Algebraic Number Theory

Dietrich Burde

Lecture Notes 2022

Contents

CHAPTER 1

Introduction

Number theory is a branch of pure mathematics devoted to the properties of integers and integer-valued functions in the broadest sense. It is one of the oldest sciences. The main subdivisions of number theory are elementary number theory, analytic number theory, algebraic number theory, Diophantine geometry, probabilistic number theory, arithmetic combinatorics and computational number theory. There is also an area called *arithmetic geometry*, which is a sort of number theory using the methods of algebraic geometry over $\mathbb{Z}, \mathbb{Q}, \mathbb{F}_p$ instead of $\mathbb{C}$, or over other algebraically closed fields. Many problems however include several sub-directions. A prominent example is the proof of *Fermat's Last Theorem - FLT*, which uses almost every area of number theory and many other methods, too.

Fermat's equation is the Diophantine equation $x^n + y^n = z^n$ for $n \geq 2$ over the integers. It also had a great influence in the development of algebraic number theory. It shows us a motivation to study rings of integers in number fields. Already for exponent $n = 3$ we see how important this is. An integer solution (x, y, z) of $x^n + y^n = z^n$ is called *trivial*, if $xyz = 0$. Indeed, we have infinitely many trivial solutions, e.g., $(0, y, y)$.

Proposition 1.0.1 (Euler 1770). *The Diophantine equation $x^3 + y^3 = z^3$ has no nontrivial integral solution.*

Proof. We don't want to give a full prove here, which can be found, say, in [**6**]. We only want to give an idea, why and how rings of integers are important for the proof. Let $\zeta = \zeta_3$ be a primitive third root of unity, so for example $\zeta = e^{\frac{2\pi i}{3}}$. The minimal polynomial of ζ over $\mathbb{Q}$ is $x^2 + x + 1$. Thus $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ is a quadratic field extension and $\mathbb{Q}(\zeta)$ is a vector space over $\mathbb{Q}$ with basis $\{1, \zeta\}$. The polynomial $t^3 - 1$ splits over $\mathbb{Q}(\zeta)$ as

$$t^3 - 1 = (t - 1)(t - \zeta)(t - \zeta^2).$$

Substituting $t = -x/y$ and multiplying up yields

$$z^3 = x^3 + y^3 = (x + y)(x + \zeta y)(x + \zeta^2 y). \tag{1.1}$$

Thus we have written Fermat's equation as a product decomposition of a third power over the ring

$$\mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}.$$

This ring is also called the *ring of Eisenstein integers*. It has very good properties for solving Fermat's equation with exponent 3. It is a *Euclidean ring* and hence a PID and a UFD. The unit group is isomorphic to C_6, given by the six units $\pm 1, \pm\zeta, \pm\zeta^{-1}$. The ring $\mathbb{Z}[\zeta]$ is the ring of integers of the quadratic number field $\mathbb{Q}(\zeta)$. Note that $1 + \zeta + \zeta^2 = 0$.

Now suppose that (x, y, z) is a nontrivial solution of Fermat's equation and all integers are pairwise coprime. Then it follows that $3 \mid xyz$, because otherwise we would have $x^3 + y^3 \equiv -2, 0, 2 \mod 9$ and $z^3 \equiv 1, -1$ so that $x^3 + y^3 \neq z^3$. Consequently, at least one of the integers

x, y, z is divisible by 3. We may assume $3 \mid z$ and $3 \nmid xy$. Then we can reformulate the problem as follows. We need to show that the equation

$$x^3 + y^3 = (3^m z)^3 \tag{1.2}$$

has no nontrivial integral solutions, with x, y, z pairwise coprime, $3 \nmid xyz$, and $m \geq 0$ a nonnegative integer. For $m = 0$ we just have seen that there are no nontrivial solutions. From (1.2) we derive, like from (1.1) earlier, that

$$(3^m z)^3 = (x + y)(x + \zeta y)(x + \zeta^2 y)$$

in $\mathbb{Z}[\zeta]$. The three factors are not pairwise coprime. However, it is easy to see that their greatest common divisor is each time given by the prime element $1 - \zeta$. For example, because of $3 = (1 - \zeta)(1 - \zeta^2)$ we have $1 - \zeta \mid 3 \mid x + y$ and hence $1 - \zeta \mid x + y$.

Now we come to a crucial argument, using that the ring $\mathbb{Z}[\zeta]$ is *factorial*. The three factors in the equation are again cubes, up to units and powers of $1 - \zeta$. Arguing with elementary division properties in $\mathbb{Z}[\zeta]$ one can show that we have

$$x + y = 3^{3m-1} c^3,$$
$$x + \zeta y = (1 - \zeta)\rho^3$$

with $\rho \in \mathbb{Z}[\zeta]$, $c \in \mathbb{Z}$, where c and ρ are coprime and not divisible by $1 - \zeta$. Hence we also have $3 \nmid c$. Writing $\rho = a + \zeta b$ with $a, b \in \mathbb{Z}$ in the second equation, we obtain, with $\zeta^2 = -1 - \zeta$, that

$$\begin{aligned} x + \zeta y &= (1 - \zeta)(a + b\zeta)^3 \\ &= (1 - \zeta)(a^3 - 3ab^2 + b^3 + 3a^2 b\zeta - 3ab^2\zeta) \\ &= (a^3 + b^3 + 3a^2 b - 6ab^2) + \zeta(-a^3 - b^3 + 6a^2 b - 3ab^2). \end{aligned}$$

A comparison of the coefficients yields $x = a^3 + b^3 + 3a^2 b - 6ab^2$ and $y = -a^3 - b^3 + 6a^2 b - 3ab^2$, so that $9ab(a - b) = x + y = 9(3^{m-1}c)^3$, i.e.,

$$ab(a - b) = (3^{m-1}c)^3.$$

Because of $xyz \neq 0$ we also have that $a, b, a - b$ are nonzero. Moreover they are pairwise coprime. Since the ring $\mathbb{Z}$ is factorial, $a, b, a - b$ are also cubes in $\mathbb{Z}$, namely

$$\{a, b, a - b\} = \{x_1^3, y_1^3, (3^{m-1}z_1)^3\}$$

with x_1, y_1, z_1 pairwise coprime and with $3 \nmid z_1$. Since $a + (-b) = a - b$, $a + (b - a) = b$ and $b + (a - b) = a$ we obtain an equation of the form (1.2) with $x_0^3 + y_0^3 = (3^{m-1}z_0)^3$, where x_0, y_0, z_0 are pairwise coprime with $3 \nmid x_0 y_0 z_0$, *but* with exponent $m - 1$ instead of m. So we can descend to $m = 0$ (the method of *descent* was already used by Fermat for his equation $x^4 + y^4 = z^4$ with exponent four). But the case $m = 0$ is impossible and the proof is finished. □

One would like to use this idea for all equations $x^p + y^p = z^p$ with p prime, but unfortunately then the ring $\mathbb{Z}[\zeta_p]$, for a primitive p-th root of unity, is no longer factorial for bigger p - actually it is factorial if and only if $p \leq 19$. Moreover the units of $\mathbb{Z}[\zeta_p]$ are not all of the form $\pm\zeta^j$ with $j \geq 0$. After all, at least $\mathbb{Z}[\zeta_p]$ is still the ring of integers of the number field $\mathbb{Q}(\zeta_p)$, and it is rewarding to study these rings.

However *Kummer* made big progress with Fermat's equation by replacing the lost uniqueness of the factorization of irreducible elements of $\mathbb{Z}[\zeta_p]$ by the unique factorization of *ideals* in $\mathbb{Z}[\zeta_p]$ into prime ideals. This was in a way the birth of modern algebraic number theory.

CHAPTER 2

Integral ring extensions

We always assume that a ring is commutative and has a unit, if not said otherwise.

2.1. Global fields and integral closure

We denote by $\mathbb{F}_p$ the finite field $\mathbb{Z}/p\mathbb{Z}$ for a prime p, and by $\mathbb{F}_p[t]$ the polynomial ring in one variable with coefficients in $\mathbb{F}_p$. The quotient field of $\mathbb{F}_p[t]$ is denoted by $\mathbb{F}_p(t)$. The quotient field of $\mathbb{Z}$ is given by $\mathbb{Q}$.

Definition 2.1.1. A *number field* is a finite field extension of $\mathbb{Q}$. A *function field* is a finite field extension of $\mathbb{F}_p(t)$.

Number fields and function fields have many things in common and are called *global fields*. Of course they are different, e.g., a number field has characteristic zero and a function field has characteristic $p > 0$.

Example 2.1.2. *Let K be a field extension of degree 2 over $\mathbb{Q}$. There there is a squarefree $d \in \mathbb{Z}$ with $K = \mathbb{Q}(\sqrt{d})$.*

Here $\mathbb{Q}(\sqrt{d})$ is called a *quadratic number field.*

Example 2.1.3. *Let K be a field extension of degree 2 over $\mathbb{F}_p(t)$. Then there exists a squarefree polynomial $D \in \mathbb{F}_p[t]$ with $K = \mathbb{F}_p(t, \sqrt{D}) = \{A + B\sqrt{D} \mid A, B \in \mathbb{F}_p(t)\}$.*

Here $\mathbb{F}_p(t, \sqrt{D})$ is called a *quadratic function field.*

Definition 2.1.4. Let $A \subset B$ be a ring extension. An element $x \in B$ is called *integral over A*, if there exists a monic polynomial $f \in A[t]$ with $f(x) = 0$. In other words, x satisfies a monic polynomial equation of the form

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0$$

with coefficients $a_1, \ldots, a_n$ in A.

Example 2.1.5. *Let $A = \mathbb{Z}$ and $B = \mathbb{R}$. Then $\sqrt{2}$ is integral over $\mathbb{Z}$, but $\frac{1}{2}$ is not integral over $\mathbb{Z}$.*

Indeed, $\sqrt{2}$ is a root of the monic polynomial $t^2 - 2$ in $\mathbb{Z}[t]$. And suppose that $\frac{1}{2}$ satisfies a polynomial equation as above. Then by multiplying with 2^n we obtain

$$1 + 2a_1 + \cdots + 2^n a_n = 0,$$

with integer coefficients. This is impossible as we see by considering the equation modulo 2.

Definition 2.1.6. A ring extension $A \subset B$ is called *integral*, if every element $b \in B$ is integral over A.

Proposition 2.1.7. *Let $A \subset B$ be a ring extension. The elements $b \in B$ which are integral over A form a subring of B.*

Proof. We will gives two proofs. The first one uses Newton's theory of symmetric functions and needs no further preparations. The only drawback is that we need to assume that A is a domain. The second proof is the standard proof by Dedekind, which is given in most books on algebraic number theory. It argues with finitely generated A-modules.

So let us start with the first proof. A polynomial $P(x_1, \dots, x_r)$ in the polynomial ring $A[x_1, \dots, x_r]$ is called *symmetric*, if

$$P(x_{\sigma(1)}, \dots, x_{\sigma(r)}) = P(x_1, \dots, x_r)$$

for all permutations $\sigma \in \mathcal{S}_n$. In particular the polynomials

$$S_1 = \sum_i x_i, \quad S_2 = \sum_{i<j} x_i x_j, \ \dots \ , S_r = x_1 x_2 \cdots x_r$$

are all symmetric. They are called *elementary symmetric polynomials.* We know that the elementary symmetric polynomials generate the ring of symmetric polynomials. Every symmetric polynomial $P(x_1, \dots, x_r)$ is a polynomial in the elementary symmetric polynomials, i.e., it is in $A[S_1, \dots, S_r]$.

Claim: Let Ω be an algebraically closed field containing A. If $\alpha_1, \dots, \alpha_n$ are the roots of a monic polynomial of $A[x]$ in Ω, then every polynomial $g(\alpha_1, \dots, \alpha_n)$ with coefficients in A is a root of a monic polynomial in $A[x]$.

Indeed,

$$h(x) := \prod_{\sigma \in \mathcal{S}_n} ((x - g(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}))$$

is a monic polynomial, whose coefficients are symmetric polynomials in the α_i, and hence lie in A. But obviously $g(\alpha_1, \dots, \alpha_n)$ is one of the roots of $h(x)$.

Now we can finish the first proof. Let α_1 and α_2 be two elements of B, which are integral over A. So there is a monic polynomial in $A[x]$, which has α_1 and α_2 both as roots. We can apply now the above remark by choosing g as $\alpha_1 + \alpha_2$ or as $\alpha_1 \alpha_2$. Then it follows that these elements are integral over A. □

Before coming to Dedekind's proof we need to introduce further notions.

Definition 2.1.8. Let $A \subset B$ be a ring extension. The ring of all elements $b \in B$, which are integral over A is denoted by $\overline{A}^B$. If $\overline{A}^B = A$, then A is called *integrally closed in* B. If a domain A is integrally closed in its quotient field K we call A *integrally closed.*

Instead of $\overline{A}^K$ we usually just write $\overline{A}$.

Example 2.1.9. *The domain $\mathbb{Z}$ is integrally closed, i.e., we have $\overline{\mathbb{Z}} = \mathbb{Z}$.*

The proof follows from the rational root theorem. Let $A = \mathbb{Z}$. Then the quotient field is $K = \mathbb{Q}$. Let $x \in \mathbb{Q}$ be integral over $\mathbb{Z}$. Then x is a root of a monic polynomial

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

with integral coefficients. If $x = \frac{p}{q}$, then $q \mid a_0 = 1$ and $p \mid a_n$ by the rational root theorem. Hence we have $x \in \mathbb{Z}$.

Proposition 2.1.10. *Let $A \subset B$ be a ring extension and $b \in B$. Then the following statements are equivalent.*

(1) *The element b is integral over A.*

(2) *The ring* $A[b] = \{\sum_{i=0}^n a_i b^i \mid n \in \mathbb{N},\ a_i \in A\}$ *is a finitely generated* A*-module.*
(3) *The ring* $A[b]$ *is contained in a subring* C *of* B*, where* C *is a finitely generated* A*-module.*

Proof. (1) $\Rightarrow$ (2): by assumption b satisfies an equation

$$b^n + a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_n = 0$$

with $a_i \in A$. So we have for all $j \geq 0$ that

$$b^{n+j} = -(a_1 b^{n+j-1} + a_2 b^{n+j-2} + \cdots + a_{n-1} b^{j+1} + a_n b^j).$$

By induction we see that $b^k \in A[1, b, b^2, \dots, b^{n-1}]$ for all $k \geq 0$. Hence the ring $A[b]$ is generated as an A-module by finitely many elements $1, b, b^2, \dots, b^{n-1}$.

