NUMBER FIELDS, LENT 2025

PÉTER P. VARJÚ

Disclaimer, acknowledgement, etc

I prepared these notes primarily for the benefit of the students taking my lectures on Number Fields that I gave in the Lent term, 2025 at the University of Cambridge. Others may find one of the standard textbooks on the subject more useful. In particular, I am happy to recommend the book of Marcus [4], which was the primary source for these notes. Chapters 10-12 in the book of Baker [2] cover a good part of the material in a very concise hands-on way. The book of Alaca and Williams [1] is another useful source giving a very detailed and leisurely exposition. Writings of Edwards, in particular the paper [3], give an interesting historical account on the origins of the theory of ideals.

I am grateful to Professor Scholl for sharing his notes and example sheets with me, which have been extremely helpful.

All results in these notes are due to 19th century mathematicians. Any novelty must lie in the mistakes I have unintentionally introduced.

Please send comments to: pv270@dpmms.cam.ac.uk.

1. Introduction and motivation

Recall the following definitions from Part II Galois theory. If $L \supset K$ are fields, we call L an extension of K, and this is denoted by $L|K$. We can think of L as a vector space over K, and the dimension of this vector space is called the degree of L over K. The degree is denoted by $[L : K]$.

Definition 1. A number field is a subfield of the complex numbers $\mathbf{C}$ that is a finite degree extension of the rationals $\mathbf{Q}$.

Example 2. The field of rational numbers $\mathbf{Q}$ is a number field.

Example 3. Take your favourite algebraic number α, that is, a root of a polynomial with integer coefficients. Then $\mathbf{Q}(\alpha)$, the smallest subfield of $\mathbf{C}$ containing α, is a number field. Its degree is the degree of the minimal polynomial of α.

By the primitive element theorem (Part II Galois theory), every number field is of the form $\mathbf{Q}(\alpha)$ for some $\alpha \in \mathbf{C}$.

In this course, two families of number fields will recur.

Version of 20 March 2025.

Example 4 (Quadratic fields)**.** Let $m \neq 0, 1$ be a square-free integer. Then $\mathbf{Q}(m^{1/2})$ is a number field of degree 2, called a quadratic field.

Example 5 (Cyclotomic fields)**.** Let $n \geq 3$, and let $\theta_n = e^{2\pi i/n}$. Observe that $\theta_n^n = 1$, that is, θ_n is an n-th root of unity, and n is the smallest positive exponent with this property. Let $\varphi(n)$ denote the number of residue classes $\mod n$ that are coprime to n. Then $\mathbf{Q}(\theta_n)$ is a number field of degree $\varphi(n)$, called a cyclotomic field.

1.1. **Why bother?** Number theory is the study of integers. As we will soon see, the notion of integers can be extended to include certain elements in number fields, and most questions about rational integers, that is, $\mathbf{Z}$, can be naturally extended to this setting.

This may not sound very convincing. However, number fields are also very useful for solving many problems that are entirely about rational integers. As an example, in this course, we will consider the Fermat equation

$$x^k + y^k = z^k, \qquad x, y, z \in \mathbf{Z}. \tag{1}$$

We first recall the $k = 2$ case of this equation, whose solutions are Pythagorean triples. We aim to find all primitive solutions, that is, those with $\gcd(x, y, z) = 1$. One may get all solutions by multiplying primitive solutions by arbitrary integers. Furthermore, we will only look for solutions with $x, y, z \in \mathbf{Z}_{\geq 0}$. Observe that any common prime factor of x and y must also divide z by the equation, so a primitive solution also satisfies $\gcd(x, y) = 1$. Now we assume, as we may, that $2 \nmid y$, and rewrite the equation as

$$(z + x)(z - x) = z^2 - x^2 = y^2.$$

We observe that any common prime factor of $(x + z)$ and $(x - z)$ must also divide $2x = (z + x) - (z - x)$ and y (because $x + z | y^2$). Then $\gcd(z + x, z - x) | \gcd(2x, y) = 1$ by $\gcd(x, y) = 1$ and $2 \nmid y$. Observe that y^2 contains all prime factors with even multiplicity. When we distribute the prime factors of y^2 between $z + x$ and $z - x$, all instances of the same prime must go to the same factor, because the two factors are coprime.

Therefore, there are odd $m \geq n \in \mathbf{Z}_{\geq 0}$ with $\gcd(m, n) = 1$ such that $z + x = m^2$ and $z - x = n^2$. A simple calculation yields that any non-negative primitive solution of our equation must satisfy

$$x = \frac{m^2 - n^2}{2}, \quad y = mn, \quad z = \frac{m^2 + n^2}{2}.$$

It is easy to verify that all x, y, z in this form are non-negative primitive solutions, provided m and n satisfy the conditions we imposed. Therefore, we solved the equation.

Remark 6. It is more customary to write the solution in the equivalent form

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2$$

with the assumptions that $m > n \in \mathbf{Z}_{\geq 0}$, $\gcd(m, n) = 1$ and exactly one of them is even.

Fermat claimed that there are no solutions of (1) with $x, y, z \in \mathbf{Z}_{\geq 1}$ and $k \geq 3$. We try to generalize the above argument. The first step is a suitable factorization of the equation. The $k = 2$ case was based on $X^2 - 1 = (X + 1)(X - 1)$. For general k, we have

$$X^k - 1 = \prod_{j=0}^{k-1} (X - \theta_k^j).$$

Indeed, θ_k^j for $j = 0, \ldots, k - 1$ are all the k'th roots of unity. Where k is odd, which we will now assume, this can be more conveniently rewritten as

$$X^k + 1 = \prod_{j=0}^{k-1} (X + \theta_k^j)$$

using the substitution $X \to -X$. Now we plug in $X = x/y$ and get

$$z^k = x^k + y^k = \prod_{j=0}^{k-1} (x + \theta_k^j y).$$

Our next step would be to show that $(x + \theta_k^j y)$ are k'th powers in $\mathbf{Z}[\theta_k]$, but there are two major difficulties. The first, and more serious one is that our argument in the $k = 2$ case relied on unique factorization. However, $\mathbf{Z}[\theta_k]$ is a unique factorization domain (UFD) only for finitely many k's. This property already fails for $k = 23$, and, in fact, for all primes $k \geq 23$. The second issue is that even if $\mathbf{Z}[\theta_k]$ is a UFD, an element that contains all primes with multiplicity divisible by k, may not be an k'th power. All that we can say is that it is of the form $u\alpha^k$, where $\alpha \in \mathbf{Z}[\theta_k]$ and u is a unit in $\mathbf{Z}[\theta_k]$, that is, $u, u^{-1} \in \mathbf{Z}[\theta_k]$.

Despite these difficulties, Kummer was able to show the following result in 1850.

Theorem 7 (Kummer)**.** *Let $p > 2$ be a regular prime. Then the equation*

$$x^p + y^p = z^p, \qquad x, y, z \in \mathbf{Z}_{\geq 1}$$

has no solutions.

We will define what a regular prime is later in the course. Here we just note that there are only three irregular primes less than 100: 37, 59 and 67. Moreover, it has been conjectured (later by Siegel) that

the density of regular primes is $e^{-1/2} \approx 0.6065\ldots$, however even the infinitude of regular primes is an open problem.

In any case, this is a great result. Its proof relies on a remarkable theory of Kummer that "restores" unique factorization in cyclotomic fields. This has been extended by Dedekind and Kronecker in the second half of the 19th century to all number fields using two conceptually different but equivalent constructions.

1.2. **Aims of the course.** In this course, we will first discuss what the appropriate notion of an integer is in general number fields. Then we will develop a substitute for unique factorization following Dedekind. Next we will study the structure of units. In the final part of the course we will put most of the fire power we will have acquired to good use and prove Kummer's above quoted theorem under the additional assumption that $p \nmid xyz$.

2. Rings of integers

Let α be an algebraic number. Recall that there is a unique monic polynomial $P \in \mathbf{Q}[x]$ of minimal degree such that $P(\alpha) = 0$. This polynomial is called the minimal polynomial of α, and it is necessarily irreducible in $\mathbf{Q}[x]$.

Definition 8. A complex number is an algebraic integer if it is algebraic and its minimal polynomial has integer coefficients.

Remark 9. If $f(\alpha) = 0$ for some monic $f \in \mathbf{Z}[x]$, then α is an algebraic integer even if f is not the minimal polynomial. Indeed, we must have $f = g \cdot h$, where g is the minimal polynomial of α and $h \in \mathbf{Q}[x]$ is monic. By Gauss's lemma (Part IB Groups, Rings and Modules), we must have $g, h \in \mathbf{Z}[x]$, so g, the minimal polynomial, has integer coefficients. (*Exercise:* think through the details.)

Theorem 10. *Algebraic integers form a ring.*

This ring is denoted by $\mathcal{O}$.

Definition 11. Let K be a number field. We write $\mathcal{O}_K = \mathcal{O} \cap K$, and call it the ring of integers of K.

Soon we will see that it is crucial for the theory that we develop as a substitute for unique factorization that we work with $\mathcal{O}_K$ rather than a subring of it. Introducing it was one of the key inventions of Dedekind and Kronecker when they generalized Kummer's approach from cyclotomic fields to general number fields.

The purpose of this section is to prove Theorem 10. Before we start, we give a few examples.

Example 12. The ring of integers in $\mathbf{Q}$ is $\mathbf{Z}$. Indeed, the minimal polynomial of a/b with $\gcd(a, b) = 1$ is $x - a/b$.

Example 13. Let $m \neq 0, 1 \in \mathbf{Z}$ be square-free, and $K = \mathbf{Q}(\sqrt{m})$. Then

$$\mathcal{O}_K = \begin{cases} \left\{ a + b \cdot \dfrac{1+\sqrt{m}}{2} : a, b \in \mathbf{Z} \right\} & \text{if } m \equiv 1 \mod 4 \\ \{ a + b\sqrt{m} : a, b \in \mathbf{Z} \} & \text{otherwise.} \end{cases}$$

Hint: Observe that $a + b\sqrt{m}$ with $a, b \in \mathbf{Q}$ is a root of the polynomial

$$(x - a - b\sqrt{m})(x - a + b\sqrt{m}) = x^2 - 2ax + (a^2 - b^2 m),$$

and it is an algebraic integer if and only if both $2a \in \mathbf{Z}$ and $a^2 - b^2 m \in \mathbf{Z}$. The details are left as an exercise.

Example 14. Let $n \geq 3$, let $\theta_n = e^{2\pi i/n}$, and let $K = \mathbf{Q}(\theta_n)$. Then

$$\mathcal{O}_K = \mathbf{Z}[\theta_n] = \mathbf{Z} \oplus \theta_n \mathbf{Z} \oplus \ldots \oplus \theta_n^{\varphi(n)} \mathbf{Z}.$$

Later in the course we will prove this in the case where n is a prime.

Consider a number field $\mathbf{Q}(\alpha)$, where α is an algebraic number. All elements of $\mathbf{Q}(\alpha)$ have a unique representation of the form

$$a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1}$$

where $a_0, \ldots, a_{d-1} \in \mathbf{Q}$ and d is the degree of α.

Lemma 15. *Let α be an algebraic integer. Then the elements*

$$a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1} \tag{2}$$

with all $a_0, \ldots, a_{d-1} \in \mathbf{Z}$ form a ring, which is the smallest ring containing α and $\mathbf{Z}$, and we denote it by $\mathbf{Z}[\alpha]$.

By Theorem 10, $\mathbf{Z}[\alpha] \subset \mathcal{O}_K$, but as the example of $\mathbf{Q}(\sqrt{m})$ for $m \equiv 1 \mod 4$ shows strict containment is possible.

A number field K is called monogenic if there is some $\alpha \in K$ such that $\mathcal{O}_K = \mathbf{Z}[\alpha]$. The above examples show that quadratic and cyclotomic fields are monogenic. However, this is not true in general. See the second example sheet for an example.

Proof of Lemma 15. The elements

$$a_0 + a_1\alpha + \ldots + a_k\alpha^k$$

for arbitrary $k \in \mathbf{Z}_{\geq 0}$ and $a_0, \ldots, a_k \in \mathbf{Z}$ certainly form a ring. (Check directly that they are closed under subtraction and multiplication.) It is enough to check that these elements can be written in the form (2).

If fact, it is enough to check this for the elements α^k, because elements of the form (2) are closed under integer linear combinations. Writing $f(x) = x^d + b_{d-1}x^{d-1} + \ldots + b_1 x + b_0$ for the minimal polynomial of α and using $f(\alpha)\alpha^{k-d} = 0$, we can write

$$\alpha^k = -b_{d-1}\alpha^{k-1} - \ldots - b_1\alpha^{k-b+1} - b_0\alpha^{k-b},$$

so α^k may be written as an integer linear combination of lower powers of α for all $k \geq d$. We may iterate this as long as, we have a power

higher than $k-1$ in our expression. In the end, we get a representation in the form (2), as required. □

We turn to the proof of Theorem 10. It relies an the following alternative characterizations of algebraic integers.

Proposition 16. *Let $\alpha \in \mathbf{C}$. The following are equivalent.*

(1) *The number α is an algebraic integer.*
(2) *The ring $\mathbf{Z}[\alpha]$ is a finitely generated $\mathbf{Z}$-module, that is, there are $\beta_1, \dots, \beta_n \in \mathbf{Z}[\alpha]$ such that*
$$\mathbf{Z}[\alpha] = \beta_1\mathbf{Z} + \dots + \beta_n\mathbf{Z}.$$
(3) *There is a finitely generated $\mathbf{Z}$-submodule of $\mathbf{C}$ that is closed under multiplication by α.*

Proof. We have already seen that (1) implies (2) in Lemma 15.

Item (2) implies item (3) trivially.

We turn to the proof that item (3) implies item (1). Let $\beta_1\mathbf{Z} + \dots + \beta_n\mathbf{Z}$ be a module that is closed under multiplication by α. We want to show that α is an algebraic integer, and to that end, we exhibit a monic polynomial in $\mathbf{Z}[x]$ that vanishes at α.

For all $i = 1, \dots, n$, there are integers $m_{i,1}, \dots, m_{i,n}$ such that
$$\alpha\beta_i = m_{i,1}\beta_1 + \dots + m_{i,n}\beta_n.$$
We consider the matrix M with entries $m_{i,j}$ for $i, j = 1, \dots, n$, and observe
$$M \cdot \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} \alpha\beta_1 \\ \vdots \\ \alpha\beta_n \end{pmatrix}.$$
We see that α is an eigenvalue of the matrix M, hence it is a root of the characteristic polynomial $\det(x\,\mathrm{Id} - M)$. □

Proof of Theorem 10. Let $\alpha, \beta \in \mathcal{O}$. We show that $\alpha - \beta$ and $\alpha\beta \in \mathcal{O}$, which is enough to show that $\mathcal{O}$ is a ring.

We prove that $\mathbf{Z}[\alpha, \beta]$ is a finitely generated module. This is closed under multiplication by $\alpha - \beta$ and $\alpha\beta$, hence $\alpha - \beta, \alpha\beta \in \mathcal{O}$ by Proposition 16, as needed.

By Proposition 16, $\mathbf{Z}[\alpha]$ and $\mathbf{Z}[\beta]$ are finitely generated $\mathbf{Z}$-modules. Let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_m$ be generators for them, respectively. Then $\mathbf{Z}[\alpha, \beta]$ is generated by $\{\alpha_i\beta_j : i = 1, \dots, n, j = 1, \dots, m\}$, and the theorem is proved. □

Remark 17 (Non-examinable)**.** Theorem 10 can also be proved using the theory of symmetric polynomials. We briefly sketch this here. For details, see [2, Chapter 10].

We denote by $e_0(X_1, \dots, X_n), \dots, e_n(X_1, \dots, X_n)$ the elementary symmetric polynomials in n indeterminates. The polynomial e_j also depends on n, of course, but we make this explicit in our notation only

when we list the arguments. The key result (from Part II Galois Theory) we use is that for any symmetric polynomial $f(X_1, \ldots, X_n)$, there is a polynomial $g(Y_0, \ldots, Y_n)$ such that $f = g(e_0, \ldots, e_n)$, and the coefficients of g can be taken from the same ring where the coefficients of f come from.

Now let α and β be two algebraic integers of degrees n and m respectively. We write $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ for the roots of the minimal polynomials of α and β respectively. (These lists contain α and β of course.) We note that $(-1)^k e_k(\alpha_1, \ldots, \alpha_n)$ and $(-1)^k e_k(\beta_1, \ldots, \beta_m)$ are the coefficients of the minimal polynomials of α and β respectively, and hence they are integers. We claim that $e_k(\ldots, \alpha_i + \beta_j, \ldots)$ with i and j running thorough their respective ranges is an integer for each $k = 1, \ldots, nm$. Then $\alpha + \beta$ is the root of a monic polynomial with integer coefficients, hence it is an algebraic integer.

To show the claim, it is enough to show that for each k, there is a polynomial $g(U_0, \ldots, U_n, V_0, \ldots, V_m)$ with integer coefficients such that

$$e_k(\ldots, X_i + Y_j, \ldots) = g(e_0(X_1, \ldots, X_n), \ldots, e_n(X_1, \ldots, X_n), e_0(Y_1, \ldots, Y_m), \ldots, e_m(Y_1, \ldots, Y_m)). \tag{3}$$

This can be proved by two applications of the "key result" mentioned above. First we consider the left hand side of (3) a symmetric polynomial in $Y_1, \ldots, Y_m$ with coefficients in the ring $\mathbf{Z}[X_1, \ldots, X_n]$, and write it as a polynomial g_0 in $e_l(Y_1, \ldots, Y_m)$, $l = 0, \ldots, m$ with coefficients in $\mathbf{Z}[X_1, \ldots, X_n]$. Now each of the coefficients of g_0 is a symmetric polynomial in $X_1, \ldots, X_n$, hence they can be written as polynomials in $e_l(X_1, \ldots, X_n)$, $l = 0, \ldots, n$ with integer coefficients.

