_0^{n/d}$. In particular, one has $\mathsf{T}(\alpha)$, $\mathsf{N}(\alpha) \in K$. If α is an algebraic integer and $K = \mathbb{Q}$, then even $\mathsf{T}(\alpha)$, $\mathsf{N}(\alpha) \in \mathbb{Z}$.

Proof. First consider the field $K' = K(\alpha)$, which is an intermediate field of K and L. Because $n = [L:K] = [L:K'][K':K]$ and $[K':K] = d$, we have $[L:K'] = n/d$. Factoring f in $\mathbb{C}[X]$,

$$f = \prod_{\sigma \in \operatorname{Hom}_K(K',\mathbb{C})} (X - \sigma(\alpha)),$$

and so

$$a_0 = (-1)^d \prod_{\sigma \in \operatorname{Hom}_K(K',\mathbb{C})} \sigma(\alpha) = (-1)^d\,\mathsf{N}_K^{K'}(\alpha),$$

and

$$a_{d-1} = -\sum_{\sigma \in \operatorname{Hom}_K(K',\mathbb{C})} \sigma(\alpha) = -\,\mathsf{T}_K^{K'}(\alpha).$$

If we consider T_K^L and N_K^L, it suffices to notice that each $\sigma \in \operatorname{Hom}_K(K',\mathbb{C})$ extends to precisely n/d distinct $\widetilde{\sigma} \in \operatorname{Hom}_K(L,\mathbb{C})$. Thus each factor (respectively summand) is repeated n/d times, and

$$\mathsf{N}_K^L(\alpha) = (-1)^n a_0^{n/d} \quad \text{and} \quad \mathsf{T}_K^L(\alpha) = -\frac{n}{d}a_{d-1}.$$

Now $\mathsf{T}(\alpha)$, $\mathsf{N}(\alpha) \in K$, because the coefficients of f are in K by definition. If $K = \mathbb{Q}$ and α is an algebraic integer, then $f \in \mathbb{Z}[X]$ (Lemma 2.15), and hence $\mathsf{N}(\alpha)$, $\mathsf{T}(\alpha) \in \mathbb{Z}$ □

Remark 2.33. In general (without assuming $K = \mathbb{Q}$) it still holds that $\mathsf{T}(\alpha)$, $\mathsf{N}(\alpha) \in \mathcal{O}_K$ for algebraic integers $\alpha \in \mathcal{O}_L$. However, to see this, one has to show: if $\alpha \in L$ is an algebraic integer and $f \in K[X]$ is the minimal polynomial of α over K, then $f \in \mathcal{O}_K[X]$. This is true, but the proof we used for $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$ does not carry over, as we have used that $\mathbb{Z}$ is a UFD and, in general, $\mathcal{O}_K$ is not a UFD. Instead one can use that $\mathcal{O}_K$ is integrally closed in its quotient field K. See [Neu99, § 2.1, p.5–8] for details.

Lemma 2.34. *Let $K \subseteq L \subseteq M$ be number fields. Then $\mathsf{N}_K^M = \mathsf{N}_K^L \circ \mathsf{N}_L^M$ and $\mathsf{T}_K^M = \mathsf{T}_K^L \circ \mathsf{T}_L^M$.*

Proof. Let $\alpha \in M$. On $\operatorname{Hom}_K(M, \mathbb{C})$ we define an equivalence relation by $\sigma \sim \sigma'$ if and only if $\sigma|_L = \sigma'|_L$. There are precisely $m = [L : K]$ equivalence classes. Let $\sigma_1, \dots, \sigma_m \in \operatorname{Hom}_K(M, \mathbb{C})$ be a set of representatives for these classes. Then

$$\begin{aligned}\mathsf{T}_K^M(\alpha) &= \sum_{i=1}^m \sum_{\substack{\sigma \in \operatorname{Hom}_K(M,\mathbb{C}) \\ \sigma \sim \sigma_i}} \sigma(\alpha) = \sum_{i=1}^m \sum_{\sigma \in \operatorname{Hom}_{\sigma_i(L)}(\sigma_i(M),\mathbb{C})} \sigma(\sigma_i(\alpha)) \\ &= \sum_{i=1}^m \mathsf{T}_{\sigma_i(L)}^{\sigma_i(M)}(\sigma_i(\alpha)) = \sum_{i=1}^m \sigma_i(\mathsf{T}_L^M(\alpha)) = \mathsf{T}_K^L(\mathsf{T}_L^M(\alpha)).\end{aligned}$$

The proof for the norm is the same, with sums replaced by products. □

Example. If $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ not a square, then there are two embeddings of K into $\mathbb{C}$, namely $a + b\sqrt{d} \mapsto a \pm b\sqrt{d}$. Hence

$$\mathsf{N}(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \quad \text{and} \quad \mathsf{T}(a + b\sqrt{d}) = 2a \quad (a, b \in \mathbb{Q}).$$

In the quadratic case $\alpha \in \mathcal{O}_K$ if and only if $\mathsf{N}(\alpha)$, $\mathsf{T}(\alpha) \in \mathbb{Z}$, because these are, up to sign, the only two coefficients of the minimal polynomial, except for the leading one, which is always 1.□

Lemma 2.36. *Let $\alpha \in K$ be an algebraic integer. Then $\alpha \in \mathcal{O}_K^\times$ if and only if $\mathsf{N}_{\mathbb{Q}}^K(\alpha) = \pm 1$.*

Proof. If $\alpha \in \mathcal{O}_K^\times$, then the fact that $\mathsf{N}_{\mathbb{Q}}^K : \mathcal{O}_K^\bullet \to \mathbb{Z}^\bullet$ is a homomorphism of multiplicative monoids and $\mathbb{Z}^\times = \{\pm 1\}$ show $\mathsf{N}(\alpha) = \pm 1$.

Conversely, let $m_\alpha = X^d + a_{d-1}X^{d-1} + \dots + a_0 \in \mathbb{Z}[X]$ be the minimal polynomial of α. By assumption $a_0 = \pm 1$, and

$$\pm 1 = -a_0 = \alpha(\alpha^{d-1} + \alpha^{d-2}a_{d-1} + \dots + \alpha a_2 + a_1).$$

The factor on the right side is contained in $\mathcal{O}_K$. Therefore $\alpha \in \mathcal{O}_K^\times$. □

An immediate consequence is: if $\alpha \in \mathcal{O}_K$ and $\mathsf{N}_{\mathbb{Q}}^K(\alpha) \in \mathbb{P}$, then α is irreducible in $\mathcal{O}_K$.

Remark. If $K \subseteq L$ are number fields, then $\alpha \in L$ induces a K-linear map $\varphi_\alpha: L \to L$, $x \mapsto \alpha x$. It is now not hard to see that $\mathsf{T}^L_K(\alpha) = \operatorname{tr}(\varphi_\alpha)$ and $\mathsf{N}^L_K(\alpha) = \det(\varphi_\alpha)$.

2.3.1 Discriminant

Let K be a number field of degree n with $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$.

Definition 2.37. *If $\alpha_1, \dots, \alpha_n \in K$, the* discriminant *of the tuple $(\alpha_1, \dots, \alpha_n)$ is*

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) := \det\big((\sigma_i(\alpha_j))_{1 \le i,j \le n}\big)^2 = \det\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{pmatrix}^2.$$

Because we are taking the square of the determinant, the discriminant actually does not depend on the chosen order of $\alpha_1, \dots, \alpha_n$ or $\sigma_1, \dots, \sigma_n$.

Proposition 2.38. (1) *We have* $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(\mathsf{T}^K(\alpha_i\alpha_j)_{1 \le i,j \le n})$.

(2) $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$, *and if* $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, *then* $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.

(3) *If* $(\beta_1, \dots, \beta_n)^T = A(\alpha_1, \dots, \alpha_n)^T$ *for some matrix* $A \in M_n(\mathbb{Q})$, *then*

$$\operatorname{disc}(\beta_1, \dots, \beta_n) = \det(A)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n).$$

Proof. (1) Let $C = (\sigma_i(\alpha_j))_{i,j} \in M_n(\mathbb{C})$. Then

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(C)\det(C) = \det(C^T)\det(C) = \det(C^T C).$$

But

$$(C^T C)_{i,j} = \sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i\alpha_j) = \mathsf{T}^K(\alpha_i\alpha_j),$$

and the claim follows.

(2) This follows from Proposition 2.32, because $\mathsf{T}^K(\alpha_i\alpha_j) \in \mathbb{Q}$, respectively, $\mathsf{T}^K(\alpha_i\alpha_j) \in \mathbb{Z}$ if α_i, α_j are algebraic integers.

(3) Let $A = (a_{ij})_{i,j} \in M_n(\mathbb{Q})$. Because

$$\sigma_i(\beta_j) = \sigma_i\Big(\sum_{k=1}^n a_{jk}\alpha_k\Big) = \sum_{k=1}^n a_{jk}\sigma_i(\alpha_k),$$

we get $(\sigma_i(\beta)_j)_{i,j} = (\sigma_i(\alpha_j))_{i,j} \cdot A^T$, and hence

$$\det(\sigma_i(\beta)_j)^2_{i,j} = \det(\sigma_i(\alpha_j))^2_{i,j} \det(A)^2.$$

□

When $K = \mathbb{Q}(\alpha)$, we get a nice formula for the discriminant in terms of α.

Proposition 2.39. *Let $K = \mathbb{Q}(\alpha)$ with $n = [K : \mathbb{Q}]$ and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the algebraic conjugates of α. Then*

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \, \mathsf{N}^K(f'(\alpha)).$$

(*The sign on the right is* $+$ *if* $n \equiv 0, 1 \mod 4$ *and* $-$ *if* $n \equiv 2, 3 \mod 4$.)

Proof. After a possible reindexing, we can assume $\sigma_i(\alpha) = \alpha_i$. So

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{pmatrix}^2 = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2,$$

because this is the square of a Vandermonde determinant.

For the second formula, first note $f = \prod_{i=1}^n (X - \alpha_i)$ and therefore

$$f' = \sum_{i=1}^n \prod_{\substack{j=1 \\ j \ne i}}^n (X - \alpha_j) \quad \text{and} \quad f'(\alpha_i) = \prod_{\substack{j=1 \\ j \ne i}}^n (\alpha_i - \alpha_j).$$

Now

$$\begin{aligned} \mathsf{N}^K(f'(\alpha)) &= \prod_{i=1}^n \sigma_i(f'(\alpha)) = \prod_{i=1}^n f'(\sigma_i(\alpha)) = \prod_{i=1}^n f'(\alpha_i) \\ &= \prod_{i=1}^n \prod_{\substack{j=1 \\ j \ne i}}^n (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2} \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)^2 \\ &= (-1)^{n(n-1)/2} \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}). \end{aligned}$$

For the correct sign, note that there are $n(n-1)$ factors in the product, and in the second to last step, we swap the signs of half of them. □

Theorem 2.40. *Let K be a number field, $n = [K : \mathbb{Q}]$, and let $\alpha_1, \ldots, \alpha_n \in K$. Then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \ne 0$ if and only if $(\alpha_1, \ldots, \alpha_n)$ is a $\mathbb{Q}$-basis of K.*

Proof. There exists some $\beta \in K$ such that $K = \mathbb{Q}(\beta)$, and thus $(1, \beta, \ldots, \beta^{n-1})$ is a $\mathbb{Q}$-basis of K. We can therefore write

$$(\alpha_1, \ldots, \alpha_n)^T = A(1, \beta, \ldots, \beta^{n-1}),$$

with $A \in M_n(\mathbb{Q})$. From (3) of Proposition 2.38, we get

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(A)^2 \operatorname{disc}(1, \beta, \ldots, \beta^{n-1}).$$

By Proposition 2.39, we have $\operatorname{disc}(1, \beta, \dots, \beta^{n-1}) \neq 0$.

If $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \neq 0$, then necessarily $\det(A) \neq 0$ and so $A \in \mathrm{GL}_n(\mathbb{Q})$. Thus $(\alpha_1, \dots, \alpha_n)^T = A(1, \beta, \dots, \beta^{n-1})$ is a basis. Conversely, if $(\alpha_1, \dots, \alpha_n)$ is a $\mathbb{Q}$-basis, then necessarily $A \in \mathrm{GL}_n(\mathbb{Q})$ and so $\det(A) \neq 0$. Hence $\operatorname{disc}(\alpha_1, \dots, \alpha_n) \neq 0$. □

2.4 Integral Bases

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Observe

$$K = \left\{ \frac{\alpha}{d} : d \in \mathbb{Z}^{\bullet}, \alpha \in \mathcal{O}_K \right\}.$$

Indeed, if $\beta \in K$, then β is algebraic, and hence satisfies some equation

$$a_n \beta^n + a_{n-1}\beta^{n-1} + \cdots + a_0 = 0,$$

fore some $n \geq 1$, $a_n, \dots, a_0 \in \mathbb{Z}$ (after clearing denominators) and $a_n \neq 0$. Multiplying by a_n^{n-1}, we get a monic polynomial for $a_n\beta$, and hence $a_n\beta \in \mathcal{O}_K$. Thus K is the quotient field of $\mathcal{O}_K$, and furthermore $\mathcal{O}_K$ contains a $\mathbb{Q}$-basis of K. We seek something stronger, namely a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

Recall that a $\mathbb{Z}$-module is the same thing as an abelian group. We are only concerned with finitely generated (f.g.) modules. A f.g. $\mathbb{Z}$-module M is free if $M \cong \mathbb{Z}^n$ for some $n \geq 0$. In this case, the number n is uniquely determined (if $\mathbb{Z}^n \cong \mathbb{Z}^m$, then $\mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}^m/2\mathbb{Z}^m$ and $2^n = |\mathbb{Z}^n/2\mathbb{Z}^n| = |\mathbb{Z}/2\mathbb{Z}^m| = 2^m$). We call n the rank of M. Equivalently, M is free of rank n if and only if there exists a basis of cardinality n of M, that is, elements $b_1, \dots, b_n \in M$ such that $M = \langle b_1, \dots, b_n \rangle_{\mathbb{Z}}$ and the b_i are linearly independent over $\mathbb{Z}$. Also equivalent is that $M = b_1\mathbb{Z} \oplus \cdots \oplus b_n\mathbb{Z}$ as internal direct sum.

If M has two bases $(b_1, \dots, b_n)$ and $(a_1, \dots, a_n)$, then it is easy to see that there is a matrix $A \in \mathrm{GL}_n(\mathbb{Z})$ such that $A(b_1, \dots, b_n)^T = (a_1, \dots, a_n)^T$. (Note the matrix is invertible over $\mathbb{Z}$, because there is also some $A' \in M_n(\mathbb{Z})$ with $A'(a_1, \dots, a_n)^T = (b_1, \dots, b_n)^T$, and then $AA' = A'A = I$ is the identity matrix.) In particular, this matrix has $\det(A) = \pm 1$. The following structure theorem for finitely generated abelian groups is non-trivial. We will in particular need (2), but state the full theorem for context. [4]

Theorem 2.41 (Structure Theorem for Finitely Generated Abelian Groups).

(1) *If M is a f.g. $\mathbb{Z}$-module, then $M = F \oplus T$, where F is a f.g. free $\mathbb{Z}$-module and T is finite. Here, T is the torsion submodule of M.*

(2) *Let F be a f.g. free $\mathbb{Z}$-module of rank n. If $G \subseteq F$ is a $\mathbb{Z}$-submodule, then G is f.g. free and $m \coloneqq \operatorname{rank}(G) \leq \operatorname{rank}(F)$.*

[4] The part for finite groups, (3), appears in [Bre19, Chapter 5.5].

Further, there exist a basis $(b_1, \dots, b_n)$ of F and $d_1 \mid d_2 \mid \cdots \mid d_m \in \mathbb{N}$ such that $(d_1 b_1, \dots, d_m b_m)$ is a $\mathbb{Z}$-basis of G.

(3) *Let T be a finite abelian group. Then $T \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$ with $r \geq 0$ and $1 < n_1 \mid n_2 \mid \cdots \mid n_r$. The numbers n_1, …, n_r are uniquely determined and are called the* **elementary divisors** *of T.*

From (2) we immediately see if $G \subseteq F$ are finitely generated free $\mathbb{Z}$-modules, then $F/G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^{n-m}$ is finite if and only if $\operatorname{rank}(G) = \operatorname{rank}(F)$.

Remark 2.42. The Structure Theorem holds, with minor modifications in the formulation, more generally for finitely generated modules over principal ideal domains. (One needs to replace finite abelian groups with modules of finite length, and the elementary divisors are only unique up to units.) Proofs can be found in many standard algebra textbooks, though most often in this more general setting.

Definition 2.43. *Let K be a number field. An* **integral basis** *of $\mathcal{O}_K$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$ as $\mathbb{Z}$-module. Explicitly, an integral basis is a tuple $(\alpha_1, \dots, \alpha_n)$ of algebraic integers, such that every $\beta \in \mathcal{O}_K$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of α_1, …, α_n.*

Unlike the existence of a $\mathbb{Q}$-basis for K, the existence of an integral basis of $\mathcal{O}_K$ is not immediate (at this point, we don't know whether $\mathcal{O}_K$ is a f.g. $\mathbb{Z}$-module).

Lemma 2.44. *Let $(\alpha_1, \dots, \alpha_n)$ be a $\mathbb{Q}$-basis of K that is contained in $\mathcal{O}_K$ and define $d \coloneqq \operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Then*

$$d\mathcal{O}_K \subseteq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Proof. Let $\beta \in \mathcal{O}_K$, with $\beta = \sum_{i=1}^n x_i \alpha_i$ and $x_i \in \mathbb{Q}$. Then, for $1 \leq i \leq n$,

$$\mathsf{T}(\alpha_i \beta) = \mathsf{T}\Big(\alpha_i\big(\sum_{j=1}^n x_j \alpha_j\big)\Big) = \sum_{j=1}^n \mathsf{T}(\alpha_i \alpha_j) x_j.$$

Set $\mathbf{x} = (x_1, \dots, x_n)^T$ and $C = (\mathsf{T}(\alpha_i \alpha_j))_{i,j} \in M_n(\mathbb{Z})$. Setting $\mathbf{b} = (\mathsf{T}(\alpha_1\beta), ..., \mathsf{T}(\alpha_n\beta))^T \in \mathbb{Z}^n$, we have a linear system $\mathbf{b} = C\mathbf{x}$ with $\det(C) = d$. Then

$$\mathbf{x} = C^{-1}\mathbf{x} = \frac{\operatorname{adj}(C)\mathbf{x}}{d} \in \frac{1}{d}\mathbb{Z}^n.$$

□

Theorem 2.45. *The ring of integers $\mathcal{O}_K$ of a number field K is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, that is, it has an integral basis. Furthermore, the ring $\mathcal{O}_K$ is noetherian, and every nonzero ideal $I \subseteq \mathcal{O}_K$ is free of rank n as well.*

Proof. Let $(\alpha_1, \dots, \alpha_n)$ be a $\mathbb{Q}$-basis of K that is contained in $\mathcal{O}_K$. Let $M = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$. Then $M \subseteq \mathcal{O}_K \subseteq \frac{1}{d}M$. Submodules of finitely generated free $\mathbb{Z}$-modules are finitely generated and free (Theorem 2.41). Hence $\mathcal{O}_K$ is free. Because of $n = \operatorname{rank}(M) \le \operatorname{rank}(\mathcal{O}_K) = \operatorname{rank}(\frac{1}{d}M) = n$, it follows that $\operatorname{rank}(\mathcal{O}_K) = n$. If $0 \ne I$ is an ideal and $\gamma \in I$, then $\gamma\mathcal{O}_K \subseteq I \subseteq \mathcal{O}_K$ and the same argument shows that I is free of rank n. □

Finding an integral basis is not always easy. The following theorem is sometimes useful.

Theorem 2.46. *Let K be a number field and let $I \subseteq \mathcal{O}_K$ be a finitely generated free $\mathbb{Z}$-module that contains a $\mathbb{Q}$-basis $(\alpha_1, \dots, \alpha_n)$ of K. Let $d \coloneqq |\operatorname{disc}(\alpha_1, \dots, \alpha_n)| \in \mathbb{N}$ and write $d = d_0^2 d_1$ with d_1 squarefree. For each $1 \le i \le n$, let $c_{ij} \in \mathbb{Z}$ with $j < i$ and $c_{ii} \in \mathbb{N}$ with $c_{ii} \in \mathbb{N}$ minimal such that*

$$\beta_i \coloneqq \frac{1}{d_0}\sum_{j=1}^{i} c_{ij}\alpha_j \in I,$$

Then $(\beta_1, \dots, \beta_n)$ is a $\mathbb{Z}$-basis for I.

Before we prove this theorem we make a useful observation about discriminants. Let $I \subseteq K$ be a f.g. free $\mathbb{Z}$-module that contains a $\mathbb{Q}$-basis $(\alpha_1, \dots, \alpha_n)$ of K. If $(\beta_1, \dots, \beta_n)$ is a second such basis, then there exists $A \in \mathrm{GL}_n(\mathbb{Z})$ with $(\beta_1, \dots, \beta_n) = A(\alpha_1, \dots, \alpha_n)$, and hence $\operatorname{disc}(\beta_1, \dots, \beta_n) = \det(A)^2 \operatorname{disc}(\alpha_1, \dots, \beta_n)$ and $\det(A)^2 = 1$. We can therefore define the discriminant of I as $\operatorname{disc}(I) \coloneqq \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.

Suppose now $J \subseteq I$ are two such f.g. free $\mathbb{Z}$-modules each containing a $\mathbb{Q}$-basis of K. By (2) of Theorem 2.41 we can find a basis $(\alpha_1, \dots, \alpha_n)$ of I and $d_1, \dots, d_n \in \mathbb{N}$ such that $(d_1\alpha_1, \dots, d_n\alpha_n)$ is a $\mathbb{Z}$-basis of J. Then $|I : J| = |I/J| = d_1 \cdots d_n$ (here $|I : J|$ denotes the index of the abelian group J in I). Letting D be the diagonal matrix with entries $d_1, \dots, d_n$ and applying (3) of Proposition 2.38 we get

$$\operatorname{disc}(J) = |I : J|^2 \operatorname{disc}(I).$$

Proof (of Theorem 2.46). Let $J \coloneqq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. Then $J \subseteq I \subseteq \mathcal{O}_K$. Therefore $\operatorname{disc}(I)$, $\operatorname{disc}(J) \in \mathbb{Z}$. Then $d_0^2 d_1 = \operatorname{disc}(J) = |I : J|^2 \operatorname{disc}(I)$. Because d_1 is squarefree, the index $|I : J|$ divides d_0. Hence $d_0 I \subseteq J$.

Note

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \frac{1}{d_0} \begin{pmatrix} c_{1,1} & 0 & 0 & \dots & 0 \\ c_{2,1} & c_{2,2} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & c_{n,2} & 0 & \dots & c_{n,n} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

The matrix has entries in $\mathbb{Z}$ and is, because of $c_{ii} \ne 0$, invertible over $\mathbb{Q}$. Hence $(\beta_1, \dots, \beta_n)$ is a $\mathbb{Q}$-basis of K. By construction, we have $\beta_i \in I$ for $1 \le i \le n$. It only remains to show $I \subseteq \langle \beta_1, \dots, \beta_n \rangle_{\mathbb{Z}}$.

Suppose this is not the case. Noting $I \subseteq \frac{1}{d_0}J$, then there exists some minimal s such that there exist $x_1, \dots, x_s \in \mathbb{Z}$ with $x_s \ne 0$ and

$$\gamma \coloneqq \frac{1}{d_0}(x_1\alpha_1 + \cdots + x_s\alpha_s) \in I \smallsetminus \langle \beta_1, \dots, \beta_n \rangle_{\mathbb{Z}}.$$

We can also assume that among all such elements, γ is chosen with $|x_s|$ minimal. Replacing γ by $-\gamma$ if necessary, we can assume $x_s > 0$. By choice of c_{ss} we must have $x_s \geq c_{ss}$. But then $\gamma - \beta_s \in \langle \beta_1, \dots, \beta_n \rangle$ by minimality, and hence the same is true for γ, a contradiction. □

Corollary 2.47. *$\mathcal{O}_K$ has an integral basis of the form $(1, \beta_2, \dots, \beta_n)$.*

Proof. Apply the previous theorem with a $\mathbb{Q}$-basis of K contained in $\mathcal{O}_K$ for which $\alpha_1 = 1$. Then $c_{1,1} = d_0$ and hence $\beta_1 = 1$. □

Another corollary to Theorem 2.46 that is sometimes useful is the following: if $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ are such that $\mathrm{disc}(\alpha_1, \dots, \alpha_n)$ is square-free, then $(\alpha_1, \dots, \alpha_n)$ is already an integral basis of $\mathcal{O}_K$.

Because any two integral bases have the same discriminant, it makes sense to speak of the discriminant of a number field. The discriminant of a number field is an important invariant.

Definition 2.48. *Let K be a number field and $(\alpha_1, \dots, \alpha_n)$ an integral basis. The* discriminant *of K is*

$$\mathrm{disc}(K) \coloneqq \mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^\bullet.$$

For quadratic fields, we have already determined integral bases in Proposition 2.22.

Example. Let K be a quadratic field with $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ a squarefree integer. Then

$$\mathrm{disc}(K) = \begin{cases} \mathrm{disc}(\mathbb{Z}[\sqrt{d}]) = 4d & \text{if } d \equiv 2, 3 \mod 4, \\ \mathrm{disc}(\mathbb{Z}[\frac{1+\sqrt{d}}{2}]) = d & \text{if } d \equiv 1 \mod 4. \end{cases}$$

□

Remark 2.50 (Warning). Let K be a number field of degree n. By the primitive element, there always exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Then K has a $\mathbb{Q}$-basis $(1, \alpha, \dots, \alpha^{n-1})$. However, in general, we cannot obtain $\mathcal{O}_K$ from $\mathbb{Z}$ by adjoining a single element. There exist number fields K where $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_K$ for all $\alpha \in \mathcal{O}_K$.

Determining integral bases for cyclotomic fields is considerably more work than for quadratic fields.

2.4.1 Integral Bases of Cyclotomic Fields

Let $K = \mathbb{Q}(\zeta)$ with ζ an n-th primitive root of unity. We will eventually show $\mathcal{O}_K = \mathbb{Z}[\zeta]$, but although this looks natural, it is quite non-trivial to prove. We will first deal with the case where $n = p^e$ is a prime power, and then extend this to the composite case. As a first step, we need to know something about $\mathrm{disc}(\mathbb{Z}[\zeta])$.

Lemma 2.51. *Let $n = p^e$ with $p \in \mathbb{P}$ and $e \geq 1$ and consider $K = \mathbb{Q}(\zeta)$ with $\zeta \in \mu_n^*(\mathbb{C})$.*

(1) *We have*

$$\mathsf{N}^K(1-\zeta) = \prod_{\substack{j=1\\ p\nmid j}}^{n}(1-\zeta^j) = p.$$

Unless $n = 2$, *also* $\mathsf{N}^K(\zeta - 1) = p$.

(2) $(1-\zeta)^{\phi(n)}$ *divides* p *in* $\mathbb{Z}[\zeta]$.

Proof. (1) The formula $\mathsf{N}^K(1-\zeta) = \prod_{\substack{j=1\\ p\nmid j}}^{n}(1-\zeta^j)$ holds because the embeddings of $\mathbb{Q}(\zeta)$ into $\mathbb{C}$ are precisely the homomorphisms defined by $\zeta \mapsto \zeta^j$ with $1 \le j \le n$ and $p \nmid j$ by Proposition 2.26. We have (geometric sum)

$$\Phi_{p^e} := \frac{X^{p^e}-1}{X^{p^{e-1}}-1} = \sum_{j=0}^{p-1} X^{jp^{e-1}} \in \mathbb{Q}[X].$$

On the other hand, the roots of Φ_{p^e} are precisely the p^e-th primitive roots of unity, so

$$\Phi_{p^e} = \prod_{\substack{j=1\\ p\nmid j}}^{n}(X-\zeta^j).$$

Substituting $X = 1$ yields

$$\prod_{\substack{j=1\\ p\nmid j}}^{n}(1-\zeta^j) = p.$$

The number of factors in the product is $\phi(n) = p^{e-1}(p-1)$. Since this number is even unless $p = 2$ and $e = 1$, also $\mathsf{N}^K(1-\zeta) = \mathsf{N}^K(\zeta-1)$.