(2) $\Rightarrow$ (3): let $C := A[b] \subset B$.

(3) $\Rightarrow$ (1): let C be generated as A-module by the elements $c_1, c_2, \dots, c_n$. We have $A \subseteq A[b] \subseteq C \subseteq B$. Hence all elements bc_i lie in C, so that there exist $a_{ij} \in A$ with

$$bc_i = \sum_{j=1}^n a_{ij} c_j.$$

Let $M = (m_{ij}) \in M_n(A[b])$ be the matrix with $m_{ij} = \delta_{ij} b - a_{ij}$. Denote by M' the adjoint matrix of M. We have $M'M = \det(M) I_n$. With $u = (c_1, \dots, c_n)^t$ we have $M'Mu = 0$ and $\det(M)c_i = 0$ for all $i = 1, \dots, n$. Thus we have $\det(M)c = 0$ for all $c \in C = \sum_{i=1}^n Ac_i$. Since C contains the unit as a subring of B we obtain $\det(M) = 0$. This yields the polynomial for b, which we need. Indeed, $f(x) = \det(\delta_{ij} x - a_{ij})$ is a monic polynomial with coefficients in A such that $f(b) = \det(M) = 0$. □

There is another variant of this proposition, which we will also use. Let L be a field containing A and let $b \in L$. Then b is integral over A if and only if there exists a nonzero finitely generated A-submodule C of L with $bC \subseteq C$ (for example, possibly $C = A[b]$).

Corollary 2.1.11. *Let* C *be also a finitely-generated* A*-module. Then* $A \subset C$ *is an integral ring extension.*

Corollary 2.1.12 (Transitivity). *Let* $A \subset B$ *and* $B \subset C$ *be integral ring extensions. Then also* $A \subset C$ *is an integral ring extension.*

Proof. Let $c \in C$. It satisfies an equation

$$c^n + b_1 c^{n-1} + \cdots + b_n = 0$$

with $b_i \in B$. By Proposition 2.1.10 we know that $A[b_i]$ is a finitely generated A-module for each i, because B is integral over A. Similar to the proof of (1) $\Rightarrow$ (2) from above it follows inductively that $A[b_1, \dots, b_n]$ is a finitely generated A-module. Hence all its elements are integral over A, in particular also the element $c \in A[b_1, \dots, b_n]$. □

Here is the second proof of Proposition 2.1.7 by Dedekind.

Corollary 2.1.13 (Dedekind). *Let* $A \subset B$ *be a ring extension. Then* $\overline{A}^B$ *is a ring.*

Proof. Let $x, y \in \overline{A}^B$. Then the A-modules $A[x]$ and $A[y]$ are finitely generated by Proposition 2.1.10. It follows that the A-module $A[x, y]$ is finitely generated. Indeed, if $\{e_1, \dots, e_n\}$ generate the A-module $A[x]$, and if $\{f_1, \dots, f_m\}$ generate the A-module $A[y]$, then

$\{e_1f_1, \ldots, e_if_j, \ldots, e_nf_m\}$ generate the A-module $A[x,y]$. Since the elements $x \pm y$ and xy lie in $A[x,y]$, they are integral over A, so they lie in $\overline{A}^B$. □

Example 2.1.14. *The $\mathbb{Z}$-module $M = \mathbb{Z}[\frac{1}{2}]$ is not finitely generated.*

Indeed, M is an infinite abelian group with $M/2M = 0$, so that it cannot be finitely generated. So by Proposition 2.1.10 we see again that $\frac{1}{2}$ is not integral over $\mathbb{Z}$. We had seen this differently in Example 2.1.5. More generally we know by Example 2.1.9 that $\mathbb{Z}$ is integrally closed. In fact, *every* factorial ring is integrally closed.

Proposition 2.1.15. *Let A be a factorial ring. Then A is integrally closed.*

Proof. Let K be the quotient field of A and let $a/s \in K$ be integral over A with $a, s \in A$, $s \neq 0$ and a, s coprime. We need to show that $a/s \in A$. There exist an $n \geq 1$ and elements $a_0, \ldots, a_{n-1} \in A$ with

$$(a/s)^n + a_{n-1}(a/s)^{n-1} + \cdots + a_1(a/s) + a_0 = 0.$$

Multiplying this equation with s^n we obtain

$$a^n + sa_{n-1}a^{n-1} + \cdots + s^{n-1}a_1a + s^na_0 = 0.$$

Since s divides each summand, except for the first one, it follows that $s \mid a^n$. This is a contradiction to the fact that a and s are coprime, since A is factorial. Thus s is a unit in A and therefore $a/s \in A$. □

For example, we know that $\mathbb{Z}$ and $\mathbb{Z}[i]$ are PIDs and hence factorial. So they are integrally closed. We can also use the result for showing that certain rings are not factorial, because they would be integrally closed otherwise.

Example 2.1.16. *The ring $\mathbb{Z}[\sqrt{5}]$ is not factorial.*

Suppose that $\mathbb{Z}[\sqrt{5}]$ is factorial. Then it is also integrally closed. However, the element $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}[\sqrt{5}]$ since it is a root of the monic polynomial $x^2 - x - 1$. Since this element is not contained in $\mathbb{Z}[\sqrt{5}]$, this ring is not integrally closed and we have a contradiction.

Unfortunately the converse of Proposition 2.1.15 does not hold in general. Hence we often cannot use this argument. For example, the ring $\mathbb{Z}[\sqrt{-5}]$ is integrally closed as we will see in 2.2.5, but it is not factorial.

Example 2.1.17. *The ring $\mathbb{Z}[\sqrt{-5}]$ is not factorial.*

We show directly that not every element has a unique factorization, up to units and permutations. The standard example is

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

By using the norm map one shows that all elements are irreducible and not associated. We have $N(z) = z\overline{z}$ for $z = a + b\sqrt{-5}$, so that $a + b\sqrt{-5} \mapsto a^2 + 5b^2$. The norm map is multiplicative and $\alpha \in \mathbb{Z}[\sqrt{-5}]$ satisfies $N(\alpha) = 1$ if and only if α is a unit. Suppose that $1 + \sqrt{-5} = \alpha\beta$. Then we have

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1 + \sqrt{-5}) = 6,$$

and hence $N(\alpha) = 1, 2, 3$ or 6. In the first case α is a unit, and in the last case β is a unit. The other cases are impossible, because $a^2 + 5b^2 = 2, 3$ has no solution in in $\mathbb{Z}$. Hence $1 + \sqrt{-5}$ is irreducible. The same argument shows that the other elements are irreducible as well. Suppose that two elements here are associated. Then they have the same norm. So it is enough to verify that $1+\sqrt{-5}$ and $1+\sqrt{-5}$ are not associated. If so we would have

$$1+\sqrt{-5}=(a+b\sqrt{-5})(1-\sqrt{-5})$$

with integers a, b. But this is impossible.

Example 2.1.18. *The ring $\mathbb{Z}[\sqrt{-2}]$ is factorial.*

Even better, one can easily show that this ring is Euclidean and hence factorial. However, we want to compare this example with the previous one. Again it seems that we can give a counterexample for the unique factorization property by

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

The difference here is that the factors in $\mathbb{Z}[\sqrt{-2}]$ here are *not* irreducible. Indeed, we have

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

Then the two seemingly different factorizations of 6 become equivalent:

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

2.2. Rings of integers

Definition 2.2.1. Let K be a number field. The integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K and is denoted by $\mathcal{O}_K$.

By Proposition 2.1.10 rings of integers are indeed rings.

Proposition 2.2.2. *Rings of integers are integrally closed.*

Proof. Let $\mathcal{O}$ be the integral closure of $B=\mathcal{O}_K$ in $C=K$. Then the ring extensions $B\subset C$ and $A=\mathbb{Z}\subset B$ are integral. By the transitivity, Corollary 2.1.12, it follows that also $\mathcal{O}$ is integral over $\mathbb{Z}$, and hence $\mathcal{O}\subset\mathcal{O}_K$. So $\mathcal{O}=\mathcal{O}_K$. □

Example 2.2.3. *The ring of integers of the number field $\mathbb{Q}$ is $\mathbb{Z}$, i.e., $\mathcal{O}_{\mathbb{Q}}=\mathbb{Z}$.*

We want to determine the rings of integers for quadratic number fields $\mathbb{Q}(\sqrt{d})$, where d is a squarefree integer. We'll use the shorter notation $\mathcal{O}_d$ for $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Proposition 2.2.4. *The ring of integers of a quadratic number field $\mathbb{Q}(\sqrt{d})$ is given by $\mathcal{O}_d=\mathbb{Z}\oplus\mathbb{Z}\omega_d=\{a+b\omega_d \mid a,b\in\mathbb{Z}\}$, where*

$$\omega_d=\begin{cases}\sqrt{d}, & \textit{falls } d\equiv 2,3(4),\\ \frac{1}{2}(1+\sqrt{d}), & \textit{falls } d\equiv 1(4).\end{cases}$$

Proof. We have $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})=\{\mathrm{id},\sigma\}$, where $\sigma(\sqrt{d})=-\sqrt{d}$. Let $\alpha=a+b\sqrt{d}\in\mathcal{O}_d$ with $a,b\in\mathbb{Q}$. Then $P(\alpha)=0$ for a polynomial

$$P(x)=x^n+a_1x^{n-1}+\cdots+a_n,$$

with integral coefficients. Now consider the polynomial

$$\begin{aligned} Q(x) &= (x-\alpha)(x-\sigma(\alpha)) \\ &= x^2 - (\alpha+\sigma(\alpha))x + \alpha\sigma(\alpha) \\ &= x^2 - (a+b\sqrt{d}+a-b\sqrt{d})x + (a+b\sqrt{d})(a-b\sqrt{d}) \\ &= x^2 - 2ax + (a^2-b^2d) \end{aligned}$$

because of $Q(\alpha)=0$ we have $Q(x) \mid P(x)$. The Gauss Lemma implies that $Q(x)$ has integer coefficients. In particular we have $2a \in \mathbb{Z}$ and $a^2-b^2d \in \mathbb{Z}$. This implies $4a^2 \in \mathbb{Z}$ and hence $4b^2d \in \mathbb{Z}$. So we have $2b \in \mathbb{Z}$ since d is squarefree. Together we have then either $a,b \in \mathbb{Z}$, or $a,b \in \frac{1}{2}+\mathbb{Z}$. Writing $a=\frac{u}{2}$ and $b=\frac{v}{2}$ with $u,v \in \mathbb{Z}$, we see that $a^2-b^2d \in \mathbb{Z}$ is equivalent to $\frac{u^2-v^2d}{4} \in \mathbb{Z}$, i.e., to $u^2-v^2d \equiv 0(4)$. For $d \equiv 2,3(4)$ this implies $u^2 \equiv v^2 \equiv 0(4)$, so that u and v are even and $a,b \in \mathbb{Z}$. For $d \equiv 1(4)$ we have in addition that $u^2 \equiv v^2 \equiv 1(4)$ is possible, i.e., that also $a,b \in \frac{1}{2}+\mathbb{Z}$. □

Example 2.2.5. *The ring of integers of* $\mathbb{Q}(\sqrt{-5})$ *is given by* $\mathbb{Z}[\sqrt{-5}]$. *Hence* $\mathbb{Z}[\sqrt{-5}]$ *is integrally closed by Proposition* 2.2.2.

Note that the ring of integers of $\mathbb{Q}(\sqrt{-3})$ is *not* $\mathbb{Z}[\sqrt{-3}]$, but rather

$$\mathbb{Z} \oplus \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right).$$

This holds in an analogous way for every $d \equiv 1(4)$. In this case $\mathbb{Z}[\sqrt{d}]$ is never integrally closed, because the element $\frac{1+\sqrt{d}}{2}$ is integral over $\mathbb{Z}[\sqrt{d}]$ (consider the monic polynomial $x^2-x+\frac{1-d}{4}$), however this element is not contained in $\mathbb{Z}[\sqrt{d}]$.

Remark 2.2.6. As we have already seen, it is an interesting question about rings of integers $\mathcal{O}_d$ of quadratic number fields, which ones are factorial rings and which ones are not. We will see that rings of integers are Dedekind rings, which are factorial if and only if they are PIDs. Here a classification of all rings of integers $\mathcal{O}_d$, which are PIDs, is known for $d<0$, i.e., for the imaginary-quadratic case. The Theorem by Baker-Heegner-Stark [**11**] states that $\mathcal{O}_d$ for $d<0$ squarefree is a PID or is factorial if and only if

$$d = -1,-2,-3,-7,-11,-19,-43,-67,-163.$$

For $d>0$ we do not have such a classification. It seems that quite a lot of such rings are factorial. For example, the first numbers d here are

$$d = 1,2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41,43,46,47,\cdots$$

There is a famous conjecture by Gauß saying that $\mathcal{O}_d$ is factorial for *infinitely many* positive squarefree numbers d.

Remark 2.2.7. Let K be a function field. The integral closure of $\mathbb{F}_p[t]$ in K is called the ring of integers of K. For example, the ring of integers of $K=\mathbb{F}_p(t)$ is $\mathbb{F}_p[t]$. So the role of $\mathbb{Z}$ in the number field case here is played by $\mathbb{F}_p[t]$. Both rings are PIDs, this is the crucial point. Therefore we now have the definition of a ring of integers for global fields.