3. Additive structure of the ring of integers

Let K be a number field with $d = [K : \mathbf{Q}]$. The aim of this section is to show that there are $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \alpha_1 \mathbf{Z} \oplus \ldots \oplus \alpha_d \mathbf{Z}.$$

Such a collection of elements $\alpha_1, \ldots, \alpha_d$, if exists, is called an integral basis for K.

Let M be a finitely generated $\mathbf{Z}$-submodule (or equivalently an additive subgroup) of K. By the structure theorem of finitely generated modules (Part IB Groups, Rings and Modules) we know that

$$M \cong \mathbf{Z}^r \oplus (\mathbf{Z}/q_1\mathbf{Z}) \oplus \ldots \oplus (\mathbf{Z}/q_s\mathbf{Z})$$

for some r, s and $q_1, \ldots, q_s$. Since K does not contain any elements of finite additive order, $M \cong \mathbf{Z}^r$, hence

$$M = \alpha_1 \mathbf{Z} \oplus \ldots \oplus \alpha_r \mathbf{Z}$$

for some $\alpha_1, \ldots, \alpha_r$.

Since $\alpha_1, \ldots, \alpha_r$ are linearly independent over $\mathbf{Q}$, we must have $r \leq d$. In addition, $\mathcal{O}_K$ contains d linearly independent elements over $\mathbf{Q}$ (just

take $1, \alpha, \dots, \alpha^{d-1}$ for some $\alpha \in \mathcal{O}_K$ with $K = \mathbf{Q}(\alpha)$). Therefore, if we knew that $\mathcal{O}_K$ is a finitely generated module, then we also knew that an integral basis exists.

In what follows, we attach a quantity called the discriminant to tuples of elements $(\alpha_1, \dots, \alpha_d) \in \mathcal{O}_K^d$. We will show that the discriminant is always an integer, and it is 0 if and only if the elements in the tuple are linearly dependent over $\mathbf{Q}$. We will also show that the discriminant depends only on the module generated by the tuple and that it decreases in absolute value when we add new elements to the module. After this, the existence of an integral basis will follow easily.

3.1. **Trace and norm.** First we recall some facts and definitions from Part II Galois Theory. Let $L|K$ be a finite extension of fields. With $\alpha \in L$, we write m_α for the linear transformation on L considered a vector space over K given by $x \mapsto \alpha \cdot x$. Then the trace and norm of α is defined as

$$\mathrm{Tr}_{L|K}(\alpha) = \mathrm{tr}(m_\alpha), \quad \mathrm{N}_{L|K}(\alpha) = \det(m_\alpha).$$

The trace and the norm have the following properties.

- If $\alpha \in K$, then $\mathrm{Tr}_{L|K}(\alpha) = [L : K]\alpha$ and $\mathrm{N}_{L|K}(\alpha) = \alpha^{[L:K]}$.
- The trace is additive and the norm is multiplicative:

$$\begin{aligned} \mathrm{Tr}_{L|K}(\alpha + \beta) &= \mathrm{Tr}_{L|K}(\alpha) + \mathrm{Tr}_{L|K}(\beta), \\ \mathrm{N}_{L|K}(\alpha\beta) &= \mathrm{N}_{L|K}(\alpha)\,\mathrm{N}_{L|K}(\beta). \end{aligned}$$

- If $M|L|K$ are finite extensions, then

$$\begin{aligned} \mathrm{Tr}_{M|K}(\alpha) &= \mathrm{Tr}_{L|K}(\mathrm{Tr}_{M|L}(\alpha)), \\ \mathrm{N}_{M|K}(\alpha) &= \mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\alpha)). \end{aligned}$$

Now let K be a number field with $d = [K : \mathbf{Q}]$. We write Tr and N for $\mathrm{Tr}_{K|\mathbf{Q}}$ and $\mathrm{N}_{K|\mathbf{Q}}$. Recall that there are d distinct embeddings of K into $\mathbf{C}$, which we denote by $\sigma_1, \dots, \sigma_d$. (If $K = \mathbf{Q}(\alpha)$, and f is a minimal polynomial of α, then the images of α under the embeddings are precisely the roots of f, and the image of α determines the embedding uniquely.) We can express the trace and the norm using the embeddings as

$$\mathrm{Tr}(\alpha) = \sigma_1(\alpha) + \ldots + \sigma_d(\alpha), \quad \mathrm{N}(\alpha) = \sigma_1(\alpha) \cdots \sigma_d(\alpha)$$

for $\alpha \in K$.

Let $\alpha \in K$, and let $f(x) = x^d + \ldots + a_1 x + a_0 \in \mathbf{Z}[x]$ be its minimal polynomial. Then

$$\mathrm{Tr}(\alpha) = -a_{d-1}, \quad \mathrm{N}(\alpha) = (-1)^d a_0.$$

As a corollary of this, we see that traces and norms of algebraic integers are (rational) integers.

3.2. **Discriminants.** Let K be a number field of degree d and denote by $\sigma_1, \dots, \sigma_d : K \to \mathbf{C}$ the complex embeddings, as above.

Definition 18. The discriminant of a d-tuple $(\alpha_1, \dots, \alpha_d) \in K$ is defined as

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det(\sigma_i(\alpha_j))^2.$$

Here and throughout this note, we will write $\det(a_{ij})$ for determinants whose entries are a_{ij} with the indices running through their ranges, which should always be clear form the context.

Example 19. Let $\alpha \in K$ such that $K = \mathbf{Q}(\alpha)$, and write f for its minimal polynomial. An important d-tuple is $1, \alpha, \dots, \alpha^{d-1}$, because it is a basis for $\mathbf{Z}[\alpha]$ as a $\mathbf{Z}$-module. For this tuple, we have

$$\operatorname{disc}(1, \alpha, \dots, \alpha^{d-1}) = \prod_{1 \le i < j \le d} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{n(n-1)/2} \operatorname{N}(f'(\alpha)).$$

This can be proved by computing the Vandermonde determinant $\det(\sigma_i(\alpha^j))$. See the first example sheet.

Lemma 20. *We have*

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det(\operatorname{Tr}(\alpha_i \alpha_j)).$$

If $\alpha_1 \dots, \alpha_d \in \mathcal{O}_K$, $\operatorname{disc}(\alpha_1, \dots, \alpha_d) \in \mathbf{Z}$.

Proof. Writing $[a_{ij}]_{ij}$ for the $d \times d$ matrix whose ij entry is a_{ij}, we have

$$[\operatorname{Tr}(\alpha_i \alpha_k)]_{ik} = [\sigma_j(\alpha_i)]_{ij} [\sigma_j(\alpha_k)]_{jk}.$$

Using that the determinant does not change if we take the transpose of a matrix, and that it is multiplicative, we get

$$\det(\operatorname{Tr}(\alpha_i \alpha_j)) = \det(\sigma_i(\alpha_j))^2,$$

as required. □

Lemma 21. *We have*

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = 0$$

if and only if $\alpha_1, \dots, \alpha_d$ *are linearly dependent over* $\mathbf{Q}$.

Proof. If $\alpha_1, \dots, \alpha_d$ are linearly dependent over $\mathbf{Q}$, then the rows (and also the columns) of the matrix

$$[\operatorname{Tr}(\alpha_i \alpha_j)]_{ij}$$

are linearly dependent, hence its determinant is 0, as required.

For the converse, we suppose to the contrary that $\alpha_1, \dots, \alpha_d$ are linearly independent over $\mathbf{Q}$, yet $\det(\operatorname{Tr}(\alpha_i \alpha_j)) = 0$. Then the rows of $[\operatorname{Tr}(\alpha_i \alpha_j)]_{ij}$ are linearly dependent over $\mathbf{Q}$, hence there are $a_1, \dots, a_d \in \mathbf{Q}$, not all 0, such that

$$0 = a_1 \operatorname{Tr}(\alpha_1 \alpha_j) + \dots + a_d \operatorname{Tr}(\alpha_d \alpha_j) = \operatorname{Tr}((a_1 \alpha_1 + \dots + a_d \alpha_d) \alpha_j)$$

for all j.

Since $\alpha_1, \dots, \alpha_d$ are linearly independent, they form a $\mathbf{Q}$-basis of K. By linearity of the trace, we have

$$\mathrm{Tr}((a_1\alpha_1 + \ldots + a_d\alpha_d)\beta) = 0$$

for all $\beta \in K$. Using again the linear independence of $\alpha_1, \dots, \alpha_d$, we see that $(a_1\alpha_1 + \ldots + a_d\alpha_d) \neq 0$. We plug in $\beta = (a_1\alpha_1 + \ldots + a_d\alpha_d)^{-1}$ into the above identity and get

$$\mathrm{Tr}(1) = 0,$$

which is our desired contradiction. □

Corollary 22. *The numbers $\alpha_1, \dots, \alpha_d$ are linearly independent over $\mathbf{Q}$ if and only if the vectors $(\sigma_1(\alpha_j), \dots, \sigma_d(\alpha_j)) \in \mathbf{C}^d$ for $j = 1, \dots, d$ are linearly independent over $\mathbf{C}$.*

Proof. Both properties are equivalent to $\mathrm{disc}(\alpha_1, \dots, \alpha_d) \neq 0$. □

3.3. **Geometric interpretation.** We give a geometric interpretation of discriminants. For now, this is not strictly necessary for our development of the theory, and it will just serve as a source of intuition. However, later on in the course, we will rely on it more.

Let K be a number field of degree d over $\mathbf{Q}$. Recall the d distinct embeddings $\sigma_1, \dots, \sigma_d : K \to \mathbf{C}$. We denote by r the number of the real embeddings, that is those that send K into $\mathbf{R}$. We assume, as we may, that $\sigma_1, \dots, \sigma_r$ are the real embeddings. The remaining embeddings come in pairs of complex conjugates. We write $s = (d - r)/2$, and denote by $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$ the s pairs of complex embeddings of K. (These are just a relabelling of $\sigma_{r+1}, \dots, \sigma_d$.)

We consider the map $\Sigma : K \to \mathbf{R}^d$ defined by

$$\Sigma(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \dots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha)))^T.$$

This is clearly a homomorphism of additive groups.

Lemma 23. *For $\alpha_1, \dots, \alpha_d \in K$, we have*

$$(-4)^s \det(\Sigma(\alpha_1), \dots, \Sigma(\alpha_d))^2 = \mathrm{disc}(\alpha_1, \dots, \alpha_d),$$

where the determinant on the left is a combination of d column vectors listed. In particular, $\Sigma(\alpha_1), \dots, \Sigma(\alpha_d)$ are linearly independent over $\mathbf{R}$ if and only if $\mathrm{disc}(\alpha_1, \dots, \alpha_d) \neq 0$.

Proof. Fix some $k \in \{1, \dots, s\}$. Two of the rows of the matrix $[\sigma_i(\alpha_j)]_{ij}$ are equal to $\tau_k(\alpha_1), \dots, \tau_k(\alpha_d)$ and $\overline{\tau_k}(\alpha_1), \dots, \overline{\tau_k}(\alpha_d)$. We add the second of these to the first, and then subtract half of the result from the second. After these row operations, the two rows of the matrix will be replaced by

$$2\,\mathrm{Re}(\tau_k(\alpha_1)), \dots, 2\,\mathrm{Re}(\tau_k(\alpha_d)), \quad \text{and} \quad -i\,\mathrm{Im}(\tau_k(\alpha_1)), \dots, -i\,\mathrm{Im}(\tau_k(\alpha_d)).$$

We can do this for all k, and get

$$(-2i)^s \cdot \det(\Sigma(\alpha_1), \dots, \Sigma(\alpha_d)) = \pm \det(\sigma_i(\alpha_j)),$$

with the sign depending on the sign of the permutation that moves $\sigma_{r+1}, \ldots, \sigma_d$ into $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$. Squaring the above equation will give the claim. □

Let Λ be a lattice in $\mathbf{R}^d$, that is, an additive subgroup of the form $v_1\mathbf{Z} \oplus \ldots \oplus v_d\mathbf{Z}$ for some linearly independent $v_1, \ldots, v_d \in \mathbf{R}^d$. A fundamental domain for Λ is a bounded Borel set $F \subset \mathbf{R}^d$ that contains exactly 1 point in each coset $u + \Lambda$ for $u \in \mathbf{R}^d$. (Many authors use a different notion of a fundamental domain. If you do not know what a Borel set is, do not despair; it is a regularity condition that allows a nice definition of volume. For the purposes of this course, you do not need to know more.)

Example 24. The fundamental parallelepiped, that is the set

$$[0,1) \cdot v_1 + \ldots + [0,1) \cdot v_d$$

is a fundamental domain and it has volume (that is, Lebesgue measure) $|\det(v_1, \ldots, v_d)|$.

Lemma 25. *All fundamental domains of a lattice have the same volume.*

This common value of volume is called the covolume of Λ and it is denoted by $\mathrm{coVol}(\Lambda)$. We note that

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_d) = (-4)^s \,\mathrm{coVol}(\Sigma(\alpha_1)\mathbf{Z} + \ldots + \Sigma(\alpha_d)\mathbf{Z})^2.$$

The discriminant can be interpreted as a quantity that measures how dense the lattice spanned by $\Sigma(\alpha_j)$ is in $\mathbf{R}^d$.

Proof. Let F_1, F_2 be two fundamental domains. Notice that $\mathbf{R}^d$ is a disjoint union of the sets $F_1 + u$ for $u \in \Lambda$. We have

$$\mathrm{Vol}(F_2) = \sum_{u \in \Lambda} \mathrm{Vol}(F_2 \cap (F_1 + u)).$$

(By the boundedness condition for fundamental domains, the above sum can be made finite, but if you took Part II Probability and Measure, you will know that countable sums are OK.) Similarly,

$$\mathrm{Vol}(F_1) = \sum_{u \in \Lambda} \mathrm{Vol}(F_1 \cap (F_2 - u)).$$

Now the claim follows by

$$F_2 \cap (F_1 + u) = F_1 \cap (F_2 - u) + u$$

and translation invariance of volume. □

3.4. **More on discriminants.** We show that the discriminant of a tuple depends only on the module it generates, and then we discuss the relationship between the discriminants of a module and a submodule. These follow easily from the above geometric interpretation, but we give an algebraic proof.

Let K be a number field of degree d over $\mathbf{Q}$.

Proposition 26. *Let $\alpha_1, \dots, \alpha_d \in K$ and $\beta_1, \dots, \beta_d \in K$ be two tuples of $\mathbf{Q}$-linearly independent elements. Let $A \in \mathbf{Q}^{d\times d}$ be such that*

$$(\beta_1, \dots, \beta_d)^T = A(\alpha_1, \dots, \alpha_d)^T.$$

Then

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

If $\beta_1, \dots, \beta_d \in \mathbf{Z}\alpha_1 + \dots + \mathbf{Z}\alpha_d$, then

$$|\operatorname{disc}(\beta_1, \dots, \beta_d)| \geq |\operatorname{disc}(\alpha_1, \dots, \alpha_d)|.$$

If the tuples $\alpha_1, \dots, \alpha_d$ and $\beta_1, \dots, \beta_d$ generate the same module then their discriminants equal.

Thanks to this proposition, we can define the discriminant of a module as the discriminant of any generating d-tuple. Where the rank of the module is less than d, its discriminant is 0.

Proof. We note that

$$[\sigma_j(\beta_i)]_{ij} = A[\sigma_j(\alpha_i)]_{ij}.$$

Now the claim follows by the definition of discriminants and the multiplicative property of determinants.

If $\beta_1, \dots, \beta_d \in \mathbf{Z}\alpha_1 + \dots + \mathbf{Z}\alpha_d$, then A has integer entries, and hence $\det(A)^2 \in \mathbf{Z}_{\geq 0}$. By linear independence, $\det(A) \neq 0$, and

$$|\operatorname{disc}(\beta_1, \dots, \beta_d)| \geq |\operatorname{disc}(\alpha_1, \dots, \alpha_d)|.$$

If $\alpha_1, \dots, \alpha_d$ and $\beta_1, \dots, \beta_d$ generate the same module, we get the reverse inequality by exchanging the roles of the two bases. The fact that the two discriminants have the same sign follows from the first claim, because $\det(A)^2 > 0$. This also follows from our observation in the previous section that the sign of the discriminant depends only on the number of complex embeddings of K. □

Proposition 27. *Let $M_1 \subset M_2$ be two modules in K of rank d. Then*

$$\operatorname{disc}(M_1) = |M_2/M_1|^2 \operatorname{disc}(M_2).$$

This follows from the previous proposition, if we are able to compute the determinant of the change of basis matrix. This is made easy by the following result from Part IB Groups, Rings and Modules.

Theorem 28. *Let $M_1 \subset M_2$ be two free $\mathbf{Z}$-modules of rank d. Then M_2 has a basis $\alpha_1, \dots, \alpha_d$, and there are $a_1, \dots, a_d \in \mathbf{Z}$ such that $a_1|a_2|\dots|a_d$ and that $a_1\alpha_1, \dots, a_d\alpha_d$ is a basis for M_1.*

Proof of Proposition 27. This follows by Proposition 26 and Theorem 28. □

Theorem 29. *Let K be a number field of degree d. A tuple $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ is an integral basis if and only if $|\operatorname{disc}(\alpha_1, \ldots, \alpha_d)|$ is minimal among all tuples subject to the condition that it is not 0. In particular, an integral basis always exists.*

Proof. Let $|\operatorname{disc}(\alpha_1, \ldots, \alpha_d)| \neq 0$ be minimal among all tuples in $\mathcal{O}_K$. Write $M = \mathbf{Z}\alpha_1 + \ldots + \mathbf{Z}\alpha_d$. Let $\beta \in \mathcal{O}_K$. We need to show that $\beta \in M$. Consider the module $M + \beta\mathbf{Z}$. By the previous proposition, we have

$$\operatorname{disc}(M) = |(M + \beta\mathbf{Z})/M|^2 \operatorname{disc}(M + \beta\mathbf{Z}).$$

By the minimality of $|\operatorname{disc}(M)|$, we have $|(M + \beta\mathbf{Z})/M| = 1$, hence $M = M + \beta\mathbf{Z}$, and $\beta \in M$.