(2) Note that $1-\zeta^j = (1-\zeta)\sum_{k=0}^{j-1}\zeta^k$, so $1-\zeta$ divides $1-\zeta^j$ in $\mathbb{Z}[\zeta]$. Since the product in (2) has $\phi(n)$ factors, this shows that $(1-\zeta)^{\phi(n)}$ divides p. □

Lemma 2.52. *If* $p \in \mathbb{P}$ *and* $\zeta = \zeta_p$ *is a primitive* p*-th root of unity, then*

$$\operatorname{disc}(1,\zeta,\ldots,\zeta^{p-2}) = \pm p^{p-2}.$$

The sign is

$$\begin{cases} + & \text{if } p \equiv 1,2 \mod 4,\\ - & \text{if } p \equiv 3 \mod 4.\end{cases}$$

Proof. The minimal polynomial of ζ is $\Phi_p = (X^p-1)/(X-1) = \sum_{j=0}^{p-1} X^j \in \mathbb{Z}[X]$. To differentiate it, it is best to write $(X^p-1) = (X-1)\Phi_p(X)$, to get

$$pX^{p-1} = \Phi_p(X) + (X-1)\Phi_p'(X) \quad \text{so} \quad p\zeta^{p-1} = (\zeta-1)\Phi_p'(\zeta). \tag{2.4}$$

Note that $\mathsf{N}(\zeta^{p-1}) = (-1)^{p-1}$ by Proposition 2.32, because ζ^{p-1} is also a p-th primitive root of unity, and hence also has minimal polynomial Φ_p. By Lemma 2.51 also $\mathsf{N}(\zeta-1) = (-1)^{p-1}\mathsf{N}(1-\zeta)$. Thus (2.4) gives

$$\mathsf{N}(\Phi'_p(\zeta)) = \frac{\mathsf{N}(p)\,\mathsf{N}(\zeta^{p-1})}{\mathsf{N}(\zeta-1)} = \frac{p^{p-1}}{\mathsf{N}(1-\zeta)}.$$

We have $\mathsf{N}(1-\zeta) = p$ by Lemma 2.51. So

$$\mathsf{N}(\Phi'_p(\zeta)) = p^{p-2} \quad \text{and (by Proposition 2.39)} \quad \operatorname{disc}(1,\zeta,\dots,\zeta^{p-2}) = (-1)^{(p-1)(p-2)/2}p^{p-2}.$$

If $p \neq 2$, then $p-2$ is odd and we get $(-1)^{(p-1)(p-2)/2} = (-1)^{(p-1)/2}$. From this, the statement about the sign follows. □

We could also just restrict to odd primes p in the proof (simplifying some sign considerations), by noting that $p = 2$ gives $K = \mathbb{Q}$, and $\operatorname{disc}(1) = 1$ in $\mathbb{Q}$.

For later use, we need some information in the case of composite n as well.

Lemma 2.53. *If $n \in \mathbb{N}$ and $\zeta \in \mu_n^*(\mathbb{C})$, then*

$$\operatorname{disc}(1,\zeta,\zeta^2,\dots,\zeta^{\phi(n)-1}) \mid n^{\phi(n)}.$$

Proof. We have

$$X^n - 1 = \Phi_n(X)g(X)$$

for some $g \in \mathbb{Z}[X]$. Thus

$$nX^{n-1} = \Phi'_n(X)g(X) + \Phi_n(X)g(X) \quad \text{and} \quad n\zeta^{n-1} = \Phi'_n(\zeta)g(\zeta).$$

Now $\zeta \in \mathbb{Z}[\zeta]^\times \subseteq \mathcal{O}_K^\times$ and $g(\zeta) \in \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$. Taking norms and keeping in mind $[\mathbb{Q}(\zeta):\mathbb{Q}] = \phi(n)$,

$$\pm n^{\phi(n)} = \mathsf{N}(\Phi'_n(\zeta))\underbrace{\mathsf{N}(g(\zeta))}_{\in\mathbb{Z}},$$

so $\operatorname{disc}(1,\zeta,\zeta^2,\dots,\zeta^{\phi(n)-1}) = \pm\mathsf{N}(\Phi'_n(\zeta)) \mid n^{\phi(n)}$ □

Theorem 2.54. *Let $K = \mathbb{Q}(\zeta)$ with $\zeta \in \mu_n^*(\mathbb{C})$ where $n = p^e$, $p \in \mathbb{P}$, and $e \geq 1$. Then*

$$\mathcal{O}_K = \mathbb{Z}[\zeta] = \mathbb{Z} \oplus \zeta\mathbb{Z} \oplus \zeta^2\mathbb{Z} \oplus \cdots \oplus \zeta^{\phi(n)-1}\mathbb{Z}.$$

Proof. Let $m = [K:\mathbb{Q}]$. We already know $m = \phi(p^e) = p^{e-1}(p-1)$. From Lemma 2.53, we know $\operatorname{disc}(1,\zeta,\dots,\zeta^{m-1}) = p^t$ for some $t \geq 0$. Clearly $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$, and by Lemma 2.44, we get

$$\mathcal{O}_K \subseteq \left\langle \frac{1}{p^t}, \frac{1-\zeta}{p^t}, \frac{(1-\zeta)^2}{p^t}, \dots, \frac{(1-\zeta)^{m-1}}{p^t} \right\rangle_{\mathbb{Z}}.$$

Suppose $\mathbb{Z}[1-\zeta] \subsetneq \mathcal{O}_K$. Then there exists

$$\alpha = \frac{a_i(1-\zeta)^i + a_{i+1}(1-\zeta)^{i+1} + \cdots + a_{m-1}(1-\zeta)^{m-1}}{p} \in \mathcal{O}_K$$

with $0 \le i \le m-1$, a_i, …, $a_{m-1} \in \mathbb{Z}$ and $p \nmid a_i$. In $\mathbb{Z}[1-\zeta]$, the element $(1-\zeta)^{i+1}$ divides p by Lemma 2.51, and we get

$$\underbrace{\frac{p\alpha}{(1-\zeta^{i+1})}}_{\in\mathbb{Z}[1-\zeta]} = \frac{a_i}{1-\zeta} + \underbrace{\sum_{j=i+1}^{m-1} a_j(1-\zeta)^{j-i-1}}_{\in\mathbb{Z}[1-\zeta]}.$$

Thus $a_i/(1-\zeta) \in \mathbb{Z}[\zeta]$. Then $\mathsf{N}(1-\zeta) \mid \mathsf{N}(a_i) \in \mathbb{Z}$. But $\mathsf{N}(1-\zeta) = \pm p$, while $\mathsf{N}(a_i) = a_i^m$ is not divisible by p, a contradiction. □

To deal with the case of composite n, we will represent $\mathbb{Q}(\zeta_n)$ as a compositum of fields according to the factorization of n into prime powers.

Let K and L be two number fields. The composite of K and L, denoted by KL, is the smallest subfield of $\mathbb{C}$ that contains both K and L. Thus it is the smallest subfield of $\mathbb{C}$ containing all products $\alpha\beta$ with $\alpha \in K$, $\beta \in L$. Suppose $(\alpha_1, \dots, \alpha_m)$ and $(\beta_1, \dots, \beta_n)$ are $\mathbb{Q}$-bases of K and L respectively. Then it is easy to see that, as a $\mathbb{Q}$-vector space, the field KL is spanned by $\alpha_i\beta_j$ with $1 \le i \le m$ and $1 \le j \le n$. [5] In particular, $[KL : \mathbb{Q}] \le [K : \mathbb{Q}][L : \mathbb{Q}]$ and KL is a number field. If $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$, then the pairwise products $\alpha_i\beta_j$ even form a $\mathbb{Q}$-basis of KL.

As far as the rings of integers are concerned, we obtain $\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_{KL}$. However, as the following example shows, this inclusion can be proper.

Example. Let $K = \mathbb{Q}(\sqrt{3})$ and $L = \mathbb{Q}(\sqrt{7})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ and $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$ (Proposition 2.22). Now

$$\mathcal{O}_K\,\mathcal{O}_L = \langle 1, \sqrt{3}, \sqrt{7}, \sqrt{3}\sqrt{7}\rangle \subseteq \mathcal{O}_{KL}.$$

However $\alpha \coloneqq (\sqrt{3}+\sqrt{7})/2$ has minimal polynomial $X^4 - 5X^2 + 1$, and so $\alpha \in \mathcal{O}_{KL} \setminus \mathcal{O}_K\,\mathcal{O}_L$. □

In general, we can therefore not expect to obtain an integral basis for $\mathcal{O}_{KL}$ from pairwise products of integral bases for $\mathcal{O}_K$ and $\mathcal{O}_L$. However, under the following conditions, this is possible.

Theorem 2.56. *Let K and L be number fields with $m = [K : \mathbb{Q}]$ and $n = [L : \mathbb{Q}]$. Suppose that $[KL : \mathbb{Q}] = mn$ and that $\gcd(\operatorname{disc}(K), \operatorname{disc}(L)) = 1$. If $(\alpha_1, \dots, \alpha_m)$ and $(\beta_1, \dots, \beta_n)$ are integral bases of $\mathcal{O}_K$, respectively, of $\mathcal{O}_L$, then*

$$(\alpha_i\beta_j : 1 \le i \le m, 1 \le j \le n)$$

[5] The subring $R = K[\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_m]$ of $\mathbb{C}$ is spanned by these elements and contains KL. Because R is a finite-dimensional integral domain, it is a field, and hence $R = KL$.

is an integral basis of $\mathcal{O}_{KL}$*. Furthermore* $\operatorname{disc}(KL) = \operatorname{disc}(K)^{[L:\mathbb{Q}]}\operatorname{disc}(L)^{[K:\mathbb{Q}]}$.

Before we prove the theorem, we note the following.

Lemma 2.57. *Let* K*,* L *be number fields with* $m = [K : \mathbb{Q}]$ *and* $n = [L : \mathbb{Q}]$*. If* $[KL : \mathbb{Q}] = mn$*, then for every* $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ *and every* $\varphi \in \operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ *there exists a unique* $\psi \in \operatorname{Hom}_{\mathbb{Q}}(KL, \mathbb{C})$ *with* $\psi|_K = \sigma$ *and* $\psi|_L = \varphi$*.*

Proof. We know $|\operatorname{Hom}_{\mathbb{Q}}(KL, \mathbb{C})| = mn$, $|\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})| = m$, and $|\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})| = n$. Every $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ can be extended to a $\psi \in \operatorname{Hom}_{\mathbb{Q}}(KL, \mathbb{C})$ in $n = [KL : K]$ distinct ways. Then $\psi|_L \in \operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$. Because the latter set has cardinality n and ψ is completely determined by its image on K and on L, the claim follows. □

Proof (of Theorem 2.56). The mn products $\alpha_i\beta_j$ span KL as a $\mathbb{Q}$-vector space, and because $[KL : \mathbb{Q}] = mn$ they even form a basis. Let $\gamma \in \mathcal{O}_{KL}$, and let

$$\gamma = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}\alpha_i\beta_j \quad \text{with } c_{ij} \in \mathbb{Q}.$$

We have to show $c_{ij} \in \mathbb{Z}$ for all i, j. Define $\xi_j \coloneqq \sum_{i=1}^{m} c_{ij}\alpha_i \in K$ for $1 \le j \le n$, so that $\gamma = \sum_{j=1}^{n} \xi_j\beta_j$.

Now let $\operatorname{Hom}_K(KL, \mathbb{C}) = \{\varphi_1, \dots, \varphi_n\}$. These are precisely the extensions of the homomorphisms of $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$, to L that fix K elementwise (by Lemma 2.57). Then

$$\underbrace{\begin{pmatrix} \varphi_1(\gamma) \\ \vdots \\ \varphi_n(\gamma) \end{pmatrix}}_{=:\mathbf{b}} = \underbrace{\begin{pmatrix} \varphi_1(\beta_1) & \dots & \varphi_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \varphi_n(\beta_1) & \dots & \varphi_n(\beta_n) \end{pmatrix}}_{=:C} \underbrace{\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}}_{=:\mathbf{x}}.$$

By definition of the discriminant, $\det(C)^2 = \operatorname{disc}(L) =: d$. We have

$$d\mathbf{x} = dC^{-1}\mathbf{b} = d\frac{\operatorname{adj}(C)}{\det(C)}\mathbf{b} = \det(C)\operatorname{adj}(C)\mathbf{b}.$$

Now all entries of $\det(C)\operatorname{adj}(C)$ and $\mathbf{b}$ are algebraic integers (though they may not be contained in KL). It follows that all $d\xi_j$ are algebraic integers. Since also $d\xi_j \in K$, we get $d\xi_j \in \mathcal{O}_K$. However,

$$d\xi_j = \sum_{i=1}^{m}(dc_{ij})\alpha_i \qquad \text{with } dc_{ij} \in \mathbb{Q},$$

and $(\alpha_1, \dots, \alpha_n)$ is an integral basis of $\mathcal{O}_K$. Thus $dc_{ij} \in \mathbb{Z}$ for all i, j. By symmetry (swap the roles of K and L), for $d' \coloneqq \operatorname{disc}(K)$, we also get $d'c_{ij} \in \mathbb{Z}$ for all i, j. By assumption $\gcd(d, d') = 1$, so there exist x, $y \in \mathbb{Z}$ such that $dx + d'y = 1$. Hence $c_{ij} = xdc_{ij} + yd'c_{ij} \in \mathbb{Z}$. This shows $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.

We still have to show the statement about the discriminant. Let $\mathrm{Hom}_L(KL, \mathbb{C}) = \{\sigma_1, \dots, \sigma_m\}$, and let $\psi_{ij} \in \mathrm{Hom}_{\mathbb{Q}}(KL, \mathbb{C})$ denote the homomorphism with $\psi_{ij}|_K = \sigma_i$ and $\psi_{ij}|_L = \varphi_j$ (Lemma 2.57, $1 \le i \le m$, $1 \le j \le n$).

Let $A \coloneqq (\psi_{ij}(\alpha_s \beta_t))_{1 \le i,s \le m, 1 \le j,t \le n}$. We can think of this as an $mn \times mn$-matrix, and $\mathrm{disc}(KL) = \det(A)^2$. Observe $\psi_{ij}(\alpha_s\beta_t) = \psi_{ij}(\alpha_s)\psi_{ij}(\beta_t) = \sigma_i(\alpha_s)\psi_j(\beta_t)$. After a suitable reindexing, the matrix A can be seen as an $m \times m$ block matrix with blocks of size $n \times n$, as follows

$$A = \begin{pmatrix} \sigma_1(\alpha_1)B & \dots & \sigma_1(\alpha_m)B \\ \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1)B & \dots & \sigma_m(\alpha_m)B \end{pmatrix} \quad \text{with} \quad B = \begin{pmatrix} \varphi_1(\beta_1) & \dots & \varphi_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \varphi_n(\beta_1) & \dots & \varphi_n(\beta_n). \end{pmatrix}$$

With I the $n \times n$ identity matrix,

$$A = \begin{pmatrix} B & 0 & \dots & 0 \\ 0 & B & \vdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1)I & \dots & \sigma_1(\alpha_m)I \\ \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1)I & \dots & \sigma_m(\alpha_m)I \end{pmatrix}.$$

The first factor has determinant $\det(B)^m$. The second factor has determinant $\det(\sigma_i(\alpha_s))_{i,s}^n$ (an easy way to see it is to reindex from a $m \times m$ block matrix containing blocks of size $n \times n$, to an $n \times n$ matrix containing blocks of size $m \times m$; then the matrix of constant blocks becomes a block-diagonal matrix like the first one). Thus $\mathrm{disc}(KL) = \det(B)^{2m} \det(\sigma_i(\alpha_s))_{i,s}^{2n} = \mathrm{disc}(K)\,\mathrm{disc}(L)$.□

Theorem 2.58. *Let $n \ge 1$ and let $\zeta \in \mu_n^*(\mathbb{C})$. An integral basis of the n-th cyclotomic field $K \coloneqq \mathbb{Q}(\zeta)$ is given by $(1, \zeta, \zeta^2, \dots, \zeta^{\phi(n)-1})$. In particular, $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Proof. Let $\zeta_n \coloneqq \zeta$. This is now an easy inductive argument using Theorem 2.56 and our already acquired knowledge of cyclotomic fields.

The claim holds trivially for $n = 1$, as then $K = \mathbb{Q}$. Assume $n > 1$ and that the claim holds for all $m < n$. If n is a prime power, the claim holds by Theorem 2.54. Thus we may assume n is not a prime power, and then $n = st$ with $\gcd(s,t) = 1$ and s, $t < 1$. If $\zeta_s \in \mu_s^*(\mathbb{C})$ and $\zeta_t \in \mu_t^*(\mathbb{C})$, it is easy to see that $\zeta_s\zeta_t \in \mu_n^*(\mathbb{C})$ (see the proof of Corollary 2.27). Hence $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_s)\mathbb{Q}(\zeta_t)$. Note that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = \phi(s)\phi(t) = [\mathbb{Q}(\zeta_s) : \mathbb{Q}][\mathbb{Q}(\zeta_t) : \mathbb{Q}]$ (using Proposition 2.26). By the induction hypothesis, the claims hold for $\mathbb{Q}(\zeta_s)$ and $\mathbb{Q}(\zeta_t)$. In particular, their rings of integers are $\mathbb{Z}[\zeta_s]$, respectively, $\mathbb{Z}[\zeta_t]$. Thus Lemma 2.52 implies that $\mathrm{disc}(\mathbb{Q}(\zeta_s))$ and $\mathrm{disc}(\mathbb{Q}(\zeta_t))$ are coprime. Now we are in a position to apply Theorem 2.56 to get $\mathcal{O}_K = \mathbb{Z}[\zeta_s, \zeta_t] \subseteq \mathbb{Z}[\zeta]$. □

Remark 2.59. Let $K = \mathbb{Q}(\zeta)$ with $\zeta \in \mu_n^*(\mathbb{C})$ and $n > 2$. Unless $n \in \mathbb{P}$, we have not determined an exact formula for $\mathrm{disc}(K)$ (and we will not need it). With a little bit more work, one can show

$$\mathrm{disc}(K) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{\substack{p \in \mathbb{P} \\ p \mid n}} p^{\phi(n)/(p-1)}}.$$

One possibility is to introduce a relative notion of the discriminant, and then show a suitable formula for relative extensions of number fields (cf. [Mar18, Chapter 2, Exercise 23(b)]). Combined with the formula from Theorem 2.56 this allows one to deduce the formula. Alternatively, one can compute the values for n a prime power directly [Was97, Proposition 2.1], and then use Theorem 2.56.

We make one final observation about the discriminant that is sometimes useful. Recall that for a quadratic field, if $d \in \mathbb{Z}$ is square-free, the discriminant is $4d$ if $d \equiv 2, 3 \mod$ and it is d if $d \equiv 1 \mod 4$. In particular, the discriminant is 0 or $1 \mod 4$. In fact, this holds for arbitrary discriminants of number fields.

Theorem 2.60 (Stickelberger's Discriminant Theorem). *Let K be a number field and $d \coloneqq \operatorname{disc}(K)$ its discriminant. Then $d \equiv 0, 1 \mod 4$.*

Proof. Let $L \supseteq K$ be the Galois closure of K, i.e., the smallest number field L containing K which has the property that every $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ has $\sigma(L) \subseteq L$, and is therefore an automorphism of L. Hence $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C}) = \operatorname{Gal}(L/\mathbb{Q})$. [6] We will use the following fact from Galois theory: if $\alpha \in L$, then $\alpha \in \mathbb{Q}$ if and only if $\sigma(\alpha) = \alpha$ for all $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(L, L)$ [Bre19, Theorem 7.145].

Let $n = [K : \mathbb{Q}]$ and let $\sigma_1, \ldots, \sigma_n \in \operatorname{Gal}(L/\mathbb{Q})$ be arbitrary extensions of the elements of $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Let $(\alpha_1, \ldots, \alpha_n)$ be an integral basis of $\mathcal{O}_K$. Let $C \coloneqq (\sigma_i(\alpha_j))_{i,j} \in M_n(L)$, so that $\operatorname{disc}(K) = \det(C)^2$. By the Leibniz formula,

$$\det(C) = \sum_{\substack{\pi \in \mathfrak{S}_n \\ \operatorname{sgn}(\pi) = 1}} \sigma_{\pi(1)}(\alpha_1) \cdots \sigma_{\pi(n)}(\alpha_n) - \sum_{\substack{\pi \in \mathfrak{S}_n \\ \operatorname{sgn}(\pi) = -1}} \sigma_{\pi(1)}(\alpha_1) \cdots \sigma_{\pi(n)}(\alpha_n).$$

Write P for the first sum and N for the second sum. Then

$$\operatorname{disc}(K) = (P - N)^2 = (P + N)^2 - 4PN.$$

From the definition of P and N, it is clear that $P + N$, $PN \in \mathcal{O}_L$. If we are able to show that $P + N$, $PN \in \mathbb{Q}$, then $P + N$, $PN \in \mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$. Then, because squares are $\equiv 0, 1 \mod 4$, we will get $\operatorname{disc}(K) \equiv 0, 1 \mod 4$.

To show $P + N$, $PN \in \mathbb{Q}$, it suffices to show $\varphi(P + N) = P + N$ and $\varphi(PN) = PN$ for all $\varphi \in \operatorname{Gal}(L/\mathbb{Q})$. First note that $\varphi \circ \sigma_i|_K \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. Thus, there exists a permutation $\tau \in \mathfrak{S}_n$ such that $\varphi \circ \sigma_i|_K = \sigma_{\tau(i)}|_K$. Because of $\operatorname{sgn}(\tau \circ \pi) = \operatorname{sgn}(\tau)\operatorname{sgn}(\pi)$, we get

$$\varphi(P) = \sum_{\substack{\pi \in \mathfrak{S}_n \\ \operatorname{sgn}(\pi) = 1}} \sigma_{\tau \circ \pi(1)}(\alpha_1) \cdots \sigma_{\tau \circ \pi(n)}(\alpha_n) = \sum_{\substack{\pi \in \mathfrak{S}_n \\ \operatorname{sgn}(\pi) = \operatorname{sgn}(\tau)}} \sigma_{\pi(1)}(\alpha_1) \cdots \sigma_{\pi(n)}(\alpha_n).$$

so either $\varphi(P) = P$ (if τ is even) or $\varphi(P) = N$ (if τ is odd). Analogously $\varphi(N) = N$ if τ is even, and $\varphi(N) = P$ if τ is odd. In either case, $\varphi(P + N) = P + N$ and $\varphi(PN) = PN$. □

[6] Such a field always exists by results from field theory. Indeed, it is the composite $L = \prod_{\varphi \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \varphi(K)$.

Chapter 3

Dedekind Domains

If K is a number field, then every element $\alpha \in \mathcal{O}_K^\bullet$ factors as a product of *irreducible elements.* This is an easy consequence of the fact that $|\mathsf{N}^K(\alpha)| \in \mathbb{N}$ and that $|\mathsf{N}^K(\alpha)| = 1$ implies $\alpha \in \mathcal{O}_K^\times$.

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $\mathcal{O}_K^\times = \{\pm 1\}$ because $\mathsf{N}(a + b\sqrt{-5}) = a^2 + 5b^2 = 1$ has only $(a, b) = (\pm 1, 0)$ as solution. In $\mathcal{O}_K$, we can write

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}), \tag{3.1}$$

with the factors being pairwise non-associated. To see that these factors are irreducible, note $\mathsf{N}(2) = 4$, $\mathsf{N}(3) = 9$ and $\mathsf{N}(1 + \sqrt{-5}) = 6$. Any proper non-unit divisor would have norm 2 or 3, but $a^2 + 5b^2 \notin \{2, 3\}$ for all a, $b \in \mathbb{Z}$. Thus $\mathcal{O}_K$ is *not* a UFD.

Now consider the ideals

$$\mathfrak{p} = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5}), \qquad \mathfrak{q}_1 = (3, 1 + \sqrt{-5}), \qquad \mathfrak{q}_2 = (3, 1 - \sqrt{-5}) \qquad \text{of } \mathcal{O}_K.$$

Then $\mathfrak{p}^2 = (4, 2 + 2\sqrt{-5}, 6) = (2)$, which implies $(2) \subseteq \mathfrak{p} \subseteq \mathcal{O}_K$. Noting $(2) \subsetneq \mathfrak{p}$, we must also have $\mathfrak{p} \subsetneq \mathcal{O}_K$ (otherwise $\mathfrak{p}^2 = \mathfrak{p}$, but we just saw this is not the case). Hence $(2) \subsetneq \mathfrak{p} \subsetneq \mathcal{O}_K$. Because $|\mathcal{O}_K/(2))| = 4$, and $\mathcal{O}_K/\mathfrak{p}$ is a proper, nonzero quotient group of $\mathcal{O}_K/(2)$, this implies $|\mathcal{O}_K/\mathfrak{p}| = 2$. But then $\mathcal{O}_K/\mathfrak{p}$ is a field, and so $\mathfrak{p}$ is a maximal ideal (in particular, a prime ideal). In a similar manner, one shows $|\mathcal{O}_K/\mathfrak{q}_i| = 3$ for $i \in \{1, 2\}$, and so the $\mathfrak{q}_i$ are maximal as well.

Observing $\mathfrak{q}_1\mathfrak{q}_2 = (3)$, $\mathfrak{p}\mathfrak{q}_1 = (1 + \sqrt{-5})$, and $\mathfrak{p}\mathfrak{q}_2 = (1 - \sqrt{-5})$, we get

$$\begin{aligned} (6) = (2) \cdot (3) &= \mathfrak{p}^2(\mathfrak{q}_1\mathfrak{q}_2) \\ = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) &= (\mathfrak{p}\mathfrak{q}_1)(\mathfrak{p}\mathfrak{q}_2). \end{aligned}$$

So we recover unique factorization by factoring principal ideals into prime *ideals.* In this chapter, we will see that this is not a coincidence.

We need an additional algebraic notion, that of integral elements. Let D be a domain. Then D has a quotient field K that is unique up to unique isomorphism. We may represent elements of K in the form $\frac{a}{b}$ with $a \in D$ and $b \in D^\bullet$. If K is a number field and $D = \mathcal{O}_K$, then the quotient field of $\mathcal{O}_K$ is just K, as we already saw.

Definition 3.1. *Let $D \subseteq D'$ be domains. Let K be the quotient field of D.*

(1) *$\alpha \in D'$ is integral over D if there exists a monic polynomial $f \in D[X]$ such that $f(\alpha) = 0$.*

(2) *D is integrally closed if*

$$D = \{\, \alpha \in K : \alpha \text{ is integral over } D \,\}.$$

So, an algebraic number $\alpha \in K$ is an algebraic integer if and only if it is integral over $\mathbb{Z}$, and $\mathbb{Z}$ is integrally closed (in its quotient field $\mathbb{Q}$). We will see in a bit that analogously also $\mathcal{O}_K$ is integrally closed in K.

We also recall some basic notions from undergraduate algebra. Let R be a ring.

- R is noetherian if the following equivalent conditions hold:
  (a) Every ideal of R is finitely generated.
  (b) If $I_1 \subseteq I_2 \subseteq \cdots I_n \subseteq \cdots$ is an ascending chain of ideals, then there exists some $m \geq 1$ such that $I_n = I_m$ for all $n \geq m$.
  (c) Every nonempty set of ideals of R contains a maximal element.
- An ideal M of R is a maximal ideal if it is maximal among all proper ideals ($M \subsetneq R$). Equivalently, the factor ring R/M is a field.
- A proper ideal I of R is a prime ideal if, whenever a, $b \in R$ are such that $ab \in P$, then $a \in P$ or $b \in P$. Equivalently, the factor ring R/P is a domain.
- Every proper ideal of R is contained in a maximal ideal (using Zorn's Lemma).
- Maximal ideals are prime ideals (because fields are domains), but the converse is not true. For instance, (x,y) in $\mathbb{Q}[x,y]$ is maximal because $\mathbb{Q}[x,y]/(x,y) \cong \mathbb{Q}$, however (x) is prime but not maximal, because $\mathbb{Q}[x,y]/(x) \cong \mathbb{Q}[y]$.

We start with an observation about factors of rings of algebraic integers.

Lemma 3.2. *Let K be a number field. Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal.*

(1) *We have $|\mathcal{O}_K/\mathfrak{a}| < \infty$.*

(2) *If $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some $p \in \mathbb{P}$. The ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field extension of $\mathbb{Z}/p\mathbb{Z}$. In particular, $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p.*

Proof. (1) Let $0 \neq \alpha \in \mathfrak{a}$. Then there exist $a_0, \ldots, a_{m-1} \in \mathbb{Z}$ with $\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0$, and $a_0 \neq 0$. Rearranging terms to isolate a_0, we see $a_0 \in \mathfrak{a} \cap \mathbb{Z}^\bullet$. Then $a_0\mathcal{O}_K \subseteq \mathfrak{a} = \mathfrak{a}\mathcal{O}_K$. Hence $\mathcal{O}_K/\mathfrak{a}$ is a quotient of $\mathcal{O}_K/a_0\mathcal{O}_K$. Since $\mathcal{O}_K$ and $a_0\mathcal{O}_K$ are both free abelian groups of the same rank, this quotient is finite (Theorem 2.41).

(2) Now let $\mathfrak{a} = \mathfrak{p}$ be a nonzero prime ideal. As a finite domain, the ring $\mathcal{O}_K/\mathfrak{p}$ is a field[1]. Because $a_0 \in \mathfrak{p} \cap \mathbb{Z}$, the intersection is nonzero. Because $\mathfrak{p}$ is a prime ideal, one checks easily that its intersection with $\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Thus $\mathfrak{p} = p\mathbb{Z}$ for some $p \in \mathbb{P}$. The kernel of the ring homomorphism $\mathbb{Z} \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ is $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, so

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

is injective. □

Theorem 3.3. *Let K be a number field. Then $\mathcal{O}_K$ is a noetherian integrally closed domain and every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof. We have already seen that $\mathcal{O}_K$ is noetherian in Theorem 2.45.

We show that $\mathcal{O}_K$ is integrally closed. Let $\alpha \in K$ be integral over $\mathcal{O}_K$. Let

$$f = X^m + \beta_{m-1}X^{m-1} + \cdots + \beta_0 \in \mathcal{O}_K[X]$$

be such that $f(\alpha) = 0$. Then $\alpha^m = -\sum_{j=0}^{m-1} \beta_j \alpha^j$, and hence the ring extension $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathcal{O}_K$-module (it is generated by 1, α, …, α^{m-1}). Because $\mathcal{O}_K$ is itself a finitely generated $\mathbb{Z}$-module, also $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathbb{Z}$-module (take pairwise products of generators). Then Proposition 2.16 implies that α is an algebraic integer, that is, $\alpha \in \mathcal{O}_K$. [2]

Finally, let $0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. Then Lemma 3.2 shows that $\mathcal{O}_K/\mathfrak{p}$ is a field, and hence $\mathfrak{p}$ is maximal. □

This motivates the following definition.