Proposition 2.2.8. *Let A be a domain with quotient field K, and $L \supset K$ be a field extension. If $\alpha \in L$ is algebraic over K, then there exists an element $d \in A$, such that $d\alpha$ is integral over A.*

Proof. By assumption α satisfies a polynomial equation

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

with $a_i \in K$. Let d be the common denominator of the a_i, i.e., with $da_i \in A$ for all i. After multiplication by d^m we obtain

$$d^m\alpha^m + a_1 d^m \alpha^{m-1} + \cdots + d^m a_m = 0,$$

or

$$(d\alpha)^m + a_1 d(d\alpha)^{m-1} + \cdots + a_m d^m = 0.$$

The coefficients $1, a_1 d, \ldots, a_m d^m$ all lie in A, so that $d\alpha$ is integral over A. □

Corollary 2.2.9. *Let A, K and L be as before and let B be the integral closure of A in L. If the field extension $L \supset K$ is algebraic, then L is the quotient field of B.*

Proof. Let $\alpha \in L$. By Proposition 2.2.8 we can write $\alpha = \beta/d$ with $\beta \in B$ and $d \in A$. □

Corollary 2.2.10. *The quotient field of a ring of integers $\mathcal{O}_K$ is K.*

Proposition 2.2.11. *Let $A \subset B$ be an integral ring extension and B be a domain. Then A is a field if and only if B is a field.*

Proof. Suppose that B is a field. Let $a \in A$ be nonzero. We have $a^{-1} \in B$. Since a^{-1} is integral over A, there is an equation of the form

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0$$

with $c_i \in A$. After multiplication by a^{n-1} we obtain

$$a^{-1} = -(c_{n-1} + \cdots + c_1 a^{n-2} + c_0 a^{n-1}) \in A.$$

Hence A is a field.

Assume that A is a field and let $b \in B^\times$. Since b is integral over A, we know by Proposition 2.1.10 that $A[b]$ is a finitely generated A-module, i.e., a finite dimensional A-vector space. Let $f \in \operatorname{End}(A)$ be given by the left multiplication with b, i.e., by $f(z) = bz$ for $z \in A[b]$. Now $A[b]$ is an integral domain being a subring of B. Thus f is injective: $bz = 0$ and $b \neq 0$ imply that $z = 0$. Since $A[b]$ is finite dimensional, f is surjective. Hence for our $b \neq 0$ there is a $c \in A[b] \subseteq B$ with $bc = 1$. Hence B is a field. □

2.3. Krull dimension

Definition 2.3.1. Let A be a ring (commutative, nontrivial with unit). A chain of $n+1$ different prime ideals

$$P_0 \subset P_1 \subset \ldots \subset P_n$$

has the *length* n. The *Krull dimension* $\dim(A)$ of A is the maximal length of a chain of prime ideals.

In case that there is no such chain of finite length we set $\dim(A) = \infty$. This may indeed happen, even for Noetherian rings. By definition a prime ideal P is a chain of prime ideals of length zero. A field K has only one prime ideal, namely $P = 0$. Thus K has Krull dimension zero, i.e., $\dim(K) = 0$.

Example 2.3.2. *The ring $\mathbb{Z}$ has Krull dimension* 1.

Indeed, there is no chain of prime ideals $P_0 = 0 \subset P_1 \subset P_2$ of length 2 in $\mathbb{Z}$, because P_1 and P_2 are maximal ideals and hence equal. On the other hand $0\mathbb{Z} \subset p\mathbb{Z}$ is a chain of length 1 for every prime number p. Hence we have $\dim(\mathbb{Z}) = 1$. In general we have the following result.

Proposition 2.3.3. *Let A be a PID. Then $\dim(A) = 1$ if and only if A is not a field.*

Proof. Let A be a field. For a prime ideal P in A the maximal chain length is exactly 1 if and only if $P = (p)$ for an irreducible element p of A. □

We already proved the following result in the lecture of commutative algebra [**1**].

Proposition 2.3.4. *Let $A \subset B$ be an integral ring extension. Then we have*

$$\dim(A) = \dim(B).$$

For example, for the ring extension $\mathbb{Z} \subset \mathbb{Q}$ we have

$$\dim(\mathbb{Z}) = 1 \neq \dim(\mathbb{Q}) = 0.$$

Hence this extension is not integral. Of course we know this already, because $\mathbb{Z}$ is integrally closed, or because of Proposition 2.2.11 since $\mathbb{Z}$ is not a field. In general, rings of integers have Krull dimension 1.

Corollary 2.3.5. *Let K be a global field with ring of integers $\mathcal{O}_K$. Then we have $\dim(\mathcal{O}_K) = 1$.*

Proof. For number fields K we have $\dim(\mathcal{O}_K) = \dim(\mathbb{Z}) = 1$ by the above corollary. Similarly, for function fields K we have $\dim(\mathcal{O}_K) = \dim(\mathbb{F}_p[t]) = 1$, since $\mathbb{F}_p[t]$ is a PID, too. □

Let us mention the following result. For a proof see for example [**4**].

Proposition 2.3.6. *The Krull dimension of a polynomial ring $K[x_1, \ldots, x_n]$ in n variables over a field K equals n.*

More generally, $\dim(A[x_1, \ldots, x_n]) = \dim(A) + n$ for Noetherian rings A. For example, we have $\dim(\mathbb{Z}[x]) = 2$.

2.4. Norm and trace

For studying rings of integers $\mathcal{O}_K$ we will introduce the trace and the norm of fields extensions, together with discriminants. Our aim is to show that rings of integers are finitely generated as $\mathbb{Z}$-modules, and conclude then that they are Noetherian rings. Recall that a ring A is called *Noetherian*, if every ideal is finitely generated. For more details see our lectures notes on commutative algebra [**1**].

Let $L \supset K$ be an algebraic field extension and $\alpha \in L$. Denote by $m(\alpha)$ the minimal polynomial of α, which is the monic polynomial of smallest degree with coefficients in K having α as a root. The left multiplication with α defines a K-linear map

$$\ell_\alpha \colon K(\alpha) \to K(\alpha),\ x \mapsto \alpha x.$$

We have the following lemma.

Lemma 2.4.1. *Let $L \supset K$ be an algebraic field extension and $\alpha \in L$. Then the minimal polynomial $m(\alpha)$ is exactly the characteristic polynomial $p_\alpha(x) = \det(x \operatorname{id} - \ell_\alpha)$ of the left multiplication ℓ_α on $K(\alpha)$.*

PROOF. We have $\deg(p_\alpha) = [K(\alpha) : K] = \deg(m(\alpha))$, and p_α is monic. By Cayley-Hamilton we have $p_\alpha(\ell_\alpha) = 0$ as map $K(\alpha) \to K(\alpha)$. The evaluation in 1 yields $p_\alpha(\alpha) = p_\alpha(\ell_\alpha(1)) = 0$. Hence p_α satisfies all properties of the minimal polynomial $m(\alpha)$. □

Let $\ell_\alpha \colon L \to L$ now be the left multiplication with α extended to L, and

$$P_\alpha(x) = \det(x \operatorname{id} - \ell_\alpha)$$

be the characteristic polynomial of α.

DEFINITION 2.4.2. Let $L \supset K$ be a finite field extension and $\alpha \in L$. The *norm* of α is defined by $N_{L/K}(\alpha) = \det(\ell_\alpha)$. The *trace* of α is defined by $\operatorname{tr}_{L/K}(\alpha) = \operatorname{tr}(\ell_\alpha)$.

We can also write the characteristic polynomial as

$$P_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

with $n = [L : K]$, $a_{n-1} = -\operatorname{tr}_{L/K}(\alpha)$ and $a_0 = (-1)^n N_{L/K}(\alpha)$. Furthermore we have

$$\begin{aligned} N_{L/K}(\alpha\beta) &= N_{L/K}(\alpha) N_{L/K}(\beta), \\ \operatorname{tr}_{L/K}(\alpha + \beta) &= \operatorname{tr}_{L/K}(\alpha) + \operatorname{tr}_{L/K}(\beta) \end{aligned}$$

for all $\alpha, \beta \in L$, so that $N \colon L^\times \to K^\times$ and $\operatorname{tr} \colon L \to K$ are homomorphisms. If $\beta \in L$ lies even in K, we have

$$\operatorname{tr}_{L/K}(\beta) = n\beta, \quad N_{L/K}(\beta) = \beta^n.$$

EXAMPLE 2.4.3. *Let $L = \mathbb{Q}(\sqrt{d})$, $K = \mathbb{Q}$ and $\alpha = a + b\sqrt{d}$ be in L. Then $\{1, \sqrt{d}\}$ is a basis for L/K, and the left multiplication with respect to this basis has the matrix*

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

Hence we have $\operatorname{tr}_{L/K}(\alpha) = 2a$ and $N_{L/K}(\alpha) = a^2 - b^2 d$.

Compare this with the computation in the proof of Proposition 2.2.4. Recall that $P_\alpha(x) = \det(x \cdot \operatorname{id} - \ell_\alpha)$ for the left multiplication by α on L.

PROPOSITION 2.4.4. *Let $L \supset K$ be a finite and separable field extension, $\alpha \in L$ and $r = [L : K(\alpha)]$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of P_α in an algebraic closure $\overline{K}$ of K, and let $\sigma_i \colon L \to \overline{K}$ be the embeddings with $\sigma_i|_K = \operatorname{id}$ for $i = 1, \ldots, n$. Then we have*

$$\begin{aligned} P_\alpha(x) &= m(\alpha)(x)^r = \prod_{i=1}^n (x - \alpha_i) = \prod_{i=1}^n (x - \sigma_i(\alpha)), \\ \operatorname{tr}_{L/K}(\alpha) &= \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \sigma_i(\alpha), \\ N_{L/K}(\alpha) &= \prod_{i=1}^n \alpha_i = \prod_{i=1}^n \sigma_i(\alpha). \end{aligned}$$

PROOF. By Lemma 2.4.1 we have $p_\alpha(x) = m(\alpha)(x)$. Also $\deg(p_\alpha) = d = [K(\alpha) : K]$ and $rd = [L : K(\alpha)][K(\alpha) : K] = [L : K] = n$. We claim that we have for the characteristic polynomials P_α and p_α of the left multiplication on L, respectively on $K(\alpha)$, that

$$P_\alpha(x) = p_\alpha(x)^r.$$

This implies of course $P_\alpha(x) = m(\alpha)(x)^r$. To prove the claim, let $\{y_1, \dots, y_r\}$ be a basis of $L/K(\alpha)$ and $\{z_1, \dots, z_d\}$ be a basis of $K(\alpha)/K$. Then

$$\{y_i z_j \mid i = 1, \dots, r,\ j = 1, \dots, d\}$$

is a basis of L/K. With respect to this basis the matrix of ℓ_α on L has block diagonal form with r block matrices A, where A is just the matrix of ℓ_α on $K(\alpha)$ with respect to the basis $z_1, \dots, z_d$. Taking the characteristic polynomial of this block diagonal matrix yields the claim. If $\alpha_1, \dots, \alpha_d$ are the distinct roots of $m(\alpha)$, then $m(\alpha)(x) = \prod_{i=1}^d (x - \sigma_i(\alpha))$, and thus

$$P_\alpha(x) = m(\alpha)(x)^r = \prod_{i=1}^d (x - \sigma_i(\alpha))^r = \prod_{i=1}^n (x - \sigma_i(\alpha)).$$

Furthermore we have

$$\{\alpha_1, \dots, \alpha_n\} = \{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}$$

as sets with multiplicities, because each of the d embeddings $K(\alpha) \to \overline{K}$ can be extended in exactly r ways to L. □

Example 2.4.5. *Let $L = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}$. Then L/K is a Galois extension with Galois group $\{\mathrm{id}, \sigma\}$, where $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. For $\alpha = a + b\sqrt{d} \in L$ we have*

$$\begin{aligned}
\mathrm{tr}_{L/K}(\alpha) &= \mathrm{id}(\alpha) + \sigma(\alpha) = a + b\sqrt{d} + a - b\sqrt{d} \\
&= 2a, \\
N_{L/K}(\alpha) &= \mathrm{id}(\alpha)\sigma(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) \\
&= a^2 - b^2 d, \\
P_\alpha(x) &= (x - \alpha)(x - \sigma(\alpha)) = x^2 - 2ax + (a^2 - b^2 d) \\
&= x^2 - \mathrm{tr}(\alpha)x + N(\alpha).
\end{aligned}$$

Corollary 2.4.6. *Let $L \supset K$ be a separable extension of global fields and $\alpha \in \mathcal{O}_L$. Then we have $P_\alpha \in \mathcal{O}_K[x]$. In particular, the trace $\mathrm{tr}_{L/K}(\alpha)$ and the norm $N_{L/K}(\alpha)$ are in $\mathcal{O}_K$.*

Proof. Since α is integral over $\mathcal{O}_K$, it satisfies an equation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with coefficients in $\mathcal{O}_K$. But then all $\sigma_i(\alpha)$ satisfy this equation, because the action of the Galois group of the splitting field, which permutes the $\sigma_i(\alpha)$, is a homomorphism and hence leaves the coefficients of the above equation invariant. Hence all $\sigma_i(\alpha)$ are integral over $\mathcal{O}_K$. Because of $P_\alpha(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$ then all coefficients of P_α are integral over $\mathcal{O}_K$ and lie in K. Since $\mathcal{O}_K$ is integrally closed, all coefficients lie in $\mathcal{O}_K$. □

In particular, for $L = \mathbb{Q}(\sqrt{d})$, $K = \mathbb{Q}$ and $\alpha = a + b\sqrt{d} \in L$ we have

$$P_\alpha(x) = x^2 - 2ax + (a^2 - b^2 d) \in \mathbb{Z}[x].$$

Now we will introduce the *discriminant* of a field extension L/K, and even more generally for a ring extension B/A, where B is a free A-module of rank n, with basis $\{x_1, \dots, x_n\}$. This could be, for example, some ring extension $\mathcal{O}_K/\mathbb{Z}$. Even in the general case B/A the left multiplication with a $\beta \in B$ defines an A-linear map on L, and the trace $\mathrm{tr}_{B/A}(\beta)$ and the norm $N_{B/A}(\beta)$ are well defined.