Since the discriminant only takes integer values, the minimum is attained, hence an integral basis exists. □

Definition 30. Let K be a number field. The discriminant $\operatorname{disc}(K)$ of K is defined as the discriminant of any integral basis of $\mathcal{O}_K$.

Example 31. Let $m \in \mathbf{Z}$ be a square free number, and let $K = \mathbf{Q}(\sqrt{m})$. If $m \equiv 1 \mod 4$, then an integral basis of K is

$$1, \frac{1+\sqrt{m}}{2},$$

and

$$\operatorname{disc}(K) = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = \Big(\frac{1-\sqrt{m}}{2} - \frac{1+\sqrt{m}}{2}\Big)^2 = m.$$

If $m \not\equiv 1 \mod 4$, then an integral basis of K is $1, \sqrt{m}$ and

$$\operatorname{disc}(K) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = (-\sqrt{m} - \sqrt{m})^2 = 4m.$$

Proposition 32. *Let $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ be $\mathbf{Q}$-linearly independent. Then there is $q \in \mathbf{Z}_{>0}$ with $q^2 | \operatorname{disc}(\alpha_1, \ldots, \alpha_d)$ such that all elements of $\mathcal{O}_K$ can be written in the form*

$$\frac{a_1\alpha_1 + \ldots + a_d\alpha_d}{q}$$

for some $a_1, \ldots, a_d \in \mathbf{Z}$.

Proof. We take

$$q = \Big(\frac{\operatorname{disc}(\alpha_1, \ldots, \alpha_d)}{\operatorname{disc}(K)}\Big)^2.$$

Then we know that

$$|\mathcal{O}_K/(\mathbf{Z}\alpha_1 + \ldots + \mathbf{Z}\alpha_d)| = q.$$

Let $\beta \in \mathcal{O}_K$. We have $q\beta \in \mathbf{Z}\alpha_1 + \ldots + \mathbf{Z}\alpha_d$, which proves the claim. □

4. Unique factorization of ideals

The ring of integers of a number field may fail to be a unique factorisation domain. Indeed, consider the number field $K = \mathbf{Q}(\sqrt{-5})$ and its ring of integers $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$. Now we have the equation

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

Seeing this, one might hope that there are some primes $\pi_1, \pi_2, \pi_3, \pi_4$ such that

$$2 = \pi_1\pi_2, \quad 3 = \pi_3\pi_4, \quad 1 + \sqrt{-5} = \pi_1\pi_3, \quad 1 - \sqrt{-5} = \pi_2\pi_4.$$

However, looking at norms, we see that we must have

$$N(\pi_1) | \gcd(N(2), n(1 + \sqrt{-5})) = 2.$$

Unfortunately, the numbers that occur as norms of elements of $\mathcal{O}_K$ are precisely the numbers of the form a^2+5b^2 with $a, b \in \mathbf{Z}$, and ± 2 are not of this form. So no such π_1 may exist. (We cannot have $N(\pi_1) = \pm 1$, because then π_1 was a unit. We will discuss this later in the course.)

To remedy this issue, Kummer had a brilliant idea. He was motivated by geometers who added "ideal points" to the Euclidean plane to make parallel lines meet, and this way they constructed the projective plane. [(1)] He thought that when two numbers that should have a common prime divisor does not have one, we could introduce an "ideal prime" that will be this common divisor. He gave a very hands-on construction of "ideal primes" in cyclotomic fields, and he also described how to decompose the elements in the ring of integers as products of them.

This construction of Kummer was extremely successful. One of the crucial insights needed to generalize it to arbitrary number fields is that one needs to work with the ring of integers rather than another subring of K. Kummer was lucky that $\mathcal{O}_{\mathbf{Q}(\theta_n)} = \mathbf{Z}[\theta_n]$ for cyclotomic fields, so the "obvious" ring he chose to work with was also the right one. To illustrate the issue, consider the following calculation in the ring $\mathbf{Z}[\sqrt{5}]$:

$$(1 + \sqrt{5})^3 = 16 + 8\sqrt{5} = 2^3 \cdot (2 + \sqrt{5}).$$

Now $(2+\sqrt{5})$ is a unit, because $(2+\sqrt{5})(\sqrt{5}-2) = 1$, hence $(1+\sqrt{5})^3$ and 2^3 should have the same factorization to "ideal primes", because they are associates. On the other hand $1 + \sqrt{5}$ and 2 are not associates, so they should have different factorizations. (Indeed, neither $(1 + \sqrt{5})/2$, nor $2/(1 + \sqrt{5}) = (\sqrt{5} - 1)/2$ are in the ring $\mathbf{Z}[\sqrt{5}]$.) This problem is resolved if we work in the ring of integers, which is

[(1)] This is historically inaccurate. He was motivated by the work of Poncelet on "ideal secants".

$\mathbf{Z}[(1+\sqrt{5})/2]$. Indeed, in that ring $(1+\sqrt{5})/2$ is a unit, hence 2 and $1+\sqrt{5}$ are associates.

The generalization to arbitrary number fields was achieved by Dedekind and Kronecker in two conceptually different ways. We follow Dedekind. There are two tasks. We need to construct the set of "ideal numbers", and then we need to find out which elements of the ring of integers are divisible by which "ideal primes". Dedekind had a brilliant idea to do both of these in one go. He decided to identify "ideal numbers" with the set of elements in $\mathcal{O}_K$ that are divisible by them. This way he only needed to work out which subsets of $\mathcal{O}_K$ will correspond to an "ideal number" in that manner. He arrived at the notion of ideals, which will be familiar from Part 1B Groups, Rings and Modules.

Definition 33. Let K be a number field. An ideal in $\mathcal{O}_K$ is a subset I that is closed under addition and multiplication by elements of $\mathcal{O}_K$, that is, $\alpha \in \mathcal{O}_K$ and $\beta \in I$ implies $\alpha\beta \in I$.

Example 34. The principal ideal generated by an element $\alpha \in \mathcal{O}_K$ is

$$\langle \alpha \rangle = \langle \alpha \rangle_{\mathcal{O}_K} = \alpha\mathcal{O}_K = \{\alpha\beta : \beta \in \mathcal{O}_K\}.$$

This way we can associate for each element $\alpha \in \mathcal{O}_K$ a corresponding ideal $\langle \alpha \rangle$, and we have $\langle \alpha \rangle = \langle \beta \rangle$ if and only if $\alpha = u\beta$ for some unit $u \in \mathcal{O}_K$. [Exercise: check this.] This is very nice, because α and β should have the same prime factorization if and only if $\alpha = u\beta$ for some unit $u \in \mathcal{O}_K$.

We can introduce a multiplication operation on ideals as follows:

$$IJ = \{\alpha_1\beta_1 + \ldots + \alpha_k\beta_k : k \in \mathbf{Z}_{\geq 1}, \alpha_j \in I, \beta_j \in J\}.$$

This is easily seen to be associative. Observe that for principal ideals, we have $\langle \alpha\beta \rangle = \langle \alpha \rangle \langle \beta \rangle$, so the map $\alpha \mapsto \langle \alpha \rangle$ is homomorphism of semigroups.

An ideal $I \subsetneq \mathcal{O}_K$ is a prime ideal if whenever $\alpha\beta \in I$ for some $\alpha, \beta \in \mathcal{O}_K$ then at least one of α and β is in I. This is easily seen to be equivalent to the property that $\mathcal{O}_K/I$ is an integral domain, that is, a non-zero (unital, commutative) ring[(2)] without zero divisors. In addition, a principal ideal $\langle \alpha \rangle$ is a prime ideal if and only if α is a prime element of $\mathcal{O}_K$.

Our next goal is the following remarkable theorem.

Theorem 35. *Let K be a number field. Then every non-zero ideal of $\mathcal{O}_K$ can be written as a product of non-zero prime ideals and this decomposition is unique up to the order of the prime ideals.*

Definition 36. We call a non-zero prime ideal in $\mathcal{O}_K$ a prime.

[(2)]For the purposes of this note, every ring is assumed to be commutative and unital.

Remark 37. A word of caution. Even though ideals have unique factorization, this does not mean that we have a unique factorization domain. While there is a natural way to define addition on ideals by

$$I + J = \{\alpha + \beta : \alpha \in I, \beta \in I\},$$

this does not turn the set of ideals into a ring, and we do not have $\langle\alpha\rangle + \langle\beta\rangle = \langle\alpha + \beta\rangle$, in general.

Ideals in $\mathcal{O}_K$ have three important properties that we will rely on in this section.

Lemma 38.

(1) *Every ideal in $\mathcal{O}_K$ is finitely generated, that is, it is of the form $\alpha_1\mathcal{O}_K + \ldots + \alpha_k\mathcal{O}_K$ for some $k \in \mathbf{Z}_{>0}$ and $\alpha_1, \ldots, \alpha_k \in \mathcal{O}_K$.*
(2) *Every increasing sequence $I_1 \subset I_2 \subset I_3 \subset \ldots$ of ideals must stabilize, that is, $I_k = I_{k+1} = I_{k+2} = \ldots$ for some k.*
(3) *Every collection of ideals contains one that is maximal with respect to inclusion.*

These three properties are, in fact equivalent. When they hold for some ring, it is called Noetherian.

Proof. Item (1) follows because ideals are finitely generated even as $\mathbf{Z}$-modules, being submodules of the finitely generated $\mathbf{Z}$-module $\mathcal{O}_K$.

For item (2), consider $I = \bigcup I_j$. This is an ideal, so must be finitely generated. Then the generators are all contained in I_k for some k, hence $I_k = I$ for all $j \geq k$.

If item (3) was not true, we could find an infinite sequence of strictly increasing ideals contradicting item (2). □

To state the second property, we need a definition.

Definition 39. An ideal $I \subsetneq \mathcal{O}_K$ is maximal if the only ideals $J \subset \mathcal{O}_K$ with $I \subset J$ are $J = I$ and $J = \mathcal{O}_K$.

It follows immediately from the definitions that an ideal I is maximal if and only if $\mathcal{O}_K/I$ is a field.

Lemma 40. *Maximal ideals and non-zero prime ideals are the same.*

Proof. First we show that the quotient ring $\mathcal{O}_K/I$ is finite for all ideals I. Since every ideal contains a principal ideal, it is enough to see this for principal ideals. If $\alpha_1, \ldots, \alpha_d$ is an integral basis and $I = \langle\beta\rangle$, then $\beta\alpha_1, \ldots, \beta\alpha_d$ generate I freely as a $\mathbf{Z}$-module. Then I has the same rank as a $\mathbf{Z}$-module as $\mathcal{O}_K$, hence $\mathcal{O}_K/I$ is indeed finite. Now we note that finite integral domains are all fields. (Show that they are equal to their quotient fields.) From this it follows that maximal and non-zero prime ideals are indeed the same. □

Lemma 41. *Let $\alpha \in K$ Suppose that there is a finitely generated $\mathcal{O}_K$-module M with $\alpha M = M$, then we have $\alpha \in \mathcal{O}_K$.*

When an integral domain satisfies this property, with its field of fractions playing the role of K, it is said to be integrally closed.

Proof. Note that finitely generated $\mathcal{O}_K$-modules are the same as finitely generated $\mathbf{Z}$-modules, because $\mathcal{O}_K$ is finitely generated as a $\mathbf{Z}$-module. Hence an α satisfying the above property is an algebraic integer, therefore is contained in $\mathcal{O}_K$. □

Integral domains that satisfy the conclusions of the above three lemmata are called Dedekind domains, and the ideals of these also satisfy the unique factorization property. For concreteness, we give the proof for $\mathcal{O}_K$, but it carries over to Dedekind domains without significant change.

4.1. **Proof of unique factorization.** Let $I \subset \mathcal{O}_K$ be an ideal. By the Noetherian property the set of proper ideals containing I has a maximal element P. Then P must also be a maximal ideal and hence a prime ideal, and $P \supset I$ by construction.

Now it would be very helpful if we could also conclude that $P|I$, that is, there is some ideal $I' \subset \mathcal{O}_K$ such that $I = PI'$. This is not unreasonable to expect. Indeed, for principal ideals, $\langle\alpha\rangle|\langle\beta\rangle$ is trivially equivalent to $\langle\alpha\rangle \supset \langle\beta\rangle$, and if $J|I$ for some arbitrary ideals $I, J \subset \mathcal{O}_K$, then $J \supset I$ again trivially. We hope that the converse may also be true. This is not true for general rings, but it holds for $\mathcal{O}_K$ and even for all Dedekind domains. This is closely related to Theorem 35, and we will prove the two things together.

It is useful to extend the notion of ideals.

Definition 42. Let K be a number field. A fractional ideal in K is a finitely generated $\mathcal{O}_K$-submodule of K.

Lemma 43. *If $I \subset K$ is a fractional ideal, then there is some $a \in \mathbf{Z}$ such that*

$$aI = \{a \cdot \alpha : \alpha \in I\}$$

is an ideal in $\mathcal{O}_K$.

Conversely, if $I \subset \mathcal{O}_K$ is an ideal and $\alpha \in K$, then αI is a fractional ideal.

Proof. For the first claim, let $I = \alpha_1\mathcal{O}_K + \ldots + \alpha_n\mathcal{O}_K$ be a fractional ideal generated by some $\alpha_1, \ldots, \alpha_n \in K$. Write the α_j as $\mathbf{Q}$-linear combinations of some integral basis of $\mathcal{O}_K$, and choose a to be the common denominator of all the coefficients.

The converse follows easily from the definitions and we leave it as an exercise. □

We can extend the multiplication operation to fractional ideals using the same formula as for ideals in $\mathcal{O}_K$. It would be very helpful if nonzero fractional ideals formed a multiplicative group, but we do not

know yet if there is always an inverse. As a first step, we prove this for prime ideals.

Proposition 44. *Let K be a number field, and let $P \subset \mathcal{O}_K$ be a non-zero prime ideal. Then there is a fractional ideal P' such that $PP' = \langle 1 \rangle$.*

Begining the proof of Proposition 44. It is natural to try defining

$$P' = \{\alpha \in K : \alpha P \subset \mathcal{O}_K\}.$$

This is clearly an $\mathcal{O}_K$ module, and $\beta P' \subset \mathcal{O}_K$ for any $\beta \in P$, so P' is a fractional ideal. If there is some fractional ideal P' with the required properties, this will be it.

By definition, $PP' \subset \mathcal{O}_K$ and it is an ideal. Also, $\mathcal{O}_K \subset P'$, hence $PP' \supset P\mathcal{O}_K = P$. Since P is a prime ideal, it is also a maximal ideal by the second property of $\mathcal{O}_K$ discussed above. Therefore, either $PP' = \langle 1 \rangle$ or $PP' = P$. To rule out the second case, it is enough to prove that there is some $\alpha \in P'$ that is not in $\mathcal{O}_K$. Indeed, if we manage to do this, then $PP' \supset \alpha P \not\subset P$, for otherwise $\alpha \in \mathcal{O}_K$ by virtue of $\mathcal{O}_K$ being integrally closed. In what follows, we will exhibit a suitable α, but this requires some preparations. □

Lemma 45. *Let $I \subset \mathcal{O}_K$ be an non-zero ideal. Then there are $k \in \mathbf{Z}_{\geq 0}$ and non-zero prime ideals $P_1, \dots, P_k$ (with repetitions allowed) such that $P_1 \cdots P_k \subset I$.*

In the following proof, we introduce a proof technique called Noetherian induction.

Proof. Suppose to the contrary that the statement of the lemma is not true for all ideals. Let I be an ideal that is maximal among those ideals for which the lemma fails. Then I cannot be a prime ideal, for we may take $k = 1$ and $P_1 = I$ to show that the lemma holds for prime ideals.

Then there are some $\alpha, \beta \in \mathcal{O}_K \backslash I$ such that $\alpha\beta \in I$, for otherwise I would be a prime ideal. Now $\langle \alpha \rangle + I, \langle \beta \rangle + I \supsetneq I$, hence there are prime ideals $P_1, \dots, P_k$ and $Q_1, \dots, Q_l$ such that $P_1 \cdots P_k \subset \langle \alpha \rangle + I$ and $Q_1 \cdots Q_l \subset \langle \beta \rangle + I$. We observe that

$$P_1 \cdots P_k Q_1 \cdots Q_l \subset (\langle \alpha \rangle + I)(\langle \beta \rangle + I) \subset I$$

showing that the lemma holds for I, a contradiction. □

We will need the following observation in the upcoming proof. If I, J are ideals and $IJ \subset P$ for a prime ideal P, then $I \subset P$ or $J \subset P$. Note that for principal ideals $I = \langle \alpha \rangle$ and $J = \langle \beta \rangle$, this is just the defining property of prime ideals. It is easy to verify the above more general statement. Indeed, suppose to the contrary that $I \not\subset P$ and $J \not\subset P$. Then there are $\alpha \in I \backslash P$ and $\beta \in J \backslash P$. Hence $\alpha\beta \in P$, but $\alpha, \beta \notin P$, a contradiction.

Completing the proof of Proposition 44. Let P and P' be as in the beginning of the proof. Let $\beta \in P$ be arbitrary. We aim to find a suitable $\gamma \in \mathcal{O}_K$ such that $\gamma \notin \langle\beta\rangle$ but $\langle\gamma\rangle P \subset \langle\beta\rangle$. Taking $\alpha = \gamma/\beta$, we have $\alpha \notin \mathcal{O}_K$, but $\alpha P \subset \mathcal{O}_K$. In light of the first part of the proof, we will be done once a suitable γ with the claimed properties is constructed.

Let k be minimal such that there are non-zero prime ideals $P_1, \ldots, P_k$ with $P_1 \cdots P_k \subset \langle\beta\rangle$. We note that $P_1 \cdots P_k \subset P$, hence $P_j \subset P$ for some j, by the observation we made before the proof. But P_j is also a prime ideal, and hence a maximal ideal, so $P = P_j$. We assume, as we may that $j = k$.