Definition 3.4. *A Dedekind domain is a noetherian integrally closed domain in which every nonzero prime ideal is maximal.*

Remark 3.5. That every nonzero prime ideal is maximal can also be expressed as $\dim(D) \leq 1$ (Krull dimension). If $\dim(D) = 0$, then 0 is the only prime ideal (that 0 is indeed a prime ideal, is equivalent to D being a domain). Because every maximal ideal is prime, a domain D therefore has $\dim(D) = 0$ if and only if D has no nonzero, proper ideal. This is equivalent to D being a field. So the (Dedekind) domains with $\dim(D) = 0$ are precisely the fields. Some authors exclude this (sometimes annoying) corner case in the definition of a Dedekind domain by requiring $\dim(D) = 1$ (equivalently, D is not a field), while others permit fields as Dedekind domains.

[1] Let F be a finite domain. For each $a \in F \setminus \{0\}$, the map $x \mapsto ax$ is injective because F is a domain. By finiteness of F, it is also surjective, so there exists $a' \in F$ with $aa' = 1$.

[2] We used that $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$. It actually suffices to observe that $S = \mathbb{Z}[\beta_1, \ldots, \beta_{m-1}]$ is a finitely generated $\mathbb{Z}$-module, which is a simple consequence of Proposition 2.16.

3.1 Prime Ideal Factorization in Dedekind Domains

Instead of showing directly that ideals of $\mathcal{O}_K$ factor uniquely into prime ideals, we do it more generally for Dedekind domains. We will establish the following theorem.

Theorem 3.6. *If D is a Dedekind domain, then every nonzero ideal is a product of prime ideals and such a representation is unique up to the order of the factors.*

Before we can prove Theorem 3.6, we need a few lemmas. Let us first explain the notion of an *invertible* ideal. Let D be a domain. Then ideals of D form a monoid with multiplication

$$IJ = \langle\, ab : a \in I, b \in J \,\rangle_D = \Big\{ \sum_{i=1}^{n} a_i b_i : n \ge 0, a_i \in I, b_i \in J \Big\}.$$

The ring D itself acts as a neutral element, but if $IJ = D$ then necessarily $I = J = D$ because $IJ \subseteq I \cap J \subseteq D$, so this monoid has no invertible elements except for D itself. To get a useful notion of inverses, we consider *fractional ideals.*

Definition 3.7. *Let D be a domain and K its quotient field.*

(1) *A fractional ideal of D is a D-submodule of K that is of the form $c^{-1}I$ with $c \in D^\bullet$ and $0 \ne I$ an ideal of D.*

(2) *A fractional ideal I is invertible if there exists a fractional ideal J such that $IJ = D$.*

In particular, every nonzero ideal I of D is a fractional ideal. If I, J are fractional ideals, it is easy to check that $IJ = \langle xy : x \in I, y \in J \rangle_D$ is also a fractional ideal, and this gives the fractional ideals the structure of a monoid (again D is the neutral element). So a nonzero ideal is invertible if and only if it is invertible in the monoid of fractional ideals. More explicitly, an ideal I is invertible if and only if there exists an ideal J in D such that $IJ = aD$ with $a \in D^\bullet$.

For a fractional ideal I, let

$$I^{-1} \coloneqq \{\, x \in K : xI \subseteq D \,\}.$$

It is easy to see that I^{-1} is a D-module (we just have to check that x, $y \in I^{-1}$ and $d \in D$ imply $x + y \in I^{-1}$ and $dx \in I^{-1}$, and this is immediate). Then $I^{-1}y \subseteq D$ is a nonzero ideal for all $0 \ne y \in I$, and so the set I^{-1} is also a fractional ideal.

If I is invertible and J is a fractional ideal such that $IJ = D$, then $J \subseteq I^{-1}$. So $D = IJ \subseteq II^{-1} \subseteq D$. Equality throughout implies $II^{-1} = D$ and so $I^{-1} = J$ is the unique inverse of I in the monoid of fractional ideals. (But be careful, the fractional ideal I^{-1} as defined always exists, even if I is not invertible.)

Lemma 3.8. *Let D be a Dedekind domain that is not a field. For every $0 \ne I$ ideal of D, there exist $r \ge 0$ and nonzero prime ideals $P_1, \ldots, P_r$ of D such that*

$$P_1 \cdots P_r \subseteq I.$$

Proof. The proof is by "noetherian induction": let Ω be the set of all ideals I for which the claimed property does not hold. Suppose $\Omega \neq \varnothing$. Because D is noetherian, there exists $I \in \Omega$ that is maximal in Ω. Then I cannot be a prime ideal (otherwise take $r = 1$ and $P_1 = I$). We must also have $I \neq D$, because D itself certainly satisfies the property (take any maximal ideal of D). Hence there exist a, $b \in D \setminus I$ such that $ab \in I$. Now $I + aD$, $I + bD \supsetneq I$. By maximality of I in Ω, we have $I + aD$, $I + aD \notin \Omega$. Hence there exist prime ideals $P_1, \dots, P_r$ and $Q_1, \dots, Q_s$ of D such that $P_1 \cdots P_r \subseteq I + aD$ and $Q_1 \cdots Q_s \subseteq I + bD$. Then

$$P_1 \cdots P_r Q_1 \cdots Q_s \subseteq (I + aD)(I + bD) \subseteq I,$$

a contradiction (to $\Omega \neq \varnothing$). □

Lemma 3.9. *Let D be a Dedekind domain that is not a field. Let $0 \neq P$ be a prime ideal of D. For every nonzero ideal I of D,*

$$I \subsetneq IP^{-1}.$$

Proof. We first consider the case $I = D$, that is, we show $P^{-1} \neq D$ (it always holds that $D \subseteq P^{-1}$). Let $0 \neq a \in P$. By Lemma 3.8 there exist nonzero prime ideals $P_1, \dots, P_r$ of D such that $P_1 \cdots P_r \subseteq aD \subseteq P$. Among all such products, we take one with $r \geq 0$ minimal. Because P is a proper ideal, necessarily $r \geq 1$. Because P is a prime ideal, there exists $1 \leq i \leq r$ with $P_i \subseteq P$ (otherwise, take $a_j \in P_j \setminus P$ for all $1 \leq j \leq r$. Then $a_1 \cdots a_r \in P$, but none of the factors is contained in P). Without restriction $P_1 \subseteq P$. Because D is a Dedekind domain, the prime ideal P_1 must be maximal. Hence $P_1 = P$. Because $P_2 \cdots P_r \nsubseteq aD$ (by minimality of r), there exists $b \in P_2 \cdots P_r$ such that $b \notin aD$ but $bP \subseteq P_1 \cdots P_r \subseteq aD$. Thus $a^{-1}b \notin D$, but $a^{-1}b \in P^{-1}$.

Now let $0 \neq I$ be an arbitrary ideal of D. Because D is noetherian, the ideal I is finitely generated, say $I = \langle a_1, \cdots, a_m \rangle_D$. Suppose, for the sake of contradiction, $I = IP^{-1}$. We will show that this leads to $D = P^{-1}$, in contradiction to what we already showed. Let $x \in P^{-1}$. Because D is integrally closed, it suffices to show that x is integral over D.

For each $1 \leq i \leq n$, let $c_{i1}, \dots, c_{1m} \in D$ be such that

$$xa_i = \sum_{j=1}^{m} c_{ij} a_j.$$

Let $C = (c_{ij})_{i,j} \in M_m(D)$ and $\mathbf{v} = (a_1, \dots, a_m)^T$. Then $x\mathbf{v} = C\mathbf{v}$ and so $(xI - C)\mathbf{v} = 0$. Because $\mathbf{v} \neq 0$, this means $\det(xI - C) = 0$, and expanding the determinant gives the desired monic polynomial for x with coefficients in D. [3] □

Proof (of Theorem 3.6). Suppose first that $D = K$ is a field. Then the only ideals are 0 and K. Now the ideal K factors as the empty product, so the claim is trivially true. Now suppose D is not a field.

[3] This should look familiar. We already treated the special case $D = \mathbb{Z}$ in Proposition 2.16.

We first show **existence** of factorizations into prime ideals. The ideal D always has the factorization as a trivial product with zero factors. Let Ω be the set of all ideals $0 \neq I \subsetneq D$ of D which cannot be written as a product of prime ideals. Because D is noetherian, there is a maximal $I \in \Omega$. Let P be a maximal ideal of D containing I. By Lemma 3.9, we have $I \subsetneq IP^{-1}$ and $P \subsetneq PP^{-1} \subseteq D$. Because P is maximal, necessarily $PP^{-1} = D$. By maximality of I, there exist prime ideals $P_2, \ldots, P_r$ of D such that $IP^{-1} = P_2 \cdots P_r$. Now

$$I = DI = PP^{-1}I = PP_2 \cdots P_r.$$

Let us now show **uniqueness**. Let $0 \neq I = P_1 \cdots P_r = Q_1 \cdots Q_s$ with prime ideals P_i, Q_j $(r, s \geq 0)$. Then $Q_1 \cdots Q_s \subseteq P_1$. Because P_1 is prime, this implies that there exists some j with $Q_j \subseteq P_1$. After renumbering, without restriction, $Q_1 \subseteq P_1$. By maximality of Q_1, we must have $Q_1 = P_1$. Multiplying with P_1^{-1}, and using $P_1 \subsetneq P_1P_1^{-1} = D$, gives $P_2 \cdots P_r = Q_2 \cdots Q_r$. Proceeding by induction on r, we eventually get $r = s$ and $P_i = Q_i$ for all $1 \leq i \leq r$ (after possibly renumbering).□

In the course of the proof, we crucially observed that every prime ideal is invertible ($PP^{-1} = D$). Of course, this now extends to arbitrary fractional ideals.

Corollary 3.10. *If D is a Dedekind domain, then every fractional ideal is invertible.*

Proof. Let I be a fractional ideal. Then cI is a nonzero ideal of D for some $c \in D^\bullet$, hence $cI = P_1 \cdots P_r$ with nonzero prime ideals P_i. For each P_i we have already concluded (using Lemma 3.9) that $P_1 \subsetneq P_iP_i^{-1} \subseteq D$, and by maximality $P_iP_i^{-1} = D$. Therefore $cI(P_1^{-1} \cdots P_r^{-1}) = D$.□

3.2 Fractional Ideals and the Class Group

Let D be a Dedekind domain. Grouping the primes, each nonzero ideal I of D has a unique representation

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

with pairwise distinct prime ideals P_i and $e_i > 0$. Here the prime ideals and the coefficients are (up to order) uniquely determined. By allowing negative exponents, we can also represent the fractional ideals (uniquely).

We can phrase this a bit more algebraically: Let $\mathcal{P}(D)$ denote the set of all nonzero prime ideals of D. Then the monoid of all nonzero ideals, denote it by $\mathcal{I}(D)^\bullet$ is a *free abelian monoid* with basis $\mathcal{P}(D)$. The monoid of fractional ideals, denote it by $\mathcal{F}(D)$, is a *free abelian group* on the same basis. For $P \in \mathcal{P}(D)$ and $I \in \mathcal{F}(D)$, let $\mathsf{v}_P(I) \in \mathbb{Z}$ denote the exponent of P in the factorization of I. By uniqueness of the representation, this is well-defined. We call this map the P-adic valuation. For a given I, we have $\mathsf{v}_P(I) = 0$ for all but finitely many P. So we have the compact notation

$$I = \prod_{P \in \mathcal{P}(D)} P^{\mathsf{v}_P(I)}.$$

Note $\mathsf{v}_P(IJ) = \mathsf{v}_P(I) + \mathsf{v}_P(J)$, again by uniqueness of the representation. Summarizing this more formally, we have the following isomorphism.

Theorem 3.11. *There is a group isomorphism*

$$\mathcal{F}(D) \to \mathbb{Z}^{(\mathcal{P}(D))},\ I \mapsto \big(\mathsf{v}_P(I)\big)_{P\in\mathcal{P}(D)},$$

that restricts to a monoid isomorphism $\mathcal{I}(D)^\bullet \to \mathbb{N}_0^{(\mathcal{P}(D))}$.

For $I,\ J \in \mathcal{I}(D)^\bullet$, we have

$$I \mid J \quad\Leftrightarrow\quad \forall P \in \mathcal{P}(D) : \mathsf{v}_P(J) \ge \mathsf{v}_P(I) \quad\Leftrightarrow\quad J \subseteq I.$$

The second equivalence remains true for fractional ideals. Because $\mathcal{I}(D)^\bullet$ is a free abelian monoid, there are also gcds and lcms. Indeed $\gcd(I,J) = I + J$ and $\operatorname{lcm}(I,J) = I \cap J$ for $I,\ J \in \mathcal{I}(D)^\bullet$. In terms of the valuations,

$$\mathsf{v}_P(\gcd(I,J)) = \min\{\mathsf{v}_P(I), \mathsf{v}_P(J)\} \qquad \mathsf{v}_P(\operatorname{lcm}(I,J)) = \max\{\mathsf{v}_P(I), \mathsf{v}_P(J)\}.$$

We have defined the valuations on fractional ideals. By considering (fractional) principal ideals, we can extend this to elements of $K^\times$. For $a \in K^\times$, we simple define $\mathsf{v}_P(a) \coloneqq \mathsf{v}_P(aD)$. Setting $\mathsf{v}_P(0) = \infty$, we get a discrete valuation $\mathsf{v}_P\colon K \to \mathbb{Z} \cup \{\infty\}$, that is, v_P has the following properties (we define $\infty + a = \infty + \infty = \infty$ for all $a \in \mathbb{Z}$ and $\infty > a$ for all $a \in \mathbb{Z}$):

- $\mathsf{v}_P(ab) = \mathsf{v}_P(a) + \mathsf{v}_P(b)$,
- $\mathsf{v}_P(a + b) \ge \min\{\mathsf{v}_P(a), \mathsf{v}_P(b)\}$.
- $\mathsf{v}_P(a) = \infty$ if and only if $a = 0$.

If $\mathsf{v}_P(a) \ne \mathsf{v}_P(b)$, then even $\mathsf{v}_P(a + b) = \min\{\mathsf{v}_P(a), \mathsf{v}_P(b)\}$. (Indeed, suppose without restriction $\mathsf{v}_P(a) < \mathsf{v}_P(b)$. Then $\mathsf{v}_P(a) = \mathsf{v}_P((a + b) - b) \ge \min\{\mathsf{v}_P(a + b), \mathsf{v}_P(b)\}$ forces $\mathsf{v}_P(a + b) \le \mathsf{v}_P(a)$.)

We know that the fractional ideals $\mathcal{F}(D)$ form a (free abelian) group. The nonzero principal ideals $\mathcal{H}(D) \coloneqq \{\, aD : a \in K^\times \,\}$ form a subgroup. Their quotient is again an abelian group.

Definition 3.12. *Let D be a Dedekind domain. The abelian group*

$$\mathcal{C}(D) \coloneqq \mathcal{F}(D)/\mathcal{H}(D)$$

is the class group of D.

Note that $aD = bD$ (for $a,\ b \in K^\times$) if and only if there exists a unit $\varepsilon \in D^\times$ such that $a = b\varepsilon$. Thus there is an exact sequence

$$1 \to D^\times \to K^\times \to \mathcal{F}(D) \to \mathcal{C}(D) \to 1.$$

The class group measures the failure of fractional ideals to be principal.

Theorem 3.13. *Let D be a Dedekind domain. Then the following statements are equivalent.*

(a) *D is UFD.*

(b) *The class group $\mathcal{C}(D)$ is trivial.*

(c) *D is a principal ideal domain (PID).*

Proof. Convince yourself that (in any domain): a principal ideal aD ($a \neq 0$) is a prime ideal if and only if the element a is a prime element of D.

(a) ⇒ (b) Because every nonzero ideal is a product of prime ideals, it suffices to show that every prime ideal is principal. Let $0 \neq P \subseteq D$ be a nonzero prime ideal. Let $0 \neq a \in P$. Then $a = p_1 \cdots p_r$ with prime elements p_i of D. Because P is a prime ideal, there exists some i with $p_i \in P$. Then $p_i D$ is a prime ideal with $p_i D \subseteq P$. Because D is a Dedekind domain, the ideal $p_i D$ is maximal. Hence $P = p_i D$.

(b) ⇒ (c) This is immediate from the definition of the class group.

(c) ⇒ (a) Every PID is a UFD, even without the Dedekind assumption [Bre19, Theorem 5.80]. For Dedekind domains, we can also reason as follows: For all $0 \neq a \in D$, we can factor

$$aD = P_1 \cdots P_r,$$

with nonzero prime ideals P_i. By (c), each P_i is principal, that is $P_i = p_i D$ with $0 \neq p_i \in D$. Now each of these is a prime element, and so $aD = p_1 D \cdots p_r D = p_1 \cdots p_r D$. There exists a unit $\varepsilon \in D^\times$ such that $a = p_1 \cdots (p_r \varepsilon)$, and this is a prime factorization of a. □

Example. We already know $\mathcal{C}(\mathbb{Z}) = \mathcal{C}(\mathbb{Z}[i]) = 0$, because both of these rings are Euclidean. We also know $\mathcal{C}(\mathbb{Z}[\sqrt{-5}]) \neq 0$, because $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, as we showed at the beginning of the chapter. We do not yet have the tools that would allow us to compute the class group, but in fact $\mathcal{C}(\mathbb{Z}[\sqrt{-5}]) \cong \mathbb{Z}/2\mathbb{Z}$. □

As an aside, we note the following.

Proposition 3.15. *Every PID is a Dedekind domain.*

Proof. Let D be a PID and K its quotient field. Because every ideal is generated by a single element, clearly D is noetherian. We have to check it is integrally closed and at most one-dimensional.

Let $a/b \in K$ with $a \in D$, $b \in D^\bullet$, and $f = X^m + c_{m-1}X^{m-1} + \cdots + c_0 \in D[X]$ a monic polynomial with $f(a/b) = 0$. Because D is a UFD [Bre19, Theorem 5.80], we can assume that a and b have no common non-unit factor. Now

$$0 = b^m f(a/b) = a^m + c_{m-1}a^{m-1}b + c_{m-2}a^{m-2}b^2 + \cdots c_0 b^m.$$

It follows that $b \mid a^m$ in D. If b is a non-unit, then there exists a prime element $p \in D$ dividing b and hence also dividing a, in contradiction to a and b being coprime. Hence $b \in D^\times$ and so $a/b \in D$. Thus D is integrally closed.

Now let $0 \neq P \subsetneq D$ be a prime ideal. Let $P \subseteq M \subsetneq D$ be a maximal ideal. Then $P = pD$ and $M = qD$ with prime elements p, $q \in D$. Then $q \mid p$. Because p is prime, this is only possible if $qD = pD$, that is, $P = M$ is maximal. □

In the previous proof we actually also showed that every UFD is integrally closed.

The polynomial ring $K[x]$ with K any field is a Dedekind domain. While every PID is a Dedekind domain, not every UFD is a Dedekind domain. By Gauss's Lemma, every polynomial ring over a UFD is a UFD. So $\mathbb{Z}[x]$ and $\mathbb{C}[x,y]$ are UFDs, but they are not Dedekind domains (in $\mathbb{Z}[x]$ there is a chain of prime ideals $0 \subsetneq (p) \subsetneq (p,x)$, and in $\mathbb{C}[x,y]$ there is $0 \subsetneq (x) \subsetneq (x,y)$).

Remark 3.16. The following remark adds some extra information about Dedekind domains in the context of commutative algebra, to provide some context for those students interested or already familiar with these topics.

(1) Several of the properties we have shown for a Dedekind domain actually lead to equivalent characterizations. The following statements are equivalent for a domain D.

   (a) D is noetherian, integrally closed, and $\dim(D) \leq 1$.
   (b) Every nonzero ideal of D is uniquely a product of prime ideals.
   (c) Every nonzero ideal of D is invertible.

(2) While UFDs need not be Dedekind domains, there is a generalization of Dedekind domains that covers all UFDs. By the equivalence of the characterizations in (1) of this remark, it is impossible to expect factorization into prime ideals in UFDs D with $\dim(D) > 1$ (e.g. multivariate polynomial rings). One can get around this problem by modifying the multiplication, replacing IJ by $\big((IJ)^{-1}\big)^{-1}$ and restricting to a particular class of ideals (divisorial ideals), which are those with $I = (I^{-1})^{-1}$. This leads to the notion of *Krull domains*. For a Krull domain, one can again define a (divisor) class group, and a Krull domain is a UFD if and only if the class group is trivial. However, now one even gets

$$D \text{ is a UFD} \quad \Leftrightarrow \quad D \text{ is a Krull domain with trivial class group.}$$

   So being a UFD implies being a Krull domain. The Dedekind domains are precisely the Krull domains of dimension ≤ 1.

(3) A second important source of Dedekind domains arises in geometry. If C is an irreducible affine algebraic curve defined over a field K, then the coordinate ring $K[C]$ is a Dedekind domain if and only if C is non-singular.

3.3 Chinese Remainder Theorem and an Application

We recall a version of the Chinese Remainder Theorem (CRT) for rings.

Theorem 3.17 (Chinese Remainder Theorem). *Let R be a ring. Let $I_1, \dots, I_m$ be ideals that are pairwise comaximal (that is $I_i + I_j = R$ for $i \neq j$). Then*

$$R/(I_1 \cap \cdots \cap I_m) \cong R/I_1 \times \cdots \times R/I_m, \quad r + I_1 \cap \cdots \cap I_m \mapsto (r + I_1, \dots, r + I_m),$$

is an isomorphism of R-algebras. In particular, for any choice $a_1, \dots, a_m \in R$, there exists $a \in R$ such that

$$a \equiv a_i \mod I_i \quad \textit{for all } 1 \le i \le m,$$

and the element a is unique modulo $I_1 \cap \cdots \cap I_m$.

Proof. The homomorphism $\varphi \colon R \to R/I_1 \times \cdots \times R/I_m$, $r \mapsto (r+I_1, \cdots, r+I_m)$ has kernel $I_1 \cap \cdots \cap I_m$. It therefore suffices to show that φ is surjective. Let $a_1, \dots, a_m \in R$.

For all $1 \le i \neq j \le m$, there exist $x_{ij} \in I_i$ and $y_{ij} \in I_j$ such that $1 = x_{ij} + y_{ij}$. Then, for every $1 \le i \le m$,

$$1 = \prod_{j \neq i} (x_{ij} + y_{ij}) \equiv \prod_{j \neq i} y_{ij} \mod I_i.$$

Setting $z_i \coloneqq \prod_{j \neq i} y_{ij}$ we have $z_i \equiv 1 \mod I_i$ and $z_i \equiv 0 \mod I_j$ for $j \neq i$. So $\varphi(a_1 z_1 + \cdots + a_n z_n) = (a_1 + I_1, \dots, a_m + I_m)$. □

In a Dedekind domain D, the condition $I_i + I_j = D$ reduces to the ideals being coprime because $\gcd(I_i, I_j) = I_i + I_j$. In particular, we can apply the result when the ideals are distinct prime powers. Furthermore,

$$a \equiv b \mod P^e \quad \Leftrightarrow \quad a - b \in P^e \quad \Leftrightarrow \quad \mathsf{v}_P(a-b) \ge e.$$

We get the following immediate reformulation of the Chinese Remainder Theorem.

Corollary 3.18. *Let D be a Dedekind domain. Let $P_1, \dots, P_m$ be pairwise distinct nonzero prime ideals, and $e_1, \dots, e_m \in \mathbb{N}_0$. If $a_1, \dots, a_m \in D$, then there exists $a \in D$, such that for all $1 \le i \le m$,*

$$a \equiv a_i \mod P_i^{e_i}.$$

The congruence can equivalently be expressed as $\mathsf{v}_{P_i}(a - a_i) \ge e_i$.

Another useful variant is the following. Because of the uniqueness of prime ideal factorization, we have $P_i^{e_i+1} \subsetneq P_i^{e_i}$. Hence there exists $a_i \in P_i^{e_i} \setminus P_i^{e_i+1}$. If we pick $a \in D$ with $\mathsf{v}_{P_i}(a - a_i) \ge e_{i+1}$ (using Weak Approximation), then

$$\mathsf{v}_{P_i}(a) = \mathsf{v}_{P_i}(a_i + (a - a_i)) = \min\{\mathsf{v}_{P_i}(a_i), \mathsf{v}_{P_i}(a - a_i)\} = e_i,$$

(the crucial equality with the minimum holds because of $\mathsf{v}_{P_i(a_i)} \neq \mathsf{v}_{P_i}(a - a_i)$). We have proven.

Corollary 3.19. *Let D be a Dedekind domain. Let $P_1, \ldots, P_m$ be pairwise distinct nonzero prime ideals, and $e_1, \ldots, e_m \in \mathbb{Z}$. Then there exists $x \in K^\times$ with $\mathsf{v}_{P_i}(x) = e_i$ for all $1 \leq i \leq m$ and $\mathsf{v}_P(x) \geq 0$ for all nonzero primes $P \neq P_i$.*

Proof. We have just shown the case when $e_i \geq 0$ for all i. For the general case, without restriction, $e_1, \ldots, e_l \geq 0$ and $e_{l+1}, \ldots, e_m < 0$. Let $b \in D$ with $\mathsf{v}_{P_i}(b) = -e_i$ for $l < i < m$ and $\mathsf{v}_{P_i}(b) = 0$ for $1 \leq i \leq l$. Let $Q_1, \ldots, Q_s$ denote the set of primes (distinct from the P_i) for which $\mathsf{v}_{Q_i}(b) > 0$ (there are only finitely many). Let $a \in D$ be such that $\mathsf{v}_{P_i}(a) = e_i$ for $1 \leq i \leq l$, $\mathsf{v}_{P_i}(a) = 0$ for $l < i \leq m$, and $\mathsf{v}_{Q_i}(a) = \mathsf{v}_{Q_i}(b)$ for $1 \leq i \leq s$. Then $x = a/b$ has the required property. □

As a straightforward consequence, we get that every ideal in a Dedekind domain can be generated by just two elements, and the first one can be chosen essentially arbitrary.

Theorem 3.20. *Let D be a Dedekind domain, and let $0 \neq I \subseteq D$ be an ideal. If $0 \neq a \in I$, then there exist $b \in I$, such that $I = (a, b)$.*

Proof. Here our abstract notation becomes quite handy. Because $aD \subseteq I$, we have $\mathsf{v}_P(aD) \geq \mathsf{v}_P(I)$ for all $P \in \mathcal{P}(D)$. Our goal is to find $b \in D$ such that

$$\mathsf{v}_P(bD) \geq \mathsf{v}_P(I) \quad \text{and} \quad \mathsf{v}_P(I) = \min\{\mathsf{v}_P(aD), \mathsf{v}_P(bD)\} = \mathsf{v}_P(aD + bD).$$

Then we will have $I = aD + bD$.

Let $P_1, \ldots, P_n$ denote the (pairwise distinct) nonzero prime ideals for which $\mathsf{v}_{P_i}(aD) > 0$. There are only finitely many such prime ideals. Let $e_i := \mathsf{v}_{P_i}(I)$. Let $b \in D$ with $\mathsf{v}_{P_i}(b) = e_i$. So we have $\mathsf{v}_P(bD) \geq \mathsf{v}_P(I)$ for all $P \in \mathcal{P}(D)$, and also

$$\min\{\mathsf{v}_P(aD), \mathsf{v}_P(bD)\} = \begin{cases} \mathsf{v}_P(I) & \text{if } \mathsf{v}_P(aD) > 0, \\ 0 = \mathsf{v}_P(I) & \text{if } \mathsf{v}_P(aD) = 0 \end{cases}$$

□

Chapter 4

Minkowsi Theory

4.1 Lattices

Definition 4.1. *Let V be an $\mathbb{R}$-vector space of dimension n.*

(1) *A* lattice *is a subgroup*

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m \subseteq V,$$

with $\mathbb{R}$-linearly independent vectors $v_1, \ldots, v_m \in V$.

(2) *The tuple $(v_1, \ldots, v_m)$ is called a* basis *of the lattice. The lattice is* complete *if $m = n$.*

(3) *The set*

$$F = \{ x_1 v_1 + \cdots + x_m v_m \in V : x_i \in [0,1), 1 \le i \le m \},$$

is the fundamental domain *of the basis $(v_1, \ldots, v_m)$.*

Example. $\mathbb{Z}^n \subseteq \mathbb{R}^n$ is a complete lattice with the standard basis vectors as basis. The fundamental domain is a hypercube. Note that $\mathbb{Z}[i] \subseteq \mathbb{C}$, with $\mathbb{C}$ viewed as 2-dimensional $\mathbb{R}$-vector space gives this lattice for $n = 2$. From $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\zeta_6] \subseteq \mathbb{C}$ we get another complete lattice in $\mathbb{R}^2$, with (one possible) basis

$$(1,0),\ (\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}).$$

The fundamental domain is a parallelogram.