Definition 2.4.7. Let $B \supset A$ be a ring extension and B be a free A-module with basis $\{x_1, \dots, x_n\}$. Let $(\mathrm{tr}_{B/A}(x_i x_j))_{i,j}$ be the fundamental matrix of the symmetric bilinear form $B \times B \to A$, $(x, y) \mapsto \mathrm{tr}_{B/A}(xy)$ with respect to this basis. Then

$$D(x_1, \dots, x_n) = \det((\mathrm{tr}_{B/A}(x_i x_j))_{i,j}) \in A$$

is called the *discriminant* of the basis $\{x_1, \dots, x_n\}$.

For example 2.4.3 with $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ we have

$$D(1, \sqrt{d}) = \det \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\sqrt{d}) \\ \mathrm{tr}(\sqrt{d}) & \mathrm{tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d,$$

since $\mathrm{tr}(a + b\sqrt{d}) = 2a$.

We would like to have a definition of a discriminant, which is independent of the basis. Let us compute, how $D(x_1, \dots, x_n)$ and $D(y_1, \dots, y_n)$ differ from each other for two different bases of the free A-module B.

Lemma 2.4.8. *If $y_j = \sum_{i=1}^n a_{ji} x_i$ with $a_{ij} \in A$ and $M = (a_{ij})_{i,j}$, then we have*

$$D(y_1, \dots, y_n) = \det(M)^2 D(x_1, \dots, x_n).$$

Proof. Let $\psi \colon B \times B \to A$ be a symmetric bilinear form. Then we have

$$\psi(y_k, y_l) = \sum_{i,j} \psi(a_{ki} x_i, a_{lj} x_j) = \sum_{i,j} a_{ki} \psi(x_i, x_j) a_{lj},$$

and hence the matrix equation

$$(\psi(y_k, y_l))_{k,l} = M \cdot (\psi(x_i, x_j)) \cdot M^t$$

Taking the determinant on both sides and using $\det(MM^t) = \det(M)^2$ we obtain the claim with $\psi(x, y) = \mathrm{tr}_{B/A}(xy)$. □

Note that $\det(M)$ for bases x_i and $y_j$of B over A is a unit. So discriminants of each two bases just differ by the square of a unit in A. Hence the *ideal* in A generated by the discriminant, is independent of the basis. For $A = \mathbb{Z}$ only 1 is a square of a unit. Hence there all discriminants are equal and independent of the basis.

Definition 2.4.9. The discriminant $\mathcal{D}_{B/A}$ of a ring extension B/A with a free A-module B is the ideal in A generated by the discriminant of a basis of B.

Sometimes also the element $D(x_1, \dots, x_n)$ in $A/(A^\times)^2$ is just called the discriminant of B/A.

Lemma 2.4.10. *Let L/K be a finite, separable field extension of degree n and $\sigma_1, \dots, \sigma_n$ be the different K-embeddings $L \hookrightarrow \overline{K}$, and $\{x_1, \dots, x_n\}$ be a basis of L/K. Then*

$$D(x_1, \dots, x_n) = \det((\sigma_i(x_j))_{i,j})^2 \neq 0.$$

In particular we have $\mathcal{D}_{L/K} \neq 0$.

Proof. By Proposition 2.4.4 we have

$$\mathrm{tr}_{L/K}(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j),$$

so that

$$\begin{aligned} D(x_1,\dots,x_n) &= \det((\mathrm{tr}_{L/K}(x_ix_j))_{i,j}) \\ &= \det\left(\left(\sum_{k=1}^{n}\sigma_k(x_i)\sigma_k(x_j)\right)_{i,j}\right) \\ &= \det((\sigma_k(x_i))_{k,i})\cdot\det((\sigma_k(x_j))_{k,j}) \\ &= \det((\sigma_k(x_j))_{k,j})^2. \end{aligned}$$

Suppose that this determinant vanishes. Then there are $c_1,\dots,c_n\in\overline{K}$, not all zero, with

$$\sum_{i=1}^{n} c_i\sigma_i(x_j)=0$$

for all j. Since the x_j are a basis, we have $\sum_{i=1}^{n} c_i\sigma_i=0$ as maps from $L^\times\to\overline{K}$. As group homomorphisms $L^\times\to(\overline{K})^\times$ the maps σ_i are linearly independent by Dedekind's result on the linear independence of characters. This is a contradiction. □

Corollary 2.4.11. *Let K be the quotient field of A and L be a finite, separable field extension of K of degree n, so that B, the integral closure of A in L, is a free A-module of rank n. Then we have $\mathcal{D}_{B/A}\neq 0$.*

Proof. Each basis of B/A is also a basis of L/K by Proposition 2.2.8. Hence $\mathcal{D}_{B/A}$ is represented by $\mathcal{D}_{L/K}$ and therefore nonzero by Lemma 2.4.10. □

Remark 2.4.12. The assumption of separability in Proposition 2.4.10 is essential. The trace pairing $L\times L\to K$, $(x,y)\mapsto \mathrm{tr}_{L/K}(xy)$ is non-degenerate if and only if L/K is separable. Indeed we have $\mathcal{D}_{L/K}=0$, if L/K is not separable.

Now we are able to show that rings of integers $\mathcal{O}_K$ are finitely-generated $\mathbb{Z}$-modules.

Proposition 2.4.13. *Let A be an integrally closed domain with quotient field K and L/K be a separable field extension of degree n. Let B denote the integral closure of A in L. Then, if A is Noetherian, B is a finitely generated, Noetherian A-module. If A is a PID, then B is a free A-module of rank n.*

Proof. We will show that there exist finitely generated, free A-modules N and M of rank n such that $N\subset B\subset M$. This implies the statements claimed. Indeed, if A is Noetherian then every finitely generated A-module is again Noetherian by Proposition 3.4.9 in [**1**]. Hence every A-submodule of M is finitely generated. In particular $B\subset M$ is finitely generated. If $I\subset B$ is an ideal of B, then I is an A-module, hence finitely generated, as we just saw, But then I is also finitely generated as B-module, i.e., as ideal. Hence every ideal of B is finitely generated and B is a Noetherian ring. If A is a PID, then B is free of rank $r\le n$, since B is contained in a free A-module M of rank n This follows from the structure theorem for finitely generated modules over a PID, because every A-submodule B of a free A-module is again free and has at most the same rank. In the same way we obtain $r\ge n$, since B contains a free A-module N of rank n. Hence $r=n$.

It remains to show the claim given at the beginning. Let $\{x_1,\dots,x_n\}$ be a basis of L/K. by Proposition 2.2.8 there exists a $d\in A$ with $dx_i\in B$ for all i. Then $\{dx_1,\dots,dx_n\}$ is still a basis of L/K. So we may assume from the beginning that all x_i are in B. Since the trace pairing is non-degenerate, there exists a dual basis $\{x_1', \dots, x_n'\}$ of L/K with $\mathrm{tr}_{L/K}(x_i x_j') = \delta_{ij}$. Define

$$N := Ax_1 + \cdots + Ax_n, \quad M := Ax_1' + \cdots + Ax_n'.$$

Of course we have $N \subset B$. We'll show that $B \subset M$. So let $x \in B$. There exists a unique representation $x = \sum_{j=1}^n b_j x_j'$ with $b_j \in K$. Since x and all x_i are in B, we have $xx_i \in B$, and hence $b_i = \mathrm{tr}_{L/K}(xx_i) \in A$, i.e., $x \in M$. Indeed, we have

$$\begin{aligned} \mathrm{tr}_{L/K}(xx_i) &= \mathrm{tr}\left(\sum_{j=1}^n b_j x_j' x_i\right) \\ &= \sum_{j=1}^n b_j \cdot \mathrm{tr}_{L/K}(x_j' x_i) = \sum_{j=1}^n b_j \delta_{ij} \\ &= b_i. \end{aligned}$$

□

Corollary 2.4.14. *Rings of integers of number fields are integrally closed, Noetherian rings of Krull dimension* 1.

Proof. Let L be a number field. Chose $A = \mathbb{Z}$ and $B = \mathcal{O}_L$ in the proposition. Then $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. Moreover $\mathcal{O}_L$ is a Noetherian ring by the proposition, since $\mathbb{Z}$ is Noetherian. By Proposition 2.2.2 rings of integers are integrally closed. By Corollary 2.2.2 they have Krull dimension 1. □

Corollary 2.4.15. *Rings of integers $\mathcal{O}_L$ are free $\mathbb{Z}$-modules of finite rank $n = [L : \mathbb{Q}]$.*

Proof. Let L be a number field of degree n over $\mathbb{Q}$. Then $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of rank n by the proposition, because $\mathbb{Z}$ is a PID. □

Remark 2.4.16. Let L/K be an extension of number fields. Then $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. However, $\mathcal{O}_L$ need not be a *free* $\mathcal{O}_K$-module, in case that $\mathcal{O}_K$ is not a PID. For this consider the following example. Let $K = \mathbb{Q}(\sqrt{-14})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ is *not* a PID. For the number field extension L/K with $L = \mathbb{Q}(\sqrt{-14}, \sqrt{-7})$ one can show, that $\mathcal{O}_L$ is not free as a $\mathcal{O}_K$-module.

Remark 2.4.17. The results for $\mathcal{O}_K$ are also true for global fields in general. For the proof one needs to take care of the inseparable case in addition, which can happen for function fields. If L/K is a finite extension of global fields, then $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module.

Definition 2.4.18. Let K be a number field of degree n. A basis $\omega_1, \dots, \omega_n$ of the free $\mathbb{Z}$-module $\mathcal{O}_K$ is called *integral basis* of $\mathcal{O}_K$ over $\mathbb{Z}$, or over K. The *discriminant of* K, denoted by $d = d_K$, is defined by $D(\omega_1, \dots, \omega_n)$.

The discriminant of K is indeed the discriminant of an integral basis of $\mathcal{O}_K/\mathbb{Z}$ in the sense of definition 2.4.7.

Example 2.4.19. *An integral basis of the quadratic number field $\mathbb{Q}(\sqrt{d})$ with $d \equiv 2, 3 \bmod 4$ is given by $\{1, \sqrt{d}\}$, i.e., we have $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Then*

$$D(1, \sqrt{d}) = 4d,$$

as we have seen in the example after definition 2.4.7. *For* $d \equiv 1 \mod 4$ *an integral basis is given by* $\{1, \frac{1+\sqrt{d}}{2}\}$, *i.e., we have* $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\, \frac{1+\sqrt{d}}{2}$. *Then we have*

$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = \det \begin{pmatrix} \operatorname{tr}(1) & \operatorname{tr}(\frac{1+\sqrt{d}}{2}) \\ \operatorname{tr}(\frac{1+\sqrt{d}}{2}) & \operatorname{tr}(\frac{1+2\sqrt{d}+d}{4}) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} = d.$$

So altogether we have

$$\mathcal{D}_{\mathcal{O}_d/\mathbb{Z}} = \begin{cases} 4d & \text{for } d \equiv 2,3 \mod 4, \\ d & \text{for } d \equiv 1 \mod 4. \end{cases}$$

In particular, the ring of integers of a quadratic number field is *uniquely determined* by its discriminant. This is no longer true in general. There are already counter examples for cubic number fields.

Example 2.4.20. *The cubic numbers fields* $K = \mathbb{Q}(\sqrt[3]{6})$ *and* $K = \mathbb{Q}(\sqrt[3]{12})$ *both have discriminant* $\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}} = -2^2 3^5 = -972$, *but they are not isomorphic.*

Let $\alpha = \sqrt[3]{6}$. The minimal polynomial $m(\alpha)(x) = x^3 - 6$ is of degree three and $\{1, \alpha, \alpha^2\}$ is a basis for $K = \mathbb{Q}(\sqrt[3]{6})$ over $\mathbb{Q}$. Since α is integral over $\mathbb{Z}$ we have $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. With a bit of work one can show equality, and that $\{1, \alpha, \alpha^2\}$ is an integral basis of K with discriminant

$$D(1, \alpha, \alpha^2) = \det \begin{pmatrix} \operatorname{tr}(1) & \operatorname{tr}(\alpha) & \operatorname{tr}(\alpha^2) \\ \operatorname{tr}(\alpha) & \operatorname{tr}(\alpha^2) & \operatorname{tr}(\alpha^3) \\ \operatorname{tr}(\alpha^2) & \operatorname{tr}(\alpha^3) & \operatorname{tr}(\alpha^4) \end{pmatrix}$$

$$= \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 18 \\ 0 & 18 & 0 \end{pmatrix} = -3 \cdot 18^2 = -972.$$

Here we have used that $\operatorname{tr}(\alpha) = \operatorname{tr}(\alpha^2) = 0$ and $\operatorname{tr}(a) = 3a$ for $a \in \mathbb{Q}$. For $K = \mathbb{Q}(\sqrt[3]{12})$ one can show that $\{1, \sqrt[3]{12}, \frac{1}{2}(\sqrt[3]{12})^2\}$ is an integral basis of K, see Theorem 6.4.13 in Cohen's book [**3**]. It is easy to see that

$$D\left(1, \sqrt[3]{12}, \frac{1}{2}(\sqrt[3]{12})^2\right) = -972.$$

The computation of integral bases for cubic number fields of the form $\mathbb{Q}(\sqrt[3]{d})$ goes back to Dedekind.

Remark 2.4.21. By the primitive element theorem each number field K of degree n is of the form $K = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathcal{O}_K$. Therefore $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $K/\mathbb{Q}$. Unfortunately this basis is not a basis for the ring of integers $\mathcal{O}_K$ over $\mathbb{Z}$ in general. In general we have

$$\mathcal{O}_K \neq \mathbb{Z}[\alpha] = \mathbb{Z}1 \oplus \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}.$$

We have already seen this for $\mathbb{Q}(\sqrt{5})$, where $\{1, \sqrt{5}\}$ is not an integral basis. The element $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$, but not contained in $\mathbb{Z} \oplus \mathbb{Z}\sqrt{5}$. On the other hand, there exists another element $\beta \in K$ with $\mathcal{O}_K = \mathbb{Z}[\beta]$, for example $\beta = \frac{1+\sqrt{5}}{2}$.