By the minimality of k, we have $P_1 \cdots P_{k-1} \not\subset \langle\beta\rangle$. Therefore, there is $\gamma \in P_1 \cdots P_{k-1} \backslash \langle\beta\rangle$. On the other hand $\gamma P \subset P_1 \cdots P_{k-1} P \subset \langle\beta\rangle$. Therefore, γ satisfies both the required properties, and the proof is complete. □

From now on we write P^{-1} for the ideal P' in Proposition 44.

Proof of Theorem 35. Let $I \subset \mathcal{O}_K$ be an ideal. We first show that I can be written as a product of prime ideals. We use Notherian induction again. Suppose to the contrary that there are some ideals that are not products of prime ideals, and let I be a maximal one among such ideals. We have already observed that there is some prime ideal P_1 such that $I \subset P_1$. Write $J = P_1^{-1} I$. We observe that $J \subset P_1^{-1} P_1 = \mathcal{O}_K$, hence J is an ideal. Also $P_1 J = P_1 P_1^{-1} I = I$. Now $P_1 J = I$ implies $J \supset I$. On the other hand, $J = P_1^{-1} I$ implies $J \neq I$. Indeed, otherwise, we would have $\alpha I \subset I$ for all $\alpha \in P_1^{-1}$, which would imply $P_1^{-1} \subset \mathcal{O}_K$, which is not the case.

By the maximality of I, J can be written as a product $J = P_2 \cdots P_k$ of prime ideals, and hence $I = P_1 J = P_1 \cdots P_k$, a contradiction proving our claim.

Finally, we show the uniqueness of prime factorization. To this end, we prove that if

$$P_1 \cdots P_k = Q_1 \cdots Q_l$$

for some prime ideals $P_1, \ldots, P_k, Q_1, \ldots, Q_l$, then $k = l$ and $P_j = Q_{\sigma j}$ for some permutation σ.

We prove this by induction on $k + l$. The claim is trivial if $k + l = 0$. We suppose that $k + l > 0$ and that the claims holds for all smaller values of $k + l$. We assume, as we may, that $k > 0$. Now it is enough to show that $l > 0$ and $P_1 = Q_j$ for some $j \leq l$. To this end, we note that $P_1 \supset Q_1 \cdots Q_l$. This immediately implies that $l > 0$ and that $Q_j \subset P_1$ for some j. Being a prime ideal, Q_j is also a maximal ideal, hence $Q_j = P_1$, as required. □

Corollary 46. *Every non-zero fractional ideal $I \subset K$ has an inverse, that is, there is a fractional ideal I^{-1} such that $II^{-1} = \langle 1\rangle$. In other words, fractional ideals form a group with respect to multiplication.*

Proof. We have already proved this for prime ideals. Then all ideals $J \subset \mathcal{O}_K$ also have inverses. Indeed, we can get the inverse of J by multiplying together the inverses of all prime factors of J. Finally, a fractional ideal I can be written in the form $I = J_1 J_2^{-1}$. (We may even take J_2 to be principal.) We see that the fractional ideal $J_1^{-1} J_2$ is an inverse of I. □

Corollary 47. *Let $I, J \subset \mathcal{O}_K$ be two ideals. Then $I \supset J$ if and only if there is an ideal $I_2 \subset \mathcal{O}_K$ such that $II_2 = J$.*

Where one and hence both of the above two equivalent conditions hold for some ideals I and J, we say that I divides J and denote this fact by $I|J$.

Proof. We have already discussed that $II_2 = J$ implies $I \supset J$. For the converse, it is enough to show that $I \supset J$ implies $I^{-1}J \subset \mathcal{O}_K$. To this end, we observe that $\alpha I \subset J \subset I$ for all $\alpha \in I^{-1}J$. Thus $\alpha \in \mathcal{O}_K$ as $\mathcal{O}_K$ is integrally closed. □

In analogy with $\mathbf{Z}$, for two ideals I and J we define their greatest common divisor $\gcd(I, J)$ as the smallest ideal dividing both I and J. This may sound odd, but the point is that the smaller the ideal, the larger the residue ring. Similarly, we define the least common multiple $\mathrm{lcm}(I, J)$ as the largest ideal that is divisible by both I and J. We observe that for all prime ideals P, its multiplicity in the prime factorization of $\gcd(I, J)$ is the minimum of its multiplicities in I and J. Similarly, the multiplicity of P in $\mathrm{lcm}(I, J)$ is the maximum of its multiplicities in I and J. We note further that

$$\gcd(I, J) = I + J, \quad \text{and} \quad \mathrm{lcm}(I, J) = I \cap J.$$

We leave the proof of these facts as exercises.

Corollary 48. *The ring of integers $\mathcal{O}_K$ in a number field is a UFD if and only if it is a PID.*

Proof. Every PID is a UFD, and for $\mathcal{O}_K$ this also follows from the unique factorisation of ideals.

We show that the converse is also true for $\mathcal{O}_K$. Assume that $\mathcal{O}_K$ is a UFD. We note that if $\alpha \in \mathcal{O}_K$ is a prime element, then $\langle \alpha \rangle$ is a prime ideal. Thus, every principal ideal in $\mathcal{O}_K$ is a product of principal prime ideals. Now let I be an arbitrary non-zero ideal, and let $\alpha \in I$. Then $I|\langle \alpha \rangle$, and all prime factors of I are also prime factors of $\langle \alpha \rangle$, hence they must be principal ideals. Then I is a product of principal ideals, hence it must be a principal ideal, too. □

5. Norms of ideals

Definition 49. Let K be a number field, and let $I \subset \mathcal{O}_K$ be a non-zero ideal. The norm $\mathrm{N}(I)$ of I is defined as $|\mathcal{O}_K / I|$.

Recall that we have already observed that $\mathrm{N}(I) < \infty$ for all non-zero ideals. See the proof of Lemma 40. Recall also from Proposition 27 that if $\alpha_1, \dots, \alpha_d$ generate I as a $\mathbf{Z}$-module, then

$$\mathrm{N}(I) = \Big(\frac{\mathrm{disc}(\alpha_1, \dots, \alpha_d)}{\mathrm{disc}(K)}\Big)^{1/2}. \tag{4}$$

Proposition 50. *The norm of ideals is multiplicative, that is, we have*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$$

for all non-zero ideals $I, J \in \mathcal{O}_K$.

Proof. We show this in the special case, where J is a prime ideal. Using this special case repeatedly, we conclude that for all ideals $\widetilde{I}$ with prime factorization $P_1 \cdots P_k$, we have

$$\mathrm{N}(\widetilde{I}) = \mathrm{N}(P_1) \cdots \mathrm{N}(P_k).$$

Using this for I, J and IJ, the general case follows.

From now on, we assume that J is a prime ideal. Let $\alpha_1, \dots, \alpha_{\mathrm{N}(J)}$ be a system of representatives for the residue classes in $\mathcal{O}_K/J$. Let $\beta \in I \backslash IJ$. (We have $IJ \subsetneq I$, for equality would contradict the uniqueness of prime factorization among other things.) We show that $\beta\alpha_1, \dots, \beta\alpha_{\mathrm{N}(J)}$ is a system of representatives for the residue classes modulo IJ in I/IJ. This proves $\mathrm{N}(J) = |I/IJ|$, and we can conclude by $|\mathcal{O}_K/IJ| = |\mathcal{O}_K/I| \cdot |I/IJ|$.

Since $\beta \in I$, $\beta\alpha_1, \dots, \beta\alpha_{\mathrm{N}(J)}$ are all in I. We show that they represent all residue classes modulo IJ. To this end, let $\gamma \in I$. We note that $\langle\beta\rangle = IP_1 \cdots P_k$ for some prime ideals $P_1, \dots, P_k$, none of which is J. Thus $\langle\beta\rangle + IJ = \gcd(\langle\beta\rangle, IJ) = I$. This shows that $\gamma - \beta\alpha \in IJ$ for some $\alpha \in \mathcal{O}_K$. We have $\alpha - \alpha_j \in J$ for some j, so $\gamma - \beta\alpha_j \in IJ$. This shows that $\beta\alpha_1, \dots, \beta\alpha_{\mathrm{N}(J)}$ indeed represent all classes in I/IJ.

Now we show that $\beta\alpha_1, \dots, \beta\alpha_{\mathrm{N}(J)}$ represent distinct classes. Suppose that $\beta\alpha_i - \beta\alpha_j \in IJ$ for some i, j. We show that then $i = j$ necessarily. Indeed, we have $IJ | \langle\beta\rangle\langle\alpha_i - \alpha_j\rangle$. We have already observed that $\langle\beta\rangle = IP_1 \cdots P_k$ for some prime ideals $P_1, \dots, P_k$, none of which is J. Then $J | \langle\alpha_i - \alpha_j\rangle$, hence $i = j$, as required. □

Proposition 51. *Let $\alpha \in \mathcal{O}_K$. Then*

$$\mathrm{N}(\langle\alpha\rangle) = |\,\mathrm{N}(\alpha)|,$$

where the N *on the right stands for the field norm* $\mathrm{N} = \mathrm{N}_{K|Q}$.

Proof. Let $\alpha_1, \dots, \alpha_d$ be an integral basis. By definition

$$\mathrm{disc}(K) = \mathrm{disc}(\alpha_1, \dots, \alpha_d) = \det(\sigma_i(\alpha_j))^2,$$

where $\sigma_1, \dots, \sigma_j : K \to \mathbf{C}$ are the complex embeddings. In addition, $\alpha\alpha_1, \dots, \alpha\alpha_d$ generate $\langle\alpha\rangle$ as a $\mathbf{Z}$-module, and

$$\mathrm{disc}(\alpha\alpha_1, \dots, \alpha\alpha_d) = \det(\sigma_i(\alpha)\sigma_i(\alpha_j))^2.$$

Pulling out the factor $\sigma_i(\alpha)$ from the i'th row for each i, we get

$$\operatorname{disc}(\alpha\alpha_1, \dots, \alpha\alpha_d) = \sigma_1(\alpha)^2 \dots \sigma_d(\alpha)^2 \det(\sigma_i(\alpha_j))^2 = \mathrm{N}(\alpha)^2 \operatorname{disc}(K).$$

Now the claim follows by (4). □

6. Ideals in field extensions

In this section, we discuss how to find all primes in a number field.

Let $L|K$ be an extension of number fields. We will discuss how the primes in L can be related to those of K. For a fractional ideal $I \subset K$, we can associate a fractional ideal in L in a natural way. We define

$$I\mathcal{O}_L = \{\alpha_1\beta_1 + \dots + \alpha_k\beta_k : k \in \mathbf{Z}_{\geq 1}, \alpha_j \in I, \beta_j \in \mathcal{O}_L\}.$$

We observe that $I\mathcal{O}_L$ is indeed a fractional ideal in L, and it is the smallest fractional ideal that contains all elements of I.

We can also associate a fractional ideal in K to a fractional ideal $J \subset L$ by considering $J \cap K$. Again, it is easy to see that this is indeed a fractional ideal.

We note that

$$(I_1\mathcal{O}_L)(I_2\mathcal{O}_L) = (I_1I_2)\mathcal{O}_L \tag{5}$$

for any fractional ideals $I_1, I_2 \subset K$. On the other hand, $(J_1 \cap K)(J_2 \cap K)$ may differ from $J_1J_2 \cap K$ for $J_1, J_2 \subset L$ in general.

If $I \subset \mathcal{O}_K$ and $J \subset \mathcal{O}_L$ are ideals, then $I\mathcal{O}_L$ and $J \cap K$ are also ideals.

Lemma 52. *Let $P \subset \mathcal{O}_K$ and $Q \subset \mathcal{O}_L$ be primes. Then the following two statements are equivalent.*

1. $Q|P\mathcal{O}_L$.
2. $P = Q \cap \mathcal{O}_K$.

Where either (and hence both) of the two statements hold, we say that Q lies over (or above) P and P lies under (or below) Q.

Proof. Assume $Q|P\mathcal{O}_L$. Then $Q \supset P\mathcal{O}_L \supset P$, hence $P \subset Q \cap \mathcal{O}_K$. In addition, $1 \notin Q$, so $Q \cap \mathcal{O}_K \subsetneq \mathcal{O}_K$. Since P is a maximal ideal, we must have $P = Q \cap \mathcal{O}_K$.

Now we prove the other implication. Assume $P = Q \cap \mathcal{O}_K$. Clearly $Q \supset (Q \cap \mathcal{O}_K)\mathcal{O}_L = P\mathcal{O}_L$, so $Q|P\mathcal{O}_L$, as required. □

Lemma 53. *For every prime $Q \subset \mathcal{O}_L$, there is a unique prime $P \subset \mathcal{O}_K$ that lies under it. For every prime $P \subset \mathcal{O}_K$, there is at least one prime $Q \subset \mathcal{O}_L$ that lies above it.*

Proof. For the first statement, we only need to show that $P := Q \cap \mathcal{O}_K$ is a prime. We note that $1 \notin Q$, hence $1 \notin P$ and $P \neq \mathcal{O}_K$. In addition, $\mathcal{O}_L/Q$ is finite, but $\mathcal{O}_K$ is infinite, so there are two distinct $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha - \beta \in Q$. Then necessarily $\alpha - \beta \in P$ so P is non-zero.

Now we show that P is a prime ideal. To that end, let $\alpha, \beta \in \mathcal{O}_K$ with $\alpha\beta \in P \subset Q$. Since Q is a prime ideal, $\alpha \in Q$ or $\beta \in Q$. Then necessarily $\alpha \in P$ or $\beta \in P$, as required.

For the second statement, we show that $P\mathcal{O}_L \subsetneq \mathcal{O}_L$. Then it must have at least one prime divisor. Suppose to the contrary that $P\mathcal{O}_L = \mathcal{O}_L$. Then $(P^{-1}\mathcal{O}_L)(P\mathcal{O}_L) = \mathcal{O}_L$ implies $P^{-1}\mathcal{O}_L = \mathcal{O}_L$. In particular $P^{-1} \subset \mathcal{O}_L$, but also $P^{-1} \subset K$, hence $P^{-1} \subset \mathcal{O}_L \cap K \subset \mathcal{O}_K$. Then

$$\mathcal{O}_K = PP^{-1} \subset P\mathcal{O}_K = P,$$

which is impossible. This contradiction completes the proof. □

Let $Q \subset \mathcal{O}_L$ be a prime that lies above a prime $P \subset \mathcal{O}_K$. There are two important numbers attached to the pair Q, P. The first one is the ramification index $e(Q|P)$, which is the largest integer e such that $Q^e | P\mathcal{O}_L$.

To define the second one, we observe that $\mathcal{O}_L/Q$ and $\mathcal{O}_K/P$ are both finite fields and the latter can be naturally identified with a subfield of the former, because $\mathcal{O}_K \cap Q = P$. Now we define the inertial degree of Q over P as

$$f(Q|P) = [\mathcal{O}_L/Q : \mathcal{O}_K/P].$$

We note that

$$\mathrm{N}(Q) = \mathrm{N}(P)^{f(Q|P)}.$$

We note that the following tower laws hold. Let $M|L|K$ be field extensions of number fields and let $P \subset \mathcal{O}_K$, $Q \subset \mathcal{O}_L$ and $R \subset \mathcal{O}_M$ be primes such that Q lies over P and R lies over Q. Then R also lies over P and we have

$$f(R|P) = f(R|Q)f(Q|P),$$
$$e(R|P) = e(R|Q)e(Q|P).$$

The first of these follows by the tower law for the degrees of field extensions, and the second follows by (5) and Lemma 53.

Our next goal is the following result about the ramification indices and inertial degrees of primes lying over a given prime in a field extension.

Theorem 54. *Let $L|K$ be an extension of number fields. Let $P \subset \mathcal{O}_K$ be a prime and let $Q_1, \dots, Q_r \subset \mathcal{O}_L$ be the primes lying above P. Then*

$$[L : K] = \sum_{j=1}^{r} e(Q_j|P)f(Q_j|P).$$

We note that

$$\mathrm{N}(P\mathcal{O}_L) = \mathrm{N}(Q_1^{e(Q_1|P)} \cdots Q_r^{e(Q_r|P)}) = \mathrm{N}(P)^{e(Q_1|P)f(Q_1|P)+\dots+e(Q_1|P)f(Q_1|P)}.$$

The theorem follows at once if we show that

$$\mathrm{N}(P\mathcal{O}_L) = \mathrm{N}(P)^{[L:K]}.$$

This is the content of the next proposition.

Proposition 55. *Let $L|K$ be an extension of number fields. Let $I \subset \mathcal{O}_K$ be a non-zero ideal. Then*

$$\mathrm{N}(I\mathcal{O}_L) = \mathrm{N}(I)^{[L:K]}.$$

In the proof, we use the following lemma, which will be proved later on in the course.

Lemma 56. *Let K be a number field and let $I \subset \mathcal{O}_K$ be an ideal. Then there is some $k \in \mathbf{Z}_{>0}$ such that I^k is a principal ideal.*

Proof of Proposition 55. Let k be such that $I^k = \alpha\mathcal{O}_K$ for some α. Then $I^k\mathcal{O}_L = \alpha\mathcal{O}_L$, and we have

$$\mathrm{N}(I^k\mathcal{O}_L) = |\,\mathrm{N}_{L|\mathbf{Q}}(\alpha)| = |\,\mathrm{N}_{K|\mathbf{Q}}(\alpha)|^{[L:K]}.$$

We also note that $(I\mathcal{O}_L)^k = I^k\mathcal{O}_L$, hence

$$\mathrm{N}(I\mathcal{O}_L) = \mathrm{N}(I^k\mathcal{O}_L)^{1/k} = |\,\mathrm{N}_{K|\mathbf{Q}}(\alpha)|^{[L:K]/k} = \mathrm{N}(I^k)^{[L:K]/k} = \mathrm{N}(I)^{[L:K]},$$

as required. □

6.1. **Dedekind's theorem on the factorization of primes in extensions.** Let $L|K$ be an extension of number fields and let $P \subset \mathcal{O}_K$ be a prime. Our next goal is to find a way to compute the factorization of $P\mathcal{O}_L$ into primes in L. The next theorem of Dedekind achieves this in many cases.