On the other hand $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \subseteq \mathbb{R}$ is *not* lattice, because 1 and $\sqrt{2}$ are linearly dependent over $\mathbb{R}$ (despite being linearly independent over $\mathbb{Z}$ and hence $\mathbb{Q}$). □

The fundamental domain F depends on the choice of basis of Γ. Note that

$$\mathbb{R}\Gamma = \biguplus_{\gamma \in \Gamma} \gamma + F$$

with the union being disjoint, giving a tiling of $\mathbb{R}\Gamma$ by copies of F (here $\mathbb{R}\Gamma$ denotes the $\mathbb{R}$-vector space spanned by Γ). In particular, the set F is a system of representatives for the quotient group $\mathbb{R}\Gamma/\Gamma$. If Γ is complete, then F gives a tiling of V and at the same time a system of representatives for V/Γ.

Every lattice is a free $\mathbb{Z}$-submodule of $\mathbb{R}^n$, but the converse is not true, as we saw with $\mathbb{Z}[\sqrt{2}]$. The following gives an intrinsic characterization of lattices. Recall that every finite-dimensional $\mathbb{R}$-vector space is a (complete) normed vector space, with respect to an arbitrary norm.[1]. All norms on a finite-dimensional vector space are equivalent, so the topology does not depend on the choice of norm.

Proposition 4.3. *Let V be an n-dimensional $\mathbb{R}$-vector space, and let $\Gamma \subseteq V$ be a subgroup. Then the following statements are equivalent.*

(a) *Γ is a lattice.*

(b) *0 is not an accumulation point of Γ.*

(c) *Γ is discrete (that is, Γ has no accumulation points*[2]*).*

Proof. (a) ⇒ (b) Let $(v_1, \dots, v_m)$ be a basis of Γ, and extend it to a basis of V by choosing $v_{m+1}, \dots, v_n \in V$. The set

$$\left\{ \sum_{i=1}^{n} x_i v_i : x_i \in (-1, 1) \right\}$$

is an open neighborhood of 0 that does not contain any other lattice point.

(b) ⇒ (c) Suppose that $\gamma \in \Gamma$ is an accumulation point, and let $(\gamma_n)_{n\geq 1}$ be a sequence in $\Gamma \setminus \{\gamma\}$ for which $(\gamma_n)_{n\geq 1} \to \gamma$. Passing to a subsequence, we can without restriction assume $\gamma_n \neq \gamma_m$ for $n \neq m$. Then $(\gamma_{n+1} - \gamma_n)_{n\geq 1}$ is a sequence in $\Gamma \setminus \{0\}$ that converges to 0.

(c) ⇒ (a) Let $W \coloneqq \mathbb{R}\Gamma$ be the $\mathbb{R}$-vector subspace of V spanned by Γ. We can choose a basis $(w_1, \dots, w_m)$ of W that is contained in Γ. Now

$$\Gamma_0 \coloneqq w_1\mathbb{Z} \oplus \cdots \oplus w_m\mathbb{Z} \subseteq \Gamma$$

is a complete lattice in W. Let $F_0 = \{ x_1 w_1 + \cdots + x_m w_m : x_i \in [0, 1) \}$ be the fundamental domain. Because $\Gamma_0 \subseteq W$ is a complete lattice, the set F_0 is a system of representatives for the abelian group W/Γ_0. In particular, we can choose a system of representatives $R \subseteq F_0$ for Γ/Γ_0. Then R is bounded (because F_0 is), and discrete (because Γ is). By the Heine–Borel Theorem, the set R is finite. Hence $|\Gamma : \Gamma_0| \eqqcolon d < \infty$. Thus $d\Gamma \subseteq \Gamma_0$, and

$$\Gamma \subseteq \tfrac{1}{d}\Gamma_0 = \tfrac{w_1}{d}\mathbb{Z} \oplus \cdots \oplus \tfrac{w_m}{d}\mathbb{Z}.$$

Now the Structure Theorem for Finitely Generated Abelian Groups, Theorem 2.41, shows that Γ is finitely generated free abelian of rank m. Since Γ spans W as $\mathbb{R}$-vector space and $\dim(W) = m$,

[1] Here we are talking about norms in the sense of analysis. A norm on a real vector space is a map $\|\cdot\| \colon V \to \mathbb{R}$ such that $\|x\| = 0$ if and only if $x = 0$, $\|\lambda x\| = |\lambda| \|x\|$, and $\|x + y\| \leq \|x\| + \|y\|$ for all $\lambda \in \mathbb{R}$, $x, y \in V$. This must not be confused with the (field) norm Definition 2.30

[2] Equivalently, every $\gamma \in \Gamma$ has an open neighborhood in V not containing any points of $\Gamma \setminus \{\gamma\}$

the generators must also be $\mathbb{R}$-linearly independent. Hence Γ is a lattice. □

A characterization of the completeness of a lattice is also useful.

Lemma 4.4. *A lattice $\Gamma \subseteq V$ is complete if and only if V/Γ has a bounded system of representatives*

Proof. If Γ is a complete lattice, we have already seen that any fundamental domain gives a bounded system of representatives for V/Γ.

Suppose that $\Gamma \subseteq V$ is a lattice and $B \subseteq V$ is a bounded set such that

$$V = \bigcup_{\gamma \in \Gamma} \gamma + B. \tag{4.1}$$

Let W be the vector subspace spanned by Γ. As a vector subspace of the finite-dimensional vector space V, the space W is closed in V.

Let $v \in V$. For every $n \in \mathbb{N}$, we can write

$$nv = \beta_n + \gamma_n \qquad \text{with } \beta_n \in B,\ \gamma_n \in \Gamma \subseteq W.$$

Then $v = \frac{1}{n}\beta_n + \frac{1}{n}\gamma_n$. Because B is bounded, $\lim_{n\to\infty} \frac{1}{n}\beta_n = 0$. Because W is closed,

$$v = \lim_{n\to\infty} \tfrac{1}{n}\gamma_n \in W.$$

Hence $V = W$. □

On the Euclidean space $\mathbb{R}^n$ we have the usual Lebesque measure, which assigns to a measurable set X the volume $\operatorname{vol}(X)$. The volume of the n-dimensional hypercube is 1. More generally, If $v_1, \ldots, v_n$ are linearly independent, then the parallelotope

$$P \coloneqq \{\, x_1 v_1 + \cdots + x_n v_n : x_i \in [0,1),\ 1 \le i \le n \,\} \subseteq \mathbb{R}^n$$

has volume

$$\operatorname{vol}(P) = |\det(v_1, v_2, \ldots, v_n)|.$$

Suppose that $\Gamma \subseteq \mathbb{R}^n$ is a complete lattice with basis $(v_1, \ldots, v_n)$. The fundamental domain F of Γ is a parallelotope (minus some faces). The set F depends on the choice of basis. However, if $(w_1, \ldots, w_n)$ is another basis of the lattice Γ, then the basis transformation matrix is in $\mathrm{GL}_n(\mathbb{Z})$, and therefore has determinant ±1. Hence the volume of the fundamental domain is independent of the choice of basis, and we tacitly[3] define

$$\operatorname{vol}(\Gamma) \coloneqq \operatorname{vol}(F).$$

[3] Strictly speaking, $\operatorname{vol}(\Gamma)$ is already defined as the volume of the set Γ; but that is always 0 because the set is discrete, so there is no harm in reusing the notation $\operatorname{vol}(\Gamma)$ for something else.

Theorem 4.5 (Minkowski's Theorem). *Let $\Gamma \subseteq \mathbb{R}^n$ be a complete lattice. Let $X \subseteq \mathbb{R}^n$ be a set that*

- *is symmetric with respect to the origin (if $x \in X$, then $-x \in X$),*
- *is convex (for all x, $y \in X$ and $t \in [0,1]$ we have $tx + (1-t)y \in X$), and*
- *has*

$$\operatorname{vol}(X) > 2^n \operatorname{vol}(\Gamma).$$

Then X contains a nonzero lattice point of Γ. [4]

Proof. It suffices to show that there exist $\gamma_1 \neq \gamma_2 \in \Gamma$ such that

$$\big(\gamma_1 + \frac{1}{2}X\big) \cap \big(\gamma_2 + \frac{1}{2}X\big) \neq \varnothing.$$

Because then $\gamma_1 + \frac{1}{2}x_1 = \gamma_2 + \frac{1}{2}x_2$ for some x_1, $x_2 \in X$, and

$$0 \neq \gamma_2 - \gamma_1 = \tfrac{1}{2}x_1 - \tfrac{1}{2}x_2 = \tfrac{1}{2}x_1 + \tfrac{1}{2}(-x_2) \in \Gamma \cap X,$$

(by convexity and symmetry of X).

Suppose all translates $\gamma + \frac{1}{2}X$ with $\gamma \in \Gamma$ are pairwise disjoint. Let F be a fundamental domain for Γ. Because $\mathbb{R}^n = \biguplus_{\gamma\in\Gamma}(\gamma + F)$, we get

$$\tfrac{1}{2}X = \biguplus_{\gamma\in\Gamma}(\tfrac{1}{2}X \cap (\gamma + F)),$$

(with the union being disjoint). Using translation invariance and countable additivity of the Lebesque measure (Γ is countable), we find

$$\operatorname{vol}(\tfrac{1}{2}X) = \sum_{\gamma\in\Gamma}\operatorname{vol}(\tfrac{1}{2}X \cap (\gamma + F)) = \sum_{\gamma\in\Gamma}\operatorname{vol}\big((\tfrac{1}{2}X - \gamma\big) \cap F) \leq \operatorname{vol}(F),$$

where the final inequality uses that the translates $\gamma + \frac{1}{2}X$ are disjoint. Because $\operatorname{vol}(\Gamma) = \operatorname{vol}(F)$ and $\operatorname{vol}(\frac{1}{2}X) = \frac{1}{2^n}\operatorname{vol}(X)$, this contradicts $\operatorname{vol}(X) > 2^n \operatorname{vol}(\Gamma)$. □

4.2 From Ideals to Lattices

Let K be a number field of degree n. We will embed K into $\mathbb{R}^n$ as a $\mathbb{Q}$-vector space.

We already know that K has precisely n embeddings into $\mathbb{C}$, and if $K = \mathbb{Q}(\alpha)$, then each embedding corresponds to a root of the minimal polynomial of α. If $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, we can have either $\sigma(K) \subseteq \mathbb{R}$, in which case σ is a real embedding, or $\sigma(K) \nsubseteq \mathbb{R}$, in which case σ is a complex embedding. In the latter case the complex conjugate $\overline{\sigma} \neq \sigma$ is also a complex embedding.

[4] Convex subsets of $\mathbb{R}^n$ are measurable, so $\operatorname{vol}(X)$ is well-defined.

Thus complex embeddings come in pairs (corresponding to the fact that complex roots of the minimal polynomial of α come in complex conjugate pairs).

We use the following notation throughout the remaining chapter. Let σ_1, …, σ_r $(0 \le r \le n)$ denote the distinct real embeddings of K, and let $\sigma_{r+1}, \ldots, \sigma_{r+s}$ denote a system of representatives for the s pairs of complex embeddings $(0 \le s \le n/2)$. We also set $\sigma_{r+s+i} = \overline{\sigma_{r+i}}$ for $1 \le i \le s$. Then $n = r + 2s$. The map

$$j\colon K \to \mathbb{R}^n \tag{4.2}$$

defined by

$$j(\alpha) = \big(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}(\sigma_{r+1}(\alpha)), \ldots, \mathrm{Re}(\sigma_{r+s}(\alpha)), \mathrm{Im}(\sigma_{r+1}(\alpha)), \ldots, \mathrm{Im}(\sigma_{r+s}(\alpha))\big)^T$$

is a monomorphism of $\mathbb{Q}$-vector spaces.

Example.

- Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree and $d < 0$. Then there is one pair of complex conjugate embeddings ($r = 0$, $s = 1$), given by $\alpha = a + b\sqrt{d} \mapsto a \pm bi\sqrt{|d|}$. Hence

  $$j(\alpha) = (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))^T = (a, b\sqrt{|d|})^T.$$

  For instance, for $K = \mathbb{Q}(i)$, we get $j(a + bi) = (a, b)^T$. Here $j(\mathbb{Z}[i])$ is a lattice with basis $(1, 0)$ and $(0, 1)$. The volume of the fundamental domain is 1. For $K = \mathbb{Q}(\sqrt{-5}) = \mathbb{Q}(\zeta_6)$, we get $j(a + b\sqrt{-5}) = (a, \sqrt{5}b)^T$. The lattice $j(\mathbb{Z}[\sqrt{-5}])$ has a basis $(1, 0)^T$, $(0, \sqrt{5})^T$ and therefore has volume $\sqrt{5}$.

  Note that

  $$|a + b\sqrt{d}| = a^2 + db^2 = |a - b\sqrt{d}|,$$

  so while the embeddings are different, still $|\sigma_1(\alpha)| = |\overline{\sigma_1(\alpha)}|$.

- Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree and $d > 1$. Then there exist two distinct real embeddings ($r = 2$, $s = 0$). They again map $\alpha = a + b\sqrt{d}$ to $a \pm b\sqrt{d}$, so now

  $$j(\alpha) = (a + b\sqrt{d}, a - b\sqrt{d})^T.$$

  For $K = \mathbb{Q}(\sqrt{2})$, we get $j(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2})^T$. Note that $(1, 1)$ and $(\sqrt{2}, -\sqrt{2})$ are linearly independent even over $\mathbb{R}$. So $j(\mathbb{Z}[\sqrt{2}]) \subseteq \mathbb{R}^2$ is a lattice!

  The volume of its fundamental domain (a rectangle) is

  $$\left|\det\begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}\right| = 2\sqrt{2}.$$

  Note that now, e.g.

  $$|1 + \sqrt{2}| \ne |1 - \sqrt{2}|,$$

so the embeddings induce different absolute values.

- Let $K = \mathbb{Q}(\sqrt[3]{2})$ and $\zeta_3 = \frac{-1+\sqrt{3}i}{2}$. There are three embeddings of K into $\mathbb{C}$, determined by

$$\sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}, \quad \sqrt[3]{2} \mapsto \overline{\zeta_3}\sqrt[3]{2}.$$

  The first one is real, while the others constitute a pair of complex embeddings. Hence $r = 1$ and $s = 1$, for $r + 2s = 3$. □

Proposition 4.7. *If $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_K$, then $j(\mathfrak{a})$ is a complete lattice whose fundamental domain has the volume*

$$\operatorname{vol}(j(\mathfrak{a})) = 2^{-s}\sqrt{|\operatorname{disc}(\mathfrak{a})|}.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$ (which exists by Theorem 2.45). Then $\operatorname{disc}(\mathfrak{a}) = \det(\sigma_k(\alpha_l))^2_{1\le k,l\le n}$ by definition[5]. For $\alpha \in K$, let us compare $j(\alpha)$ to $(\sigma_k(\alpha))^T_{1\le k\le n}$. The first r entries of $j(\alpha)$ are just $\sigma_k(\alpha)$ for $1 \le k \le r$ (the real embeddings). For $1 \le l \le s$, we get

$$\begin{pmatrix} \operatorname{Re}\sigma_{r+l}(\alpha) \\ \operatorname{Im}\sigma_{r+l}(\alpha) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2i} & -\frac{1}{2i} \end{pmatrix} \begin{pmatrix} \sigma_{r+l}(\alpha) \\ \overline{\sigma_{r+l}}(\alpha) \end{pmatrix}.$$

Because of $\overline{\sigma_{r+l}} = \sigma_{r+l+s}$, we get altogether a block matrix representation (I_r, I_s are the identity matrices of size $r \times r$, respectively, $s \times s$)

$$j(\alpha) = \underbrace{\begin{pmatrix} I_r & 0 & 0 \\ 0 & \frac{1}{2}I_s & \frac{1}{2}I_s \\ 0 & \frac{1}{2i}I_s & -\frac{1}{2i}I_s \end{pmatrix}}_{=:C} \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}.$$

Subtracting $1/i$ times the second row of blocks from the third, we see $\det(C) = (-2i)^{-s}$ and so $|\det(C)| = 2^{-s}$.

Because $\det(\sigma_k(\alpha_l))_{k,l} \ne 0$, it follows that $j(\alpha_1), \ldots,, j(\alpha_n)$ is a basis of $\mathbb{R}^n$, and that

$$\operatorname{vol}(j(\mathfrak{a})) = |\det(j(\alpha_1), \ldots, j(\alpha_n))| = 2^{-s}\sqrt{|\operatorname{disc}(\mathfrak{a})|}.$$ □

Combining the fact that $j(\mathfrak{a})$ is a lattice with Minkowski's Theorem on lattice points (Theorem 4.5) allows us to prove results showing that ideals contain "small" elements.

[5] Strictly speaking we had defined it only for nonzero ideals so far, not for fractional ideals, but it is the same definition.

Theorem 4.8. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. For $1 \le i \le r+s$, let $c_i \in \mathbb{R}_{>0}$ be such that*

$$\prod_{i=1}^{r} c_i \prod_{i=1}^{s} c_{r+i}^2 > \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathfrak{a})|}.$$

Then there exists a nonzero $\alpha \in \mathfrak{a}$ such that

$$|\sigma_i(\alpha)| < c_i \qquad \text{for all } 1 \le i \le r+s.$$

Proof. Let

$$X := \left\{ (x_1, \dots, x_n)^T \in \mathbb{R}^n : |x_i| < c_i \text{ for } 1 \le i \le r,\ x_{r+i}^2 + x_{r+i+s}^2 < c_{r+i}^2 \text{ for } 1 \le i \le s \right\}.$$

The set X is convex and symmetric around the origin. For the volume,

$$\mathrm{vol}(X) = \prod_{i=1}^{r}(2c_i) \cdot \prod_{i=1}^{s}(c_{r+i}^2 \pi) = 2^r \pi^s c,$$

with $c := c_1 \cdots c_r (c_{r+1})^2 \cdots (c_{r+s})^2$. By assumption,

$$\mathrm{vol}(X) > 2^{r+s}\sqrt{|\mathrm{disc}(\mathfrak{a})|} = 2^{r+2s}\,\mathrm{vol}(j(\mathfrak{a})) = 2^n\,\mathrm{vol}(j(\mathfrak{a})).$$

By Minkowski's Theorem on lattice points (Theorem 4.5), the set $j(\mathfrak{a}) \cap X$ contains a nonzero element. Its preimage under j is the desired $\alpha \in \mathfrak{a}^\bullet$. □

In particular, the previous theorem allows us to choose $\alpha \in \mathfrak{a}^\bullet$ with

$$|\mathsf{N}_{\mathbb{Q}}^{K}(\alpha)| < \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathfrak{a})|} + \varepsilon,$$

for arbitrarily small $\varepsilon > 0$. Because $\mathfrak{a}$ is a fractional ideal, there exists $d \in \mathbb{N}$ such that $d\mathfrak{a} \subseteq \mathcal{O}_K$. If $\alpha \in \mathfrak{a}$ therefore $\mathsf{N}^K(\alpha) \in d^{-n}\mathbb{Z}$, and so the norms of elements in $\mathfrak{a}$ have bounded denominator. So, choosing ε sufficiently small, we get

$$|\mathsf{N}_{\mathbb{Q}}^{K}(\alpha)| \le \left(\frac{2}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathfrak{a})|}. \tag{4.3}$$

It is worth improving the factor in this result.

Theorem 4.9 (Minkowski). *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Then there exists a nonzero $\alpha \in \mathfrak{a}$ with*

$$|\mathsf{N}_{\mathbb{Q}}^{K}(\alpha)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathfrak{a})|},$$

where $n = [K : \mathbb{Q}]$ and s is the number of pairs of complex conjugate embeddings of K.

Proof. Let $c \in \mathbb{R}_{>0}$ be such that

$$c^n > n! \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|}, \tag{4.4}$$

and let

$$Y = Y_{r,s,c} \coloneqq \Big\{ (x_1, \dots, x_n)^T \in \mathbb{R}^n : \sum_{i=1}^{r} |x_i| + 2 \sum_{i=1}^{s} \sqrt{x_{r+i}^2 + x_{r+i+s}^2} < c \Big\}.$$

The set Y is symmetric around the origin and convex. By induction on r and s, one can show (left as an exercise)

$$\operatorname{vol}(Y) = 2^r \left(\frac{\pi}{2}\right)^s \frac{c^n}{n!} = 2^{r+s} \left(\frac{\pi}{4}\right)^s \frac{c^n}{n!} > 2^{r+s} \sqrt{|\operatorname{disc}(\mathfrak{a})|} = 2^n (2^{-s} |\operatorname{disc}(\mathfrak{a})|) = 2^n \operatorname{vol}(j(\mathfrak{a})).$$

By Minkowski's Theorem there exists a nonzero element in $Y \cap j(\mathfrak{a})$. Let $\alpha \in \mathfrak{a}$ be the preimage of such a point. Using the inequality between the arithmetic and the geometric mean[6], we find

$$\begin{aligned} \sqrt[n]{|\mathsf{N}_{\mathbb{Q}}^K(\alpha)|} &= \sqrt[n]{\prod_{i=1}^{r} |\sigma_i(\alpha)| \prod_{i=1}^{s} \left(\sqrt{\operatorname{Re}(\sigma_{r+i}(\alpha))^2 + \operatorname{Im}(\sigma_{r+i}(\alpha))^2}\right)^2} \\ &\le \frac{1}{n} \left(\sum_{i=1}^{r} |\sigma_i(\alpha)| + 2 \sum_{i=1}^{s} \sqrt{\operatorname{Re}(\sigma_{r+i}(\alpha))^2 + \operatorname{Im}(\sigma_{r+i}(\alpha))^2} \right) < \frac{c}{n}. \end{aligned}$$

Therefore

$$|\mathsf{N}_{\mathbb{Q}}^K(\alpha)| < \frac{c^n}{n!} \le \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|} + \varepsilon.$$

Choosing c sufficiently small (subject to (4.4)), and keeping in mind that $|\mathsf{N}_{\mathbb{Q}}^K(\alpha)| \in d^{-1}\mathbb{N}$ for some $d \in \mathbb{N}$ (that depends on $\mathfrak{a}$ but not α), we get

$$|\mathsf{N}_{\mathbb{Q}}^K(\alpha)| \le \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{a})|}.$$

□

4.3 Finiteness of the Class Group

If $0 \neq \mathfrak{a}$ is an ideal of $\mathcal{O}_K$, then the quotient $\mathcal{O}_K/\mathfrak{a}$ is finite by Lemma 3.2. This allows us to extend the notion of the (field) norm $\mathsf{N}_{\mathbb{Q}}^K$ from elements to ideals.

Definition 4.10. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal. Then*

$$\mathsf{N}(\mathfrak{a}) \coloneqq |\mathcal{O}_K/\mathfrak{a}|.$$

Like the norm on elements, the norm on ideals turns out to be multiplicative. It also matches the element norm for principal ideals.

[6] For all $n \ge 1$ and $x_1, \dots, x_n \in \mathbb{R}_{\ge 0}$, it holds that $\sqrt[n]{x_1 \cdots x_n} \le \frac{1}{n}(x_1 + \cdots + x_n)$

Proposition 4.11. *Let K be a number field.*

(1) *If $0 \neq \mathfrak{a}$, $\mathfrak{b}$ are ideals of $\mathcal{O}_K$, then*
$$\mathsf{N}(\mathfrak{a}\mathfrak{b}) = \mathsf{N}(\mathfrak{a})\,\mathsf{N}(\mathfrak{b}).$$

(2) *If $\mathfrak{a} = \alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K^{\bullet}$, then*
$$\mathsf{N}(\mathfrak{a}) = |\mathsf{N}_{\mathbb{Q}}^{K}(\alpha)|.$$

Proof. (1) The Chinese Remainder Theorem shows $\mathcal{O}_K/\mathfrak{a}\mathfrak{b} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}$ if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, which implies the claim for $\mathfrak{a}$ and $\mathfrak{b}$ coprime. It therefore suffices to consider the prime power case, and really it suffices to show $\mathsf{N}(\mathfrak{p}^{e+1}) = \mathsf{N}(\mathfrak{p}^{e})\,\mathsf{N}(\mathfrak{p})$ for all nonzero prime ideals $\mathfrak{p}$ and $e \geq 0$. We have
$$\mathcal{O}_K \supseteq \mathfrak{p}^{e} \supseteq \mathfrak{p}^{e+1}.$$

We will be done if we can show $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^{e}/\mathfrak{p}^{e+1}$. First note that, by uniqueness of the factorization into prime ideals, $\mathfrak{p}^{e_1} \subsetneq \mathfrak{p}^{e}$. Let $a \in \mathfrak{p}^{e} \setminus \mathfrak{p}^{e+1}$. The homomorphism of $\mathcal{O}_K$-modules,
$$\mathcal{O}_K \to \mathfrak{p}^{e}/\mathfrak{p}^{e+1}, \ x \mapsto ax + \mathfrak{p}^{e+1},$$

induces a homomorphism $\mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^{e}/\mathfrak{p}^{e+1}$. In this way, $\mathfrak{p}^{e}/\mathfrak{p}^{e+1}$ becomes a (nonzero) $\mathcal{O}_K/\mathfrak{p}$-vector space (remember that $\mathcal{O}_K/\mathfrak{p}$ is a finite field). It will suffice to show that its dimension is one. Suppose not. Then $\mathfrak{p}^{e}/\mathfrak{p}^{e+1}$ has a proper, nonzero $\mathcal{O}_K/\mathfrak{p}$-subspace, necessarily of the form $\mathfrak{b}/\mathfrak{p}^{e+1}$ with $\mathfrak{b}$ an ideal of $\mathcal{O}_K$ with $\mathfrak{p}^{e+1} \subsetneq \mathfrak{b} \subsetneq \mathfrak{p}^{e}$, hence $\mathfrak{p} \subsetneq \mathfrak{b}\mathfrak{p}^{-e} \subsetneq \mathcal{O}_K$, in contradiction to $\mathfrak{p}$ being a maximal ideal of $\mathcal{O}_K$.

(2) Let $\beta_1, \dots, \beta_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then $\alpha\beta_1, \dots, \alpha\beta_n$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$. We already know $\operatorname{disc}(\mathfrak{a}) = |\mathcal{O}_K : \mathfrak{a}|^2 \operatorname{disc}(\mathcal{O}_K) = \mathsf{N}(\mathfrak{a})^2 \operatorname{disc}(\mathcal{O}_K)$. It will therefore suffice to show $\operatorname{disc}(\mathfrak{a}) = \mathsf{N}_{\mathbb{Q}}^{K}(\alpha)^2 \operatorname{disc}(\mathcal{O}_K)$. The computation
$$\begin{aligned}\operatorname{disc}(\mathfrak{a}) &= \det(\sigma_k(\alpha\beta_l))_{k,l}^2 = \det(\sigma_k(\alpha)\sigma_k(\beta_l))_{k,l}^2 = \prod_{k=1}^{n} \sigma_k(\alpha)^2 \cdot \det(\sigma_k(\beta_l))_{k,l}^2 \\ &= \mathsf{N}_{\mathbb{Q}}^{K}(\alpha)^2 \operatorname{disc}(\mathcal{O}_K),\end{aligned}$$

shows this. □

By uniqueness of the factorization of fractional ideals, the norm extends to a multiplicative homomorphism $\mathsf{N}\colon \mathcal{F}(\mathcal{O}_K) \to \mathbb{Q}^{\times}$, by setting
$$\mathsf{N}(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}) = \mathsf{N}(\mathfrak{p}_1)^{e_1} \cdots \mathsf{N}(\mathfrak{p}_r)^{e_r} \qquad \text{for } e_i \in \mathbb{Z}.$$

We can now prove the finiteness of the class group (and a little bit more).

Theorem 4.12. *If K is a number field, then the class group $\mathcal{C}(\mathcal{O}_K)$ is finite. Every ideal class has a representative $\mathfrak{a}$ with*

$$\mathsf{N}(\mathfrak{a}) \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|},$$

where $n = [K:\mathbb{Q}]$ and s is the number of pairs of complex conjugate embeddings.

Proof. We first show: for every $M > 0$, there exist only finitely many ideals $0 \ne \mathfrak{a} \subseteq \mathcal{O}_K$ with $\mathsf{N}(\mathfrak{a}) \le M$. Indeed, if $\mathcal{O}_K/\mathfrak{a}$ is an abelian group of cardinality $\le M$, then $M \cdot \mathcal{O}_K/\mathfrak{a} = 0$. Thus

$$M\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K.$$

However $\mathcal{O}_K/M\mathcal{O}_K$ is finite (because $\mathcal{O}_K$ is finitely generated free abelian), hence there are only finitely many possibilities for $\mathfrak{a}$.