A number field K is called *monogeneous*, if its ring of integers admits a power integral basis, i.e., if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Quadratic number fields $\mathbb{Q}(\sqrt{d})$ and cyclotomic fields $\mathbb{Q}(\zeta)$ are indeed monogeneous. However, there exist already cubic number fields, which are not monogeneous. For example, let $p \equiv 1 \mod 9$ be a prime, which can be represented by $7x^2 + 3xy + 9y^2$ with $x, y \in \mathbb{Z}$. Then $\mathbb{Q}(\sqrt[3]{p})$ is *not* monogeneous. For $x = y = 1$ we obtain the example $K = \mathbb{Q}(\sqrt[3]{19})$. On the other hand, the two cubic number fields from Example 2.4.20 are both monogeneous. The criterion is as follows.

Let $K = \mathbb{Q}(\sqrt[3]{d})$ and $d = ab^2$ be cubicfree with coprime, squarefree integers a and b. If $a^2 \not\equiv b^2 \mod 9$, then K is monogeneous if and only if $ax^3 + by^3 = 1$ has an integer solution. If $a^2 \equiv b^2 \mod 9$, then K is monogeneous if and only if $ax^3 + by^3 = 9$ has an integer solution.

Lemma 2.4.22. *Let L/K be an extension of number fields of degree n and $L = K(\alpha)$ with $\alpha \in L$. Then the discriminant of the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ satisfies*

$$D(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \dots, \alpha_n$ are the conjugates of the α in $\overline{K}$.

Proof. Denote by $\sigma_i \colon K(\alpha) \to \overline{K}$ the K-embeddings. Then the conjugates of α are precisely the $\sigma_i(\alpha)$. Hence by Lemma 2.4.10 we have

$$\begin{aligned} D(1, \alpha, \dots, \alpha^{n-1}) &= \det((\sigma_i(\alpha^{j-1}))_{i,j})^2 \\ &= \det((\alpha_i^{j-1})_{i,j})^2 \\ &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2, \end{aligned}$$

using the Vandermonde determinant. □

Proposition 2.4.23. *Let $K(\alpha)/K$ be an extension of number fields of degree n. Then $D(1, \alpha, \dots, \alpha^{n-1})$ is the discriminant of the minimal polynomial $p = m(\alpha)$ of α over K. Denoting by p' the formal derivative of p we obtain*

$$D(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{K(\alpha)/K}(p'(\alpha)).$$

Proof. We have

$$\begin{aligned} D(1, \alpha, \dots, \alpha^{n-1}) &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{n(n-1)/2} \prod_i \Big(\prod_{j \ne i} (\alpha_i - \alpha_j) \Big) \\ &= (-1)^{n(n-1)/2} \prod_j p'(\alpha_j) \\ &= (-1)^{n(n-1)/2} N_{K(\alpha)/K}(p'(\alpha)). \end{aligned}$$

□

Proposition 2.4.24. *Let A be an integrally closed domain with quotient field K and L/K be a finite, separable extensions, and B be the integral closure of A in L. Let $\{x_1, \dots, x_n\}$ be a basis of L/K lying in B. Then the discriminant $d = D(x_1, \dots, x_n)$ satisfies $dB \subseteq Ax_1 + \dots + Ax_n$.*

Proof. Let $\alpha = \sum_{i=1}^n a_i x_i \in B$ with $a_i \in K$. Then we have

$$\operatorname{tr}_{L/K}(x_i \alpha) = \sum_{j=1}^n \operatorname{tr}_{L/K}(x_i x_j) \cdot a_j$$

for $i = 1, \ldots, n$. This is a system of linear equations for $a_1, \ldots, a_n$, with matrix $M = (\mathrm{tr}_{L/K}(x_i x_j))_{i,j}$. The coefficients lie A. We have $d = \det(M)$ by definition. By Cramer's rule we have $a_j = a'_j/d$ for $a'_j \in A$, hence $d\alpha \in Ax_1 + \ldots Ax_n$. □

CHAPTER 3

Ideals of Dedekind rings

3.1. Fractional ideals

There are several equivalent definitions of a Dedekind ring, see our lecture notes [**1**]. Let us take the following definition.

Definition 3.1.1. A *Dedekind ring* is a Noetherian, integrally closed ring of Krull dimension 1.

By definition an integrally closed ring is a domain. having Krull dimension 1 means that the ring is not a field and that every nonzero prime ideal is maximal. This gives a reformulation of the definition as follows.

Proposition 3.1.2. *A Dedekind ring is a domain, which is not a field, having the following properties. It is Noetherian, integrally closed and every nonzero prime ideal is maximal.*

Example 3.1.3. *Every PID, which is not a field, is a Dedekind ring.*

Indeed, let A be a PID, which is not a field. By Proposition 2.1.15, A is integrally closed. We have $\dim(A) = 1$ by Proposition 2.3.3. Of course every PID is Noetherian. So by definition A is a Dedekind ring. In particular, $\mathbb{Z}$ is a Dedekind ring. Note that not every Dedekind ring is a PID.

Example 3.1.4. *None of the rings $\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[x]$, $\mathbb{C}[x, y]$ is a Dedekind ring.*

All four rings are Noetherian, but $\mathbb{Z} \oplus \mathbb{Z}$ is not even a domain, $\mathbb{Z}[\sqrt{5}]$ is not integrally closed and $\mathbb{Z}[x]$ and $\mathbb{C}[x, y]$ have Krull dimension 2.

On the other hand, $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind ring, since it is the ring of integers of the number field $\mathbb{Q}(\sqrt{-5})$, see Example 2.2.5. We have the following general result.

Proposition 3.1.5. *Every ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind ring.*

Proof. This follows directly from corollary 2.4.14. □

For an example of a Dedekind ring, which is not a ring of integers, see Remark 3.2.11.

Definition 3.1.6. Let A be a domain with quotient field K. A *fractional ideal* of A is an A-submodule $I \subset K$ with a common denominator, i.e., such that there exists a $d \neq 0$ in A with $dI \subseteq A$.

Every usual ideal I of A is also a fractional ideal with $d = 1$. Sometimes it is called an *integral* ideal then.

Lemma 3.1.7. *Every finitely generated A-submodule $I \subset K$ is a fractional ideal. Conversely, if A is Noetherian, then every fractional ideal is a finitely generated A-submodule of K.*

Proof. If I is generated by $x_1, \ldots, x_n$, and d is the common denominator of the x_i, then we have $dI \subseteq A$. Conversely, if $dI \subseteq A$, then dI is a finitely generated ideal, since A is Noetherian. Hence also I is finitely generated. □

Let I and J be two fractional ideals of A. Denote by IJ the ideal generated by all products ab with $a \in I$, $b \in J$, and denote

$$I^{-1} := \{\alpha \in K \mid \alpha I \subseteq A\}.$$

Note that we have $0 \in I^{-1}$. The notation is a bit misleading. It follows that IJ and I^{-1} are again fractional ideals. We have $II^{-1} \subseteq A$, but equality need not hold in general.

Definition 3.1.8. A fractional ideal I of A is called *invertible*, if $II^{-1} = A$.

Again, the notation I^{-1} does not imply that I is invertible.

Example 3.1.9. *Let $A = \mathbb{Z}$. Then $I = \frac{1}{2}\mathbb{Z}$ is a fractional ideal with $I^{-1} = 2\mathbb{Z}$. Hence $II^{-1} = A$ and I is invertible.*

If A is a PID then all fractional ideals are of the form $I = Ab$ with $b \in K$, and $I^{-1} = Ab^{-1}$. The multiplication of fractional ideals then has the special form $Ab \cdot Ac = A(bc)$.

3.2. Unique factorization of ideals

In this section we will show that every proper ideal in a Dedekind ring has a unique factorization into finitely many prime ideals. This requires a few lemmas.

Lemma 3.2.1. *Let A be a Noetherian ring, and let I be a nonzero ideal. Then there exist nonzero prime ideals $P_1, \ldots, P_n$ with $P_1 \cdots P_n \subseteq I$.*

Proof. Let Φ be the set of all nonzero ideals I in A, which do *not* satisfy the statement. Suppose that $\Phi \neq \emptyset$. Since A is Noetherian, Φ has a maximal element M. By assumption the ideal M is not prime. Hence there are $x, y \in A \setminus M$ with $xy \in M$ and we have $M \subsetneq M + (x)$ and $M \subsetneq M + (y)$. It follows that the ideals $M + (x)$ and $M + (y)$ are not in Φ, since M was maximal. Therefore they contain a product of nonzero prime ideals,

$$P_1 \cdots P_n \subseteq M + (x),$$
$$Q_1 \cdots Q_m \subseteq M + (y).$$

However, this implies that $P_1 \cdots P_n \cdot Q_1 \cdots Q_m \subseteq (M + (x))(M + (y)) = M$ because of $xy \in M$. We obtain $M \notin \Phi$, which is a contradiction. Hence Φ is empty and we are done. □

Lemma 3.2.2. *Let A be a Noetherian integral domain of dimension 1 and M be a maximal ideal in A. Then $A \subsetneq M^{-1}$ is a proper inclusion.*

Proof. Because of $1 \in M^{-1}$ we have $A \subseteq M^{-1}$. Let $a \neq 0$ in M. Since every nonzero prime ideal is maximal by assumption, Lemma 3.2.1 implies that there are maximal ideals $P_1, \ldots, P_n$ with $P_1 \cdots P_n \subseteq Aa = (a)$. Choose such ideals with minimal $n \geq 1$. Then $P_1 \cdots P_n \subseteq M$ implies $P_i = M$ for some i, and without loss of generality $P_1 = M$. Since n was minimal, we have $P_2 \cdots P_n \subsetneq (a)$. Hence there exists an element $b \in P_2 \cdots P_n$ with $b \notin (a)$. We have $Mb = P_1 b \subseteq (a)$, hence $Mba^{-1} \subseteq A$. In other words, we have $ba^{-1} \in M^{-1}$. Since $b \notin (a)$ we have $ba^{-1} \notin A$. It follows that ba^{-1} is in M^{-1}, but not in A, so that the inclusion is proper. □

Lemma 3.2.3. *Let A be a Dedekind ring, I be a nonzero ideal in A, and P be a nonzero prime ideal in A. Then $I \subsetneq IP^{-1}$ is a proper inclusion.*

Proof. Since $1 \in P^{-1}$ we have $I \subseteq IP^{-1}$. Assume that $I = IP^{-1}$ and let $\alpha \in P^{-1}$. Then we have $I\alpha \subseteq I$. Now α is integral over A if and only if there is a finitely generated A-submodule $N \neq 0$ with $N\alpha \subseteq N$, e.g., $N = A[\alpha]$, see the proof of Proposition 2.1.10, part (3). Such a submodule is given here by I, so that α is integral over A. Hence we have $\alpha \in A$, since A is integrally closed. This implies $P^{-1} \subseteq A$. By Lemma 3.2.2 we have $A \subsetneq P^{-1}$. This is a contradiction. □

Now we are ready to show the following result.

Proposition 3.2.4. *Let A be a Dedekind ring. Then every maximal ideal is invertible with respect to the multiplication of fractional ideals.*

Proof. Let M be a maximal ideal of A. Then $M \subsetneq MM^{-1} \subseteq A$ by Lemma 3.2.3. Since M is maximal it follows that $MM^{-1} = A$. □

Corollary 3.2.5 (Decomposition into prime ideals). *Let A be a Dedekind ring. Then every nonzero ideal is a finite product of maximal ideals and is invertible.*

Proof. Let Φ be the set of all proper ideals of A, which are not a finite product of maximal ideals. Assume that $\Phi \neq \emptyset$. Then Φ has a maximal element I, and there is a maximal ideal M in A with $I \subseteq M$. By definition we have $M \notin \Phi$. By Lemma 3.2.3 we have $I \subsetneq IM^{-1}$. We also have $IM^{-1} \neq A$, because otherwise $I = M$, contradicting $I \in \Phi$ and $M \notin \Phi$. Since I is a maximal element in Φ, we have $IM^{-1} \notin \Phi$, and we can write $IM^{-1} = P_1 \cdots P_n$ with maximal ideals $P_1, \ldots, P_n$. This implies $I = IM^{-1}M = P_1 \cdots P_n M$, a contradiction to $I \in \Phi$. Hence we have $\Phi = \emptyset$, and we can write every ideal $I \neq 0$ as $I = P_1 \cdots P_n$ with maximal ideals $P_1, \ldots, P_n$. By Proposition 3.2.4 we have

$$IP_1^{-1} \cdots P_n^{-1} = P_1 \cdots P_n \cdot P_1^{-1} \cdots P_n^{-1} = A,$$

so that I is invertible. □

Proposition 3.2.6. *Let A be a Dedekind ring. Then every proper ideal I has, up to permutation, a unique decomposition $I = P_1 \ldots P_n$ into prime ideals.*

Proof. The existence of such a decomposition follows from Corollary 3.2.5. For the uniqueness, assume that we have two prime decompositions for a given proper ideal I,

$$I = P_1 \cdots P_n = Q_1 \cdots Q_m.$$

For all prime ideals P we may conclude from $IJ \subseteq P$ that either $I \subseteq P$ or $J \subseteq P$. Because of $I \subseteq P_1 \cdots P_n \subseteq P_1$ it follows that P_1 contains some Q_j, say, $Q_1 \subseteq P_1$. Since $Q_1 \neq 0$ is a maximal ideal, we have $Q_1 = P_1$. Now we can multiply the two prime decompositions for I by $P^{-1} = Q^{-1}$. We obtain, since $P^{-1}P = Q^{-1}Q = A$, then $I = P_2 \cdots P_n = Q_2 \cdots Q_m$. We can proceed by induction and obtain $n = m$ and $P_i = Q_i \ \forall\, i$. □

Denote by $\operatorname{Spm}(A)$ the set of all maximal ideals of a commutative ring A. This is also called the *maximal spectrum* of A. We denote by $\operatorname{Spec}(A)$ the set of all prime ideals of A, the so called *spectrum* of A. For Dedekind rings we have

$$\operatorname{Spec}(A) = \operatorname{Spm}(A) \cup \{(0)\}.$$

We can generalize Proposition 3.2.6 to fractional ideals of A.