Theorem 57. *Let K be a number field and let $P \subset \mathcal{O}_K$ be a prime. Let p be the rational prime that lies under P. Let $g \in \mathcal{O}_K[x]$ be a monic irreducible polynomial. Let α be a root of g, and let $L = K(\alpha)$. Assume that $p \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Let $\overline{g}$ be the image of g in $(\mathcal{O}_K/P)[x]$. Let*

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

where $\overline{g}_j$ is an irreducible monic polynomial in $(\mathcal{O}_K/P)[x]$ for each j. Let $g_j \in \mathcal{O}_K[x]$ be monic and such that $g_j \equiv \overline{g}_j \mod P$ for each j.

Then

$$Q_j = P\mathcal{O}_L + g_j(\alpha)\mathcal{O}_L$$

is a prime lying over P and $f(Q_j|P) = \deg g_j$ for each j. In addition, the Q_j are distinct, and

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}.$$

Here and everywhere in these notes, where we write that two polynomials are congruent modulo an ideal, we mean this coefficient-wise.

Dedekind's theorem allows us to compute the decomposition of all primes where $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, and all but finitely many in general. One might hope that even if no α exists with $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, it might be possible to choose an α for each prime P depending on P such that the condition of the theorem is satisfied. Unfortunately, this is not always possible.

We turn to the proof of the theorem. We first prove half of the last claim.

Proposition 58. *With the notation and assumptions of Theorem 57, we have*

$$P\mathcal{O}_L \supset Q_1^{e_1} \cdots Q_r^{e_r}.$$

Proof. The set $P \cup \{g_j(\alpha)\}$ is a generating set for Q_j. We choose e_j (not necessarily distinct) elements from $P \cup \{g_j(\alpha)\}$ for each j, and multiply together these $e_1 + \ldots + e_r$ elements. We collect all of these products that we can obtain in this way in a set $A \subset \mathcal{O}_L$. By the definition of products of ideals, A generates the ideal $Q_1^{e_1} \cdots Q_r^{e_r}$. Therefore, it is enough to show that $A \subset P\mathcal{O}_L$.

All but one element of A contains a factor in P. These are obviously in $P\mathcal{O}_L$. The remaining element is

$$g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r} \equiv g(\alpha) = 0 \mod P\mathcal{O}_L,$$

hence $g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r} \in P\mathcal{O}_L$, as required. □

We turn our attention to the quotients $\mathcal{O}_L/Q_j$.

Proposition 59. *With the notation and assumptions of Theorem 57, the ring $\mathcal{O}_L/Q_j$ is isomorphic to a factor of*

$$(\mathcal{O}_K/P)[x]/\langle \overline{g}_j \rangle. \tag{6}$$

We observe that the ring (6) is a field, a degree $\deg(g_j)$ extension of $\mathcal{O}_K/P$. Fields only have trivial quotients, hence $\mathcal{O}_L/Q_j$ is isomorphic to either $\{0\}$ or (6). In the former case, $Q_j = \mathcal{O}_L$, in the second case Q_j is a prime ideal lying over P with inertial degree $\deg(g_j)$. We would like to show that the second case holds always, which we will do later by considering all Q_j's together.

In the proof of the proposition we show that two rings are isomorphic by realizing them as quotients of the same ring and then comparing the kernels. We record a simple fact in ring theory that will help us computing the kernels. Where A is a subset of a ring R, we write $\langle A \rangle = \langle A \rangle_R$ for the ideal generated by A in R.

Lemma 60. *Let $\varphi_1 : R_1 \to R_2$ and $\varphi_2 : R_2 \to R_3$ be surjective homomorphisms of rings. Let $A \subset R_2$ be a (possibly infinite) set such that*

$$\operatorname{Ker} \varphi_2 = \langle A \rangle_{R_2}.$$

Let $\widetilde{A} \subset R_1$ be such that $\varphi_1(\widetilde{A}) = A$. Then

$$\operatorname{Ker}(\varphi_1 \circ \varphi_2) = \langle \widetilde{A} \rangle_{R_1} + \operatorname{Ker} \varphi_1.$$

Proof. Since $\varphi_1(\widetilde{A}) = A \subset \operatorname{Ker} \varphi_2$, we have $\widetilde{A} \subset \operatorname{Ker}(\varphi_1 \circ \varphi_2)$. Also $\varphi_1(\operatorname{Ker} \varphi_1) = \{0\} \subset \operatorname{Ker} \varphi_2$, hence $\operatorname{Ker} \varphi_1 \subset \operatorname{Ker}(\varphi_1 \circ \varphi_2)$. These two facts together and that $\operatorname{Ker}(\varphi_1 \circ \varphi_2)$ is an ideal give

$$\langle \widetilde{A} \rangle_{R_1} + \operatorname{Ker} \varphi_1 \subset \operatorname{Ker}(\varphi_1 \circ \varphi_2).$$

Now we show the opposite containment. Let $a \in \mathrm{Ker}(\varphi_1 \circ \varphi_2)$. Then $\varphi_1(a) \in \mathrm{Ker}\,\varphi_2 = \langle A \rangle_{R_2}$. Therefore, we have

$$\varphi_1(a) = r_1 a_1 + \cdots + r_k a_k$$

for some $k \in \mathbf{Z}_{\geq 0}$, $r_1, \ldots, r_k \in R_2$ and $a_1, \ldots, a_k \in A$. Using that φ_1 is surjective, and the definition of $\widetilde{A}$, there are $\widetilde{r}_1, \ldots, \widetilde{r}_k \in R_1$ and $\widetilde{a}_1, \ldots, \widetilde{a}_k \in \widetilde{A}$ such that $\varphi_1(\widetilde{r}_j) = r_j$ and $\varphi_1(\widetilde{a}_j) = a_j$ for all j. Therefore,

$$\varphi_1(a) = \varphi_1(\widetilde{r}_1 \widetilde{a}_1 + \cdots + \widetilde{r}_k \widetilde{a}_k).$$

Now $\widetilde{r}_1 \widetilde{a}_1 + \cdots + \widetilde{r}_k \widetilde{a}_k \in \langle \widetilde{A} \rangle_{R_1}$, and $a - \widetilde{r}_1 \widetilde{a}_1 + \cdots + \widetilde{r}_k \widetilde{a}_k \in \mathrm{Ker}(\varphi_1)$, hence

$$a \in \langle \widetilde{A} \rangle_{R_1} + \mathrm{Ker}\,\varphi_1,$$

as required. □

Proof of Proposition 59. Fix some $j \in \{1, \ldots, r\}$. We first prove that

$$(\mathcal{O}_K/P)[x]/\langle \overline{g}_j \rangle \cong \mathcal{O}_K[\alpha]/\langle P, g_j(\alpha) \rangle. \tag{7}$$

We show this by realizing both rings as homomorphic images of $\mathcal{O}_K[x]$ and proving that the two kernels are equal.

Let $\varphi_1 : \mathcal{O}_K[x] \to (\mathcal{O}_K/P)[x]$ and $\varphi_2 : (\mathcal{O}_K/P)[x] \to (\mathcal{O}_K/P)[x]/\langle \overline{g}_j \rangle$ be the obvious homomorphisms. Clearly both are surjective. By definition, $\mathrm{Ker}\,\varphi_2 = \langle \overline{g}_j \rangle$, and $\varphi_1(g_j) = \overline{g}_j$. By the lemma

$$\mathrm{Ker}(\varphi_1 \circ \varphi_2) = g_j \mathcal{O}_K[x] + \mathrm{Ker}\,\varphi_1 = g_j \mathcal{O}_K[x] + P\mathcal{O}_K[x].$$

Let $\psi_1 : \mathcal{O}_K[x] \to \mathcal{O}_K[\alpha]$ be the homomorphism induced by $x \mapsto \alpha$, and let $\psi_2 : \mathcal{O}_K[\alpha] \to \mathcal{O}_K[\alpha]/\langle P, g_j(\alpha) \rangle$ be the obvious homomorphism. Again, both ψ_1 and ψ_2 are surjective. We have $\mathrm{Ker}\,\psi_1 = g\mathcal{O}_K[x]$. We note that $\psi_1(P \cup \{g_j\}) = P \cup \{g_j(\alpha)\}$, which generates $\mathrm{Ker}\,\psi_2$. The lemma gives

$$\mathrm{Ker}(\psi_1 \circ \psi_2) = g_j \mathcal{O}_K[x] + P\mathcal{O}_K[x] + g\mathcal{O}_K[x].$$

We note that

$$g \equiv g_1^{e_1} \cdots g_r^{e_r} \mod P\mathcal{O}_K[x],$$

hence $g \in g_1 \mathcal{O}_K[x] + P\mathcal{O}_K[x]$. Therefore,

$$\mathrm{Ker}(\psi_1 \circ \psi_2) = g_j \mathcal{O}_K[x] + P\mathcal{O}_K[x] = \mathrm{Ker}(\varphi_1 \circ \varphi_2).$$

This proves our claim (7).

Now we relate $\mathcal{O}_L/Q_j$ to $\mathcal{O}_K[\alpha]/\langle P, g_j(\alpha) \rangle$. Clearly, $Q_j \cap \mathcal{O}_K[\alpha]$ contains $\langle P, g_j(\alpha) \rangle_{\mathcal{O}_K[\alpha]}$, hence $\mathcal{O}_K[\alpha]/(Q_j \cap \mathcal{O}_K[\alpha])$ is a factor of $\mathcal{O}_K[\alpha]/\langle P, g_j(\alpha) \rangle$. It is, therefore, enough to show that

$$\mathcal{O}_L/Q_j \cong \mathcal{O}_K[\alpha]/(Q_j \cap \mathcal{O}_K[\alpha]).$$

In other words, we need to show that the homomorphism $\varphi : \mathcal{O}_L \to \mathcal{O}_L/Q_j$ maps $\mathcal{O}_K[\alpha]$ onto $\mathcal{O}_L/Q_j$, which is equivalent to $\mathcal{O}_L = Q_j + \mathcal{O}_K[\alpha]$. This is where we use the condition $p \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$.

We note that $\mathcal{O}_L/(Q_j + \mathcal{O}_K[\alpha])$ is a factor of both $\mathcal{O}_L/Q_j$ and $\mathcal{O}_L/\mathcal{O}_K[\alpha]$. (Here we work in the category of Abelian groups, rather than in rings, because $\mathcal{O}_K[\alpha]$ need not be an ideal in $\mathcal{O}_L$.) We note that $[\mathcal{O}_L : Q_j]$ is a power of p because Q_j lies over p. Therefore,

$$[\mathcal{O}_L : (Q_j + \mathcal{O}_K[\alpha])] \,|\, \gcd([\mathcal{O}_L : Q_j], [\mathcal{O}_L : \mathcal{O}_K[\alpha]]) = 1.$$

This proves $\mathcal{O}_L = Q_j + \mathcal{O}_K[\alpha]$, as required. □

The final ingredient in the proof of Theorem 57 is the following statement, which we will use to show that the ideals $Q_1, \ldots, Q_j$ are distinct.

Proposition 61. *With the notation and assumptions of Theorem 57, we have*

$$Q_i + Q_j = \mathcal{O}_L$$

for all pairs of indices $i \neq j$.

Proof. Fix two indices $i \neq j$. Since $(\mathcal{O}_K/P)[x]$ is an Euclidean domain, and $\overline{g}_i$ and $\overline{g}_j$ are distinct irreducible polynomials, the Euclidean algorithm yields some $\overline{h}_1, \overline{h}_2 \in \mathcal{O}_K/P[x]$ such that $\overline{h}_1\overline{g}_i + \overline{h}_2\overline{g}_j = 1$. We pick some $h_1, h_2 \in \mathcal{O}_K[x]$ that project to $\overline{h}_1$ and $\overline{h}_2$ respectively. Then

$$1 = h_1 g_i + h_2 g_j + h$$

for some $h \in P\mathcal{O}_K[x]$. Then $1 \in Q_i + Q_j$, which proves the claim. □

Proof of Theorem 57. By Proposition 58, we know that there is an ideal $I \subset \mathcal{O}_L$ such that

$$P\mathcal{O}_L \cdot I = Q_1^{e_1} \cdots Q_r^{e_r}.$$

By Proposition 59, we know that $\mathrm{N}(Q_j) \leq \mathrm{N}(P)^{\deg g_j}$ for $j = 1, \ldots, r$. We conclude that

$$\mathrm{N}(P)^{[L:K]}\,\mathrm{N}(I) \leq \mathrm{N}(P)^{e_1 \deg g_1 + \ldots + e_r \deg g_j} = \mathrm{N}(P)^{[L:K]}. \tag{8}$$

From this we conclude that $\mathrm{N}(I) = 1$, hence $I = \mathcal{O}_L$, and

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}.$$

In addition, none of the inequalities $\mathrm{N}(Q_j) \leq \mathrm{N}(P)^{\deg g_j}$ can be strict, for otherwise (8) would be strict, too. Therefore, $\mathcal{O}_L/Q_j$ must be isomorphic to $(\mathcal{O}_K/P)[x]/\langle\overline{g}_j\rangle$ in Proposition 59 for all j. Thus Q_j is indeed a prime lying above P with inertial degree $\deg g_j$. Finally, now that we know that $Q_j \neq \mathcal{O}_K$ for all j, Proposition 61 shows that they must be distinct primes. The theorem is proved. □

Remark 62 (Non-examinable)**.** A rational prime $p \in \mathbf{Z}$ is said to be ramified in a number field K if there is some prime $P \subset \mathcal{O}_K$ lying over p with $e(P|p) > 1$. Let K be a monogenic field, that is, assume that there is some $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbf{Z}[\alpha]$. Let $g \in \mathbf{Z}[x]$ be the minimal polynomial of α. Let $p \in \mathbf{Z}$ be a prime. By Theorem 57, p is ramified in $\mathcal{O}_K$ if and only if $\overline{g}$ has a root in a field extension of

$\mathbf{Z}/p\mathbf{Z}$ with multiplicity more than 1. This is equivalent to $\operatorname{disc}(\overline{g}) = 0$, which in turn is equivalent to $p|\operatorname{disc}(g)$. Since $\mathcal{O}_K = \mathbf{Z}[\alpha]$, we have $\operatorname{disc}(K) = \operatorname{disc}(g)$. We can conclude that p ramifies in $\mathcal{O}_K$ if and only if $p|\operatorname{disc}(K)$. This is, in fact, true for all number fields, not just for monogenic ones, but we will not prove this in this course.

Theorem 63 (Non-examinable)**.** *A prime $p \in \mathbf{Z}$ is ramified in a number field K if and only if $p|\operatorname{disc}(K)$.*

6.2. **Application to quadratic fields.**

Theorem 64. *Let $m \neq 0, 1 \in \mathbf{Z}$ be square-free. Let $K = \mathbf{Q}(\sqrt{m})$. Let $p \in \mathbf{Z}$ be a prime.*

1. *p is ramified in $\mathcal{O}_K$, that is, $p\mathcal{O}_K = P^2$ for some prime $P \subset \mathcal{O}_K$, if and only if p is odd and $p|m$ or $p = 2$ and $m \not\equiv 1 \mod 4$.*
2. *p is split in $\mathcal{O}_K$, that is $p\mathcal{O}_K = P_1P_2$ for two distinct primes $P_1, P_2 \subset \mathcal{O}_K$, if and only if p is odd and $\left(\frac{m}{p}\right) = 1$ or $p = 2$ and $m \equiv 1 \mod 8$.*
3. *p is inert in $\mathcal{O}_K$, that is $p\mathcal{O}_K$ is a prime, if and only if p is odd and $\left(\frac{m}{p}\right) = -1$, or $p = 2$ and $m \equiv 5 \mod 8$.*

Here

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{if } p|m, \\ 1 & \text{if there is } a \neq 0 \in \mathbf{Z}/p\mathbf{Z} \text{ with } m \equiv a^2 \mod p, \\ -1 & \text{otherwise} \end{cases}$$

is the Legendre symbol.

Proof. If $p \neq 2$ or $p \not\equiv 1 \mod 4$, then $p \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt{m}]]$. Therefore, we can apply Dedekind's theorem for the polynomial $g(x) = x^2 - m$, which is the minimal polynomial of $\sqrt{m}$. The claim follows immediately.

If $p = 2$ and $m \equiv 1 \mod 4$, then $\mathcal{O}_K = \mathbf{Z}[(1 + \sqrt{m})/2]$, and we can apply Dedekind's theorem for the polynomial $g = x^2 - x + (1 - m)/4$, which is the minimal polynomial of $(1+\sqrt{m})/2$. Where $m \equiv 1 \mod 8$, $g \equiv x^2 + x = (x + 1)x \mod 2$, and Dedekind's theorem shows that 2 indeed splits in K. Where $m \equiv 5 \mod 8$, $g \equiv x^2+x+1 \mod 2$, which is irreducible in $\mathbf{Z}/2\mathbf{Z}[x]$, hence 2 is indeed inert in K. □

7. The class group

As we have seen, a consequence of the unique factorization property of ideals is that the ring of integers in a number field K is a unique factorization domain if and only if it is a principal ideal domain.

In this section, we study how far the ring of integers in a number field can be from being a principal ideal domain, which is also related to the extent of failure of the unique factorization property.

Consider the set of fractional ideals $\mathcal{I} = \mathcal{I}_K$ in a number field K. The multiplication operation turns this into a commutative group, and

the principal ideals $\mathcal{P} = \mathcal{P}_K$ form a subgroup of it. The quotient $\mathrm{Cl}(K) = \mathcal{I}/\mathcal{P}$ is called the ideal class group of K. Each element of $\mathrm{Cl}(K)$ contains an integral ideal (see Lemma 43). (We call ideals in $\mathcal{O}_K$ integral ideals, when we want to stress that they are ideals not just fractional ideals.) Hence the ideal class group can also be defined as the equivalence classes of integral ideals with respect to the relation $\sim$ defined by $I \sim J$ if and only if there is $\alpha \in K$ such that $J = \alpha I$.

Our goal in this section is to show that the ideal class group is always finite, and the proof of this will also lead to a method for calculating it.