It now suffices to show the claimed bound for $\mathsf{N}(\mathfrak{a})$. Let $[\mathfrak{a}_0] \in \mathcal{C}(\mathcal{O}_K)$ be some ideal class with $0 \ne \mathfrak{a}_0 \subseteq \mathcal{O}_K$ an ideal. Let $\alpha \in \mathcal{O}_K^\bullet$ be such that $\mathfrak{b} \coloneqq \alpha\mathfrak{a}_0^{-1} \subseteq \mathcal{O}_K$. By Theorem 4.9 there exists $0 \ne \beta \in \mathfrak{b}$ with

$$|\mathsf{N}_{\mathbb{Q}}^K(\beta)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(\mathfrak{b})|} = \underbrace{\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}}_{=:M}\,\mathsf{N}(\mathfrak{b})$$

Therefore

$$\mathsf{N}(\beta\mathfrak{b}^{-1}) = |\mathsf{N}_{\mathbb{Q}}^K(\beta)|\,\mathsf{N}(\mathfrak{b})^{-1} \le M.$$

However,

$$[\beta\mathfrak{b}^{-1}] = [\mathfrak{b}^{-1}] = [\mathfrak{a}_0] \in \mathcal{C}(\mathcal{O}_K),$$

so $\mathfrak{a} \coloneqq \beta\mathfrak{b}^{-1}$ is the claimed ideal. □

Definition 4.13. *The class number of $\mathcal{O}_K$ (and of K) is $h_K \coloneqq |\mathcal{C}(\mathcal{O}_K)|$.*

Example. (1) Let $K = \mathbb{Q}(\sqrt{-5})$. Then $n = 2$, $s = 1$, and $\operatorname{disc}(K) = -20$. The bound becomes

$$\frac{1}{2}\frac{4}{\pi}\sqrt{20} \approx 2.85.$$

The only ideal of norm 1 is $\mathcal{O}_K$. If $\mathfrak{a}$ is an ideal of norm 2, then $2 \cdot \mathcal{O}_K/\mathfrak{a} = 0$, so $\mathfrak{a}$ contains 2. Therefore $\mathfrak{a}$ divides (2) in the monoid of ideals of $\mathcal{O}_K$. However, we have already seen $(2) = \mathfrak{p}^2$ with $\mathfrak{p} = (2, 1+\sqrt{-5})$. Since no other ideals are possible, and $\mathfrak{p}$ is indeed non-principal (there are no elements of norm 2 in $\mathcal{O}_K$), we get

$$\mathcal{C}(\mathcal{O}_K) = \{[\mathcal{O}_K], [\mathfrak{p}]\}.$$

Hence $\mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$, the only group with two elements.

(2) Let $K = \mathbb{Q}(\zeta_5)$ with ζ_5 a primitive fifth root of unity. Then $n = 4$. There are two pairs of fifth roots of unity in $\mathbb{C}$ (none of them are real), so there are two pairs of complex embeddings,

that is $s = 2$. We also know $\operatorname{disc}(K) = 5^3$ (Lemma 2.52). The Minkowski constant works out to be $M \approx 1.7 < 2$. However the only ideal of norm 1 is $\mathcal{O}_K$ itself, which is principal. Hence $\mathcal{C}(\mathcal{O}_K)$ is trivial, and $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$ is a PID. □

For general number fields, this gives rise to an algorithm for computing $\mathcal{C}(\mathcal{O}_K)$: compute the (finitely many) ideals up to the Minkowski bound to obtain a generating set for the group. Then find the relations by checking which products are principal.

Remark 4.15. (1) Using the weaker bound (4.3), we could have gotten

$$\mathsf{N}(\mathfrak{a}) \le \left(\frac{2}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|},$$

in Theorem 4.12. However, from Stirling's formula, we know $n! \sim \sqrt{2\pi n}(n/e)^n$. The Minkowski constant

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sim \frac{\sqrt{2\pi n}}{e^n}\left(\frac{4}{\pi}\right)^s,$$

quickly becomes very small for large n. The extra effort in getting Minkowski's bound is worth it, to get a much more practical bound. For example, for $\mathbb{Q}(\zeta_5)$ we would have otherwise only gotten ≈ 4.53, and we would have had to start computing ideals!

(2) *Outlook:* The class group of a ring of algebraic integers is a finite abelian group, and it contains (essentially) all the information about the (multiplicative) arithmetic of $\mathcal{O}_K$. We have already seen that $\mathcal{C}(\mathcal{O}_K)$ is trivial if and only if $\mathcal{O}_K$ is a UFD. A classical theorem of Carlitz shows that the *length* of factorization is uniquely determined ($\mathcal{O}_K$ is half-factorial) if and only if $|\mathcal{C}(\mathcal{O}_K)| \le 2$. This can be taken as the starting point for the factorization theory of rings of algebraic integers, where one systematically reduces questions about factorizations in $\mathcal{O}_K$ to questions about similar questions in *monoid of zero-sum sequences* over the class group (these are essentially combinatorial objects defined in terms of $\mathcal{C}(\mathcal{O}_K)$).

4.4 Hermite–Minkowski: Discriminants of Number Fields

Straight from the definition we know $\operatorname{disc}(\mathbb{Q}) = 1$. It is however surprisingly non-trivial to observe that $|\operatorname{disc}(K)| > 1$ for any other number field!

Theorem 4.16 (Minkowski). *Let K be number field with $n = [K : \mathbb{Q}]$ and s pairs of complex conjugate embeddings. If $n \ge 2$, then*

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

and the bound goes to ∞ as $n \to \infty$.

In particular, the field of rational numbers $\mathbb{Q}$ is the unique number field with $|\operatorname{disc}(K)| = 1$.

Proof. Because $\operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}(K)$, there exists $\alpha \in \mathcal{O}_K^\bullet$ with

$$|\mathsf{N}^K(\alpha)| \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|},$$

by Theorem 4.9. Since $|\mathsf{N}^K(\alpha)| \ge 1$, this implies

$$|\operatorname{disc}(K)| \ge \left(\frac{\pi}{4}\right)^{2s}\left(\frac{n^n}{n!}\right)^2 \ge \left(\frac{\pi}{4}\right)^{n}\left(\frac{n^n}{n!}\right)^2 =: F(n). \tag{4.5}$$

Now $F(2) = \pi^2/4 > 2$ and

$$\frac{F(n+1)}{F(n)} = \frac{\pi}{4}\left(\frac{n+1}{n}\right)^{2n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \ge \frac{3\pi}{4} > 2.$$

(by Bernoulli's inequality). Hence $F(n)$ is increasing and so the right side of (4.5) is > 1 for $n \ge 2$. Note also $\lim_{n\to\infty} F(n) = \infty$ because of $F(n+1)/F(n) > 2$. □

Theorem 4.17 (Hermite). *For each $D > 0$ there exist only finitely many number fields K with $|\operatorname{disc}(K)| \le D$.*

Proof. Because the lower bound in Theorem 4.16 goes to ∞ as $n \to \infty$, the degree of such number fields must be bounded. It therefore suffices to show that there are only finitely many number fields K of a fixed degree n and discriminant $d = |\operatorname{disc}(K)|$. We may assume $n > 1$, as $\mathbb{Q}$ is the only number field of degree 1.

We also note the following: for every $M \ge 0$, there are only finitely many algebraic integers $\alpha \in \mathbb{C}$ of degree $\le n$, all of whose algebraic conjugates have absolute value $\le M$. (For such α, the coefficients and the degree of the minimal polynomial are bounded in terms of M and n. However, the coefficients are integers, so there are only finitely many possibilities.)

Now we first deal with fields K with $|\operatorname{disc}(K)| = d$, $n = [K : \mathbb{Q}]$, and K having at least one real embedding ($r > 0$). Applying Theorem 4.8 to $\mathcal{O}_K$, we can choose $\alpha \in \mathcal{O}_K^\bullet$ such that

$$|\sigma_1(\alpha)| < \sqrt{d} + 1, \quad |\sigma_i(\alpha)| < 1 \text{ for } 2 \le i \le n.$$

because $\sqrt{d} + 1 > (2/\pi)^s\sqrt{d}$. All conjugates $\sigma_i(\alpha)$ of α are bounded purely terms of d. Hence there are finitely many such $\alpha \in \mathbb{C}$ altogether.

To conclude, it will suffice to show $K = \mathbb{Q}(\alpha)$ for any such α. We have

$$|\sigma_1(\alpha)| = |\mathsf{N}^K(\alpha)| \cdot \prod_{i=2}^{n} |\sigma_i(\alpha)|^{-1} > |\mathsf{N}^K(\alpha)| \ge 1, \tag{4.6}$$

where the last inequality holds because $\mathsf{N}^K(\alpha) \in \mathbb{Z}$. So $|\sigma_1(\alpha)| > 1$ while $|\sigma_i(\alpha)| < 1$ for all $2 \le i \le n$. However, there exist precisely $[K : \mathbb{Q}(\alpha)]$ extensions of $\sigma_1|_{\mathbb{Q}(\alpha)} \in \operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{C})$ to

$\widetilde{\sigma_1} \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. For each of these $|\widetilde{\sigma_1}(\alpha)| = |\sigma_1(\alpha)| > 1$. So $\widetilde{\sigma_1} = \sigma_1$ and hence $[K : \mathbb{Q}(\alpha)] = 1$ and $K = \mathbb{Q}(\alpha)$.

In the second case, we deal with fields K all of whose embeddings are complex ($r = 0$). In that case $n = 2s$. Consider

$$X \coloneqq \{ (x_1, \dots, x_{2s})^T \in \mathbb{R}^{2s} : |x_1| < 1,\ |x_{s+1}| < 2\sqrt{d},\ x_i^2 + x_{i+s}^2 < 1 \text{ for } 2 \le i \le s \ \}.$$

Then $\mathrm{vol}(X) = 2 \cdot 2\sqrt{d} \cdot 2^{s-1} > 2^s \sqrt{d} = 2^{2s} \,\mathrm{vol}(j(\mathcal{O}_K)) = 2^n \,\mathrm{vol}(j(\mathcal{O}_K))$ (we used Proposition 4.7). By Theorem 4.5, there exists $0 \ne \alpha \in \mathcal{O}_K$ with $j(\alpha) \in X$. Then

$$|\mathrm{Re}(\sigma_1(\alpha))| < 1,\ |\mathrm{Im}(\sigma_1(\alpha))| < 2\sqrt{d}, \text{ and } |\sigma_i(\alpha)| < 1 \text{ for } 2 \le i \le n.$$

Also $|\sigma_1(\alpha)|$ is bounded in terms of d (because the real and imaginary part are), and we again get that there are only finitely many such $\alpha \in \mathbb{C}$. We again show $K = \mathbb{Q}(\alpha)$.

We have

$$|\sigma_1(\alpha)|^2 = |\mathsf{N}^K(\alpha)| \cdot \prod_{i=2}^{s} |\sigma_i(\alpha)|^{-2} > |\mathsf{N}^K(\alpha)| \ge 1,$$

and we again get $|\sigma_1(\alpha)| > 1$ while $|\sigma_i(\alpha)| < 1$ for all $2 \le i \le s$. Moreover, necessarily $\mathrm{Im}\,\sigma_1(\alpha) \ne 0$, because otherwise $|\sigma_1(\alpha)| = |\mathrm{Re}(\sigma_1(\alpha))| < 1$.

Now σ_1 and $\overline{\sigma_1}$ are the only two embeddings of K in $\mathbb{C}$ with $|\sigma_1(\alpha)| = |\overline{\sigma_1}(\alpha)| > 1$. Since $\mathrm{Im}(\sigma_1(\alpha)) = -\mathrm{Im}(\overline{\sigma_1}(\alpha)) \ne 0$, only one of them extends $\sigma|_{\mathbb{Q}(\alpha)} \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{C})$. Thus again $K = \mathbb{Q}(\alpha)$. □

Remark 4.18. A Pisot number is a real algebraic integer $\alpha > 1$ all of whose conjugates (other than itself) have absolute value < 1. The previous proof actually shows that every real algebraic number field (every number field $K \subseteq \mathbb{R}$) can be generated by a Pisot number.

4.5 Dirichlet's Unit Theorem

The last finiteness result we will obtain using Minkowski Theory is a structure theorem for $\mathcal{O}_K^\times$ as a multiplicative group.

For K a number field, let

$$\mu(K) \coloneqq \{ \zeta \in K : \zeta^m = 1 \text{ for some } m \ge 1 \},$$

denote the set of all roots of unity in K. Then $\mu(K) \subseteq \mathcal{O}_K^\times$.

Theorem 4.19 (Dirichlet's Unit Theorem). *Let K be a number field with r real and s pairs of complex conjugate embeddings. Then $\mu(K)$ is a finite cyclic group and*

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}.$$

Explicitly, there exist $\varepsilon_1, \dots, \varepsilon_{r+s-1} \in \mathcal{O}_K^\times$ such that every $\varepsilon \in \mathcal{O}_K^\times$ has a representation

$$\varepsilon = \zeta\varepsilon_1^{t_1} \cdots \varepsilon_{r+s-1}^{t_{r+s-1}},$$

with uniquely determined $\zeta \in \mu(K)$ and $t_1, \dots, t_{r+s-1} \in \mathbb{Z}$. A set $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ is a called a set of fundamental units for $\mathcal{O}_K$.

Up to now, we have dealt with the additive structure of $\mathcal{O}_K$ and used the additive embedding $K \to \mathbb{R}^n$ from Equation (4.2). As we are now interested in the multiplicative structure, we need a multiplicative version of this map. Recall that $\log\colon (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ is a group isomorphism. We define

$$\lambda\colon \mathcal{O}_K^\times \to \mathbb{R}^{r+s}, \quad \alpha \mapsto \big(\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \dots, 2\log|\sigma_{r+s}(\alpha)|\big)^T.$$

Then $\lambda(\alpha\beta) = \lambda(\alpha) + \lambda(\beta)$ for all $\alpha, \beta \in \mathcal{O}_K^\times$, so λ is a homomorphism from the multiplicative group $\mathcal{O}_K^\times$ to the additive group $\mathbb{R}^{r+s}$. If $\alpha \in \mathcal{O}_K$, then $\alpha \in \mathcal{O}_K^\times$ if and only if $|\mathsf{N}^K(\alpha)| = 1$ (by Lemma 2.36). Thus, if $\alpha \in \mathcal{O}_K^\times$, then

$$0 = \log|\mathsf{N}^K(\alpha)| = \log\left|\prod_{i=1}^r \sigma_i(\alpha) \prod_{i=1}^s \sigma_{r+i}(\alpha)^2\right| = \sum_{i=1}^r \log|\sigma_i(\alpha)| + 2\sum_{i=1}^s \log|\sigma_{r+i}(\alpha)|.$$

Therefore $\lambda(\mathcal{O}_K^\times) \subseteq H$ where H is the *Trace-Zero-Hyperplane* of $\mathbb{R}^{r+s}$, defined by the equation $x_1 + \dots + x_{r+s} = 0$.

Lemma 4.20. $\lambda(\mathcal{O}_K^\times)$ *is a lattice in* H *and therefore a free abelian group of rank* $\le r + s - 1$.

Proof. Clearly $\lambda(\mathcal{O}_K^\times)$ is a subgroup of H. By Proposition 4.3 it suffices to show that there is a neighborhood of 0 in H containing only finitely many points of $\lambda(\mathcal{O}_K^\times)$. Consider $B \coloneqq [-C, C]^{r+s} \subseteq \mathbb{R}^{r+s}$ for some $C > 0$. If $\lambda(\alpha) \in B$, then $\log|\sigma_i(\alpha)| \le C$ for all $1 \le i \le r + s$. Hence

$$|\mathrm{Re}(\sigma_i(\alpha))|, |\mathrm{Im}(\sigma_i(\alpha))| \le |\sigma_i(\alpha)| \le e^C.$$

It follows that $j(\lambda^{-1}(B)) \subseteq \mathbb{R}^n$ is bounded. Because $j(\mathcal{O}_K)$ is a lattice, therefore $j(\lambda^{-1}(B))$ is finite. Then $\lambda^{-1}(B)$ and hence $B \cap \lambda(\mathcal{O}_K)^\times$, are also finite. □

Lemma 4.21. $\ker(\lambda) = \mu(K)$, *and this is a finite cyclic group.*

Proof. If $\zeta \in \mathcal{O}_K^\times$ with $\zeta^m = 1$ then $\sigma_i(\zeta)^m = 1$ for all $1 \le i \le n$. Hence $|\sigma_i(\zeta^m)|^m = |\sigma_i(\zeta^m)| = 1$ and so $|\sigma_i(\zeta)| = 1$. Thus $\lambda(\zeta) = 0$. By definition, $\ker(\lambda)$ consists of all $\zeta \in \mathcal{O}_K$ for which $|\sigma_i(\zeta)| = 1$ for all $1 \le i \le n$. As in the previous proof, $\ker(\lambda)$ is finite. Hence, every element of $\ker(\lambda)$ has finite order and is thus a root of unity. We have shown $\ker(\lambda) = \mu(K)$ and that this group is finite.

That $\mu(K)$ is cyclic follows from the following general fact: If K is a field, and $G \le K^\times$ is a finite group, then G is cyclic (Exercise 3b of Exercise Set 6). For completeness, we recall a proof: by the Structure Theorem for Finite Abelian Groups, $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$ with $1 < n_1 | n_2 | \cdots | n_d$. Therefore every element of G is a root of the polynomial $X^{n_d} - 1 \in K[X]$. Since K is a field, this polynomial has at most n_d roots. Hence $|G| \leq n_d$, which forces $d = 1$ and $G \cong \mathbb{Z}/n_d\mathbb{Z}$. (Alternatively, prove that every finite subgroup of $S^1 \leq \mathbb{C}^\times$ is cyclic, by considering a root of unity of maximal order.) □

Proposition 4.22. *$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^t$ for some $t \leq r + s - 1$.*

Proof. We already know $\mathcal{O}_K^\times/\mu(K) \cong \mathbb{Z}^t$ for some $t \geq 0$. In other words, we have a short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mu(K) \arrow[r] & \mathcal{O}_K^\times \arrow[r, "\lambda"] & \mathbb{Z}^t \arrow[r] & 0. \end{tikzcd}$$

It is a general fact that this sequence splits, i.e., $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^t$, because the free module $\mathbb{Z}^t$ is projective. However, we are just going to show this by hand.

Let $e_1, \ldots, e_t$ denote the standard basis vectors for $\mathbb{Z}^t$. For each $1 \leq i \leq t$, let $\varepsilon_i \in \mathcal{O}_K^\times$ with $\lambda(\varepsilon_i) = e_i$. We can define a homomorphism $\varphi: \mathbb{Z}^t \to \mathcal{O}_K^\times$ by $\varphi(a_1, \cdots, a_t) = \varepsilon_1^{a_1} \cdots \varepsilon_t^{a_t}$. Then $\lambda \circ \varphi = \mathrm{id}_{\mathbb{Z}^t}$. In particular, the map φ is injective and $\varphi(\mathbb{Z}^t) \cong \mathbb{Z}^t$. We have to show $\mathcal{O}_K^\times = \mu(K)\varphi(\mathbb{Z}^t)$ and $\mu(K) \cap \varphi(\mathbb{Z}^t) = 1$.

For the first part, let $\eta \in \mathcal{O}_K^\times$, and set $\eta' \coloneqq \varphi(\lambda(\eta))$. Then $\lambda(\eta') = \lambda(\varphi(\lambda(\eta))) = \lambda(\eta) = 0$, so $\eta(\eta')^{-1} \in \ker(\lambda) = \mu(K)$. Thus $\eta = \zeta\eta'$ with $\zeta \in \mu(K)$. For the second part, suppose $\eta \in \mu(K) = \ker(\lambda)$ and $\eta = \varphi(x)$ for some $x \in \mathbb{Z}^t$. Then $0 = \lambda(\eta) = \lambda(\varphi(x)) = x$. So $\eta = \varphi(0) = 1$. □

The hard part of Dirichlet's Unit Theorem is showing equality in $t = r + s - 1$. We need a final lemma.

Lemma 4.23. *Let $M \in \mathbb{R}_{\geq 0}$. Up to associativity, there exist only finitely many elements $\alpha \in \mathcal{O}_K$ with $|\mathsf{N}^K(\alpha)| \leq M$.*

Proof. Two elements $\alpha, \beta \in \mathcal{O}_K$ are associated if and only if $\alpha = \beta\varepsilon$ with $\varepsilon \in \mathcal{O}_K^\times$ (by definition), and this is equivalent to $\alpha\mathcal{O}_K = \beta\mathcal{O}_K$. Because $\mathsf{N}(\alpha\mathcal{O}_K) = |\mathsf{N}^K(\alpha)|$, it suffices to show that there are only finitely many ideals of norm $\leq M$. But we already did that in the proof of Theorem 4.12. □

Proof (Proof of Theorem 4.19). From Proposition 4.22, we already know $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^t$ with $t \leq r + s - 1$. By Lemma 4.21, the group $\mu(K)$ cyclic. It remains to show $t = r + s - 1$. We will use Lemma 4.4, but work multiplicatively (that is, before applying the logarithms).

Let $g: \mathcal{O}_K^\times \to \mathbb{R}_{>0}^{r+s}$, $\varepsilon \mapsto (|\sigma_1(\varepsilon)|, \ldots, |\sigma_{r+s}(\varepsilon)|)$ and define $l: \mathbb{R}_{>0}^{r+s} \to \mathbb{R}^{r+s}$, $(x_1, \ldots, x_{r+s}) \mapsto (\log x_1, \ldots, \log x_r, 2\log x_{r+1}, \ldots, 2\log x_{r+s})$. Then $\lambda = l \circ g$. We also define $\|\cdot\|: \mathbb{R}_{>0}^{r+s} \to \mathbb{R}_{>0}$ by

$$\|(x_1, \ldots, x_{r+s})\| = \prod_{i=1}^{r} x_i \prod_{i=1}^{s} x_{r+i}^2.$$

Then $\|g(\varepsilon)\| = |\mathsf{N}^K(\varepsilon)| = 1$ for all $\varepsilon \in \mathcal{O}_K^\times$ and

$$S \coloneqq l^{-1}(H) = \{\, \mathbf{x} \in \mathbb{R}_{>0}^{r+s} : \|\mathbf{x}\| = 1 \,\}$$

is the *Norm-One-Surface.*

Claim: There exists a bounded set $T \subseteq S$ such that $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} g(\varepsilon)T$.

Proof of Claim: Choose $\mathbf{c} \coloneqq (c_1, \dots, c_{r+s}) \in \mathbb{R}_{>0}^{r+s}$ such that

$$\|\mathbf{c}\| > (2/\pi)^s \sqrt{|\mathrm{disc}(K)|}.$$

Define

$$X \coloneqq \{\, \mathbf{x} = (x_1, \dots, x_{r+s}) \in \mathbb{R}_{>0}^{r+s} : x_i \le c_i \,\}.$$

If $\mathbf{y} = (y_1, \dots, y_{r+s}) \in S$, then

$$\mathbf{y}X = \{\, \mathbf{x} = (x_1, \dots, x_{r+s}) \in \mathbb{R}_{>0}^{r+s} : x_i \le c_i y_i^{-1} \,\}.$$

However, $\|\mathbf{c}\mathbf{y}^{-1}\| = \|(c_1 y_1^{-1}, \dots, c_{r+s} y_{r+s}^{-1})\| = \|\mathbf{c}\|$. By Theorem 4.8, for each translate $\mathbf{y}X$, we can find an element $0 \ne \alpha \in \mathcal{O}_K$ with $g(\alpha) \in \mathbf{y}X$. For such α, then $|\mathsf{N}^K(\alpha)| \le \|\mathbf{c}\|$.

Up to associates, there are only finitely many $\alpha \in \mathcal{O}_K$ with $|\mathsf{N}^K(\alpha)| \le \|\mathbf{c}\|$ by Lemma 4.23. Choose a finite system of representatives α_1, …, $\alpha_m \in \mathcal{O}_K$.

We show that

$$T = S \cap \bigcup_{i=1}^{m} g(\alpha_i)^{-1} X$$

is as claimed. First, the set T is bounded because X, and therefore each of the finitely many translates $g(\alpha_i)^{-1}X$, is bounded. Now let $\mathbf{y} \in S$. Let $0 \ne \alpha \in \mathcal{O}_K$ and $\mathbf{x} \in X$ with $g(\alpha) = \mathbf{y}^{-1}\mathbf{x}$ and $|\mathsf{N}^K(\alpha)| \le \|\mathbf{c}\|$ (such an α exists by our argument above, applied to $\mathbf{y}^{-1}X$). Then there exists $1 \le i \le m$ such that $\alpha^{-1}\alpha_i \eqqcolon \varepsilon \in \mathcal{O}_K^\times$. Hence

$$\mathbf{y} = g(\alpha)^{-1}\mathbf{x} = g(\alpha_i \varepsilon^{-1})^{-1}\mathbf{x} = g(\varepsilon) g(\alpha_i)^{-1}\mathbf{x} \in g(\varepsilon)T.$$

(observe $\|g(\alpha_i)^{-1}\mathbf{x}\| = \|g(\alpha)\|^{-1}\|\mathbf{x}\| = \|\mathbf{y}\| = 1$). This proves the **Claim**.

For each $\mathbf{x} = (x_1, \dots, x_{r+s}) \in T$, we have that x_i is bounded from above. Because $T \subseteq S$, therefore there exists a bound $C > 0$ such that $x_i > C$ also from below. Hence $l(T) \subseteq H$ is bounded, and

$$H = l(S) = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} l(g(\varepsilon)T) = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} \lambda(\varepsilon) + l(T).$$

Hence $l(T)$ is a bounded system of representatives for $H/\lambda(\mathcal{O}_K^\times)$. □

Example. Let $d \in \mathbb{Z}$ be squarefree, and let $K = \mathbb{Q}(\sqrt{d})$. If $d < 0$, then $r = 0$, $s = 1$ (we say K is an imaginery quadratic field), so $\mathcal{O}_K^\times$ is finite. Explicitly,

$$|\mathcal{O}_K^\times| = \begin{cases} 4 & \text{if } d = -1, \\ 6 & \text{if } d = -3, \\ 2 & \text{otherwise.} \end{cases}$$

This can easily be seen by considering the (positive definite) norm equation $\mathsf{N}^K(\alpha) = 1$ for $\alpha \in \mathcal{O}_K$.

If $d > 1$, then $r = 2$, $s = 0$, and K is a real quadratic field. Now $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}$. The only roots of unity in $\mathbb{R}$ are ± 1, so $\mu(K) = \{\pm 1\}$. There are exactly four possible generators for the free part of the group (given any generator $\varepsilon \in \mathcal{O}_K^\times$, all of $\pm\varepsilon^{\pm 1}$ are generators). The unique generator ε with $\varepsilon > 1$ is called the fundamental unit of $\mathcal{O}_K$. One has

$$\mathcal{O}_K^\times = \{\pm 1\} \cdot \langle \varepsilon \rangle. \qquad \square$$

Remark 4.25. Let K be the real quadratic number field of discriminant $\Delta = \operatorname{disc}(K)$. Then the fundamental unit is of the form $\varepsilon = (a + b\sqrt{\Delta})/2$, with (a, b) the smallest solution in $\mathbb{N}^2$ of the *Pellian equation*

$$X^2 - \Delta Y^2 = \pm 4.$$

It is possible to find this solution from the continued fraction expansion of $\sqrt{\Delta}$ (which has a periodic continued fraction expansion), see [Koc00, Chapter 9.5] for details.

Chapter 5

Decomposition of Primes in Extensions

Let $K \subseteq L$ be number fields. Given an nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we can consider its extension $\mathfrak{a}\mathcal{O}_L = \{\sum_{i=1}^m \alpha_i\beta_i : \alpha_i \in \mathfrak{a}, \beta_i \in \mathcal{O}_L, m \geq 0\}$ to an ideal of $\mathcal{O}_L$. Since both $\mathfrak{a}$ and $\mathfrak{a}\mathcal{O}_L$ factor uniquely into prime ideals (in $\mathcal{O}_K$, respectively, in $\mathcal{O}_L$), we can ask how $\mathfrak{a}\mathcal{O}_L$ factors in terms of the factorization of $\mathfrak{a}$. Of course, it suffices to consider the case where $\mathfrak{a}$ is a prime ideal.

Example. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Then $\mathcal{O}_L = \mathbb{Z}[i]$ is Euclidean, and we have already determined all prime elements (and hence all prime ideals) in Proposition 2.6. We get $2\mathbb{Z}[i] = \mathfrak{P}^2$ with $\mathfrak{P} = (1+i)\mathbb{Z}[i]$. If $p \in \mathbb{P}$ with $p \equiv 1 \mod 4$, then there exist a, $b \in \mathbb{Z}$ with $a^2 + b^2 = p$ and we get

$$p\mathbb{Z}[i] = \mathfrak{Q}_1\mathfrak{Q}_2, \quad \text{with} \quad \mathfrak{Q}_1 = (a+bi)\mathbb{Z}[i],\ \mathfrak{Q}_2 = (a-bi)\mathbb{Z}[i],\ \mathfrak{Q}_1 \neq \mathfrak{Q}_2.$$

If $p \in \mathbb{P}$ with $p \equiv 3 \mod 4$, then p remains a prime element in $\mathbb{Z}[i]$, hence $p\mathbb{Z}[i]$ is itself a prime ideal. □

Lemma 5.2. *Let $K \subseteq L$ be number fields and let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$. Then*

$$\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L \quad \Leftrightarrow \quad \mathfrak{p} \subseteq \mathfrak{P} \quad \Leftrightarrow \quad \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}.$$

Proof. If $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, then $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}$. Suppose $\mathfrak{p} \subseteq \mathfrak{P}$. Then $\mathfrak{P} \cap \mathcal{O}_K$ is a proper ideal containing $\mathfrak{p}$, hence $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, because every nonzero prime ideal of $\mathcal{O}_K$ is maximal. Finally, suppose $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. Then $\mathfrak{p}\mathcal{O}_L \subseteq (\mathfrak{P} \cap \mathcal{O}_K)\mathcal{O}_L \subseteq \mathfrak{P}\mathcal{O}_L = \mathfrak{P}$. Hence $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. □

In the situation of the previous lemma, we say $\mathfrak{P}$ lies over $\mathfrak{p}$, and $\mathfrak{p}$ lies under $\mathfrak{P}$.