Proposition 3.2.7. *Let A be a Dedekind ring. Then every fractional ideal I in A has a unique product representation*

$$I = \prod_{P \in \operatorname{Spm}(A)} P^{\nu_P(I)}$$

with integers $\nu_P(I)$, which are zero except for finitely many. We have $\nu_P(I) \geq 0$ for all P if and only if I is an integral ideal.

Proof. Every fractional ideal I is the quotient $I = J(J')^{-1}$ of two integral ideals J, J' of A. hence the decomposition for integral ideals implies the decomposition for fractional ideals. A similar argument applies for uniqueness. □

Proposition 3.2.8. *Let A be a Dedekind ring. The set of fractional ideals* $\operatorname{Id}(A)$ *of A forms an abelian group under ideal multiplication.*

Proof. We have $IJ = JI$ for fractional ideals I and J of A, and $(1) = A$ is the neutral element. The associativity is also clear. It remains to show that every fractional ideal I has an inverse. Choose a $d \in K$ with $dI \subseteq A$. Then we have $(dI)^{-1} = d^{-1}I^{-1}$, and the integral ideal dI is invertible. It follows that $A = dI \cdot d^{-1}I^{-1} = II^{-1}$. Hence also I is invertible with inverse I^{-1}. □

Remark 3.2.9. Emmy Noether has also shown the converse statement, namely that an integral domain having the property that its fractional ideals form an abelian group with respect to ideal multiplication is a Dedekind ring.

We denote by $P(A)$ the set of fractional principal ideals of A, i.e., the sets $(a) = Aa \subseteq K$ for an $a \in K^\times$. Then $P(A)$ forms a subgroup of $\operatorname{Id}(A)$.

Definition 3.2.10. The quotient group $Cl(A) := \operatorname{Id}(A)/P(A)$ is called the *Ideal class group* of the ring A. Its order is called the *class number* of A.

Remark 3.2.11. There are Dedekind rings with *infinite* class number, for example the ring

$$\mathbb{C}[x,y]/(y^2 - x^3 - x - 1).$$

The ideal class group of this ring is isomorphic to $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$. It is known that *every* abelian group can be realized as the class group of some Dedekind ring, see [**2**]. For rings of integers $A = \mathcal{O}_K$ of number fields, however, the class number is always *finite*. This will be an important result of our lecture, proved in chapter 4.

For a number field K and its ring of integers $\mathcal{O}_K$ the notation $Cl(K)$ is often used for the ideal class group $Cl(\mathcal{O}_K)$ of K. The class number of K is denoted by

$$h_K = \#Cl(\mathcal{O}_K).$$

Both are important invariants of a number field K.

It is still an open question, whether or not every finite abelian group can arise as ideal class group of a number field. For imaginary quadratic fields it is known, that not every every finite abelian group can arise. The smallest example is the group $(\mathbb{Z}/3\mathbb{Z})^3$ of order 27. Note however, that this group can be realized as the ideal class group of a real quadratic number field, namely

$$CL(K) \cong (\mathbb{Z}/3\mathbb{Z})^3 \text{ for } K = \mathbb{Q}(\sqrt{188184253}).$$

Proposition 3.2.12. *Let A be a Dedekind ring. Then A is factorial if and only if it is a PID, i.e., if and only if its class number is* 1.

Proof. Every PID is factorial. The converse is not true in general, but it is true for Dedekind rings. Let A be factorial, and P be a nonzero prime ideal of A with $a \in P$. Then P contains an irreducible factor $t \mid a$, so that $(t) \subseteq P$. Since A has dimension 1 we have $P = (t)$. Hence every prime ideal is principal. By Proposition 3.2.6 we have for every ideal $I \neq 0$ that $I = P_1 \cdots P_n = (t_1) \cdots (t_n) = (t_1 \cdots t_n)$. Therefore A is a PID. By definition this is equivalent to the fact that the ideal class group of A is trivial. □

Example 3.2.13. *The class number of $\mathbb{Z}[\sqrt{-5}]$ is different from 1. In fact, it is 2.*

We already know from Example 2.1.17 that the ring of integers $\mathbb{Z}[\sqrt{-5}]$ of the number field $\mathbb{Q}(\sqrt{-5})$ is not factorial. Hence the class number cannot be 1. Independently we can also show that, say, the ideal $P = (2, 1+\sqrt{-5})$ is not principal. For this we consider the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Assume that $P = (\alpha)$ for some element α. Then there are $\beta, \gamma \in \mathbb{Z}[\sqrt{-5}]$ with $\beta\alpha = 2$ and $\gamma\alpha = 1 + \sqrt{-5}$. We obtain $N(\beta)N(\alpha) = N(2) = 4$ and $N(\gamma)N(\alpha) = N(1+\sqrt{-5}) = 6$. Hence $N(\alpha)$ is a nontrivial divisor of 4 and 6, i.e., $N(\alpha) = 2$. Writing $\alpha = x + y\sqrt{-5}$ for some $x, y \in \mathbb{Z}$ we obtain $x^2 + 5y^2 = 2$. However, this has no solution in $\mathbb{Z}$, a contradiction.

We will see later that in fact $h_{\mathbb{Q}(\sqrt{-5})} = 2$. We want to demonstrate with the example of $\mathbb{Z}[\sqrt{-5}]$, how we can recover the uniqueness of a prime decomposition, which is lost for irreducible elements, for prime ideals.

Example 3.2.14. *The two factorizations into irreducible elements*

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

in the ring of integers $\mathbb{Z}[\sqrt{-5}]$ are essentially different. The corresponding prime ideal decompositions of the principal ideal (21) , however, coincide up to permutation.

Indeed, as in Example 2.1.17 we can show that all elements 3, 7, $1 \pm 2\sqrt{-5}$ are irreducible and pairwise non-associated. Therefore the two decompositions are essentially different. Recall that the units in $\mathbb{Z}[\sqrt{-5}]$ are only ± 1. We have $N(3) = 9$, $N(7) = 49$ and $N(1 \pm 2\sqrt{-5}) = 21$. Let $K = \mathbb{Q}(\sqrt{-5})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Define the following ideals in $\mathcal{O}_K$:

$$\begin{aligned} P_1 &= (3, 1 + 2\sqrt{-5}), \\ P_2 &= (3, 1 - 2\sqrt{-5}), \\ P_3 &= (7, 1 + 2\sqrt{-5}), \\ P_4 &= (7, 1 - 2\sqrt{-5}). \end{aligned}$$

It is easy to see that

$$\begin{aligned} P_1P_2 &= (3), \\ P_3P_4 &= (7), \\ P_1P_3 &= (1 + 2\sqrt{-5}), \\ P_2P_4 &= (1 - 2\sqrt{-5}). \end{aligned}$$

The ideals $P_1, \ldots, P_4$ are all maximal. It is enough to show this for P_1, since the other cases are proven the same way. Consider the map $\varphi\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}/3$, given by $a + b\sqrt{-5} \mapsto \overline{a+b}$.

This is a ring homomorphism. The additivity is clear. Furthermore we have $\varphi(1) = 1$ and

$$\begin{aligned}\varphi((a+b\sqrt{-5})(c+d\sqrt{-5})) &= \varphi((ac-5bd)+(ad+bc)\sqrt{-5}) \\ &= \overline{ac-5bd+ad+bc} \\ &= \overline{ac+bd+ad+bc} \\ &= \overline{(a+b)(c+d)} \\ &= \varphi((a+b\sqrt{-5})\varphi(c+d\sqrt{-5})),\end{aligned}$$

hence φ is also multiplicative. Furthermore we have

$$(3) \subsetneq P_1 \subseteq \ker(\varphi) \subsetneq \mathcal{O}_K.$$

Then

$$\begin{aligned}\mathcal{O}_K/(3) &= \mathbb{Z}[x]/(x^2+5,3) \\ &= \mathbb{F}_3[x]/(x^2-1) \\ &= \mathbb{F}_3[x]/(x-1)\times\mathbb{F}_3[x]/(x+1).\end{aligned}$$

This quotient ring has 9 elements. Because the inclusion is strict, we have $\#\mathcal{O}_K/\ker(\varphi) = \#\mathcal{O}_K/P_1 = 3$, so that $P_1 = \ker(\varphi)$. Hence

$$\mathcal{O}_K/P_1 = \mathcal{O}_K/\ker(\varphi) = \mathbb{Z}/3\mathbb{Z}$$

is a field and P_1 is maximal.

Now the two ideal decompositions $(21) = (3)(7)$ and $(21) = (1+2\sqrt{-5})(1-2\sqrt{-5})$ become equal, writing out all ideals as products of prime ideals:

$$\begin{aligned}(3)(7) &= (P_1P_2)(P_3P_4) \\ &= (P_1P_3)(P_2P_4) \\ &= (1+2\sqrt{-5})(1-2\sqrt{-5}).\end{aligned}$$

So the decomposition $(21) = P_1P_2P_3P_4$ is unique.

Proposition 3.2.15. *Let A be a Dedekind ring and $I = \prod_P P^{\nu_P(I)}$, $J = \prod_P P^{\nu_P(J)}$ integral ideals of A. Then we have*

$$\begin{aligned}I \cap J &= \prod_P P^{\max\{\nu_P(I),\nu_P(J)\}}, \\ I + J &= \prod_P P^{\min\{\nu_P(I),\nu_P(J)\}}.\end{aligned}$$

Proof. By Proposition 3.2.7 the inclusion relations of ideals translate into $\geq$-relations of their exponents ν_P. In other words, $J \supseteq I$ if and only if $IJ^{-1} \subseteq A$ if and only if $\nu_P(J) \leq \nu_P(I)$ for all prime ideals P. In this case we say that J divides I. Because of $I \cap J \subseteq I$ we have $\nu_P(I \cap J) \geq \nu_P(I)$. Similarly we have $\nu_P(I \cap J) \geq \nu_P(J)$ because of $I \cap J \subseteq J$. Hence $\nu_P(I \cap J) \geq \max\{\nu_P(I), \nu_P(J)\}$ and therefore $I \cap J \subseteq \prod_P P^{\max\{\nu_P(I),\nu_P(J)\}}$. On the other hand, the RHS is contained in I and J, hence also in $I \cap J$. This shows the first statement. The second one follows similarly. □

Corollary 3.2.16. *Let A be a Dedekind ring and $I = \prod_P P^{\nu_P(I)}$ be a fractional ideal of A. Then we have*

$$A/I \simeq \prod_P A/P^{\nu_P(I)}.$$

Proof. First note that the product is finite, since almost all factors $A/P^{\nu_P(I)}$ are equal to zero. The ideals $P^{\nu_P(I)}$ are pairwise coprime for different maximal ideals, hence we have $P^{\nu_P(I)} + Q^{\nu_Q(I)} = A$ by Proposition 3.2.15. Their intersection is I by Proposition 3.2.15, since $P \cap Q = PQ$ for coprime ideals. Now the CRT yields the statement and we are done. □

Lemma 3.2.17. *Let A be a Dedekind ring and P be a maximal ideal of A. Let $\mathbb{F} = A/P$ be the residue field and $n \geq 0$ be a non-negative integer. Then $P^n/P^{n+1} \simeq \mathbb{F}$ is a 1-dimensional $\mathbb{F}$-vector space.*

Proof. Let $b \in P^n \setminus P^{n+1}$. The map $\varphi\colon A \to P^n/P^{n+1}$ with $\varphi(a) = ab$ is an A-module homomorphism with $\ker(\varphi) = P$. Hence φ induces an injective A-module homomorphism $A/P \hookrightarrow P^n/P^{n+1}$. Thus P^n/P^{n+1} has dimension at least 1 over $\mathbb{F}$. We'll show that there exists a $y \in P^n$, which generates P^n/P^{n+1}. Let $x \in P \setminus P^2$. Then $\nu_P(x) = 1$ and therefore $\nu_p(x^n) = n$. By Proposition 3.2.15 we have $(x^n) + P^{n+1} = P^n$. Hence $y = x^n$ is the required generator. □

3.3. Ideal norm

The norm of an ideal in a ring of integers is defined as follows.

Definition 3.3.1. Let $\mathcal{O}_K$ be the ring of integers of a number field K and I be a nonzero integral ideal in $\mathcal{O}_K$. Then

$$N(I) := \#(\mathcal{O}_K/I) = [\mathcal{O}_K : I]$$

is called the *ideal norm* of I.

For $K = \mathbb{Q}$ we have $\mathcal{O}_K = \mathbb{Z}$ and $I = (a)$ for a $a \neq 0$ in $\mathbb{Z}$. Then we have $N(I) = \#(\mathbb{Z}/a) = |a|$. In particular the ideal norm is *finite* in this case. This holds in general.

Lemma 3.3.2. *The ideal norm in a ring of integers is finite.*

Proof. By the structure theorem there exists a $\mathbb{Z}$–basis $x_1, \ldots, x_n$ of $\mathcal{O}_K$ and integers $a_1, \ldots, a_n$, such that $a_1x_1, \ldots, a_nx_n$ is a $\mathbb{Z}$–basis of I. This yields a group homomorphism

$$\mathcal{O}_K/I \simeq \mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_n.$$

In particular we have $N(I) = |a_1 \cdots a_n|$. □

If $p \in \mathbb{Z}$ is a prime number and $(p) = \mathcal{O}_K p = P_1^{\nu_1} \cdots P_r^{\nu_r}$ is the decomposition into prime ideals, with pairwise distinct $\nu_i \geq 1$ and P_i, the the P_i are exactly the prime ideals *lying above* p, i.e., satisfying $P_i \cap \mathbb{Z} = (p)$. Then $\mathbb{F}_p \subseteq \mathcal{O}_K/P_i$ is an extension of finite fields of degree

$$f_{P_i} := [\mathcal{O}_K/P_i : \mathbb{F}_p].$$

This degree is called the *residue field degree* of P_i. Each prime ideal $P \neq 0$ lies exactly above one prime number $p \in \mathbb{Z}$. Then the ideal norm of P is given by

$$N(P) = \#(\mathcal{O}_K/P) = p^{[\mathcal{O}_K/P:\mathbb{F}_p]}.$$

Lemma 3.3.3. *Let A be a Dedekind ring and $I = \prod_P P^{\nu_P(I)}$ be an integral ideal of A. Then we have*

$$N(I) = \prod_P N(P)^{\nu_P(I)}.$$

It follows that $N(IJ) = N(I)N(J)$, so that the ideal norm is multiplicative.