Theorem 65. *Let K be a number field. Then $|\mathrm{Cl}(K)| < \infty$.*

The class number of a number field is defined as

$$h(K) = |\mathrm{Cl}(K)|.$$

The theorem will be deduced from the following result.

Theorem 66 (Minkowski's bound 1)**.** *Let K be a number field of degree d. Denote by s the number of pairs of complex embeddings of K. Then every ideal $I \subset \mathcal{O}_K$ contains an element $\alpha \neq 0$ with*

$$|\mathrm{N}(\alpha)| \leq \frac{d!}{d^d}\Big(\frac{4}{\pi}\Big)^s |\operatorname{disc}(K)|^{1/2}\,\mathrm{N}(I).$$

Remark 67. By Stirling's approximation,

$$\frac{d!}{d^d} = (1 + o(1))(2\pi d)^{1/2}e^{-d}.$$

Since $e > (4/\pi)^{1/2}$, the constant in Minkowski's bound decreases exponentially as d grows.

In these lectures, we will only prove a weaker version of this result replacing the conclusion by $|\mathrm{N}(\alpha)| \leq |\operatorname{disc}(K)|^{1/2}\,\mathrm{N}(I)$. The proof of the stronger version is not examinable, but the statement is.

Before we do this, we discuss a few corollaries of Minkowski's bound including the finiteness of the ideal class group.

Corollary 68 (Minkowski's bound 2)**.** *Let K be a number field of degree d. Denote by s the number of pairs of complex embeddings of K. Then every element of $\mathrm{Cl}(K)$ contains an integral ideal I with*

$$\mathrm{N}(I) \leq \frac{d!}{d^d}\Big(\frac{4}{\pi}\Big)^s |\operatorname{disc}(K)|^{1/2}.$$

Proof. Let I be an integral ideal, and let J be an integral ideal in the class of I^{-1}.

We apply Theorem 66 for J, and find some $\gamma \in J$ with

$$|\mathrm{N}(\gamma)| \leq \frac{d!}{d^d}\Big(\frac{4}{\pi}\Big)^s |\operatorname{disc}(K)|^{1/2}\,\mathrm{N}(J).$$

Since $\gamma \in J$, $J|\langle\gamma\rangle$ and γJ^{-1} is an integral ideal. In addition

$$|\operatorname{N}(\gamma J^{-1})| \leq \frac{d!}{d^d}\Big(\frac{4}{\pi}\Big)^s |\operatorname{disc}(K)|^{1/2},$$

and γJ^{-1} is in the same ideal class as I. □

The above result implies $h(K) < \infty$, since there are only finitely many integral ideals of norm bounded by some number X in a number field. Indeed, all such ideals are products of at most $\log_2(X)$ primes, because a prime has norm at least 2. The primes that may occur in those products lie over rational primes that are at most X. Clearly, there are only finitely many rational primes at most X, and over each of them at most $[K : \mathbf{Q}]$ primes of K lie. Thus the number of primes that may occur in the products is also finite.

This argument also leads to a method for computing the class group. First, compute

$$X := \Big\lfloor \frac{d!}{d^d}\Big(\frac{4}{\pi}\Big)^s |\operatorname{disc}(K)|^{1/2} \Big\rfloor.$$

For example, for the quadratic fields $\mathbf{Q}(\sqrt{m})$, we get

$$X = \begin{cases} \dfrac{\sqrt{m}}{2}, & \text{if } m > 1 \text{ and } m \equiv 1 \mod 4, \\ \sqrt{m}, & \text{if } m > 1 \text{ and } m \equiv 2, 3 \mod 4, \\ \dfrac{2\sqrt{-m}}{\pi}, & \text{if } m < 0 \text{ and } m \equiv 1 \mod 4, \\ \dfrac{4\sqrt{-m}}{\pi}, & \text{if } m < 0 \text{ and } m \equiv 2, 3 \mod 4. \end{cases}$$

Second, list all rational primes up to X. Third, factorize each prime in $\mathcal{O}_K$ and list the prime ideals of norm at most X: $P_1, \dots, P_k$. Finally, find all integer vectors $m_1, \dots, m_k$ such that

$$P_1^{m_1} \cdots P_k^{m_k}$$

is a principal ideal. In order to determine whether an ideal I is principal, a good starting point is to study whether elements of norm $\operatorname{N}(I)$ exist in $\mathcal{O}_K$.

Corollary 69 (Minkowski's bound 3)**.** *Let K be a number field of degree d. Denote by s the number of pairs of complex embeddings of K. Then we have*

$$|\operatorname{disc}(K)| \geq \frac{d^{2d}}{(d!)^2}\Big(\frac{\pi}{4}\Big)^{2s}.$$

Proof. This follows from the previous result and $\operatorname{N}(I) \geq 1$. □

In light of our above comments, the discriminant of a number field grows at least exponentially with the degree, and it also follows that $|\operatorname{disc}(K)| > 1$ for all number fields except for $K = \mathbf{Q}$. In light of our remarks in the previous section, this also implies that in every number field other than $\mathbf{Q}$ at least one prime is ramified.

7.1. **Geometry of numbers.** We turn to the proof of the Minkowski bound, Theorem 66. We first recall the map $\Sigma : K \to \mathbf{R}^d$ defined by

$$\Sigma(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \dots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha)))^T,$$

where $\sigma_1, \dots, \sigma_r$ are the embeddings of K into $\mathbf{C}$ with real image and $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$ are the remaining embeddings. We discussed that $\Sigma(\mathcal{O}_K) \subset \mathbf{R}^d$ is a lattice, that is an additive subgroup generated by d linearly independent elements. Moreover, we also know that the covolume of $\Sigma(\mathcal{O}_K)$, that is, the volume of any fundamental domain is

$$\mathrm{coVol}(\Sigma(\mathcal{O}_K)) = 2^{-s} |\operatorname{disc}(K)|^{1/2}.$$

Now let $I \subset \mathcal{O}_K$ be an ideal. Then $\Sigma(I)$ is a sublattice of $\Sigma(\mathcal{O}_K)$, and

$$\mathrm{coVol}(\Sigma(I)) = 2^{-s} |\operatorname{disc}(I)|^{1/2} = 2^{-s} \operatorname{N}(I) |\operatorname{disc}(K)|^{1/2}.$$

Here $\operatorname{disc}(I)$ stands for the discriminant of I as a module, that is the discriminant of any d-tuple that generates it as a module.

Consider the function $\mathcal{N} : \mathbf{R}^d \to \mathbf{R}$ defined by

$$\mathcal{N}(x_1, \dots, x_d) = \prod_{j=1}^{r} |x_j| \prod_{j=1}^{s} (x_{r+2j-1}^2 + x_{r+2j}^2).$$

The definition of this function was made so that

$$|\operatorname{N}(\alpha)| = \mathcal{N}(\Sigma(\alpha))$$

for all $\alpha \in K$.

Now our job is to prove that the lattice $\Sigma(I)$ has a non-zero point in the region $\{x : \mathcal{N}(x) < X\}$ for some suitable X. Such problems are studied in a theory call the geometry of numbers. For our purposes the most basic result will suffice, which is due to Minkowski.

Theorem 70 (Minkowski)**.** *Let $\Lambda \subset \mathbf{R}^d$ be a lattice, and $S \subset \mathbf{R}^d$ a convex subset that is symmetric to the origin. Assume that*

$$\mathrm{Vol}(S) > 2^d \,\mathrm{coVol}(\Lambda).$$

Then $S \cap \Lambda$ contains a non-zero vector.

A set $S \subset \mathbf{R}^d$ is convex if whenever $x, y \in S$, we also have $ax + (a-1)y \in S$ for all $a \in (0,1)$, that is, the entire line segment connecting x to y is in S. A set S is symmetric to the origin if $x \in S$ implies $-x \in S$.

We note that the constant 2^d cannot be lowered in the theorem. Indeed, consider the lattice $\Lambda = \mathbf{Z}^d$ and the closed, convex and symmetric set $S = (-1,1)^d$. Then $\mathrm{coVol}(\Lambda) = 1$, $\mathrm{Vol}(S) = 2^d$ and $\Lambda \cap S = \{0\}$. However, if we add the condition, that S is closed then the $>$ relation can be relaxed to $\geq$.

The proof of the theorem is based on the following simple lemma.

Lemma 71. *Let $\Lambda \subset \mathbf{R}^d$ be a lattice, and let $S \subset \mathbf{R}^d$ be a Borel set. If*

$$\mathrm{Vol}(S) > \mathrm{coVol}(\Lambda),$$

then there are $x \neq y \in S$ with $x - y \in \Lambda$.

Proof. Let F be a fundamental domain of Λ, and for each $a \in \Lambda$, let $S(a) = ((F + a) \cap S) - a$. It is easy to see that $S(a) \subset F$ for all $a \in \Lambda$. In addition,

$$\sum_{a \in \Lambda} \mathrm{Vol}(S(a)) = \mathrm{Vol}(S) > \mathrm{coVol}(\Lambda) = \mathrm{Vol}(F).$$

Therefore, $S(a) \cap S(b) \neq \varnothing$ for some $a \neq b \in \Lambda$. Let $x \in S(a) \cap S(b)$. Then $x + a \neq x + b \in S$, and $(x + a) - (x + b) = a - b \in \Lambda$, as required. □

Proof of Theorem 70. We apply the lemma for the set

$$\frac{1}{2} \cdot S = \{x/2 : x \in S\}.$$

We get some $x/2 \neq y/2$ with $x, y \in S$ and $0 \neq x/2 - y/2 \in \Lambda$. By symmetry, we have $-y \in S$, and by convexity,

$$x/2 - y/2 = (1/2)x + (1/2)(-y) \in S.$$

This proves the theorem. □

Proof of Theorem 66. Unfortunately, the sets of the form $\{x : \mathcal{N}(x) < X\}$ are not convex. However, we can prove the theorem by choosing a sufficiently large convex subset of it and apply Minkowski's theorem for that.

We take

$$S = \{x : |x_j| < Y \text{ for each } j\}.$$

for some number $Y > 0$. This set is convex and symmetric, and has volume

$$\mathrm{Vol}(S) = (2Y)^d.$$

Moreover, $\mathcal{N}(x) \leq 2^s Y^d$ for all $x \in S$.

In addition, we take

$$\Lambda = \Sigma(I).$$

We have already noted that Λ is a lattice with

$$\mathrm{coVol}(\Lambda) = 2^{-s} \,\mathrm{N}(I) |\operatorname{disc}(K)|^{1/2}.$$

By Minkowski's theorem, $S \cap \Lambda$ contains a non-zero vector provided we take Y large enough so that

$$2^d Y^d > 2^d \cdot 2^{-s} \,\mathrm{N}(I) |\operatorname{disc}(K)|^{1/2}.$$

The conclusion is that we can find some $0 \neq x \in \Lambda$ with $\mathcal{N}(x) \leq N(I) |\operatorname{disc}(K)|^{1/2} + \varepsilon$ for any $\varepsilon > 0$. Since Λ has only finitely many

non-zero points in S, one of these must work for all $\varepsilon > 0$, so we can, in fact, take $\varepsilon = 0$. This gives some $\alpha \in I$ with

$$|\,\mathrm{N}(\alpha)| \leq \mathrm{N}(I)|\,\mathrm{disc}(K)|^{1/2}.$$

As we said, we proved the theorem with a weaker constant. To get Minkowski's bound, one needs to take

$$S = \{x \in \mathbf{R}^d : |x_1| + \ldots + |x_r| + 2((x_{r+1}^2 + x_{r+2}^2)^{1/2} + \ldots) \leq Y\}$$

for a suitably chosen Y. See Question 14 on the third example sheet. □

8. Units

Let K be a number field. An algebraic integer $\alpha \in \mathcal{O}_K$ is a unit if α^{-1} is also an algebraic integer. It is immediate from the definition, that the product of units is also a unit, and that the multiplicative inverse of units are also units. Therefore, the units in $\mathcal{O}_K$ form a group. We denote this group by $\mathcal{O}_K^\times$.

Lemma 72. *Let $\alpha \in \mathcal{O}_K$. The following are equivalent.*

(1) *α is a unit.*
(2) $\langle\alpha\rangle = \mathcal{O}_K$.
(3) $\mathrm{N}(\alpha) = \pm 1$.

Proof. First we prove that (1) ⇒ (3) The norms of algebraic integers are rational integers. Therefore, if α is a unit, then $\mathrm{N}(\alpha), \mathrm{N}(\alpha^{-1}) \in \mathbf{Z}$. In addition, $\mathrm{N}(\alpha)\,\mathrm{N}(\alpha^{-1}) = 1$ by multiplicativity of norms. We must have $\mathrm{N}(\alpha) = \pm 1$, as required.

Next we prove (3) ⇒ (2). If $\mathrm{N}(\alpha) = \pm 1$, then $\mathrm{N}(\langle\alpha\rangle) = 1$ and $\langle\alpha\rangle = \mathcal{O}_K$.

Finally, we prove (2) ⇒ (1). If $\langle\alpha\rangle = \mathcal{O}_K$, then $1 \in \alpha\mathcal{O}_K$ and there is some $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. Clearly, $\beta = \alpha^{-1} \in \mathcal{O}_K$, as required. □

The above lemma shows that we cannot distinguish between elements of $\mathcal{O}_K$ that differ from each other by a multiplicative factor that is a unit if we work with ideals. This is one reason, why units are important.

The goal of this section is to describe the structure of units in rings of integers.

8.1. **Quadratic fields.** Let m be a square-free integer, and let $K = \mathbf{Q}(m^{1/2})$. Recall that

$$\mathcal{O}_K = \begin{cases} \{a + bm^{1/2} : a, b \in \mathbf{Z}\}, & \text{if } m \not\equiv 1 \mod 4, \\ \{a + b(1 + m^{1/2})/2 : a, b \in \mathbf{Z}\}, & \text{if } m \equiv 1 \mod 4. \end{cases}$$

Recall also that

$$\mathrm{N}(a + m^{1/2}b) = (a + m^{1/2}b)(a - m^{1/2}b) = a^2 - mb^2.$$

If $m \not\equiv 1 \mod 4$, the characterization $\mathrm{N}(\alpha) = \pm 1$ of units implies that the units in K are precisely $a + m^{1/2}b$, where $a, b \in \mathbf{Z}$ are the solutions of the equations

$$a^2 - mb^2 = \pm 1. \tag{9}$$

If $m \equiv 1 \mod 4$, then the units are of the form $(a + m^{1/2}b)/2$, where $a, b \in \mathbf{Z}$ solve one of the equations

$$a^2 - mb^2 = \pm 4. \tag{10}$$

We first consider the case where $m < 0$, that is, when K is an imaginary quadratic field. If $m \leq -5$, then $a^2 - mb^2 > 4$ whenever $b \neq 1$. In this case, all solutions of (9) or (10) must satisfy $b = 0$, and hence the only units in $\mathbf{Q}(m^{1/2})$ are ± 1. If $m = -1, -2, -3$, it is easy to see that $|a|, |b| \leq 2$, and the solutions can be easily found by going through these cases. The result is that the units in $\mathbf{Q}((-1)^{1/2})$ are $\pm 1, \pm i$, the units in $\mathbf{Q}((-2)^{1/2})$ are ± 1, and in $\mathbf{Q}((-3)^{1/2})$ are

$$\pm 1, \frac{\pm 1 \pm (-3)^{1/2}}{2}.$$

Now we turn to case $m > 1$, that is, the case of real quadratic fields. The units in $\mathbf{Q}(m^{1/2})$ are described by the following.

Theorem 73. *Let $m > 1$ be a square-free integer, and let $K = \mathbf{Q}(m^{1/2})$. Then there is a smallest among all units $u \in \mathcal{O}_K^\times$ with $u > 1$, and*

$$\mathcal{O}_K^\times = \{\pm u^n : n \in \mathbf{Z}\}.$$

The unit u is called the fundamental unit.

Proof. We first observe that a unit $u > 1$ must be of the form $a + bm^{1/2}$ with $a, b \in \mathbf{Q}_{>0}$. Indeed, $\pm 1 = \mathrm{N}(u) = (a + bm^{1/2})(a - bm^{1/2})$ implies that

$$\{\pm a \pm bm^{1/2}\} = \{\pm u^{\pm 1}\}.$$

Since $u > 1$, these are four distinct numbers and u is the largest among them. Therefore, $a, b > 0$ indeed.

The proof of the fact that units greater than 1 exist is not examinable in this course. It follows from the fact that Pell's equation

$$a^2 - mb^2 = 1$$

always has positive integer solutions, which is proved in the Part II Number Theory course. Alternatively, it can be proved using Minkowski's theorem, as we will see in the next section.

Now we show that there is a smallest one among the units greater than 1. Suppose not. Then there is an infinite sequence of decreasing units $u_1 > u_2 > \ldots > 1$. Necessarily, $\lim_{j\to\infty} u_j/u_{j+1} = 1$. The elements of the sequence u_j/u_{j+1} are all units greater than 1. However, any unit greater than 1 must be at least $(1 + m^{1/2})/2 > 1$, a contradiction.

Now we show that all units are of the form $\pm u^n$ for some n. Let v be a unit. Clearly, $\pm v^{\pm 1}$ is of the required form if and only if v is, so we can assume $v > 1$. We observe that there can be no unit v in the open interval (u^n, u^{n+1}) for any $n \in \mathbf{Z}_{\geq 0}$, for otherwise $1 < vu^{-n} < u$ would contradict the minimality of u. Then $v = u^n$ necessarily for some n, as required. □

We can find the fundamental unit by searching thorough all pairs $(a, b) \in \mathbf{Z}_{>0}$ for solutions of the equations (9) or (10). To this end, it is helpful to observe the following. If a_1, b_1 and a_2, b_2 are both solutions of (9) with some choice of the sign and $b_1 < b_2$, then $b_2^2 \geq b_1^2 + 3$, so

$$a_1^2 = mb_1^2 \pm 1 < mb_2^2 \pm 1 = a_2^2,$$

and $a_2 > a_1$. Thus $a_1 + b_1 m^{1/2} < a_2 + b_2 m^{1/2}$. This means that in the $m \equiv 2, 3 \mod 4$ case, the fundamental unit will correspond to the solution of (9) with either sign such that $b > 0$ is minimal. A similar observation applies in the $m \equiv 1 \mod 4$ case, as well.