Lemma 5.3. *Let $K \subseteq L$ be number fields. Every $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ lies over a unique $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$.*

Proof. If $\mathfrak{p}$ lies under $\mathfrak{P}$, then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, so uniqueness is clear. Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be arbitrary. Define $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_K$. Then $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. We only have to show $0 \neq \mathfrak{p}$. However, by Lemma 3.2 we already know that $\mathfrak{p} \supseteq \mathfrak{p} \cap \mathbb{Z}$ contains a prime number $p \in \mathbb{P}$. □

Because $\mathcal{O}_K/\mathfrak{p}$ is finite (Lemma 3.2), trivially every $\mathfrak{p}$ lies under at most finitely many $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$. It is also true, and easy to see, that every nonzero prime ideal of $\mathcal{O}_K$ lies under at least one prime ideal of $\mathcal{O}_L$, that is, (prime) ideals do not become trivial when they are extended to $\mathcal{O}_L$. However, we will prove something much stronger in a moment (Theorem 5.6).

Suppose $\mathfrak{P}$ lies over $\mathfrak{p}$. We have a ring homomorphism $\mathcal{O}_K \hookrightarrow \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$. Its kernel is $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, giving an embedding of $\mathcal{O}_K/\mathfrak{p}$ into $\mathcal{O}_L/\mathfrak{P}$. Since both of these are finite fields (Lemma 3.2), we obtain a field extension of some finite degree $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$.

Definition 5.4. *Let $K \subseteq L$ be number fields. Let $\mathfrak{P} \subseteq \mathcal{P}(\mathcal{O}_L)$ and $\mathfrak{p} \coloneqq \mathfrak{P} \cap \mathcal{O}_L$.*

(1) *The field $\mathcal{O}_L/\mathfrak{P}$ is called the residue field of $\mathfrak{P}$.*

(2) *The degree $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ is called the inertia degree of $\mathfrak{P}$ and is denoted by $f = f(\mathfrak{P}|\mathfrak{p})$.*

(3) *The multiplicity $\mathsf{v}_{\mathfrak{P}}(\mathfrak{p}\mathcal{O}_L)$ is called the ramification index of $\mathfrak{P}$ and is denoted by $e = e(\mathfrak{P}|\mathfrak{p})$.*

Example. Consider again $L = \mathbb{Q}(i)$, $\mathcal{O}_L = \mathbb{Z}[i]$. Let $\mathfrak{P} = (1+i)\mathcal{O}_L$. Then $\mathcal{O}_L/\mathfrak{P} \cong \mathbb{F}_2$, hence $f(\mathfrak{P}|2\mathbb{Z}) = 1$ and $e(\mathfrak{P}|2\mathbb{Z}) = 2$. If $p \equiv 1 \mod 4$, and $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ are the two prime ideals above $p\mathbb{Z}[i]$, then $f(\mathfrak{Q}_i|p\mathbb{Z}) = 1 = e(\mathfrak{Q}_i|p\mathbb{Z})$. If $p \equiv 3 \mod 4$, then clearly $e(p\mathcal{O}_L|p\mathbb{Z}) = 1$. Because $\mathsf{N}^L(p) = p^2 = |\mathcal{O}_L/p\mathcal{O}_L|$, we must have $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_{p^2}$. Thus $f(p\mathcal{O}_L|p\mathbb{Z}) = 2$. □

By definition, if $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are the distinct primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$, then

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

with $e_i = e(\mathfrak{P}_i|\mathfrak{p})$. Bringing also the inertia degrees into the picture, we get the *fundamental equation.*

Theorem 5.6. *Let $K \subseteq L$ be number fields with $n = [L : K]$ and let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be the distinct prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Let $e_i \coloneqq e(\mathfrak{P}_i|\mathfrak{p})$ and $f_i = f(\mathfrak{P}_i|\mathfrak{p})$. Then*

$$\sum_{i=1}^{r} e_i f_i = n. \tag{5.1}$$

Proof. Let $\kappa \coloneqq \mathcal{O}_K/\mathfrak{p}$. We first show $\dim_\kappa \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$. To do so, let $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_L$ be representatives of a basis $\overline{\alpha_1}, \ldots, \overline{\alpha_m}$ of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ (over κ). We will show that $\alpha_1, \ldots, \alpha_m$ is a basis of L/K. Then $n = m$.

Suppose $\alpha_1, \ldots, \alpha_m$ are linearly dependent over K. By clearing denominators, we get $c_1, \ldots, c_m \in \mathcal{O}_K$, not all zero, such that $c_1\alpha_1 + \cdots + c_m\alpha_m = 0$. Consider the ideal $\mathfrak{c} \coloneqq \langle c_1, \ldots, c_m \rangle_{\mathcal{O}_K}$. Let $d \in \mathfrak{c}^{-1} \setminus \mathfrak{c}^{-1}\mathfrak{p}$. Then $\sum_{i=1}^m dc_i\alpha_i = 0$ with $dc_i \in \mathcal{O}_K$ for all $1 \le i \le m$, but $dc_i \notin \mathfrak{p}$ for some $1 \le i \le m$. Hence $\sum_{i=1}^m \overline{dc_i}\,\overline{\alpha_i} = \overline{0} \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a non-trivial linear dependence relation over κ, a contradiction.

We still have to show $L = \langle \alpha_1, \ldots, \alpha_m \rangle_K$. Consider the $\mathcal{O}_K$-module $M \coloneqq \langle \alpha_1, \ldots, \alpha_m \rangle_{\mathcal{O}_K}$, and the factor module $N = \mathcal{O}_L/M$. We have $\mathcal{O}_L = M + \mathfrak{p}\mathcal{O}_L$ (since the $\alpha_1, \ldots, \alpha_m$ span $\mathcal{O}_L/p\mathcal{O}_L$), and therefore $\mathfrak{p}N = N$. Since $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$-module, it is certainly also finitely generated as $\mathcal{O}_K$-module. But then so is the quotient N. Let β_1, …, $\beta_s \in N$ be generators of N over $\mathcal{O}_K$. Using $\mathfrak{p}N = N$, we can write

$$\beta_i = \sum_{j=1}^{s} c_{ij}\beta_j \quad \text{with } c_{ij} \in \mathfrak{p},\ 1 \leq i, j \leq s.$$

Let $C = (c_{ij})_{ij} \in M_s(\mathcal{O}_K)$, and consider $C - I$ with I the $s \times s$ identity matrix. Then $(C - I)(\beta_1, \dots, \beta_s)^T = 0$ by construction.

All but the diagonal entries of $C - I$ are in $\mathfrak{p}$, and the diagonal entries are congruent to -1 mod $\mathfrak{p}$. Hence $\det(C - I) \equiv (-1)^s \mod \mathfrak{p}$. In particular, we have $d \coloneqq \det(C - I) \neq 0$. Now

$$d(\beta_1, \dots, \beta_s)^T = \operatorname{adj}(C - I)(C - I)(\beta_1, \dots, \beta_s)^T = 0.$$

Thus $d\beta_i = 0$ for all $1 \leq i \leq s$. Since the β_i generate N, this means $dN = 0$. In other words, $d\mathcal{O}_L \subseteq M$. Hence $L = dL = d\langle \mathcal{O}_L \rangle_K \subseteq \langle M \rangle_K = \langle \alpha_1, \dots, \alpha_m \rangle_K$. We have therefore shown that α_1, …, α_m is a K-basis of L.

From $\dim_\kappa \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$ and the definitions of the ideal norm, we get

$$\mathsf{N}(\mathfrak{p}\mathcal{O}_L) = |\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L| = |\kappa|^{\dim_\kappa \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L} = \mathsf{N}(\mathfrak{p})^n.$$

On the other hand,

$$\mathsf{N}(\mathfrak{p})^n = \mathsf{N}(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{r} \mathsf{N}(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{r} \mathsf{N}(\mathfrak{p})^{f_i e_i}.$$

Comparing exponents, we have $n = \sum_{i=1}^{r} e_i f_i$. □

Let $K \subseteq L$ be number fields and let $\alpha \in \mathcal{O}_L$ be such that $L = K(\alpha)$. Then the ring $\mathcal{O}_K[\alpha]$ is a subring of $\mathcal{O}_L$. As an additive subgroup of the finitely generated free abelian group $\mathcal{O}_L$, it is itself finitely generated free abelian. Because $L = K(\alpha)$, the ring $\mathcal{O}_K[\alpha]$ contains a K-basis of L, hence its rank must be $[K : \mathbb{Q}]$. Therefore the quotient group $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ is finite, so there exists $0 \neq d \in \mathbb{Z}$ such that $d\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$. In particular,

$$\mathfrak{f} \coloneqq \left\{ \beta \in \mathcal{O}_L : \beta\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha] \right\}$$

is non-zero. The set $\mathfrak{f}$ is an ideal of both $\mathcal{O}_L$ and $\mathcal{O}_K[\alpha]$, in fact, it is the biggest set that is an ideal of both rings. One calls $\mathfrak{f}$ the conductor of $\mathcal{O}_K[\alpha]$ in $\mathcal{O}_L$.

Example. If $d \equiv 1 \mod 4$ is squarefree, then $\mathbb{Z}[\sqrt{d}] \subseteq \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathcal{O}_L$ has a non-trivial conductor dividing $2\mathcal{O}_L$. □

To be able to give a relative version of the next theorem we (finally) extend Lemma 2.15 to a relative version.

Lemma 5.8. *Let $K \subseteq L$ be number fields. If $\alpha \in \mathcal{O}_L$, then the minimal polynomial $g \in K[X]$ of α over K has its coefficients in $\mathcal{O}_K$.*

Proof. Let $n = [K(\alpha) : K]$, and let $\operatorname{Hom}_K(K(\alpha), \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$. Then $\sigma_i(\alpha)$ is an algebraic conjugate of α for all $1 \le i \le n$, and hence an algebraic integer (but not necessarily contained in L). The roots of g in $\mathbb{C}$ are $\{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$, and the coefficients of g can be expressed as symmetric functions of these roots. Hence the coefficients of g are algebraic integers, and also contained in K. Thus $g \in \mathcal{O}_K[X]$. □

The following gives us an explicit way of computing the decomposition of a prime ideal in an extension (with finitely many exceptions), by reducing the problem to factoring a polynomial over a finite field.

Theorem 5.9 (Dedekind-Kummer). *Let $K \subseteq L$ be number fields, let $\alpha \in \mathcal{O}_L$ with $L = K(\alpha)$ and let $\mathfrak{f}$ be the conductor of $\mathcal{O} := \mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L$. Let $g \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K. Suppose $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ is coprime to $\mathfrak{f} \cap \mathcal{O}_K$. Let $g_1, \dots, g_r \in \mathcal{O}_K[X]$ be monic polynomials, and $e_1, \dots, e_r \in \mathbb{N}$, such that*

$$\overline{g} = \overline{g_1}^{e_1} \cdots \overline{g_r}^{e_r} \in \mathcal{O}_K/\mathfrak{p}[X]$$

is the prime factorization of $\overline{g}$ in $\mathcal{O}_K/\mathfrak{p}[X]$.

For $1 \le i \le r$, let

$$\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L.$$

Then $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are the prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, their ramification indices are $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$, and their inertia degrees are $f(\mathfrak{P}_i|\mathfrak{p}) = \deg \overline{g_i}$.

Proof. Let $\kappa := \mathcal{O}_K/\mathfrak{p}$. We first establish ring isomorphisms

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \kappa[X]/(\overline{g}). \tag{5.2}$$

First Isomorphism. Consider $\varphi\colon \mathcal{O} \hookrightarrow \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. By coprimality of $\mathfrak{p}$ and $\mathfrak{f} \cap \mathcal{O}_K$, we have $\mathfrak{p} + (\mathfrak{f} \cap \mathcal{O}_K) = \mathcal{O}_K$, hence $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$. Because $\mathfrak{f} \subseteq \mathcal{O}$, we see that φ is surjective. Now $\ker(\varphi) = \mathcal{O} \cap \mathfrak{p}\mathcal{O}_L$, and we need to show $\mathcal{O} \cap \mathfrak{p}\mathcal{O}_L = \mathfrak{p}\mathcal{O}$. As before we get $\mathfrak{p}\mathcal{O} + \mathfrak{f} = \mathcal{O}$, hence

$$\mathcal{O} \cap \mathfrak{p}\mathcal{O}_L = (\mathfrak{p}\mathcal{O} + \mathfrak{f})(\mathcal{O} \cap \mathfrak{p}\mathcal{O}_L) \subseteq \mathfrak{p}\mathcal{O}.$$

Second Isomorphism. We have $\mathcal{O} = \mathcal{O}_K[\alpha] \cong \mathcal{O}_K[X]/(g)$. Hence

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \mathcal{O}_K[X]/(\mathfrak{p}, g) \cong (\mathcal{O}_K/\mathfrak{p})[X]/(\overline{g}) = \kappa[X]/(\overline{g}).$$

We have now established the isomorphisms in (5.2). By the Chinese Remainder Theorem,

$$\kappa[X]/(\overline{g}) \cong \kappa[X]/(\overline{g_1}^{e_1}) \times \cdots \times \kappa[X]/(\overline{g_r}^{e_r}).$$

The ideals of the ring $\kappa[X]/(\overline{g_i}^{e_i})$ are principal, generated by $\overline{g_i}^j$ for $0 \le j \le e_i$ (for instance, use that $\kappa[X]$ is a UFD). Thus $R := \kappa[x]/(\overline{g})$ has r maximal ideals $\mathfrak{m}_i$ $(1 \le i \le r)$, generated by

$$(\overline{1}, \dots, \overline{1}, \overline{g_i}, \overline{1}, \dots, \overline{1}).$$

Observe that $\dim_\kappa R/\mathfrak{m}_i = \dim_\kappa \kappa[X]/(\overline{g_i}) = \deg(\overline{g_i})$. Furthermore $\bigcap_{i=1}^r \mathfrak{m}_i^{e_i} = 0$.

These properties all lift back to $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ under the ring isomorphism: let $\overline{\mathfrak{P}_i}$ denote the preimage of $\mathfrak{m}_i$. Then $\dim_\kappa(\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/\overline{\mathfrak{P}_i} = \deg(\overline{g_i})$ and $\bigcap_{i=1}^r \overline{\mathfrak{P}_i}^{e_i} = 0$.

Now let $\mathfrak{P}_i$ be the preimage of $\overline{\mathfrak{P}_i}$ under the ring epimorphism $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$. Then $\mathfrak{P}_1$, …, $\mathfrak{P}_r$ are the maximal ideals containing $\mathfrak{p}\mathcal{O}_L$, and $f(\mathfrak{P}_i|\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P}_i : \kappa] = \deg(\overline{g_i}) =: f_i$. Now $\mathfrak{P}_i^{e_i}$ is the preimage of $\overline{\mathfrak{P}_i}^{e_i}$, because $|\{\overline{\mathfrak{P}_i}^j : 0 \le j \le e_i\}| = e_i + 1$. Therefore $\prod_{i=1}^r \mathfrak{P}_i^{e_i} = \bigcap_{i=1}^r \mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathcal{O}_L$, and so $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{m_1} \cdots \mathfrak{P}_r^{m_r}$ with $0 \le m_i \le e_i$. Because $n = \sum_{i=1}^r m_i f_i \le \sum_{i=1}^r e_i f_i = \deg(g) = n$ (crucially, using Theorem 5.6 for the first equality), we have $e_i = m_i$ for all $1 \le i \le r$. □

Definition 5.10. *Let $K \subseteq L$ be number fields, $n = [L : K]$, and let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ with $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ the factorization in $\mathcal{O}_L$. Let $f_i = f(\mathfrak{P}_i|\mathfrak{p})$ and $e_i = e(\mathfrak{P}_i|\mathfrak{p})$.*

(1) *$\mathfrak{p}$ is completely split (or totally split) if $r = n$, that is $e_i = f_i = 1$ for all i.*

(2) *$\mathfrak{p}$ is nonsplit if $r = 1$.*

(3) *$\mathfrak{p}$ is inert if $\mathfrak{p}\mathcal{O}_L$ is prime (that is, $r = 1 = e_1$, $f_1 = n$).*

(4) *$\mathfrak{P}_i$ is unramified (over K) if $e_i = 1$, and it is ramified if $e_i > 1$.*

(5) *$\mathfrak{P}_i$ is totally ramified (over K) if it is ramified and also $f_i = 1$.*

(6) *$\mathfrak{p}$ is unramified (in L) if all $\mathfrak{P}_i$ are unramified, and $\mathfrak{p}$ is ramified if at least one $\mathfrak{P}_i$ is ramified.*

Let $\sigma \in \mathrm{Gal}(L/K)$. Then σ maps algebraic integers to algebraic integers, so that $\sigma(\mathcal{O}_L) = O_L$. Therefore σ restricts to a ring automorphism of $\mathcal{O}_L$ that fixes $\mathcal{O}_K$ elementwise. In particular, if $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ and $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ lies over $\mathfrak{p}$, then $\sigma(\mathfrak{P})$ is a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$ as well. Thus, elements of the Galois group permute the prime ideals lying over $\mathfrak{p}$. (We will later see that if L/K is a Galois extension, then this action is even transitive.)

Theorem 5.11. *Let $K \subseteq L$ be number fields. If $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ is ramified in L and $p \in \mathbb{P}$ is such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, then $p \mid \mathrm{disc}(L)$. In particular, there are only finitely many $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ that are ramified in L.*

Proof. If $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ is ramified in L, then $\mathfrak{p} \cap \mathbb{Z}$ is ramified in L as well. There are only finitely many $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ over every $p \in \mathbb{P}$, so it suffices to deal with the case $K = \mathbb{Q}$.

Let $p \in \mathbb{P}$ and let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_L)$ be a prime lying over $p\mathbb{Z}$ such that $e := e(\mathfrak{p}|p\mathbb{Z}) > 1$. Let $p\mathcal{O}_L = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{a}$ an ideal of $\mathcal{O}_L$. Because $e > 1$, the ideal $\mathfrak{a}$ is contained in all prime ideals $\mathfrak{p} = \mathfrak{p}_1$, …, $\mathfrak{p}_r$ of $\mathcal{O}_L$ lying over $p\mathbb{Z}$.

Let α_1, …, α_n be an integral basis of $\mathcal{O}_L$, and let $\alpha \in \mathfrak{a} \setminus p\mathcal{O}_L$ (this is possible because $p\mathcal{O}_L \subsetneq \mathfrak{a}$). Then $\alpha \in \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$, but $\alpha \notin p\mathcal{O}_L$. Expressing $\alpha = c_1\alpha_1 + \dots + c_n\alpha_n$ with $c_i \in \mathbb{Z}$, we must therefore have $p \nmid c_i$ for some i. Say $p \nmid c_1$. Consider

$$A \coloneqq \langle \alpha, \alpha_2, \dots, \alpha_n \rangle_{\mathbb{Z}} = \langle c_1\alpha_1, \alpha_2, \dots, \alpha_n \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_L.$$

Then A is free abelian group of rank n, and

$$\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = |\mathcal{O}_L : A|^2 \operatorname{disc}(\mathcal{O}_L) = c_1^2 \operatorname{disc}(\mathcal{O}_L).$$

We have to show $p \mid \operatorname{disc}(\mathcal{O}_L)$. Because $p \nmid c_1$, it suffices to show $p \mid d \coloneqq \operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n)$.

Let $N \supseteq L$ be a finite extension such that $N \supseteq \mathbb{Q}$ is Galois. We can extend the $n = [L : \mathbb{Q}]$ embeddings of L into $\mathbb{C}$ to automorphisms σ_1, …, $\sigma_n \in \operatorname{Gal}(N/\mathbb{Q})$. If $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_N)$ lies over $p\mathbb{Z}$, then $\alpha \in \mathfrak{P}$, because $\mathfrak{P} \cap \mathcal{O}_L$ is a prime of $\mathcal{O}_L$ lying over $p\mathbb{Z}$, and hence $\alpha \in \mathfrak{P} \cap \mathcal{O}_L$. So α is contained in every prime ideal of $\mathcal{O}_N$ lying over $p\mathbb{Z}$.

Fix a $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_N)$ lying over $p\mathbb{Z}$. If $\sigma \in \operatorname{Gal}(N/\mathbb{Q})$, then $\sigma^{-1}(\mathfrak{P})$ is another prime ideal of $\mathcal{O}_N$ lying over $p\mathbb{Z}$. Hence $\alpha \in \sigma^{-1}(\mathfrak{P})$, and thus $\sigma(\alpha) \in \mathfrak{P}$ for all $\sigma \in \operatorname{Gal}(N/\mathbb{Q})$. Applying this to the σ_i, the definition of the discriminant shows $d \in \mathfrak{P}$. Then $d \in \mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, and so $p \mid d$. □

Remark 5.12. In fact, a prime $p \in \mathbb{P}$ is ramified in L *if and only if* $p \mid \operatorname{disc}(L)$, however, the converse is harder to show. If one introduces a suitable notion of a *relative discriminant* (which will then be an *ideal* of $\mathcal{O}_K$), a relative version of the previous theorem also holds (a prime ideal $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ is ramified in $\mathcal{O}_L$ if and only if it divides the relative discriminant).

5.1 Quadratic Fields and Quadratic Reciprocity

In a quadratic number field K, there are only three possibilities: a prime number p is either (totally) ramified (so $p\mathcal{O}_K = \mathfrak{p}^2$), completely split ($p\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{p} \neq \mathfrak{q}$), or inert ($p\mathcal{O}_K$ is prime). By Theorem 5.11, the ramified case is the exception.

Suppose $1 \neq d \in \mathbb{Z}$ is squarefree and let $K = \mathbb{Q}(\sqrt{d})$. The conductor $\mathfrak{f}$ of $\mathbb{Z}[\sqrt{d}]$ in $\mathcal{O}_K$ divides $2\mathcal{O}_K$, hence $\mathfrak{f} \cap \mathbb{Z} \in \{\mathbb{Z}, 2\mathbb{Z}\}$. For $p \in \mathbb{P} \setminus \{2\}$, therefore Theorem 5.9 can be applied with $\mathcal{O} = \mathbb{Z}[\sqrt{d}]$ and $g = X^2 - d$. It shows that $p \neq 2$ is

$$\begin{cases} \text{ramified if } p \mid d, \\ \text{split if } p \nmid d \text{ and } d \text{ is a square modulo } p, \\ \text{inert if } d \text{ is a non-square modulo } p. \end{cases}$$

More explicitly, and completely, we have

Theorem 5.13. *Let $K = \mathbb{Q}(\sqrt{d})$ with $1 \neq d \in \mathbb{Z}$ squarefree.*

(1) *Let $2 \neq p \in \mathbb{P}$. Then the prime factorization of $p\mathcal{O}_K$ is as follows.*

(*i*) *If $p \nmid d$ and $b \in \mathbb{Z}$ with $d \equiv b^2 \mod p$, then*

$$p\mathcal{O}_K = (p, \sqrt{d} + b) \cdot (p, \sqrt{d} - b).$$

(*ii*) *If d is a non-square modulo p, then $p\mathcal{O}_K$ is prime.*

(*iii*) *If $p \mid d$, then*

$$p\mathcal{O}_K = (p, \sqrt{d})^2.$$

(2) *For $p = 2$, the prime factorizations in $\mathcal{O}_K$ is*

$$2\mathcal{O}_K = \begin{cases} (2, \sqrt{d})^2 & \textit{if } 2 \mid d, \\ (2, 1 + \sqrt{d})^2 & \textit{if } d \equiv 3 \mod 4, \\ (2, \frac{1+\sqrt{d}}{2})(2, \frac{1-\sqrt{d}}{2}) & \textit{if } d \equiv 1 \mod 8, \\ 2\mathcal{O}_K & \textit{if } d \equiv 5 \mod 8. \end{cases}$$

Proof. First, let $p \neq 2$. We have already observed that the decomposition behavior then boils down to the factorization of $\overline{g} = X^2 - \overline{d}$ in $\mathbb{F}_p[X]$, by using Theorem 5.9. Suppose $p \nmid d$. If $d \equiv b^2 \mod p$, then $X^2 - \overline{d} = (X - \overline{b})(X + \overline{b}) \in \mathbb{F}_p[X]$. Because $p \neq 2$, the two roots are distinct. We lift $\overline{g_\pm} \coloneqq X \pm \overline{b}$ to $g_\pm \coloneqq X \pm b \in \mathbb{Z}[X]$ and the claim follows from Theorem 5.9. If d is a non-square modulo p, then $\overline{g}$ is irreducible, and $p\mathcal{O}_K$ is prime. If $d \equiv 0 \mod p$, then $X^2 - \overline{d} = X^2$, and $\overline{g_1} \coloneqq X \in \mathbb{F}_p[X]$ lifts to $g_1 \coloneqq X \in \mathbb{Z}[X]$.

Now let $p = 2$. If $d \equiv 2, 3 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and we can proceed as for the odd primes, by factoring $\overline{g} \coloneqq X^2 - \overline{d} \in \mathbb{F}_2[X]$. If $2 \mid d$, then $\overline{g} = X^2$, from which the claim is immediate. If d is odd ($d \equiv 3 \mod 4$), then

$$X^2 - \overline{d} = X^2 - \overline{1} = (X - \overline{1})(X + \overline{1}) = (X + \overline{1})^2 \in \mathbb{F}_2[X].$$

Now suppose $d \equiv 1 \mod 4$. Then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and we can apply Theorem 5.9 to this ring. The minimal polynomial of $\frac{1+\sqrt{d}}{2}$ is

$$g \coloneqq X^2 - X + \tfrac{1-d}{4} \in \mathbb{Z}[X].$$

Reducing modulo $2\mathbb{Z}$, we get

$$\frac{1-d}{4} \equiv \begin{cases} 0 \mod 2 & \text{if } d \equiv 1 \mod 8, \\ 1 \mod 2 & \text{if } d \equiv 5 \mod 8. \end{cases}$$

In the first case, we find $\overline{g} = X^2 - X = X(X - \overline{1}) \in \mathbb{F}_2[X]$, which gives the claim by substituting

$\frac{1+\sqrt{d}}{2}$ into X and $X-1 \in \mathbb{Z}[X]$. In the second case, the polynomial $X^2 - X + \overline{1} = X^2 + X + \overline{1} \in \mathbb{F}_2[X]$ is irreducible. □

For $a \in \mathbb{Z}$ and $p \in \mathbb{P}$, one also says that a is a quadratic residue modulo p if a is a square modulo p (i.e., there exists $b \in \mathbb{Z}$ such that $a \equiv b^2 \mod p$), and a is a quadratic non-residue otherwise. We define the Legendre symbol as

$$\left(\frac{a}{p}\right) \coloneqq \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

Obviously, $\left(\frac{a}{p}\right)$ only depends on the residue class of a modulo p, and by a slight abuse of notation we also consider it as a map $\mathbb{F}_p \to \{-1, 0, 1\}$. Determining the splitting of p in $\mathbb{Q}(\sqrt{d})$ for odd primes p boils down to the determination of the Legendre symbol $\left(\frac{d}{p}\right)$ by Theorem 5.13.

Let $p \in \mathbb{P} \setminus \{2\}$. Observe that $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\} \subseteq \mathbb{F}_p$ is a finite cyclic group of even order $p-1$. The squares

$$(\mathbb{F}_p^\times)^2 = \{\, a^2 : a \in \mathbb{F}_p^\times \,\},$$

are therefore the unique subgroup of index 2. Therefore a product of two non-squares is a square, so

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

In other words,

$$\mathbb{F}_p^\times \to \{\pm 1\},\ x \mapsto \left(\frac{x}{p}\right),$$

is a group homomorphism with kernel $(\mathbb{F}_p^\times)^2$. We also need the following.

Lemma 5.14. *Let $p \in \mathbb{P}$ be odd and $a \in \mathbb{Z}$. Then*

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

Proof. Because $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$, exactly half of the elements $c \in \mathbb{F}_p^\times$ satisfy $c^{\frac{p-1}{2}} = 1$, and the other half satisfy $c^{\frac{p-1}{2}} = -1$. If c is a square, then $c = b^2$ with $b \in \mathbb{F}_p^\times$, and hence $c^{\frac{p-1}{2}} = b^{p-1} = 1$. Since $(\mathbb{F}_p^\times)^2$ is a subgroup of index 2 of $\mathbb{F}_p^\times$, exactly half of the elements are squares. Then a non-square must necessarily belong to those $c \in \mathbb{F}_p^\times$ for which $c^{\frac{p-1}{2}} = -1$. □

Aside from the multiplicativity, Gauss's famous quadratic reciprocity law is essential to computing Legendre symbols.

Theorem 5.15 (Quadratic Reciprocity Law). *Let p and q be distinct odd primes. Then*

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

so

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ if } p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \quad \text{and} \quad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ if } p \equiv q \equiv 3 \mod 4.$$

Furthermore, one has the supplemental laws

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

and

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8, \\ -1 & \text{if } p \equiv \pm 5 \mod 8. \end{cases}$$

There are several hundred proofs and variations of proofs of this important theorem, see https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html for a list. We give a proof using Gauss sums, and will give a more conceptual one using the decomposition of primes in cyclotomic fields later.

Proof (of Theorem 5.15). We first dispense with the supplemental laws. The first law is immediate from Lemma 5.14.