Proof. By the CRT it suffices to consider ideals of the form $I = P^n$ for prime ideals P. For $n = 1$ the statement is true. Suppose it holds for n. We will show that it holds for $n+1$. The map

$$\mathcal{O}_K/P^{n+1} \to \mathcal{O}_K/P^n$$

is surjective with kernel P^n/P^{n+1}. By Lemma 3.2.17, P^n/P^{n+1} is a 1-dimensional $\mathcal{O}_K/P$-vector space of cardinality $N(P) = \#(\mathcal{O}_K/P)$. It follows that $N(P^{n+1}) = N(P^n)N(P) = N(P)^{n+1}$. □

The ideal norm also generalizes the norm of a field extension $K/\mathbb{Q}$ from Definition 2.4.2.

Lemma 3.3.4. *Let $\mathcal{O}_K$ be the ring of integers of a number field K and $I = (\alpha)$ a nonzero integral principal ideal in $\mathcal{O}_K$. Then we have*

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

Proof. There exists, as we know, a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ of $\mathcal{O}_K$ and integers $a_1, \ldots, a_n$, such that $a_1x_1, \ldots, a_nx_n$ is a $\mathbb{Z}$-basis for I. We have $N(I) = |a_1 \cdots a_n|$, see Lemma 3.3.2. Now we compute $N_{K/\mathbb{Q}}(\alpha)$ in such a way, that we obtain up to sign the value $N(I)$.

Consider the following three $\mathbb{Q}$-bases of the number field K: $\{x_i\}$, $\{a_ix_i\}$ and $\{\alpha x_i\}$. We obtain a commutative diagram of $\mathbb{Q}$-linear maps

$$\begin{tikzcd}
K \arrow[r, "\ell_\alpha"] \arrow[d, "\mathrm{id}"'] & K \\
K \arrow[r, "u"'] & K \arrow[u, "v"']
\end{tikzcd}$$

where u and v are defined by $u(x_i) = a_ix_i$ and $v(a_ix_i) = \alpha x_i$. We have $v(u(\mathrm{id}(x_i))) = \alpha x_i = \ell_\alpha(x_i)$, so that the diagram commutes. Consider now the determinants of these four linear maps. We have $\det(\ell_\alpha) = N_{K/\mathbb{Q}}(\alpha)$ by definition, and $\det(u) = a_1 \cdots a_n$, $\det(\mathrm{id}) = 1$. We claim that $\det(v) = \pm 1$. To see this, note that $\{a_ix_i\}$ and $\{\alpha x_i\}$ are not only $\mathbb{Q}$-bases of K, but also $\mathbb{Z}$-bases of the free $\mathbb{Z}$-module I. The matrix for the base change of a free $\mathbb{Z}$-module has a determinant, which is a unit in $\mathbb{Z}$, i.e., is equal to to ± 1. Thus we obtain

$$N_{K/\mathbb{Q}}(\alpha) = \det(\ell_\alpha) = \det(u)\det(v) = \pm a_1 \cdots a_n.$$

□

Remark 3.3.5. The definition of an ideal norm can be extended to any global field. If K is a functional field, and I an ideal in $\mathcal{O}_K$, we obtain

$$\mathcal{O}_K/I \simeq \mathbb{F}_p[t]/(\lambda_1) \times \cdots \times \mathbb{F}_p[t]/(\lambda_n)$$

with polynomials $\lambda_i \in \mathbb{F}_p[t]$. Therefore we also have

$$N(I) = \prod_{i=1}^n |\mathbb{F}_p[t]/(\lambda_i)| < \infty.$$

Similarly, Lemma 3.3.4 also holds in the function field case. We have

$$N((\lambda)) = N(N_{K/\mathbb{F}_p(t)}(\lambda)).$$

This is the analogous formula, since $N((y)) = |y|$ for $y \in \mathbb{Z}$.

CHAPTER 4

Finiteness of the class number

One major aim of this chapter is to show that the ideal class group of a number field K is *finite*. We use Minkowski theory for the proof, which gives us in addition an effective bound for the norm of ideals in each ideal class. This bound is effective enough to compute the ideal class group for some examples.

The ideal class group measures in a sense how much the ring of integers $\mathcal{O}_K$ differs from a PID. Furthermore the ideal class group and its generalizations give insights on the question, which number field extensions of K are Galois with abelian Galois group. This is studied in *class field theory*. One major result states that, given a number field K, and writing E for the maximal abelian unramified extension of K, the Galois group of E over K is canonically isomorphic to the ideal class group of K.

4.1. Minkowski theory

Let V be a n-dimensional real vector space.

Definition 4.1.1. A *lattice* Λ in V is a subgroup of the additive group of V of the form

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

where $v_1, \ldots, v_r$ are linearly independent vectors in V. For $r = n$ the lattice Λ is called a *full-rank lattice.*

A lattice is a free abelian subgroup of rank r of V, generated by linearly independent elements over $\mathbb{R}$ of V. We will see that a lattice is a *discrete* subgroup of V.

Definition 4.1.2. Let $\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$ be a lattice in V, and $\alpha \in \Lambda$. Then

$$F = \left\{ \alpha + \sum_{i=1}^{r} \xi_i v_i \mid 0 \le \xi_i < 1 \right\}$$

is called a *fundamental domain*, or a *fundamental parallelepiped* of Λ.

A lattice Λ in V has full rank if and only if all translates $\alpha + F$ with $\alpha \in \Lambda$ cover the whole vector space V.

Example 4.1.3. *The subgroup $\mathbb{Z}^n \subseteq \mathbb{R}^n$ is a full rank lattice. However, the subgroup $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2}$ of $\mathbb{R}$ is a free abelian group of rank 2, but not a lattice in $\mathbb{R}$. Indeed, it is not discrete in $\mathbb{R}$ as $(\sqrt{2}-1)^n \to 0$ for $n \to \infty$. On the other hand, $\mathbb{Z} \oplus \mathbb{Z}i$ is a full rank lattice in $\mathbb{C}$.*

Definition 4.1.4. A subgroup L of V is called *discrete*, if every point $\alpha \in L$ has an open neighborhood U in V such that $U \cap L = \{\alpha\}$.

In other words, L is discrete if and only if L is discrete with respect to the subspace topology of V.

LEMMA 4.1.5. *Let L be a subgroup of V. Then the following statements are equivalent:*

(a) *L is discrete.*
(b) *There is an open neighborhood U in V with $U \cap L = \{0\}$.*
(c) *Every compact subset of V intersects L in a finite set.*
(d) *Every bounded subset of V intersects L in a finite set.*

PROOF. $(a) \Rightarrow (b)$: This is obvious.

$(b) \Rightarrow (a)$: The translation map $t_v \colon V \to V$ with $x \mapsto x + v$ is a homeomorphism. If U satisfies the assumption in (b), then also $\alpha + U$ is an open neighborhood of α with $(\alpha + U) \cap L = \{\alpha\}$.

$(a) \Rightarrow (c)$: By assumption L is a discrete topological space with respect to the subspace topology. For a compact set K in V, $K \cap L$ is both discrete and compact, hence finite.

$(c) \Rightarrow (d)$: The closure of a bounded set in V is compact. This holds in $\mathbb{R}^n$, and hence also in V, which differs only by a choice of a basis from $\mathbb{R}^n$, and the topology is independent of the basis. Hence the claim follows by taking the closure.

$(d) \Rightarrow (b)$: Let U be a bounded open neighborhood of 0. Then $S = (U \cap L) \setminus \{0\}$ is finite and hence closed. It follows that $U \setminus S$ is an open neighborhood of 0 with $(U \setminus S) \cap L = \{0\}$. □

PROPOSITION 4.1.6. *A subgroup Λ of V is a lattice if and only if Λ is discrete.*

PROOF. Let $\{v_1, \dots, v_n\}$ be a basis of V, $\alpha = \sum_{i=1}^r a_i v_i$ and

$$\Lambda = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$$

be a lattice in V. Then

$$U = \left\{ \sum_{i=1}^n \xi_i v_i \mid \xi_i \in \mathbb{R},\ |\xi_i - a_i| < 1 \quad \forall\, i \right\}$$

is an open neighborhood of α in V with $U \cap \Lambda = \{\alpha\}$. Hence Λ is discrete.

Conversely let Λ be a discrete subgroup of V and U be the subspace of V spanned by the set Λ. Choose a basis $\{v_1, \dots, v_n\}$ of V, so that $\{v_1, \dots, v_r\}$ is a basis of U. Then

$$\Lambda' := \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r \subseteq \Lambda$$

is a full rank lattice in U. We claim that the group index $(\Lambda : \Lambda')$ is finite. Let λ_i with $i \in \mathcal{I}$ be the representatives for the cosets in Λ/Λ'. Since Λ' is full rank, we have

$$U = \bigcup_{\lambda \in \Lambda'} (\lambda + F)$$

with a fundamental domain $F = \{\sum_{i=1}^r \xi_i v_i \mid \xi_i \in [0,1)\}$. Hence we can write $\lambda_i = \lambda_i' + m_i$ for each $i \in \mathcal{I}$, with $\lambda_i' \in \Lambda'$ and $m_i \in F$. Since the set $\{m_i = \lambda_i - \lambda_i' \mid i \in \mathcal{I}\}$ is discrete and lies in the bounded set F, it is finite. Hence Λ/Λ' is finite. So with $(\Lambda : \Lambda') = k$ we have $k\Lambda \subseteq \Lambda'$, and

$$\Lambda \subseteq \frac{1}{k}\Lambda' = \frac{1}{k}\mathbb{Z}v_1 \oplus \cdots \oplus \frac{1}{k}\mathbb{Z}v_r.$$

By the structure theorem for finitely generated modules over a PID it follows that $\Lambda = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_r$, where $\{w_1, \dots, w_s\}$ is a $\mathbb{Z}$-basis with $w_i \in U$. Since the w_i also span U, we have $r = s$, and the $\{w_1, \dots, w_r\}$ are linearly independent over $\mathbb{R}$. Hence Λ is a lattice in V. □

Let V be a Euclidean vector space. This is a n-dimensional $\mathbb{R}$-vector space together with a symmetric, positive definite bilinear form $<,>: V \times V \to \mathbb{R}$. Let $M \subset \mathbb{R}^n$ be a measurable set with respect to the Lebesgue measure μ. Then the volume of M is defined by $\mathrm{vol}(M) = \mu(M)$. Let $\mathcal{B} = \{v_i\}$ be an orthonormal basis of V and $\{e_i\}$ be the standard basis $\{e_i\}$ of $\mathbb{R}^n$. Then $\varphi = \varphi_{\mathcal{B}}: \mathbb{R}^n \to V$, $e_i \mapsto v_i$ is an isometry of V, and we call a set $M \subseteq V$ *measurable*, if $\varphi^{-1}(M) \subseteq \mathbb{R}^n$ is Lebesgue measurable in $\mathbb{R}^n$. Then the volume of M in V is given by

$$\mathrm{vol}(M) := \mathrm{vol}_{\mathcal{B}}(M) = \mu(\varphi^{-1}(M)).$$

Lemma 4.1.7. *Let A be an automorphism of V. Then we have*

$$\mathrm{vol}(A(M)) = |\det(A)| \cdot \mathrm{vol}(M).$$

So the volume is independent of the choice of an orthonormal base of V.

Proof. Let $\mathcal{B}_1 = \{v_i\}$ be an orthonormal basis of V and $A = (a_{ij}) \in GL(n, \mathbb{R})$. The associated linear map $A: v_j \mapsto \sum_{i=1}^n a_{ij} v_i := w_j$ yields a new basis $\mathcal{B}_2 = \{w_j\}$ of V and isometries $\varphi_{\mathcal{B}_1}: \mathbb{R}^n \to V$, $\varphi_{\mathcal{B}_2}: \mathbb{R}^n \to V$ with $A \circ \varphi_{\mathcal{B}_1} = \varphi_{\mathcal{B}_2} = \varphi_{\mathcal{B}_1} \circ A$. Here $\mathcal{B}_2$ need not be an orthonormal basis. We have

$$\begin{aligned}\mathrm{vol}_{\mathcal{B}_2}(M) &= \mu(\varphi_{\mathcal{B}_2}^{-1}(M)) \\ &= \mu(A^{-1}\varphi_{\mathcal{B}_1}^{-1}(M)) \\ &= |\det(A^{-1})| \cdot \mu(\varphi_{\mathcal{B}_1}^{-1}(M)) \\ &= |\det(A)|^{-1} \cdot \mathrm{vol}_{\mathcal{B}_1}(M).\end{aligned}$$

But if $\mathcal{B}_2$ is again an orthonormal basis, then we have $\det(A) = \pm 1$ and $\mathrm{vol}_{\mathcal{B}_1}(M) = \mathrm{vol}_{\mathcal{B}_2}(M)$. □

The parallelepiped $F_{\mathcal{B}_1} = \{\sum_{i=1}^n \xi_i v_i \mid 0 \le \xi_i < 1\}$ with respect to the orthonormal basis $\{v_i\}$ has volume 1. For the parallelepiped $F_{\mathcal{B}_2} = \{\sum_{i=1}^n \xi_i w_i \mid 0 \le \xi_i < 1\}$ with respect to the new basis $\mathcal{B}_2$ we have $F_{\mathcal{B}_2} = A \cdot F_{\mathcal{B}_1}$, so that

$$\begin{aligned}\mathrm{vol}(F_{\mathcal{B}_2}) &= |\det(A)| \cdot \mathrm{vol}(F_{\mathcal{B}_1}) \\ &= |\det(A)| \cdot 1 \\ &= |\det((< w_i, w_j >)_{i,j})|^{\frac{1}{2}}.\end{aligned}$$

For the last step we have used that, with $< v_k, v_l >= \delta_{kl}$,

$$\begin{aligned}(< w_i, w_j >)_{i,j} &= \sum_{k,l} a_{ik} a_{jl} < v_k, v_l > \\ &= \left(\sum_k a_{ik} a_{jk}\right) \\ &= AA^t,\end{aligned}$$

because of $\det((< w_i, w_j >)_{i,j}) = \det(AA^t) = \det(A)^2$. Hence the following definition makes sense.