There is also a very efficient way to find the solutions of (9) using continued fractions, which was discussed in the Part II Number Theory course.

8.2. **Dirichlet's unit theorem.** The next result describes the structure of units in arbitrary number fields.

Theorem 74. *Let K be a number field with r real and s pairs of complex embeddings. Write W for the set of roots of unity in K, that is, numbers $\alpha \in K$ that satisfy $\alpha^k = 1$ for some $k \in \mathbf{Z}_{>0}$. Then W is finite, and there are $r + s - 1$ units $u_1, \ldots, u_{r+s-1} \in \mathcal{O}_K^\times$ such that every unit can be written uniquely in the form*

$$\theta u_1^{n_1} \cdots u_{r+s-1}^{n_{r+s-1}},$$

where $\theta \in W$ is a root of unity, and $n_1, \ldots, n_{r+s-1} \in \mathbf{Z}$.

Therefore, the unit group is isomorphic to the direct product of a finite group and a free Abelian group of rank $r + s - 1$. A collection of units $u_1, \ldots, u_{r+s-1}$ that satisfies the conclusion in the theorem is called a fundamental system of units.

For quadratic fields, we have two cases. If $m > 1$, then $r = 2$ and $s = 0$, so the rank of the free Abelian part is $r + s - 1 = 1$. The roots of unity are just $W = \{\pm 1\}$. In fact, this is already true for all number fields that have at least one real embedding, because the only roots of unity in $\mathbf{R}$ are ± 1. The the other case is $m < 0$, where $r = 0$ and $s = 1$. Then $r + s - 1 = 0$, hence the group of units is just W. These observations are compatible with our discussion in the previous section.

We turn to the proof of the unit theorem. Let K be a number field, and let $\sigma_1, \ldots, \sigma_r$ be the real and $\tau_1, \overline{\tau}_1, \ldots, \tau_s, \overline{\tau}_s$ be the pairs of

complex embeddings. We consider the map $\mathrm{Log} : K \to \mathbf{R}^{r+s}$ defined by

$$\mathrm{Log}(\alpha) = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha)|, 2\log|\tau_1(\alpha)|, \dots, 2\log|\tau_s(\alpha)|)^T.$$

This map is called the logarithmic embedding (even though it has non-trivial kernel), and it plays a key role in the proof. We first observe that Log is a homomorphism from the multiplicative group of K to the additive group $\mathbf{R}^{r+s}$.

We also observe that $\log(|\,\mathrm{N}(\alpha)|) = \sum_{j=1}^{r+s}(\mathrm{Log}(\alpha))_j$, where $(\cdot)_j$ denotes the j-th component of a vector. Denote by V the $r+s-1$ dimensional subspace of $\mathbf{R}^{r+s}$ whose points satisfy $x_1 + \ldots + x_{r+s} = 0$. Since $\mathrm{N}(\alpha) = 1$ for all units α, it follows that $\mathrm{Log}(\mathcal{O}_K^\times) \subset V$.

The theorem follows from the following three statements.

Proposition 75. *If $\alpha \in \mathcal{O}_K$ satisfies $\mathrm{Log}(\alpha) = 0$, then α is a root of unity. Additionally, W is finite.*

Proposition 76. *The group $\mathrm{Log}(\mathcal{O}_K^\times)$ is a free Abelian group generated by $\mathbf{R}$-linearly independent elements in V. In particular, the rank of $\log(\mathcal{O}_K^\times)$ is at most $r+s-1$.*

Proposition 77. *The rank of $\mathrm{Log}(\mathcal{O}_K^\times)$ is $r+s-1$.*

The proofs of Propositions 75 and 76 are examinable, while the proof of Proposition 77 is not.

Propositions 76 and 77 together imply that $\mathrm{Log}(\mathcal{O}_K^\times)$ is a lattice in V.

We can deduce Dirichlet's unit theorem easily from these statements. Indeed, we can define $u_1, \dots, u_{r+s-1}$ as some inverse images of a generating set of the lattice $\mathrm{Log}(\mathcal{O}_K^\times)$ under Log. We leave checking the remaining details as an exercise.

Remark 78. The above propositions also allow us to visualize the unit group of a number field. The logarithmic embedding maps the fundamental system of units to a basis of the vector space V, and $\mathrm{Log}(\mathcal{O}_K^\times)$ is the lattice spanned by this basis.

We begin with the proof of Proposition 75. Recall the injective homomorphism $\Sigma : K \to \mathbf{R}^d$, and that $\Sigma(\mathcal{O}_K) \subset \mathbf{R}^d$ is a lattice. In particular $\Sigma^{-1}(B) \cap \mathcal{O}_K$ is finite for any bounded set $B \subset \mathbf{R}^d$.

Proof of Proposition 75. Let $\alpha \in \mathcal{O}_K$ with $\mathrm{Log}(\alpha) = 0$. Since Log is a homomorphism, $\mathrm{Log}(\alpha^n) = 0$ for all $n \in \mathbf{Z}$. This means that $|\sigma_j(\alpha^n)| = 1$ and $|\tau_j(\alpha^n)| = 1$ for all j in the relevant ranges.

Consider $B \subset \mathbf{R}^d$ defined by $|x_j| \le 1$ for all j. Then $\Sigma(\alpha^n) \in B$ for all $n \in \mathbf{Z}$. Since $\Sigma^{-1}(B) \cap \mathcal{O}_K$ is finite, there are $n < m$ with $\alpha^n = \alpha^m$. Then $\alpha^{m-n} = 1$, and α is a root of unity, as required.

The same argument implies that $W \subset \Sigma^{-1}(B) \cap \mathcal{O}_K$, hence it is finite. □

We turn to the proof of Proposition 76. We write $B(x, R)$ for the ball of radius R around a point x in a metric space.

Lemma 79. *Let $k \in \mathbf{Z}_{>0}$, and let $\Lambda \subset \mathbf{R}^k$ be an additive subgroup. Suppose that $B(0, R) \cap \Lambda$ is finite for all $R \in \mathbf{R}_{>0}$. Then Λ is a free Abelian group generated by $\mathbf{R}$-linearly independent elements.*

In fact, it is enough to assume the hypothesis for any single $R > 0$, but we do not need to know this.

Proof. We assume, as we may, that the elements of Λ span $\mathbf{R}^k$. Indeed, if this was not the case, we could simply work in the linear span of Λ instead of $\mathbf{R}^k$. Let $x_1, \ldots, x_k \in \Lambda$ be a basis of $\mathbf{R}^k$. Denote by Λ' the lattice generated by $x_1, \ldots, x_k$, and let

$$F = [0, 1) \cdot x_1 + \ldots + [0, 1) \cdot x_k$$

be the corresponding fundamental parallelepiped. Then F can be covered by a ball $B(0, R)$ of suitably large radius radius R, which contains only finitely many points in Λ. Thus F contains only finitely many points of Λ. On the other hand, F contains a representative of each coset of Λ' in Λ, hence $[\Lambda : \Lambda'] < \infty$.

Therefore, Λ is a finitely generated $\mathbf{Z}$ module. Since Λ' is finite index in Λ, they must have the same rank, hence $r = k$. In addition, any generating set of Λ has to span $\mathbf{R}^k$ linearly, so it must be $\mathbf{R}$-linearly independent. □

Lemma 80. *Let K and V be as above. Let $R > 0$. Then $B(0, R) \cap \mathrm{Log}(\mathcal{O}_K)$ is finite.*

Proof. Fix some R. Then all $\alpha \in \mathcal{O}_K$ with $\mathrm{Log}(\alpha) \in B(0, R)$ satisfy $|\sigma_j(\alpha)| < \exp(R)$ and $|\tau_j(\alpha)| < \exp(R)$ for all j in the relevant ranges. Since $\Sigma(\mathcal{O}_K)$ is a lattice, $\mathcal{O}_K$ can contain only finitely many points with $|\sigma_j(\alpha)| < \exp(R)$ and $|\tau_j(\alpha)| < \exp(R)$ for all j in the relevant ranges. This proves the lemma. □

Proof of Proposition 76. The proposition follow immediately by combining Lemmata 79 and 80. □

Finally, we prove Proposition 77, which is not examinable.

Lemma 81 (Not examinable)**.** *Let $k \in \mathbf{Z}_{>0}$, and let $\Lambda \subset \mathbf{R}^k$ be an additive subgroup. Suppose that there is some $R \in \mathbf{R}_{>0}$ such that $B(x, R) \cap \Lambda$ is non-empty for all $x \in \mathbf{R}^k$. Then Λ is not contained in any proper linear subspace of $\mathbf{R}^k$*

Proof. Suppose to the contrary that $\Lambda \subset U$ for a proper linear subspace $U \subset \mathbf{R}^k$. Let $x \in \mathbf{R}^k$ be point of distance more than R from U. Then $\Lambda \cap B(x, R) \subset U \cap B(x, R)$ is empty, a contradiction. □

Our next task is to construct a unit u such that $\mathrm{Log}(u)$ approximates a prescribed point $x \in V$. Below we will describe a procedure to find an element with small norm instead of a unit. The next lemma will allow us to modify such an element to get a unit without changing its logarithmic embedding by much.

Lemma 82 (Not examinable)**.** *Let K be as above. Fix some $M \in \mathbf{Z}_{>0}$. There is a number $R \in \mathbf{R}_{>0}$ depending only on K and M such that the following holds. Let $\alpha \in \mathcal{O}_K$ with $|\,\mathrm{N}(\alpha)| < M$. Then there is a unit $u \in \mathcal{O}_K^\times$ with $\|\,\mathrm{Log}(\alpha) - \mathrm{Log}(u)\| < R$.*

Proof. As we have already discussed, there are only finitely many ideals of norm less than M. Among these, we consider all principal ideals I, and fix a generator α_I, for each of them. We let $R \in \mathbf{R}_{>0}$ be such that $\|\log(\alpha_I)\| < R$ for each principal ideal I of norm less than M.

Now let $\alpha \in \mathcal{O}_K$ with $|\,\mathrm{N}(\alpha)| < M$, and let $I = \langle\alpha\rangle$. Then $\langle\alpha\rangle = \langle\alpha_I\rangle$, hence $u = \alpha\alpha_I^{-1}$ is a unit. In addition,

$$\|\,\mathrm{Log}(\alpha) - \mathrm{Log}(u)\| = \|\,\mathrm{Log}(\alpha_I)\| < R,$$

as required. □

Lemma 83 (Not examinable)**.** *Let K and V be as above. Then there is some $M \in \mathbf{Z}_{>0}$ and $R \in \mathbf{R}_{>0}$ depending only on K such that the following holds. Let $x \in V$. Then there is $\alpha \in \mathcal{O}_K$ with $|\,\mathrm{N}(\alpha)| < M$ and $\|\,\mathrm{Log}(\alpha) - x\| < R$.*

Proof. Let $C_0 = |\,\mathrm{disc}(K)|^{1/2d}$. Consider

$$\begin{aligned} S = \{y \in \mathbf{R}^d :& |y_j| \le C_0 \exp(x_j) \text{ for } j = 1, \dots, r \text{ and} \\ & |y_{2j-r-1}|, |y_{2j-r}| \le C_0 \exp(x_j/2) \text{ for } j = r+1, \dots, r+s\}. \end{aligned}$$

Then S is a symmetric convex set and

$$\mathrm{Vol}(S) = 2^d C_0^d \prod_{j=1}^{r+s} \exp(x_j) = 2^d |\,\mathrm{disc}(K)|^{1/2},$$

where we used $\sum_{j=1}^{r+s} x_j = 0$. We recall that

$$\mathrm{coVol}(\Sigma(\mathcal{O}_K)) \le |\,\mathrm{disc}(K)|^{1/2}.$$

(We have equality if $s = 0$.) By Minkowski's theorem, there is some $\alpha \in \mathcal{O}_K$ with $\Sigma(\alpha) \in S$.

Then $|\sigma_j(\alpha)| \le C_0 \exp(x_j)$ for $j = 1, \dots, r$ and $|\tau_j(\alpha)|^2 \le 2C_0^2 \exp(x_{r+j})$ for $j = 1, \dots, s$. We observe that

$$|\,\mathrm{N}(\alpha)| = \prod_{j=1}^{r} |\sigma_j(\alpha)| \prod_{j=1}^{s} |\tau_j(\alpha)|^2 \le 2^s C_0^d,$$

so we can take any number larger than $2^s C_0^d$ for M.

To estimate the distance between $\mathrm{Log}(\alpha)$ and x, we also need lower bounds on $|\sigma_j(\alpha)|$ and $|\tau_j(\alpha)|$. We deduce these from

$$|\sigma_{j_0}(\alpha)| = \frac{|\,\mathrm{N}(\alpha)|}{\prod_{j\neq j_0}|\sigma_j(\alpha)|\prod_j|\tau_j(\alpha)|^2}$$
$$|\tau_{j_0}(\alpha)|^2 = \frac{|\,\mathrm{N}(\alpha)|}{\prod_j|\sigma_j(\alpha)|\prod_{j\neq j_0}|\tau_j(\alpha)|^2},$$

and $\mathrm{N}(\alpha)\geq 1$ together with the upper bounds we already have. We obtain

$$|\sigma_{j_0}(\alpha)| \geq 2^{-s}C_0^{-d+1}\prod_{j\neq j_0}\exp(-x_j)\prod_j\exp(-x_{r+j}) = 2^{-s}C_0^{-d+1}\exp(x_{j_0})$$
$$|\tau_{j_0}(\alpha)|^2 \geq 2^{-s+1}C_0^{-d+1}\prod_{j}\exp(-x_j)\prod_{j\neq j_0}\exp(-x_{r+j}) = 2^{-s+1}C_0^{-d+1}\exp(x_{r+j_0}).$$

Using the definition of $\mathrm{Log}(\alpha)$, we get that all coordinates of $\mathrm{Log}(\alpha)-x$ are bounded in absolute value by

$$\mathrm{Log}(2^sC_0^{d-1}),$$

and this proves our claim with an appropriate choice of R. □

Proof of Proposition 77. Combining Lemmata 82 and 83, we find some $R>0$ depending only on K such that for all $x\in V$, there is some unit $u\in\mathcal{O}_K^\times$ with $\|\mathrm{Log}(u)-x\|\leq R$. That is, $\mathrm{Log}(\mathcal{O}_K^\times)\cap B(x,R)\neq\varnothing$ for any $x\in V$. By Lemma 81, this implies that $\mathrm{Log}(\mathcal{O}_K^\times)$ is not contained in a proper subspace of V, so its rank is at least $r+s-1$. □

9. Cyclotomic fields and Fermat's last theorem

The goal of this section is to prove Theorem 7 under the additional assumption that $p\nmid xyz$.

9.1. **Cyclotomic fields.** Recall that for an integer $n\in\mathbf{Z}_{\geq 3}$, we write $\theta_n = e^{2\pi i/n}$. The proof of Theorem 7 involves the cyclotomic filed $\mathbf{Q}(\theta_p)$ for some prime p, and we collect some facts about it in this section.

We first recall some results from Part II Galois theory.

Theorem 84. *Let $n\in\mathbf{Z}_{\geq 1}$. Let $(\mathbf{Z}/n\mathbf{Z})^\times$ denote the residue classes* mod *n that are relatively prime to n. Let $\varphi(n)=|\mathbf{Z}/n\mathbf{Z}|^\times$.*

Then we have $[\mathbf{Q}(\theta_n):\mathbf{Q}]=\varphi(n)$. Furthermore, for each $j\in(\mathbf{Z}/n\mathbf{Z})^\times$, there is an embedding $\sigma_j:\mathbf{Q}(\theta_n)\to\mathbf{C}$ such that $\sigma_j(\theta_n)=\theta_n^j$. Moreover, $\sigma_j(\mathbf{Q}(\theta_n))=\mathbf{Q}(\theta_n)$.

If p is a prime, the minimal polynomial of θ_p is

$$\frac{x^p-1}{x-1} = x^{p-1}+\cdots+1.$$

For composite n, the notation in the theorem slightly differs from our usual convention that embeddings are indexed by $1, \dots, [K : \mathbf{Q}]$.

In what follows, let p be an odd rational prime, and let $K = \mathbf{Q}(\theta_p)$. We determine the discriminant, the ring of integers, the factorization of $\langle p \rangle$ and the roots of unity in K.

Theorem 85. *We have $\mathcal{O}_K = \mathbf{Z}[\theta_p]$ and $\operatorname{disc}(K) = (-1)^{(p-1)/2} p^{p-2}$.*

There is a prime $P \subset \mathcal{O}_K$ such that $\langle p \rangle = P^{p-1}$. For all $i \neq j \in \{0, \dots, p-1\}$, we have

$$P = \langle \theta_p^i - \theta_p^j \rangle.$$

The roots of unity in K are

$$\{\pm \theta_p^j : j = 0, \dots p-1\} = \{\theta_{2p}^j : j = 0, \dots, 2p-1\}.$$

We first prove the claim about roots of unity. We first observe that the two sets in the claim are indeed the same, which follows from

$$-\theta_p^{(p+1)/2} = e^{-i\pi} e^{2\pi i (p+1)/2p} = e^{2\pi i ((p+1)/2p - p/2p)} = e^{2\pi i/2p} = \theta_{2p}$$

and $\theta_p = \theta_{2p}^2$.

We will also use the following properties of Euler's totient function φ. If m, n are coprime, then $\varphi(mn) = \varphi(m)\varphi(n)$. If $m | n$, then $\varphi(m) | \varphi(n)$.

Proof of last part about roots of unity. Write W for the set of the roots of unity in K. Let $t \in \mathbf{R}_{>0}$ be a the smallest number such that $e^{2\pi i t} \in W$. By finiteness of W, the minimum exists.