For the second one, we compute in $\mathbb{Z}[i]$. Note

$$(1+i)^p = (1+i)\Big(\underbrace{(1+i)^2}_{=2i}\Big)^{\frac{p-1}{2}} = (1+i)2^{\frac{p-1}{2}}i^{\frac{p-1}{2}}.$$

Since $(1+i)^p \equiv 1 + i^p \mod p\mathbb{Z}[i]$ and using Lemma 5.14,

$$\left(\frac{2}{p}\right)(1+i)i^{\frac{p-1}{2}} \equiv 1 + i^p \equiv 1 + (-1)^{\frac{p-1}{2}}i \mod p\mathbb{Z}[i].$$

If $p \equiv 1 \mod 4$, we can multiply by $\overline{2}^{-1}(1-i)$ to cancel $1+i$, and get

$$\left(\frac{2}{p}\right)(-1)^{\frac{p-1}{4}} = 1, \qquad \text{so} \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}.$$

If $p \equiv 3 \mod 4$, the right side is $1 - i$. Multiplying by $\overline{2}^{-1}(1+i)$, we have

$$1 \equiv \left(\frac{2}{p}\right)i \cdot i^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right)(-1)i^{\frac{p-3}{2}} \equiv \left(\frac{2}{p}\right)(-1)(-1)^{\frac{p-3}{4}} \mod p\mathbb{Z}[i],$$

so

$$\left(\frac{2}{p}\right) = -(-1)^{\frac{p-3}{4}} = (-1)^{\frac{p+1}{4}}.$$

In the first case, $(p+1)/2$ is odd, and in the second $(p-1)/2$ is odd. Using

$$(p-1)/4 \cdot (p+1)/2 = (p+1)/4 \cdot (p-1)/2 = (p^2-1)/8,$$

we can therefore combine the cases to

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

We are left to show the quadratic reciprocity law itself. Let $\zeta = \zeta_p$ be a p-th primitive root of unity. We compute in $\mathbb{Z}[\zeta]$, and consider the *Gauss sum*

$$\tau := \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\zeta^a = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right)\zeta^j.$$

Our goal is to compute τ^q, and we first compute τ^2, with some intermediate steps. We check:

(1) $\sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) = 0$.

(2) $\sum_{a \in \mathbb{F}_p^\times} \zeta^{ab} = -1$ if $b \in \mathbb{F}_p^\times$.

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

(1) Because $(\mathbb{F}_p^\times)^2$ is a proper subgroup of $\mathbb{F}_p^\times$, there exists a non-square $c \in \mathbb{F}_p^\times$. Then $\left(\frac{c}{p}\right) = -1$, and we have

$$-\sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) = \left(\frac{c}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{ca}{p}\right) = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right).$$

Because of $p \neq 2$, this is only possible if $\sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) = 0$.

(2) Because $b \neq 0$, the element ζ^b is also a p-th primitive root of unity, and hence a root of

$$\frac{X^p - 1}{X - 1} = \sum_{j=0}^{p-1} X^j = 1 + \sum_{j=1}^{p-1} X^j.$$

(3) Note $\left(\frac{a}{p}\right) = \left(\frac{a^{-1}}{p}\right)$ for all $a \in \mathbb{F}_p^\times$. Therefore

$$\begin{aligned}\tau^2 &= \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\zeta^{a+b} = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\left(\frac{-b}{p}\right)\zeta^{a-b} = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\left(\frac{-b^{-1}}{p}\right)\zeta^{a-b} \\ &= \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab^{-1}}{p}\right)\left(\frac{-1}{p}\right)\zeta^{a-b} = \left(\frac{-1}{p}\right) \sum_{b,c \in \mathbb{F}_p^\times} \left(\frac{c}{p}\right)\zeta^{cb-b} = \left(\frac{-1}{p}\right)\left(\sum_{b \in \mathbb{F}_p^\times} 1 + \sum_{c \in \mathbb{F}_p^\times \setminus \{1\}} \left(\frac{c}{p}\right) \underbrace{\sum_{b \in \mathbb{F}_p^\times} \zeta^{(c-1)b}}_{=-1}\right) \\ &= \left(\frac{-1}{p}\right)\left((p-1) - \underbrace{\sum_{c \in \mathbb{F}_p^\times \setminus \{1\}} \left(\frac{c}{p}\right)}_{=-1}\right) = \left(\frac{-1}{p}\right)p.\end{aligned}$$

Finally, using that q is odd, and applying Lemma 5.14,

$$\tau^q = \tau(\tau^2)^{(q-1)/2} = \tau\left(\frac{-1}{p}\right)^{(q-1)/2} p^{(q-1)/2} \equiv \tau(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \mod q\mathbb{Z}[\zeta].$$

On the other hand

$$\tau^q \equiv \sum_{a\in\mathbb{F}_p^\times}\left(\frac{a}{p}\right)\zeta^{aq} = \left(\frac{q}{p}\right)\sum_{a\in\mathbb{F}_p^\times}\left(\frac{aq}{p}\right)\zeta^{aq} = \left(\frac{q}{p}\right)\sum_{b\in\mathbb{F}_p^\times}\left(\frac{b}{p}\right)\zeta^{b} = \left(\frac{q}{p}\right)\tau \mod q\mathbb{Z}[\zeta].$$

Equating the two expressions for τ^q, and multiplying by τ, we have

$$\left(\frac{-1}{p}\right)p\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv \left(\frac{-1}{p}\right)p(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \mod q\mathbb{Z}[\zeta].$$

The expressions on the left and right are actually integers, and so this is an equality in $\mathbb{Z}/q\mathbb{Z}$, where $\overline{p}$ is invertible. Cancelling p yields the claim. □

5.2 Cyclotomic Fields

If $K = \mathbb{Q}(\zeta)$ is a cyclotomic field with ζ an n-th root of unity, we already know $\mathcal{O}_K = \mathbb{Z}[\zeta]$ (Theorem 2.58). Let us consider the decomposition of primes. It is helpful to first consider the factorization of the cyclotomic polynomial Φ_m modulo p in the case $p \nmid m$.

Proposition 5.16. *Let $p \in \mathbb{P}$, $k \geq 1$, and $m \in \mathbb{N}$ with $p \nmid m$. Let*

$$f \coloneqq \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(\overline{p}) = \min\{\, l \in \mathbb{N} : p^l \equiv 1 \mod m \,\}.$$

(1) *If $\zeta \in \mathbb{F}_{p^k}$ is a primitive m-th root of unity, and $g \in \mathbb{F}_p[X]$ is its minimal polynomial, then $\mathbb{F}_{p^f} \cong \mathbb{F}_p[X]/(g) \cong \mathbb{F}_p(\zeta)$. In particular, $\deg(g) = f$.*

(2) *If $\Phi_m \in \mathbb{Z}[X]$ is the m-th cyclotomic polynomial, then*

$$\overline{\Phi_m} = \overline{g_1}\cdots\overline{g_r} \in \mathbb{F}_p[X]$$

with pairwise distinct monic irreducible polynomials $\overline{g_i} \in \mathbb{F}_p[X]$ and $\deg(\overline{g_i}) = f$ for all $1 \leq i \leq r$.

Proof. We refer to [Bre19, Chapter 7.6] for the basic theory of finite fields. In particular, for every prime power p^k, there exists, up to isomorphism, a unique finite field $\mathbb{F}_{p^k}$ of cardinality p^k. It is obtained as the splitting field of $X^{p^k} - X \in \mathbb{F}_p[X]$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Because $\mathbb{F}_{p^k}$ is a finite field, its multiplicative group $\mathbb{F}_{p^k}^\times$ is cyclic. If $\mathbb{F}_{p^l}$ and $\mathbb{F}_{p^k}$ are finite fields, then $\mathbb{F}_{p^k}$ contains a subfield isomorphic to $\mathbb{F}_{p^l}$ if and only if $l \mid k$, and this subfield is unique (so we identify it with $\mathbb{F}_{p^l}$).

(1) Because g is irreducible, the ring $\mathbb{F}_p[X]/(g) \cong \mathbb{F}_p(\zeta)$ is a (finite) field, and hence $\mathbb{F}_p[X]/(g) \cong \mathbb{F}_{p^k}$ for some $k \geq 1$. Since the multiplicative group $\mathbb{F}_{p^k}^\times$ is cyclic of order $p^k - 1$, it contains a primitive m-th root of unity (an element of order m) if and only if $m \mid p^k - 1$. Because f is the smallest such integer, we have $\mathbb{F}_{p^f} \subseteq \mathbb{F}_{p^k}$. The unique subfield of $\mathbb{F}_{p^k}$ of cardinality p^f is $\mathbb{F}_{p^f} \cong \{ x \in \mathbb{F}_{p^k} : x^{p^f} = x \}$. All primitive m-th roots of unity in $\mathbb{F}_{p^k}$ are already contained in $\mathbb{F}_{p^f}$ of $\mathbb{F}_{p^k}$, hence $\mathbb{F}_p[X]/(g) \cong \mathbb{F}_{p^f}$.

(2) We have $X^m - 1 = \prod_{l \mid m} \Phi_l \in \mathbb{Z}[X]$. Reducing modulo p, every m-th root of unity in $\mathbb{F}_{p^f}$ is a root of some $\overline{\Phi_l} \in \mathbb{F}_p[X]$ with $l \mid m$. Note that $\mathbb{F}_{p^f}$ contains $\phi(l) = \deg(\Phi_l)$ distinct primitive roots of unity of order l (if ω is a primitive m-th root of unity, then ω^k with $1 \leq k \leq m$ and $\gcd(k, m) = m/l$ are l distinct primitive l-th roots of unity). This is only possible if the roots of $\overline{\Phi_l}$ are precisely the $\phi(l)$ distinct primitive l-th roots of unity. In particular, the roots of $\overline{\Phi_m}$ are precisely the $\phi(m)$ primitive m-th roots of unity.

Thus, $\overline{\Phi_m} = \overline{g_1} \cdots \overline{g_r} \in \mathbb{F}_p[X]$ with pairwise non-associated irreducible $\overline{g_i}$, which we can take to be monic (repeated factors would mean repeated roots in $\mathbb{F}_{p^f}$). Each $\overline{g_i}$ is the minimal polynomial of a primitive m-th root of unity, and hence $\deg(\overline{g_i}) = f$ by (1). □

Theorem 5.17. *Let $p \in \mathbb{P}$ and let $n \in \mathbb{N}$. Let $v \coloneqq \mathsf{v}_p(n)$, let $m \coloneqq n/p^v$, and let*

$$f \coloneqq \operatorname{ord}_{(\mathbb{Z}/m\mathbb{Z})^\times}(\overline{p}) = \min\{ l \in \mathbb{N} : p^l \equiv 1 \mod m \}.$$

Then

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\phi(p^v)},$$

with distinct $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{P}(\mathcal{O}_K)$, all of which have inertia degree f. Here $\phi(p^v) = p^{v-1}(p-1)$ is the Euler-ϕ-function.

Proof. Because $\mathcal{O}_K = \mathbb{Z}[\zeta]$ by Theorem 2.58, the conductor is trivial, and we can apply Theorem 5.9 for all $p \in \mathbb{P}$. The minimal polynomial of ζ is the n-th cyclotomic polynomial $\Phi_n = \prod_{\zeta' \in \mu_n^*(\mathbb{C})} (X - \zeta') \in \mathbb{Z}[X]$, and we need to compute the prime factorization of $\overline{\Phi_n}$ modulo p, that is, over $\mathbb{F}_p$.

Note that $\mu_n^*(\mathbb{C}) = \{ \xi\omega : \xi \in \mu_{p^v}^*(\mathbb{C}),\ \omega \in \mu_m^*(\mathbb{C}) \}$. Hence

$$\Phi_n = \prod_{\substack{\xi \in \mu_{p^v}^*(\mathbb{C}) \\ \omega \in \mu_m^*(\mathbb{C})}} (X - \xi\omega) \in \mathcal{O}_K[X].$$

It holds that $X^{p^v} - 1 \equiv (X-1)^{p^v} \mod p$. If $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ with $\mathfrak{p} \mid p\mathcal{O}_K$ and $\xi \in \mu_{p^v}^*(\mathbb{C})$, we conclude $(\xi - 1)^{p^v} \equiv \xi^{p^v} - 1 \equiv 0 \mod \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this means $\xi \equiv 1 \mod \mathfrak{p}$. We can therefore compute

$$\Phi_n \equiv \prod_{\omega \in \mu_m^*(\mathbb{C})} (X - \omega)^{\phi(p^v)} \equiv \Phi_m^{\phi(p^v)} \mod \mathfrak{p}\mathcal{O}_K[X].$$

Since the leftmost and rightmost side are in $\mathbb{Z}[X]$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, we even get $\Phi_n \equiv \Phi_m^{\phi(p^v)} \mod p\mathbb{Z}[X]$. By (2) of Proposition 5.16, the polynomial Φ_m factors into r distinct irreducible polynomials modulo p, each of degree f. The claim follows from Theorem 5.9. □

We record the following special cases.

Corollary 5.18. (1) *$p \neq 2$ is completely split if and only if $p \equiv 1 \mod n$.*

(2) *$p \in \mathbb{P}$ is ramified if and only if $p \mid n$, except when $p = 2 = \gcd(4, n)$ (then it is unramified).*

Chapter 6

Hilbert Theory: Decomposition of Primes in Galois Extensions

In this section, we use a bit more field theory than we have needed so far. We refer to [Bre19, Chapter 7] for background, but recall the main results. Let L/K be a finite field extension, and let $\mathrm{Gal}(L/K)$ be the group of all automorphisms of L that fix K elementwise. Then $|\mathrm{Gal}(L/K)| \le [L:K]$. The extension L/K is a Galois extension if and only if $|\mathrm{Gal}(L/K)| = [L:K]$.

Suppose L/K is Galois. The *Fundamental Theorem of Galois Theory* [Bre19, Theorem 7.148] gives an inclusion-reversing bijection between intermediate fields of L/K and subgroups of G. Explicitly

$$\begin{array}{rcr} \{\,\text{intermediate fields of } L/K\,\} & \longleftrightarrow & \{\,\text{subgroups of } G\,\} \\ M & \longmapsto & \mathrm{Gal}(L/M), \\ L^H & \longmapsfrom & H, \end{array}$$

where $L^H = \{\, x \in L : \sigma(x) = x \text{ for all } \sigma \in H \,\}$ is the fixed field of H. For all intermediate fields $M = L^H$ with $H = \mathrm{Gal}(L/M)$:

- L/M is a Galois extension of degree $|H|$.
- M/K has degree $|G|/|H| = |G:H|$. Furthermore, M/K is Galois if and only if H is a normal subgroup of G.

We illustrate this in the context of finite fields (as we will need them later on). For every prime $p \in \mathbb{P}$ and every $n \ge 1$, there exists a finite field $\mathbb{F}_{p^n}$ of cardinality p^n, unique up to isomorphism. Such a field can be constructed as a splitting field of $X^{p^n} - X \in \mathbb{F}_p[X]$ over $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ [Bre19, Chapter 7.6].

Proposition 6.1. *Let $p \in \mathbb{P}$ and $n \ge 1$.*

(1) *The map $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ satisfying $\varphi(x) = x^p$ is an automorphism, called the Frobenius*

automorphism of $\mathbb{F}_{p^n}/\mathbb{F}_p$.

(2) $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *is a cyclic group of order* n*, generated by* φ.

(3) *For every* $m \mid n$*, there exists a unique subfield of* $\mathbb{F}_{p^n}$ *of cardinality* p^m*. Identifying this field with* $\mathbb{F}_{p^m}$*, we get* $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^{m'}}$ *if and only if* $m \mid m'$.

(4) *Every extension of finite fields* $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ *is Galois, with cyclic Galois group generated by* φ^m.

Proof. (1) Because the characteristic of $\mathbb{F}_{p^n}$ is p, we have $(x+y)^p = x^p + y^p$, and thus φ is indeed an automorphism.

(2) As a finite subgroup of the multiplicative group of a field, the group $\mathbb{F}_{p^n}^\times$ is cyclic of order $p^n - 1$. Let ω be a generator. Then $\varphi^l(\omega) = \omega^{p^l}$. Hence the order of φ in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is n. However, $p^n = |\mathbb{F}_{p^n}| = \mathbb{F}_p^{[\mathbb{F}_{p^n}:\mathbb{F}_p]}$ shows $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Hence φ generates $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

(3) This is now an immediate consequence of $\mathbb{Z}/n\mathbb{Z}$ having exactly one subgroup of order n/d for each $d \mid n$, together with the Fundamental Theorem of Galois Theory.

(4) Let $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ with $m \mid n$. Then $\mathbb{F}_{p^m}$ is the fixed field of φ^m with φ the Frobenius automorphism of $\mathbb{F}_{p^n}/\mathbb{F}_p$, and hence the extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ is Galois with the claimed Galois group. □

Throughout this chapter, let $K \subseteq L$ *be number fields and suppose that the relative extension* L/K *is a* Galois extension.

In this context, this just means that every $\sigma \in \mathrm{Hom}_K(L, \mathbb{C})$ has its image in L, and hence

$$G := \mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, \mathbb{C}),$$

is a finite group of order $n = [L : K]$.

We have already seen that an automorphism $\sigma \in \mathrm{Gal}(L/K)$ maps $\mathcal{O}_L$ to itself, and fixes $\mathcal{O}_K$ elementwise. As a consequence, we saw that σ permutes the prime ideals $\mathfrak{P} \subseteq \mathcal{O}_L$ lying over a given $\mathfrak{p} \subseteq \mathcal{O}_K$.

Lemma 6.2. *Let* $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$*. The action of* $\mathrm{Gal}(L/K)$ *on* $\{\, \mathfrak{P} \in \mathcal{P}(\mathcal{O}_L) : \mathfrak{P} \mid \mathfrak{p} \,\}$ *is transitive.*

Proof. We have to show: for all $\mathfrak{P}$, $\mathfrak{P}' \in \mathcal{P}(\mathcal{O}_L)$ with $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \sigma(\mathfrak{P}')$. Suppose that there exist $\mathfrak{P}$, $\mathfrak{P}'$ lying over $\mathfrak{p}$, such that $\mathfrak{P}'$ is not in the $\mathrm{Gal}(L/K)$-orbit of $\mathfrak{P}$. Then $\mathfrak{P}'$ is comaximal to each of $\{\, \sigma(\mathfrak{P}) : \sigma \in \mathrm{Gal}(L/K) \,\}$. By the Chinese Remainder Theorem, there exists $\alpha \in \mathcal{O}_L$ such that

$$\alpha \equiv 0 \mod \mathfrak{P}' \qquad \text{and} \qquad \alpha \equiv 1 \mod \sigma^{-1}(\mathfrak{P}) \quad \text{for all } \sigma \in \mathrm{Gal}(L/K).$$

Then $\mathsf{N}_K^L(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$ from the first congruence. On the other hand, the second set of congruences implies $\sigma(\alpha) \notin \mathfrak{P}$ for all $\sigma \in \mathrm{Gal}(L/K)$. Hence $\mathsf{N}_K^L(\alpha) \notin \mathfrak{P}$ (because $\mathfrak{P}$ is prime), a contraction to $\alpha \in \mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. □

In a Galois extension, the prime decomposition therefore takes a particularly symmetric form.

Proposition 6.3. *Let* $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ *and let* $\mathfrak{P}$, $\mathfrak{P}' \mid \mathfrak{p}$. *Then*

(1) $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}'|\mathfrak{p})$.

(2) $\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_L/\mathfrak{P}'$ *as* $\mathcal{O}_K/\mathfrak{p}$*-algebras and* $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p})$.

In particular,

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e \qquad \textit{and} \qquad efr = n,$$

with $f = f(\mathfrak{P}_i|\mathfrak{p})$.

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Suppose $\mathfrak{P} = \mathfrak{P}_1$ and $\mathfrak{P}' = \mathfrak{P}_i$ for some $1 \le i \le r$. Let $\sigma \in \operatorname{Gal}(L/K)$ be such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$ (using Lemma 6.2). Then

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r} = \mathfrak{P}_i^{e_1} \sigma(\mathfrak{P}_2)^{e_2} \cdots \sigma(\mathfrak{P}_r)^{e_r}.$$

So $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}'|\mathfrak{p})$.

The automomorphism σ induces a homomorphism $\mathcal{O}_L \to \mathcal{O}_L/\sigma(\mathfrak{P})$, $x \mapsto \sigma(x) + \sigma(\mathfrak{P})$ with kernel $\mathfrak{P}$. Hence $\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_L/\mathfrak{P}'$ and $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}'|\mathfrak{p})$.

The decomposition of $\mathfrak{p}\mathcal{O}_L$ is now clear, and $efr = n$ follows from Theorem 5.6 and $e_1 = \cdots = e_r = e$ and $f_1 = \cdots = f_r = f$. □

Definition 6.4. *Let* $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ *and let* $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ *with* $\mathfrak{P} \mid \mathfrak{p}$. *The group*

$$D(\mathfrak{P}) := \{ \sigma \in \operatorname{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P} \}$$

is the decomposition group *of* $\mathfrak{P}$, *and the fixed field* $L^{D(\mathfrak{P})}$ *is the* decomposition field *of* $\mathfrak{P}$.

Note that the decomposition group is the stabilizer of $\mathfrak{P}$ under the group action of $\operatorname{Gal}(L/K)$ on the r primes lying above $\mathfrak{p}$. Since this action is transitive, the orbit-stabilizer theorem implies

$$|G : D(\mathfrak{P})| = r = [L^{D(\mathfrak{P})} : K].$$

In particular, $\mathfrak{p}$ is non-split if and only if $D(\mathfrak{P}) = G$ (hence $L^{D(\mathfrak{P})} = K$), and it is completely split if and only if $D(\mathfrak{P}) = 1$ (hence $L^{D(\mathfrak{P})} = L$).

If $\mathfrak{P}' \mid \mathfrak{p}$ and $\sigma(\mathfrak{P}) = \mathfrak{P}'$, then $D(\mathfrak{P}') = \sigma D(\mathfrak{p})\sigma^{-1}$ is a conjugate subgroup. Indeed, for $\tau \in G$,

$$\tau(\mathfrak{P}') = \mathfrak{P}' \iff \tau\sigma(\mathfrak{P}) = \sigma(\mathfrak{P}) \iff \sigma^{-1}\tau\sigma(\mathfrak{P}) = \mathfrak{P} \iff \sigma^{-1}\tau\sigma \in D(\mathfrak{P}) \iff \tau \in \sigma D(\mathfrak{P})\sigma^{-1}.$$

Every $\sigma \in D(\mathfrak{P})$ induces an automorphism of residue fields

$$\overline{\sigma} \colon \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}, \; \alpha + \mathfrak{P} \mapsto \sigma(\alpha) + \sigma(\mathfrak{P}) = \sigma(\alpha) + \mathfrak{P},$$

that fixes $\mathcal{O}_K/\mathfrak{p}$ elementwise. Set $\kappa(\mathfrak{P}) \coloneqq \mathcal{O}_L/\mathfrak{P}$ and $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. Then

$$D(\mathfrak{P}) \to \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})), \ \sigma \mapsto \overline{\sigma}$$

is a group homomorphism.

Proposition 6.5. *Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \mid \mathfrak{p}$. The homomorphism $D(\mathfrak{P}) \to \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is surjective.*

Proof. Let $\alpha \in \mathcal{O}_L$ be such that $\overline{\alpha} \in \kappa(\mathfrak{P})$ is a primitive element for the field extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$. Using the Chinese Remainder Theorem, we can also assume $\alpha \equiv 0 \mod \sigma^{-1}(\mathfrak{P})$ for all $\sigma \in G \setminus D(\mathfrak{P})$. This ensures $\sigma(\alpha) \in \mathfrak{P}$ for all $\sigma \in G \setminus D(\mathfrak{P})$.

Let $\overline{g} \in \kappa(\mathfrak{p})[X]$ be the minimal polynomial of $\overline{\alpha}$, and let $h \in \mathcal{O}_L[X]$ be the minimal polynomial of α. Then $\overline{g} \mid \overline{h}$. Because L/K is Galois, the irreducible polynomial h splits into linear factors, explicitly

$$h = (X - \sigma_1(\alpha))\cdots(X - \sigma_m(\alpha)) \in \mathcal{O}_L[X],$$

where $\sigma_1, \ldots, \sigma_m \in \operatorname{Gal}(L/K)$ represent extensions of the distinct $\operatorname{Hom}_K(K(\alpha), \mathbb{C})$.

Let $\tau \in \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Then $\overline{g}(\tau(\overline{\alpha})) = \tau(\overline{g}(\overline{\alpha})) = 0$. Hence $\tau(\overline{\alpha})$ is a root of $\overline{g}$, and thus also of $\overline{h}$. This means $\tau(\overline{\alpha}) = \overline{\sigma_i(\alpha)}$ for some $1 \leq i \leq m$. Since $0 \neq \tau(\overline{\alpha})$, necessarily $\sigma_i(\alpha) \notin \mathfrak{P}$. Therefore, the choice of α ensures $\sigma_i \in D(\mathfrak{P})$, and we find $\tau = \overline{\sigma_i}$. □

Definition 6.6. *Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \mid \mathfrak{p}$. The group*

$$I(\mathfrak{P}) \coloneqq \ker\big(D(\mathfrak{P}) \to \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))\big) = \{\, \sigma \in G : \sigma(\alpha) - \alpha \in \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L \,\},$$

is the inertia group of $\mathfrak{P}$. Its fixed field $L^{I(\mathfrak{P})}$ is the inertia field of $\mathfrak{P}$.

We have subgroups $1 \leq I(\mathfrak{P}) \leq D(\mathfrak{P}) \leq G$ and corresponding field extensions $K \subseteq L^{D(\mathfrak{P})} \subseteq L^{I(\mathfrak{P})} \subseteq L$.

Theorem 6.7. *Let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ such that $\mathfrak{P} \mid \mathfrak{p}$. Let $f = f(\mathfrak{P}|\mathfrak{p})$, $e = e(\mathfrak{P}|\mathfrak{p})$, and let r be the number of primes in $\mathcal{O}_L$ lying above $\mathfrak{p}$. Let $\mathfrak{P}_I \coloneqq \mathfrak{P} \cap \mathcal{O}_{L^{I(\mathfrak{P})}}$ and $\mathfrak{P}_D \coloneqq \mathfrak{P} \cap \mathcal{O}_{L^{D(\mathfrak{P})}}$.*

(1) *$L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}$ is a Galois extension with $\operatorname{Gal}(L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}) \cong \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$,*

$$|I(\mathfrak{P})| = [L : L^{I(\mathfrak{P})}] = e, \quad \text{and} \quad |D(\mathfrak{P}) : I(\mathfrak{P})| = [L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}] = f.$$

(2) *$e(\mathfrak{P}_D|\mathfrak{p}) = f(\mathfrak{P}_D|\mathfrak{p}) = 1$.*

(3) *$e(\mathfrak{P}_I|\mathfrak{P}_D) = 1$ and $f(\mathfrak{P}_I|\mathfrak{P}_D) = f$; the ideal $\mathfrak{P}_D$ is nonsplit in L.*

(4) *$e(\mathfrak{P}|\mathfrak{P}_I) = e$ and $f(\mathfrak{P}|\mathfrak{P}_I) = 1$; the ideal $\mathfrak{P}_I$ is nonsplit in L.*

Proof. (1) By construction as a fixed field, the extension $L/L^{D(\mathfrak{P})}$ is Galois with $\mathrm{Gal}(L/L^{D(\mathfrak{P})}) = D(\mathfrak{P})$. By Proposition 6.5, the map $D(\mathfrak{P}) \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is a group epimorphism with kernel $I(\mathfrak{P})$. Thus $I(\mathfrak{P})$ is a normal subgroup of $D(\mathfrak{P})$. By Galois theory, therefore $L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}$ is a Galois extension with Galois group isomorphic to $D(\mathfrak{P})/I(\mathfrak{P}) \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. We have $efr = n = [L : K]$ and $|G : D(\mathfrak{P})| = r$, because $D(\mathfrak{P})$ is the stabilizer of the action of G on the primes above $\mathfrak{p}$. Hence $|D(\mathfrak{P})| = ef$. Now $|D(\mathfrak{P}) : I(\mathfrak{P})| = |\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))| = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f$ because extensions of finite fields are Galois Proposition 6.1, and hence $|I(\mathfrak{P})| = e$.

This shows (1). For the remaining claims, first note

$$e = e(\mathfrak{P}|\mathfrak{P}_I)\, e(\mathfrak{P}_I|\mathfrak{P}_D)\, e(\mathfrak{P}_D|\mathfrak{p}) \qquad \text{and} \qquad f = f(\mathfrak{P}|\mathfrak{P}_I)\, f(\mathfrak{P}_I|\mathfrak{P}_D)\, f(\mathfrak{P}_D|\mathfrak{p}). \tag{6.1}$$

Since the Galois group of $L/L^{D(\mathfrak{P})}$, which is $D(\mathfrak{P})$, fixes $\mathfrak{P}$ by construction, the ideal $\mathfrak{P}_D$ is nonsplit in L. From the fundamental equation applied to $L/L^{D(\mathfrak{P})}$, it then follows that

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

Comparing with (6.1), therefore $e(\mathfrak{P}_D|\mathfrak{p}) = f(\mathfrak{P}_D|\mathfrak{p}) = 1$, showing (2).

(3) and (4): The inertia group of $\mathfrak{P}_D$ in $L/L^{D(\mathfrak{P})}$ is $I(\mathfrak{P})$ as well. Applying Proposition 6.5 to the extension $L^{I(\mathfrak{P})}/L^{D(\mathfrak{P})}$ shows

$$f(\mathfrak{P}_I|\mathfrak{P}_D) = |\mathrm{Gal}(\kappa(\mathfrak{P}_I)/\kappa(\mathfrak{P}_D))| = |D(\mathfrak{P}) : I(\mathfrak{P})| = f.$$

Since this also equals $[L^{I(\mathfrak{P})} : L^{D(\mathfrak{P})}]$, the fundamental equation shows that $\mathfrak{P}_D$ is nonsplit and unramified in $L^{I(\mathfrak{P})}$. Now (6.1) necessates $e(\mathfrak{P}|\mathfrak{P}_I) = e$ and $f(\mathfrak{P}|\mathfrak{P}_I) = 1$. Since $[L : L^{I(\mathfrak{P})}] = e$, another application of the fundamental equation shows that $\mathfrak{P}_I$ is nonsplit in L.

The ideal $\mathfrak{P}_D$ is nonsplit in $L^{I(\mathfrak{P})}$, and $\mathfrak{P}_I$ is the unique prime ideal in $L^{I(\mathfrak{P})}$ lying over $\mathfrak{P}_D$. The ideal $\mathfrak{P}_I$ is itself nonsplit in L, so $\mathfrak{P}_D$ is nonsplit in L. □

To summarize, we have the following ramification indices and inertia degrees,

$$\begin{tikzcd}
L \arrow[d, dash, "e"', "1"] \\
L^{I(\mathfrak{P})} \arrow[d, dash, "1"', "f"] \\
L^{D(\mathfrak{P})} \arrow[d, dash, "1"', "1"] \\
K,
\end{tikzcd}$$

with the degrees of the field extensions (from top to bottom) being e, f, and r. In particular, $\mathfrak{P}$

is unramified if and only if $|I(\mathfrak{P})| = 1$.

6.1 Second Proof of Quadratic Reciprocity

We can now give a more conceptual proof of the quadratic reciprocity law (Theorem 5.15). We take the supplemental laws for granted because they are elementary to prove anyway.

Lemma 6.8. *Let $p \in \mathbb{P} \smallsetminus \{2\}$ and let $\zeta \in \mu_p^*(\mathbb{C})$. The unique quadratic subfield of $\mathbb{Q}(\zeta)$ is $\mathbb{Q}(\sqrt{p^*})$ with $p^* \coloneqq (-1)^{(p-1)/2}p$.*

Proof. Because $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois with cyclic Galois group by Proposition 2.26, there exists a unique quadratic subfield L, corresponding to the unique subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ of index 2. By Theorem 5.17, the prime p is the unique prime that is ramified in $\mathbb{Q}(\zeta)$. Hence also in K, only p can be ramified. By Theorem 5.13, this means $K = \mathbb{Q}(\sqrt{\varepsilon p})$ with $\varepsilon = \pm 1$ chosen such that $\varepsilon p \equiv 1 \mod 4$. This is accomplished with $\varepsilon = (-1)^{(p-1)/2}$. □

Another way to prove Lemma 6.8, is to observe that, for the Gauss sum $\tau \in \mathbb{Z}[\zeta]$ that we already computed, we have $\tau^2 = p^*$, so $\mathbb{Q}(\sqrt{p^*}) = \mathbb{Q}(\tau) \subseteq \mathbb{Q}(\zeta)$.

Theorem 6.9. *Let $p \in \mathbb{P} \smallsetminus \{2\}$, let $\zeta \in \mu_p^*(\mathbb{C})$, and $p^* = (-1)^{(p-1)/2}p$. Then $q \in \mathbb{P}$ splits in $\mathbb{Q}(\sqrt{p^*})$ if and only if q lies under an even number of prime ideals in $\mathbb{Q}(\zeta)$.*

Proof. Let $K \coloneqq \mathbb{Q}(\sqrt{p^*})$ and $L \coloneqq \mathbb{Q}(\zeta)$. First suppose $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ with distinct $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathcal{P}(\mathcal{O}_K)$. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$ (it exists by Lemma 6.2). Then σ induces a bijection between $\{\,\mathfrak{Q} \in \mathcal{P}(\mathcal{O}_L) : \mathfrak{Q} \mid \mathfrak{q}_1\mathcal{O}_L\,\}$ and $\{\,\mathfrak{Q} \in \mathcal{P}(\mathcal{O}_L) : \mathfrak{Q} \mid \mathfrak{q}_2\mathcal{O}_L\,\}$. Hence, in $\mathcal{O}_L$ there is an even number of primes lying over $q\mathbb{Z}$.

Now suppose conversely that q lies under an even number of primes of $\mathcal{O}_L$. Let $\mathfrak{Q}$ be such a prime. Then $|\mathrm{Gal}(L/\mathbb{Q}) : D(\mathfrak{Q})|$ is even, hence the decomposition field $L^{D(\mathfrak{Q})}/\mathbb{Q}$ has even degree. Therefore $L^{D(\mathfrak{Q})}$ contains the unique quadratic subfield K of L. The ramification index and inertia degree of $\mathfrak{Q} \cap \mathcal{O}_{L^{D(\mathfrak{Q})}}$ are both 1 by Theorem 6.7, and hence the same must be true for $\mathfrak{Q} \cap \mathcal{O}_K$. Thus q must be split in $\mathcal{O}_K$. □

Proof (of Quadratic Reciprocity). Let $p \neq q \in \mathbb{P} \smallsetminus \{2\}$. We have to show

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

Let $p^* = (-1)^{\frac{p-1}{2}}$. Using the elementary supplemental law $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$, we see

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

so it suffices to show $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$.

Using Theorem 6.9,

$$\begin{aligned}\left(\frac{p^*}{q}\right) = 1 &\Leftrightarrow\ q \text{ splits in } \mathbb{Q}(\sqrt{p^*})\\ &\Leftrightarrow\ q \text{ lies under an even number of primes of } \mathbb{Q}(\zeta)\end{aligned}$$

with $\zeta \in \mu_p^*(\mathbb{C})$. Let $f = \operatorname{ord}_{(\mathbb{Z}/p\mathbb{Z})^\times}(\overline{q})$. By Theorem 5.17, the prime q lies under $[\mathbb{Q}(\zeta) : \mathbb{Q}]/f = (p-1)/f$ primes in $\mathbb{Q}(\zeta)$. Now

$$\frac{p-1}{f} \text{ even } \Leftrightarrow\ f \mid \frac{p-1}{2}\ \Leftrightarrow\ q^{\frac{p-1}{2}} \equiv 1 \mod p\ \Leftrightarrow\ \left(\frac{q}{p}\right) = 1,$$

where the last equivalence comes from Lemma 5.14. □

6.2 Frobenius Elements (and Quadratic Reciprocity, once more)

As before, we consider a Galois extension L/K of number fields. Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be *unramified* and $\mathfrak{p} := \mathcal{O}_K \cap \mathfrak{P}$. Then the inertia group $I(\mathfrak{P})$ is trivial, and the decomposition group $D(\mathfrak{P})$ is isomorphic to $\operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ by Proposition 6.5. Hence $\operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ embeds into $\operatorname{Gal}(L/K)$. Let $q = |\kappa(\mathfrak{p})| = |\mathcal{O}_K/\mathfrak{p}| = \mathsf{N}(\mathfrak{p})$ (this is a power of the prime $p \in \mathfrak{P} \cap \mathbb{Z}$). The automorphism $\varphi \in \operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ with $\varphi(x) = x^q$ generates $\operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, its lift to $\operatorname{Gal}(L/K)$ plays a very important role in number theory.

Definition 6.10. *Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be unramified. The* Frobenius element *of $\mathfrak{P}$, denoted by*

$$\left(\frac{L/K}{\mathfrak{P}}\right) \in \operatorname{Gal}(L/K)$$

is the unique automorphism of L/K that maps to the Frobenius automorphism in $\operatorname{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$.

Thus $\sigma = \left(\frac{L/K}{\mathfrak{P}}\right)$ is the unique automorphism of L/K for which

$$\sigma(\alpha) \equiv \alpha^q \mod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L, \text{ where } q = |\mathcal{O}_K/\mathfrak{p}|.$$

The following is immediate.

Lemma 6.11. *Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ be unramified. The order of the Frobenius element $\left(\frac{L/K}{\mathfrak{P}}\right)$ in the group* $\operatorname{Gal}(L/K)$ *is the inertia degree $f(\mathfrak{P}|\mathfrak{p})$.*

Since $\mathfrak{P}$ is unramified by definition, the order of the Frobenius element therefore completely captures the decomposition behavior of $\mathfrak{P}$, thanks to the fundamental equation.

Lemma 6.12. *Let $\tau \in \operatorname{Gal}(L/K)$ and $\mathfrak{P}' = \tau(\mathfrak{P})$. Then*

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \tau\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1}.$$

Proof. Let $\sigma = \left(\frac{L/K}{\mathfrak{P}}\right)$. Then $\tau\sigma\tau^{-1}$ leaves $\tau(\mathfrak{P})$ invariant and

$$\tau\sigma\tau^{-1}(x) - x^q \in \tau(\mathfrak{P}) \;\Leftrightarrow\; \sigma\tau^{-1}(x) - \tau^{-1}(x)^q \in \mathfrak{P},$$

with the right side holding for $\sigma = \left(\frac{L/K}{\mathfrak{P}}\right)$ and all $x \in \mathcal{O}_L$. Hence $\tau\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1}$ is the Frobenius element of $\mathfrak{P}'$. □

To every unramified $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ we can therefore assign a conjugacy class of automorphisms in $\mathrm{Gal}(L/K)$. However, this is most interesting when $\mathrm{Gal}(L/K)$ is abelian, so that conjugacy classes are singletons and each unramified $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ determines a unique Frobenius element

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K),$$

that acts as the Frobenius element for all $\mathfrak{P} \mid \mathfrak{p}$.

Example. (1) Consider $\mathbb{Q}(\sqrt{d})$ with $1 \neq d \in \mathbb{Z}$ squarefree. The Galois group of $\mathbb{Q}(\sqrt{d})$ has two elements, and we can identify it with $\{\pm 1\}$. If $p \nmid d$ is an odd prime, then p is unramified by Theorem 5.13. By the same theorem,

$$\left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{p}\right) = \left(\frac{d}{p}\right).$$

(2) Let $K = \mathbb{Q}(\zeta)$ with $\zeta \in \mu_n^*(\mathbb{C})$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, with automorphisms defined by $\zeta \mapsto \zeta^k$ with $\gcd(k, n) = 1$ (see Proposition 2.26). If $p \nmid n$, then p is unramified in K by Theorem 5.17. We claim that $\left(\frac{K/\mathbb{Q}}{p}\right)$ is the automorphism $\sigma(\zeta) = \zeta^p$.

Indeed, let $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$ with $\mathfrak{p} \mid p$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha = \sum_{i=0}^{m-1} a_i\zeta^i$ with $a_i \in \mathbb{Z}$ (by Theorem 2.58) and $m = \phi(n)$. Hence

$$\sigma(\alpha) = \sum_{i=0}^{m-1} a_i\zeta^{pi} \equiv \sum_{i=0}^{m-1} a_i^p\zeta^{pi} \equiv \left(\sum_{i=0}^{m-1} a_i\zeta^i\right)^p \equiv \alpha^p \mod \mathfrak{p}.$$

□

We are now able to give another proof of quadratic reciprocity. It is only a small variation on the one in Section 6.1 but is conceptually even clearer because it reduces to computing the Frobenius element $\left(\frac{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}{q}\right)$ in two different ways.

We first note the following.

Lemma 6.14. *Let $K \subseteq M \subseteq L$ be such that L/K is an abelian extension*[1]*, then M/K is also abelian. If $\mathfrak{p} \in \mathcal{P}(\mathcal{O}_K)$, then*

$$\left.\left(\frac{L/K}{\mathfrak{p}}\right)\right|_M = \left(\frac{M/K}{\mathfrak{p}}\right).$$

[1] Meaning, a Galois extensions with abelian Galois group

Proof. Let $\mathfrak{P} \in \mathcal{P}(\mathcal{O}_L)$ with $\mathfrak{P} \mid \mathfrak{p}$, and let $\mathfrak{P}_M \coloneqq \mathfrak{P} \cap \mathcal{O}_M$. Let $q = |\mathcal{O}_K/\mathfrak{p}|$. Let $\sigma = \left(\frac{L/K}{\mathfrak{p}}\right)$. Because M/K is Galois, the automorphism σ restricts to $\sigma|_M \in \mathrm{Gal}(M/K)$ (by Galois theory). For $\alpha \in \mathcal{O}_M$, then

$$\sigma(\alpha) - \alpha^q \in \mathfrak{P} \cap \mathcal{O}_M = \mathfrak{P}_M. \qquad \square$$

Proof (of Theorem 5.15). Again, we do not reprove the elementary supplemental laws. Let $p \neq q$ be odd primes and $p^* = (-1)^{\frac{p-1}{2}} p$. As before, we have to show $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Let $\zeta \in \mu_p^*(\mathbb{C})$ and $L \coloneqq \mathbb{Q}(\zeta)$. Then $K \coloneqq \mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of L (Lemma 6.8). Hence

$$\left(\frac{L/\mathbb{Q}}{q}\right)\Bigg|_K = \left(\frac{K/\mathbb{Q}}{q}\right) = \left(\frac{p^*}{q}\right). \tag{6.2}$$

On the other hand, $\left(\frac{L/\mathbb{Q}}{q}\right)(\zeta) = \zeta^q$. We have

$$\begin{tikzcd}
(\mathbb{Z}/p\mathbb{Z})^\times \arrow[r, "\sim"] & \mathrm{Gal}(L/\mathbb{Q}) \arrow[r] & \mathrm{Gal}(K/\mathbb{Q}) \arrow[r, "\sim"] & \{\pm 1\} \\
a + p\mathbb{Z} \arrow[r, mapsto] & (\zeta \mapsto \zeta^a), & &
\end{tikzcd}$$

with the map of Galois groups induced by restriction, and having kernel $\left((\mathbb{Z}/p\mathbb{Z})^\times\right)^2$, the unique index 2 subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Hence $\left(\frac{L/\mathbb{Q}}{q}\right)\big|_K$ is trivial if and only if q is a square modulo p. Thus

$$\left(\frac{L/\mathbb{Q}}{q}\right)\Bigg|_K = \left(\frac{q}{p}\right),$$

and comparison with (6.2) yields the quadratic reciprocity law. $\square$

Appendix A

Complex Analysis

We summarize some results from complex analysis, focusing in particular on infinite products, as we assume the reader may not have encountered them much before. Any textbook on complex analysis can serve as a more comprehensive reference, for instance, [Ahl21; Gam01] or the two volumes [Rem91; Rem98].

Recall that in this context a domain is a nonempty, open, connected subset of $\mathbb{C}$. If $U \subseteq \mathbb{C}$ is a domain, and $f: U \to \mathbb{C}$ is a function, then f is holomorphic in $z_0 \in U$ if it is complex differentiable, and it is analytic in z_0 if it has a convergent power series expansion in a neighborhood of z_0. One of the fundamental results of complex analysis is that holomorphicity and analyticity are equivalent.

Theorem A.1 (Cauchy's integral formula). *Let $f: U \to \mathbb{C}$ be holomorphic on some domain U. Let $D \subseteq U$ be a closed disc with center z_0 contained in U. Then*

$$f(z_0) = \frac{1}{2\pi i} \int_{\partial D} \frac{f(z)}{z - z_0}\, dz,$$

where ∂D is the boundary of D.

Proof. See [Ahl21, Chapter 2.2] or [Rem91, Chapter 7.2.2]. □

Theorem A.2 (Moreara's Theorem). *Let $f: U \to \mathbb{C}$ be a continuous function in some domain U. If $\int_\gamma f(z)\, dz = 0$ for all closed piecewise C^1 curves γ in U, then f is holomorphic in U.*

Proof. See [Ahl21, p.122] or [Rem91, Theorem 8.2.2]. □

The following shows that the Laplace transform is holomorphic in a suitable domain.

Proposition A.3. *Let $f: \mathbb{R}_{\geq 0} \to \mathbb{C}$ be locally integrable*[1] *and such that $|f(t)| \leq Ae^{Bt}$ for A, $B \in \mathbb{R}_{\geq 0}$ and all $t \in \mathbb{R}_{\geq 0}$. Then*

$$F(z) = \int_0^\infty f(t) e^{-zt}\, dt$$

[1] This means integrable on every compact subset of the domain

defines a holomorphic function for all z with $\mathrm{Re}(z) > B$.

Proof. Continuity of $F(z)$ follows by dominated convergence. We apply Moreara's Theorem. Let $\gamma\colon [0,1] \to \{\, z : \mathrm{Re}(z) > B \,\}$ be a piecewise C^1-curve, and let $\sigma > B$ be such that $\mathrm{Re}(\gamma(x)) \geq \sigma$ for all $x \in [0,1]$. It holds that

$$\int_0^1 \int_0^\infty |f(t)| e^{-\mathrm{Re}(\gamma(x))t} |\gamma'(x)| \, dt \, dx \leq \int_0^1 \int_0^\infty A e^{(B-\sigma)t} |\gamma'(x)| \, dt \, dx < \infty,$$

(because $B - \sigma < 0$). By Fubini-Tonelli, we can exchange the order of integration, to get

$$\begin{aligned} \int_\gamma F(z)\, dz &= \int_0^1 \int_0^\infty f(t) e^{-\gamma(x)t} |\gamma'(x)| \, dt \, dx \\ &= \int_0^\infty \int_0^1 f(t) e^{-\gamma(x)t} |\gamma'(x)| \, dx \, dt = \int_0^\infty f(t) \int_\gamma e^{-zt} \, dz \, dt = 0. \end{aligned}$$

Hence Moreara's Theorem implies that $F(z)$ is holomorphic. □

A.1 Infinite Products

We recall some basic properties of infinite products. Given a sequence $(a_n)_{n\geq 1}$, the infinite product $\prod_{n=1}^\infty a_n$ is said to converge if there exists some $m \geq 1$ such that $a_n \neq 0$ for all $n \geq m$, and the limit of partial products $\widehat{a}_m := \lim_{n\to\infty} \prod_{n\geq m} a_n$ exists *and is nonzero*. In this case, the value of the product is defined to be

$$\prod_{n\geq 1} a_n := a_1 \cdots a_{m-1} \widehat{a}_m.$$

An infinite product that does not converge is called divergent.

These restrictions are necessary to obtain reasonable properties for infinite products. If infinitely many zero terms were allowed, every such infinite product would be convergent, irrespective of the other terms. The requirement that the limit be nonzero ensures that an infinite product is zero if and only if one of its factors is zero. (Note that $(1/n)_{n\geq 1}$ has convergent partial products, but they converge to zero.)

Convergence of the infinite product implies $\lim_{n\to\infty} a_n \to 1$. It is therefore convenient to always write convergent infinite products in the form

$$\prod_{n\geq 1} (1 + b_n)$$

with $b_n \in \mathbb{C}$. Then $\lim_{n\to\infty} b_n = 0$.

Lemma A.4. *Consider a sequence* $(1 + a_n)_{n\geq 1}$. *Then the following are equivalent.*

(a) *The infinite product* $\prod_{n\geq 1}(1 + a_n)$ *converges.*

(b) *For some* $n_0 \geq 1$, *the infinite series* $\sum_{n\geq n_0} \mathrm{Log}(1 + a_n)$ *converges* (*with* Log *denoting the principal branch of the logarithm*).

We shall actually only use the easier direction, which is (b) ⇒ (a).

Proof. Let $S_N \coloneqq \sum_{n=n_0}^{N} \operatorname{Log}(1+a_n)$ and $P_N \coloneqq \exp(S_N) = \prod_{n=n_0}^{N}(1+a_n)$.

(b) ⇒ (a) By continuity of the complex exponential function, the sequence $(P_N)_{N\geq n_0}$ converges, yielding

$$\lim_{N\to\infty} P_N = \lim_{N\to\infty} \exp(S_N) = \exp\Big(\sum_{n=n_0}^{\infty} \operatorname{Log}(1+a_n)\Big). \tag{A.1}$$

Because $\exp(z) \neq 0$ for all $z \in \mathbb{C}$, this already implies that the infinite product is convergent.

(a) ⇒ (b) Since $\lim_{n\to\infty} a_n = 0$, we may assume $1 + a_n \notin \mathbb{R}_{\leq 0}$ for all $n \geq n_0$, so that the principal branch of the logarithm is defined for all such $1 + a_n$.

Let $P \coloneqq \prod_{n=n_0}^{\infty}(1+a_n)$. By definition, we have $P \neq 0$. By taking n_0 large enough, we can also assume $P \notin \mathbb{R}_{\leq 0}$ (using convergence of the product). Now

$$\operatorname{Log}(P_N/P) = \operatorname{Log}(P_N) - \operatorname{Log}(P) + k'_N 2\pi i = S_N - \operatorname{Log}(P) + k_N 2\pi i,$$

for some k_N, $k'_N \in \mathbb{Z}$. Taking differences,

$$(k_{N+1} - k_N)2\pi i = \operatorname{Log}(P_{N+1}/P) - \operatorname{Log}(1 + a_{N+1}) - \operatorname{Log}(P_N/P).$$

Noting that $\lim_{N\to\infty} P_N/P = 1$ implies $\lim_{N\to\infty} \operatorname{Log}(P_N/P) = 0$, the right side converges to 0. However, since the k_N are integers, this is only possible if k_N is constant for all sufficiently large N, say $N \geq n_1$. For such N, we therefore have

$$\operatorname{Log}(P_N/P) = S_N - \operatorname{Log}(P) + k 2\pi i,$$

with fixed $k \in \mathbb{Z}$. It follows that S_N converges to $\operatorname{Log}(P) - 2k\pi i$. □

It is not meaningful to define the absolute convergence of an infinite product by absolute convergence of the partial products (otherwise $\prod_{n=1}^{\infty}(-1)^n$ would converge absolutely, but would not converge). Instead one says that $\prod_{n=1}^{\infty}(1+a_n)$ converges absolutely if and only if $\sum_{n=n_0}^{\infty} |\operatorname{Log}(1+a_n)|$ converges absolutely for some $n_0 \geq 1$ (this necessates $\lim_{n\to\infty} a_n = 0$, and in particular, only finitely many terms of the product can be zero). Since $\lim_{z\to 0} \operatorname{Log}(1+z)/z = 0$, the *limit comparison test* for the convergence of series, shows the following.

Lemma A.5. *An infinite product $\prod_{n=1}^{\infty}(1+a_n)$ converges absolutely if and only if $\sum_{n=1}^{\infty}|a_n|$ converges.*

For absolutely convergent infinite products, we can rearrange the factors in any order without changing the value (as a consequence of the same property for series and Equation (A.1)).

Let $U \subseteq \mathbb{C}$ be a domain. Convergence of an infinite product $\prod_{n=1}^{\infty} f_n$ of functions $f_n : U \to \mathbb{C}$ is defined pointwise. However, as for infinite series, we cannot expect to be able to exchange operations such as differentiation with infinite products under pointwise convergence.

Definition A.6. *Let $U \subseteq \mathbb{C}$ be a domain, and let $(f_n\colon U \to \mathbb{C})_{n\ge1}$ be a family of functions.*

(1) *If $K \subseteq U$ is compact, then $\prod_{n=1}^{\infty} f_n$ converges uniformly on K if and only if there exists $n_0 \ge 1$ such that the sequence of partial products $\left(\prod_{n=n_0}^{N} f_n\right)_{N\ge1}$ converges uniformly* and *$\prod_{n=n_0}^{\infty} f_n$ is nowhere zero on K.*

(2) *The product $\prod_{n=1}^{\infty} f_n$ converges compactly (or also, converges locally uniformly) if it converges uniformly on every compact subset of U.*

Compact convergence is equivalent to every point having a compact neighborhood in which the product converges uniformly.

Analogous to the pointwise convergence criterion, we get the following.

Lemma A.7. *Let U be a domain and $K \subseteq U$ be a compact set. Let $(f_n\colon U \to \mathbb{C})_{n\ge1}$ be a sequence of continuous functions such that there is an n_0 so that for all $n \ge n_0$ we have $|f_n(z)| < 1$ for all $z \in K$. Suppose there exist $M_n \in \mathbb{R}_{\ge0}$ such that*

$$\sum_{n=n_0}^{\infty} |\mathrm{Log}(1 + f_n(z))| \le \sum_{n=n_0}^{\infty} M_n < \infty$$

for all $z \in U$. Then $\prod_{n=1}^{\infty}(1 + f_n(z))$ converges uniformly and absolutely in K.

Proof. Pointwise absolute convergence follows from Lemma A.4. By our assumption, the series $\sum_{n=n_0}^{\infty} \mathrm{Log}(1 + f_n(z))$ converges uniformly. Set $F_N := \sum_{n=n_0}^{N} \mathrm{Log}(1 + f_n(z))$. We estimate, for sufficiently large N and M,

$$\begin{aligned}\left|\prod_{n=n_0}^{N} f_n(z) - \prod_{n=n_0}^{M} f_n(z)\right| &= |\exp(F_N(z)) - \exp(F_M(z))| \\ &= |\exp(F_M(z))|\,|\exp(F_N(z) - F_M(z)) - 1| \\ &\le 2\,|\exp\left(F_M(z)\right)|\,|F_N(z) - F_M(z)|.\end{aligned}$$

(where we used $|\exp(x) - 1| \le 2|x|$ for $|x| \le 1/2$ in the final step). By compactness of K and uniform convergence of $(F_N(z))_{N\ge n_0}$, the claim follows. □

We recall the following important property (which is truly a feature of complex analysis; corresponding results in real analysis need stronger hypotheses).

Theorem A.8 ([Rem91, Theorem 8.4.1]). *Let $U \subseteq \mathbb{C}$ be a domain, and let $(f_n\colon U \to \mathbb{C})_{n\ge1}$ be a sequence of holomorphic functions. If $(f_n)_{n\ge1}$ converges compactly to some function $f\colon U \to \mathbb{C}$, then f is holomorphic. Moreover, for every $k \ge 0$, the sequence of derivatives $(f_n^{(k)})_{n\ge1}$ converges compactly to $f^{(k)}$.*

Given a holomorphic $f\colon U \to \mathbb{C}$ with $f \ne 0$, one calls f'/f the logarithmic derivative. For a finite product $f = f_1 \cdots f_n$ we immediately get $f'/f = f_1'/f_1 + \cdots + f_n'/f_n$ from the product rule. The following shows that, for compactly convergent infinite products, we get the same behavior.

Proposition A.9. *Let $(f_n : U \to \mathbb{C})_{n\geq 1}$ be a sequence of meromorphic functions. Suppose that the infinite product $\prod_{n=1}^{\infty} f_n$ converges compactly to a function f. Then*

$$\frac{f'}{f} = \sum_{n=1}^{\infty} \frac{f_n'}{f_n},$$

with the series on the right side converging compactly.

Proof. Let $K \subseteq D$ be compact and let $n_0 \geq 1$ be such that $\prod_{n=n_0}^{\infty} f_n$ is nowhere zero on K. For $n \geq n_0$, define $F_n \coloneqq \prod_{m=n}^{\infty} f_n$. Then $f = f_1 \cdots f_{n-1} F_n$, and a simple application of the product rule gives

$$\frac{f'}{f} = \sum_{m=1}^{n-1} \frac{f_i'}{f_i} + \frac{F_n'}{F_n}.$$

Because the product $\prod_{n=n_0}^{\infty} f_n$ converges compactly, the factors F_n converge compactly to the constant function 1. By Theorem A.8, the derivatives F_n' converge compactly to the constant 0 function. Therefore the quotient F_n'/F_n converges compactly to 0. This shows that $\sum_{m=1}^{n-1} \frac{f_i'}{f_i}$ converges compactly to $\frac{f'}{f}$ as $n \to \infty$. □

Bibliography

[Ahl21] L. Ahlfors. *Complex analysis—an introduction to the theory of analytic functions of one complex variable*. Third. Reprint of the 1978 original [0510197]. AMS Chelsea Publishing, Providence, RI, 2021, pp. xiv+331.

[Bre19] M. Brešar. *Undergraduate algebra*. Springer Undergraduate Mathematics Series. A unified approach. Springer, Cham, 2019, pp. xxiv+316. DOI: 10.1007/978-3-030-14053-3.

[Gam01] T. W. Gamelin. *Complex analysis*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2001, pp. xviii+478. DOI: 10.1007/978-0-387-21607-2.

[Koc00] H. Koch. *Number theory*. Vol. 24. Graduate Studies in Mathematics. Algebraic numbers and functions, Translated from the 1997 German original by David Kramer. American Mathematical Society, Providence, RI, 2000, pp. xviii+368. DOI: 10.1090/gsm/024.

[Mar18] D. A. Marcus. *Number fields*. Second. Universitext. With a foreword by Barry Mazur. Springer, Cham, 2018, pp. xviii+203. DOI: 10.1007/978-3-319-90233-3.

[Neu99] J. Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. DOI: 10.1007/978-3-662-03983-0.

[Rem91] R. Remmert. *Theory of complex functions*. Vol. 122. Graduate Texts in Mathematics. Readings in Mathematics. Springer-Verlag, New York, 1991, pp. xx+453. DOI: 10.1007/978-1-4612-0939-3.

[Rem98] R. Remmert. *Classical topics in complex function theory*. Vol. 172. Graduate Texts in Mathematics. Translated from the German by Leslie Kay. Springer-Verlag, New York, 1998, pp. xx+349. DOI: 10.1007/978-1-4757-2956-6.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997, pp. xiv+487. DOI: 10.1007/978-1-4612-1934-7. URL: https://doi.org/10.1007/978-1-4612-1934-7.

[Zag97] D. Zagier. *Newman's short proof of the prime number theorem*. Amer. Math. Monthly 104.8 (1997), 705–708. DOI: 10.2307/2975232.