We claim that if $s \in \mathbf{R}_{>0}$ is such that $e^{2\pi i s} \in W$, then $s/t \in \mathbf{Z}$. Indeed, $e^{2\pi i (s - \lfloor s/t \rfloor t)} \in W$, and $0 \leq s - \lfloor s/t \rfloor t < t$, so the minimality of t implies $s - \lfloor s/t \rfloor t = 0$, and the claim follows.

Since $e^{2\pi i/(2p)} \in W$, it follows that $t = 1/(2kp)$ for some $k \in \mathbf{Z}_{>0}$. We show that $k = 1$, which completes the proof. Since $\theta_{2kp} \in \mathbf{Q}(\theta_p)$, $\varphi(2kp) = [\mathbf{Q}(\theta_{2kp}) : \mathbf{Q}] \leq [\mathbf{Q}(\theta_p) : \mathbf{Q}] \leq p - 1$. We cannot have $p | k$ for otherwise we would have $p(p-1) = \varphi(p^2) \leq \varphi(2kp) \leq p-1$. Therefore, $\varphi(2kp) = \varphi(2k)(p-1)$. Hence we must have $\varphi(2k) = 1$, which implies $k = 1$, as required. □

The next result will be used to prove both the claim about $\mathcal{O}_K$ and the factorization of $\langle p \rangle$.

Proposition 86. *We have*

$$(1 - \theta_p) \cdots (1 - \theta_p^{p-1}) = p.$$

Moreover, for all $i \neq j \in \{0, \dots, p-1\}$ there is a unit $u_{i,j} \in \mathbf{Z}[\theta_p]^\times$ such that

$$u_{i,j} (\theta_p^i - \theta_p^j)^{p-1} = p.$$

We stress that the claim is that $u_{i,j}$ is a unit in $\mathbf{Z}[\theta_p]$, which, a priori, is stronger than claiming that it is a unit in $\mathcal{O}_K$, because we are yet to prove that these two rings equal.

Lemma 87. *For all $i, j, k, l \in \{0, \dots, p-1\}$ with $i \neq j$ and $k \neq l$, we have that*

$$\frac{\theta_p^i - \theta_p^j}{\theta_p^k - \theta_p^l} \in \mathbf{Z}[\theta_p]^\times.$$

Proof. It is enough to prove that

$$\frac{\theta_p^i - \theta_p^j}{\theta_p^k - \theta_p^l} \in \mathbf{Z}[\theta_p].$$

For if we exchange the roles of i, j and k, l, we get that the inverse is also in $\mathbf{Z}[\theta_p]$.

Multiplying both the denominator and the numerator by some power of θ_p, which is a unit in $\mathbf{Z}[\theta_p]$, we may assume $i = k = 0$.

Since non-zero residues $\mod p$ form a multiplicative group, there is some $m \in \mathbf{Z}$ with $m \not\equiv 0 \mod p$ such that $j \equiv ml \mod p$. Then

$$\frac{1 - \theta_p^j}{1 - \theta_p^l} = \frac{1 - \theta_p^{ml}}{1 - \theta_p^l} = 1 + \theta_p^l + \ldots + \theta_p^{(m-1)l} \in \mathbf{Z}[\theta_p],$$

as required. □

Proof of Propositon 86. The roots of the minimal polynomial of θ_p are precisely $\theta_p, \dots, \theta_p^{p-1}$, hence

$$(x - \theta_p) \cdots (x - \theta_p^{p-1}) = x^{p_1} + \ldots + x + 1.$$

We plug in $x = 1$ to get the first claim.

For the second claim, we observe that Lemma 87 implies that

$$u_{i,j} := \frac{p}{(\theta_p^i - \theta_p^j)^{p-1}} = \frac{(1 - \theta_p) \cdots (1 - \theta_p^{p-1})}{(\theta_p^i - \theta_p^j)^{p-1}}$$

is a unit in $\mathbf{Z}[\theta_p]$. □

In the next lemma, we compute the discriminant of $\mathbf{Z}[\theta_p]$. This will imply the claim about $\operatorname{disc}(K)$ once we show the claim about the ring of integers.

Lemma 88. *We have*

$$\operatorname{disc}(\mathbf{Z}[\theta_p]) = (-1)^{(p-1)/2} p^{p-2}.$$

Proof. Write $f(x) = x^n - 1$, and $g(x) = f(x)/(x-1)$; the latter is the minimal polynomial of θ_p. We have

$$\operatorname{disc}(\mathbf{Z}[\theta_p]) = (-1)^{(p-1)(p-2)/2} \operatorname{N}(g'(\theta_p)).$$

We note that

$$f'(\theta_p) = g'(\theta_p)(\theta_p - 1) + g(\theta_p) = g'(\theta_p)(\theta_p - 1).$$

Therefore,

$$\operatorname{N}(g'(\theta_p)) = \frac{\operatorname{N}(f'(\theta_p))}{\operatorname{N}(\theta_p - 1)}.$$

By Proposition 86 (and Theorem 84), we have $\mathrm{N}(\theta_p - 1) = (-1)^{p-1}p = p$. In addition,

$$\mathrm{N}(f'(\theta_p)) = \mathrm{N}(p\theta_p^{p-1}) = p^{p-1}.$$

Here we used $\mathrm{N}(\theta_p) = 1$, which can be seen from the constant coefficient of g. We get the claim by putting together our calculations. □

Proof of Theorem 85. We begin by proving $\mathcal{O}_K = \mathbf{Z}[\theta_p]$. We suppose to the contrary that $\mathcal{O}_K \supsetneq \mathbf{Z}[\theta_p]$.

By $\mathrm{disc}(\mathbf{Z}[\theta_p]) = (-1)^{(p-1)/2}p^{p-2}$ and Proposition 32, we know that all elements of $\mathcal{O}_K$ are of the form α/d for some $\alpha \in \mathbf{Z}[\theta_p]$ and $d \in \mathbf{Z}_{>0}$ with $d^2 | p^{p-2}$. By our assumption, there is some $\beta \in \mathcal{O}_K \backslash \mathbf{Z}[\theta_p]$. Then $p^k\beta \in \mathbf{Z}[\theta_p]$ for some $k \in \mathbf{Z}_{>0}$. We have $p = u(1-\theta_p)^{p-1}$ for some $u \in \mathbf{Z}[\theta_p]^\times$. Considering the sequence

$$u^k\beta, (1-\theta_p)u^k\beta, \dots, (1-\theta_p)^{(p-1)k}u^k\beta = p^k\beta,$$

whose first element is not in $\mathbf{Z}[\theta_p]$, but whose last element is, we can find some $\gamma \in \mathcal{O}_K \backslash \mathbf{Z}[\theta_p]$ such that $(1-\theta_p)\gamma \in \mathbf{Z}[\theta_p]$.

We note that $1, 1-\theta_p, \dots, (1-\theta_p)^{p-2}$ is a basis for $\mathbf{Z}[\theta_p]$ as a $\mathbf{Z}$-module. This can be seen by observing $\mathbf{Z}[1-\theta_p] = \mathbf{Z}[\theta_p]$, which follows by $1 - \theta_p \in \mathbf{Z}[\theta_p]$ and $\theta_p \in \mathbf{Z}[1-\theta_p]$. Hence

$$(1-\theta_p)\gamma = a + (1-\theta_p)\gamma'$$

for some $a \in \mathbf{Z}$ and $\gamma' \in \mathbf{Z}[\theta_p]$. Note that $p \nmid a$, for otherwise, we would have $(1-\theta_p) | a + (1-\theta_p)\gamma'$ in $\mathbf{Z}[\theta_p]$ and hence $\gamma \in \mathbf{Z}[\theta_p]$, which is not the case. Then

$$\frac{a}{1-\theta_p} = \gamma - \gamma' \in \mathcal{O}_K.$$

Furthermore,

$$\frac{1}{u}\Big(\frac{a}{1-\theta_p}\Big)^{p-1} = \frac{a^{p-1}}{p} \in \mathcal{O}_K,$$

which is impossible. This proves $\mathcal{O}_K = \mathbf{Z}[\theta_p]$.

Now $\mathrm{disc}(K) = (-1)^{(p-1)/2}p^{p-2}$ follows from Lemma 88.

By Proposition 86, we have

$$\langle p \rangle = \langle \theta_p^i - \theta_p^j \rangle^{p-1}$$

for all $0 \le i \ne j \le p-1$. By Proposition 51, we have $\mathrm{N}(\langle p \rangle) = p^{p-1}$. Multiplicativity of norms implies

$$\mathrm{N}(\langle \theta_p^i - \theta_p^j \rangle) = p,$$

hence these must be prime ideals for all permitted pairs i, j. By uniqueness of prime factorization, these are the same prime ideals independently of i and j. This fact also follows from Lemma 87. The theorem is now proved in full. □

9.2. **Case I of Fermat's Last theorem for regular primes.** In this section, we fix some rational prime $p \geq 5$, write $\theta = \theta_p$ and $K = \mathbf{Q}[\theta]$. We say that the prime p is regular if $p \nmid h(K)$, and we assume that this holds for p. We write P for the unique prime lying over p in K.

Our purpose is to prove Theorem 7 under the additional assumption that $p \nmid xyz$. That is, we are going to show that there are no solutions of

$$x^p + y^p = z^p, \qquad x, y, z \in \mathbf{Z}_{\geq 1}$$

under the assumptions we have already made. The first step is the following.

Proposition 89. *Let $p \geq 5$ be a regular prime, and let $x, y, z \in \mathbf{Z}$ be such that $\gcd(x, y, z) = 1$, $p \nmid xyz$ and $x^p + y^p = z^p$. Then there is some $\alpha \in \mathcal{O}_K$ and some unit $u \in \mathcal{O}_K^\times$ such that*

$$x + \theta y = u\alpha^p.$$

Proof. We have already observed that $x^p + y^p = z^p$ can be factorized as

$$(x + y)(x + \theta y) \cdots (x + \theta^{p-1} y) = z^p.$$

We first show that the principal ideals generated by the factors on the left hand side are relatively prime. Suppose to the contrary that there is some prime Q that divides both $\langle x + \theta^i y \rangle$ and $\langle x + \theta^j y \rangle$ for some $0 \leq i \neq j \leq p - 1$. This means

$$x + \theta^i y, x + \theta^j y \in Q.$$

Taking appropriate linear combinations, we get

$$(\theta^i - \theta^j)y, (\theta^{-i} - \theta^{-j})x \in Q.$$

We note that

$$Q \neq P = \langle \theta^i - \theta^j \rangle = \langle \theta^{-i} - \theta^{-j} \rangle,$$

for $Q | \langle z \rangle^p$ and $P \nmid \langle z \rangle^p$ by the assumption $p \nmid z$. Therefore, we have $Q | \langle x \rangle$ and $Q | \langle y \rangle$.

On the other hand, x and y are coprime in $\mathbf{Z}$, for any common prime factor would divide also z by $z^p = x^p + y^p$. Thus $ax + by = 1$ for some $a, b \in \mathbf{Z}$. Now $x, y \in Q$ implies $1 \in Q$, a contradiction. We proved that the ideals

$$\langle x + y \rangle, \langle x + \theta y \rangle, \ldots, \langle x + \theta^{p-1} y \rangle \tag{11}$$

are pairwise coprime.

The prime factors of $\langle z \rangle^p$ all have multiplicities divisible by p. These are distributed among the ideals (11) in a manner that each prime goes to a single factor with its entire multiplicity. Now we have that

$$\langle x + \theta y \rangle = I^p$$

for some ideal $I \subset \mathcal{O}_K$.

It remains to show that I is a principal ideal. We know that I^p is principal. Since the order of the class group is not divisible by p, there is no non-unit element in the class group whose p-th power is the unit element. For this reason, I must be principal, and the proposition is proved. □

Proposition 90. *Let $p \geq 5$ be a regular prime, and let $x, y, z \in \mathbf{Z}$ be such that $\gcd(x, y, z) = 1$, $p \nmid xyz$ and $x^p + y^p = z^p$. Then $x \equiv y \mod p$.*

We write τ for the restriction of complex conjugation on K. This is an automorphism of K, and in the notation of the previous section, we have $\tau = \sigma_{p-1}$.

Lemma 91. *Let $\alpha \in \mathcal{O}_K$. Then*

$$\alpha^p \equiv \tau(\alpha)^p \mod \langle p \rangle.$$

Proof. Let

$$\alpha = a_0 + a_1\theta + \ldots + a_{p-2}\theta^{p-2}$$

for some $a_0, \ldots, a_{p-2} \in \mathbf{Z}$. Using that all binomial coefficients of the form $\binom{p}{j}$ for $j = 1, \ldots, p-1$ are divisible by p, we get that

$$(\beta_1 + \beta_2)^p \equiv \beta_1^p + \beta_2^p \mod \langle p \rangle$$

for all $\beta_1, \beta_2 \in \mathcal{O}_K$. Using this iteratively, we get

$$\alpha^p \equiv a_0^p + (a_1\theta)^p + \ldots + (a_{p-2}\theta^{p-2})^p \mod \langle p \rangle.$$

Using $\theta^p = 1$, it follows that

$$\alpha^p \equiv b \mod \langle p \rangle$$

for some $b \in \mathbf{Z}$.

Since τ is an automorphism of $\mathcal{O}_K$, we get

$$\tau(\alpha^p) \equiv \tau(b) \mod \tau(\langle p \rangle).$$

Since $\tau(p) = p$, it follows that $\tau(\langle p \rangle) = \langle p \rangle$. Using this and $\tau(b) = b$, we get

$$\tau(\alpha^p) \equiv b \mod \langle p \rangle,$$

and the claim follows. □

Lemma 92. *For all units $u \in \mathcal{O}_K^\times$, there is some root of unity $\varepsilon \in \mathcal{O}_K$ such that*

$$\tau(u) = \varepsilon u$$

Proof. The automorphisms of K all commute, and, in particular, for all embedding $\sigma : K \to \mathbf{C}$ we have $\sigma \circ \tau = \tau \circ \sigma$. Then

$$|\sigma(\tau(u))| = |\tau(\sigma(u))| = |\sigma(u)|.$$

It follows that $|\sigma(u^{-1}\tau(u))| = 1$ for all embedding σ. With the notation of Section 8.2, this means $\mathrm{Log}(u^{-1}\tau(u)) = 0$, and by Proposition 75, $\varepsilon := u^{-1}\tau$ is a root of unity, as required. □

Lemma 93. *Assume that*

$$a_0 + a_1\theta + \ldots + a_{p-1}\theta^{p-1} \equiv b_0 + b_1\theta + \ldots + b_{p-1}\theta^{p-1} \mod \langle p \rangle$$

for some integers $a_0, \ldots, a_{p-1}, b_0, \ldots, b_{p-1}$. *Assume that there is some* $j \in \{0, \ldots, p-1\}$ *such that* $a_j = b_j = 0$. *Then* $a_i \equiv b_i \mod p$ *for all* $i = 0, \ldots, p-1$.

Proof. Multiplying both sides of the congruence by θ^{p-1-j} and reducing the exponents of $\theta \mod p$, it is enough to consider the case $j = p-1$. That case follows simply from the fact that $1, \theta, \ldots, \theta^{p-2}$ is an integral basis for $\mathcal{O}_K$, hence $p, p\theta, \ldots, p\theta^{p-2}$ is a basis for $\langle p \rangle$ as a $\mathbf{Z}$-module. Therefore,

$$(a_0 - b_0) + (a_1 - b_1)\theta + \ldots + (a_{p-2} - b_{p-2})\theta^{p-2} \in \langle p \rangle$$

if and only if $p | a_j - b_j$ for all $j = 0, \ldots, p-2$. □

Proof of Proposition 90. Using Proposition 89, we have

$$x + \theta y = u\alpha^p$$

for some $u \in \mathcal{O}_K^\times$ and $\alpha \in \mathcal{O}_K$. Using Lemmata 91 and 92, we get

$$\tau(x + \theta y) = \tau(u\alpha^p) \equiv \varepsilon u \alpha^p \equiv \varepsilon(x + \theta y) \mod \langle p \rangle$$

for some root of unity ε.

By Theorem 85, we have $\varepsilon = \theta^j$ or $\varepsilon = -\theta^j$ for some $j \in \mathbf{Z}$. First we consider the former possibility. Then

$$x + \theta^{p-1} y \equiv \theta^j x + \theta^{j+1} y \mod \langle p \rangle.$$

Understanding the exponents j and $j+1$ modulo p, we can apply Lemma 93. Indeed the lemma is applicable because $p \geq 5$, hence there is some $k \in \{0, \ldots, p-1\}$ with $k \not\equiv 0, p-1, j, j+1$. Since $x, y \not\equiv 0 \mod p$, we have

$$\{0, p-1\} \equiv \{j, j+1\} \mod p.$$

This implies $j \equiv p-1 \mod p$, hence

$$x + \theta^{p-1} y \equiv \theta^{p-1} x + y \equiv \langle p \rangle.$$

Using Lemma 93 again, this gives us $x \equiv y \mod p$.

It remains to consider the case where $\varepsilon = -\theta^j$. The same calculation as above then yields $x \equiv -y \mod p$. However, then $z^p = x^p + y^p \equiv 0 \mod p$, since p is odd. This contradicts $p \nmid z$, so this case is not possible. □

Proof of Theorem 7. Suppose to the contrary that the equation $x^p + y^p = z^p$ has a solution for some integers x, y, z and some regular prime $p \geq 5$ with $p \nmid xyz$. We assume, as we may, that $\gcd(x, y, z) = 1$. We apply Proposition 90 for both the equation $x^p + y^p = z^p$ and $x^p + (-z)^p = (-y)^p$. We get $x \equiv y \equiv -z \mod p$. From $x^p + y^p + (-z)^p = 0$, we conclude $3x^p \equiv 0 \mod p$. We must have $p = 3$ or $p | x$, but

both possibilities are ruled out by our assumptions. This contradiction proves the theorem. □

References

[1] Ş. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004. MR2031707

[2] A. Baker, *A comprehensive course in number theory*, Cambridge University Press, Cambridge, 2012. MR2954465

[3] H. M. Edwards, *The genesis of ideal theory*, Arch. Hist. Exact Sci. **23** (1980/81), no. 4, 321–378. MR608312

[4] D. A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur. MR3822326