Definition 4.1.8. Let $\Lambda = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_r$ be a lattice in V with respect to a basis $\mathcal{B} = \{w_i\}$ of a subspace of V. Then define the volume of Λ by

$$\mathrm{vol}(\Lambda) = \mathrm{vol}(F_{\mathcal{B}}) = |\det((< w_i, w_j >)_{i,j})|^{\frac{1}{2}}.$$

Note that passing to another $\mathbb{Z}$-basis doesn't change the volume, since the base change matrix is in $GL(r,\mathbb{Z})$, and hence has determinant ± 1. So the volume of Λ is independent of the chosen basis.

Remark 4.1.9. Let Λ be a lattice in V, and Λ' be a sublattice of finite index in Λ. Then one can show that

$$\mathrm{vol}(\Lambda') = (\Lambda : \Lambda') \cdot \mathrm{vol}(\Lambda).$$

Let us now come to Minkowski's lattice point theorem. A first result is as follows.

Proposition 4.1.10. *Let Λ be a full rank lattice in V and S be a measurable set in V. If* $\mathrm{vol}(S) > \mathrm{vol}(\Lambda)$, *then there exist two different elements x, y in S with $y - x \in \Lambda$.*

Proof. Let D be a fundamental domain of Λ and $\mathcal{F}$ be the set of all translates of D under Λ. Then $S \cap F$ is measurable for all $F \in \mathcal{F}$, and

$$\mathrm{vol}(S) = \sum_{F \in \mathcal{F}} \mathrm{vol}(S \cap F).$$

For *each* F there exists a *unique* translate of $S \cap F$ by an element of Λ, which is a subset of D. Because of $\mathrm{vol}(S) > \mathrm{vol}(D) = \mathrm{vol}(\Lambda)$ at least two of theses translates must overlap. Hence there exist two different elements x, y in S with $x - \lambda = y - \lambda'$ for some $\lambda, \lambda' \in \Lambda$. So we have $y - x \in \Lambda$. □

Definition 4.1.11. A subset S in V is called *convex*, if for each two elements $x, y \in S$ also the whole line segment that joins them, namely

$$\{(1-t)x + ty \mid 0 \le t \le 1\}$$

lies in S.
Furthermore S is called *centrally symmetric*, if for all $x \in S$ we have $-x \in S$.

The following theorem is Minkowski's lattice point theorem.

Theorem 4.1.12 (Minkowski 1896). *Let Λ be a full rank lattice in a n-dimensional Euclidean vector space. Let S be a convex, centrally symmetric set in V. Suppose that one of the following conditions is satisfied.*

(1) $\mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Lambda)$,
(2) $\mathrm{vol}(S) \ge 2^n \cdot \mathrm{vol}(\Lambda)$, *and S is compact.*

Then S contains a nonzero lattice point.

Proof. Suppose that (1) is satisfied: For $T = \frac{1}{2}S$ we have

$$\mathrm{vol}(T) = \frac{1}{2^n}\mathrm{vol}(S) > \mathrm{vol}(\Lambda).$$

By Proposition 4.1.10 there exist $x, y \in T$ with $y - x \in \Lambda$ and $y - x \neq 0$. Then we have $2x \in S$ and $2y \in S$, hence also $-2x \in S$. The representation

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

shows that also $y - x$ is in S, since S is convex. It follows that $y - x \in S \cap \Lambda$, and that $x - y$ is a nonzero lattice point in S.

Suppose that (2) is satisfied: We apply the first case on $(1+\varepsilon)S$, with $\varepsilon > 0$. Because of $\mathrm{vol}((1+\varepsilon)S) = (1+\varepsilon)^n \mathrm{vol}(S) > 2^n \cdot \mathrm{vol}(\Lambda)$ we have

$$S_\varepsilon := (\Lambda \setminus 0) \cap (1+\varepsilon)S \neq \emptyset.$$

Every set S_ε is finite since S is compact and Λ is discrete. Therefore the set $\cap_{\varepsilon>0} S_\varepsilon$ is non-empty. Let $z \in \cap_{\varepsilon>0} S_\varepsilon$. Then we have $z \in \Lambda \setminus 0$ and

$$z \in \bigcap_{\varepsilon>0} (1+\varepsilon)S = S,$$

since S is closed. Hence $z \in S \cap \Lambda$ is a nonzero lattice point in S. □

Minkowski's lattice point theorem has many nontrivial consequences. One example is that we obtain a different proof of Lagrange's four-square theorem. Let

$$\Sigma_4 = \{x_1^2 + x_2^2 + x_3^2 + x_4^2 \mid x_1, x_2, x_3, x_4 \in \mathbb{Z}\}.$$

Suppose that $0 \in \mathbb{N}$. Of course, $0 \in \Sigma_4$.

Theorem 4.1.13 (Lagrange 1770). *Every positive integer is the sum of four squares, i.e.,* $\Sigma_4 = \mathbb{N}$.

We need two lemmas for the proof.

Lemma 4.1.14 (Euler 1748). *The set Σ_4 is multiplicatively closed.*

Proof. If $n_1 = a_1^2 + b_1^2 + c_1^2 + d_1^2$ and $n_2 = a_2^2 + b_2^2 + c_2^2 + d_2^2$, then we may associate $x_i \in \mathbb{H}$ in the quaternion algebra by

$$x_i = a_i \cdot 1 + b_i \cdot i + c_i \cdot j + d_i \cdot k.$$

The norm of $x_i \in \mathbb{H}$ is given by $N(x_i) = a_i^2 + b_i^2 + c_i^2 + d_i^2$. It satisfies $N(x_1 x_2) = N(x_1)N(x_2)$, which means

$$\begin{aligned} n_1 n_2 &= (a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) \\ &= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2)^2 + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)^2 \\ &\quad + (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)^2 + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)^2. \end{aligned}$$

□

Hence it is enough to show that every prime p is the sum of four squares. Of course we may assume that $p > 2$. We also need the following lemma, which has been proved in elementary number theory.

Lemma 4.1.15. *Let $p > 2$ be a prime and $a, b, c \in \mathbb{Z}$ be not divisible by p. Then there exist $u, v \in \mathbb{Z}$ such that*

$$a \equiv bu^2 + cv^2 \bmod p$$

Proof of Lagrange's four-square theorem: We define a suitable lattice Λ and a set S in $\mathbb{R}^4$, so that we can apply Minkowski's lattice point theorem. So let $p > 2$ be an arbitrary prime number and define

$$S := \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p\}$$

We claim that

$$\mathrm{vol}(S) = 2\pi^2 p^2.$$

In fact, we have

$$\mathrm{vol}(B^n) = \frac{\pi^{n/2}}{\left(\frac{n}{2}\right)!}$$

for the volume of the n-dimensional unit ball. In particular, $\mathrm{vol}(B^4) = \frac{\pi^2}{2}$ and $\mathrm{vol}(S) = \frac{\pi^2(2p)^2}{2} = 2\pi^2 p^2$.

Now we want to find a suitable lattice Λ. It should have volume p^2, i.e., we need to find a homomorphism $\varphi\colon \mathbb{Z}^4 \to \mathbb{F}_p^2$ with the property that for all $(x_1, x_2, x_3, x_4) \in \ker(\varphi)$ we have $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod p$. By Lemma 4.1.15 we can find $u, v \in \mathbb{Z}$ with $u^2 + v^2 + 1 \equiv 0 \bmod p$. So define $\varphi\colon \mathbb{Z}^4 \to \mathbb{F}_p^2$ by

$$(x_1, x_2, x_3, x_4) \mapsto (\overline{x_2} - \overline{u} \cdot \overline{x_1} + \overline{v} \cdot \overline{x_4}, \overline{x_3} - \overline{u} \cdot \overline{x_4} + \overline{v} \cdot \overline{x_1})$$

and define

$$\Lambda := \ker(\varphi).$$

Then for $(x_1, x_2, x_3, x_4) \in \Lambda$ we have

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &\equiv x_1^2 + (ux_1 - vx_4)^2 + (ux_4 + vx_1)^2 + x_4^2 \\ &\equiv (1 + u^2 + v^2)(x_1^2 + x_4^2) \\ &\equiv 0 \bmod p. \end{aligned}$$

Hence p divides $x_1^2 + x_2^2 + x_3^2 + x_4^2$. Obviously φ is surjective so that $\mathrm{vol}(\Lambda) = p^2$. We have

$$\mathrm{vol}(S) = 2\pi^2 p^2 > 16p^2 = 2^4 \mathrm{vol}(\Lambda),$$

so that we can apply Minkowski's theorem. It gives a nonzero quadruple

$$(0, 0, 0, 0) \neq (x_1, x_2, x_3, x_4) \in S \cap \Lambda,$$

so that we have $0 < x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2p$, where the integer in the middle is divisible by p. Hence $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and we are done. □

4.2. Rings of integers as lattices

Let K be a number field of degree $n = [K : \mathbb{Q}]$. Then there is an $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ and therefore $K \simeq \mathbb{Q}[x]/(f(x))$, where $f(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α over $\mathbb{Q}$. It has exactly n complex roots. Every complex root z induces a homomorphism $\mathbb{Q}[x] \to \mathbb{C}$ with kernel $(f(x))$. Thus we obtain n embeddings $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbb{C}$. An embedding $\sigma \colon K \hookrightarrow \mathbb{C}$ is called *real*, if $\sigma(K) \subseteq \mathbb{R}$, and *complex* otherwise.

Let r be the number of different real embeddings of K. Every complex embedding σ defines by $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ another complex embedding, which is different from σ because of $\sigma(K) \nsubseteq \mathbb{R}$. Hence we may group the different complex embeddings into pairs $\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s}$. In total we have

$$n = r + 2s$$

different embeddings of K. We order them in such a way, that the first r embeddings are real.

Example 4.2.1. *The number field $K = \mathbb{Q}(\sqrt[3]{5})$ has one real and two complex embeddings. So we have $n = 3$ and $r = s = 1$.*

The minimal polynomial of $\alpha = \sqrt[3]{5}$ is $x^3 - 5$. The embeddings into $\mathbb{C}$ arise by mapping α to the roots $\alpha, \zeta\alpha, \zeta^2\alpha$ of $x^3 - 5$ in $\mathbb{C}$. Here ζ is a primitive third root of unity.

Definition 4.2.2. The *canonical embedding* of a number field K in the Euclidean vector space $V_K := \mathbb{R}^r \times \mathbb{C}^s$ is given by

$$\sigma \colon K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_n(\alpha)).$$

We may identity V_K with $\mathbb{R}^n$ by using the basis $\{1, i\}$ for $\mathbb{C}$. This identifies $z = a + bi$ with $(a, b) = (\Re(z), \Im(z))$. With these notions we have the following lemma.

Lemma 4.2.3. *Let M be a free $\mathbb{Z}$-submodule of K and $\{x_1, \dots, x_n\}$ be a basis of M. Then $\sigma(M)$ is a full rank lattice in $\mathbb{R}^n$ with volume*

$$\operatorname{vol}(\sigma(M)) = 2^{-s} \cdot |\det((\sigma_i(x_j)_{i,j}))|.$$

Proof. Let A be the matrix with row vectors $\sigma(x_i)$. Then we have

$$\begin{aligned}\sigma(x_i) = (&\sigma_1(x_i), \dots, \sigma_r(x_i), \Re(\sigma_{r+1}(x_i)), \Im(\sigma_{r+1}(x_i)), \dots, \\ &\Re(\sigma_{r+s}(x_i)), \Im(\sigma_{r+s}(x_i))),\end{aligned}$$

and $\operatorname{vol}(\sigma(M)) = |\det(A)|$. Let B be the matrix, whose i-th row is given by

$$(\sigma_1(x_i), \dots, \sigma_r(x_i), \sigma_{r+1}(x_i), \overline{\sigma_{r+1}(x_i)}, \dots, \sigma_{r+s}(x_i), \overline{\sigma_{r+s}(x_i)}).$$

By Lemma 2.4.10 we have

$$\begin{aligned}\det(B)^2 &= D(x_1, \dots, x_n) \\ &= \det((\sigma_i(x_j)_{i,j}))^2 \neq 0\end{aligned}$$

We claim that

$$\det(B) = (-2i)^s \det(A).$$

This implies $\det(A) \neq 0$. Hence the vectors $\sigma(x_1), \dots, \sigma(x_n)$ are linearly independent over $\mathbb{R}$, and $\sigma(M)$ is a full rank lattice in $\mathbb{R}^n$. Because of $|i^s| = 1$ we also have

$$\begin{aligned} |\det((\sigma_i(x_j)_{i,j}))| &= |\det(B)| \\ &= 2^s |\det(A)| \\ &= 2^s \mathrm{vol}(\sigma(M)). \end{aligned}$$

It remains to show the claimed relationship between $\det(A)$ and $\det(B)$. For a complex number z we can express $\Re(z)$ and $\Im(z)$ by

$$\Re(z) = \frac{1}{2}(z + \overline{z}),\ \Im(z) = \frac{1}{2i}(z - \overline{z}).$$

Let us do this for $z = \sigma(x_j)$ with $j = r+1, \dots, n$. Using

$$\det(\dots, \frac{1}{2}(z + \overline{z}), \frac{1}{2i}(z - \overline{z}), \dots) = -\frac{1}{2i} \det(\dots, z, \overline{z}, \dots)$$

s-times, the claim follows. □

Corollary 4.2.4. *Let K be a number field with ring of integers $\mathcal{O}_K$ and discriminant d_K. Then $\sigma(\mathcal{O}_K)$ is a full rank lattice in $\mathbb{R}^n$ with volume*

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-s}\sqrt{|d_K|}.$$

Proof. Let $\{x_1, \dots, x_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then we have

$$d_K = D(x_1, \dots, x_n) = \det((\sigma_i(x_j)_{i,j}))^2$$

and

$$\mathrm{vol}(\sigma(\mathcal{O}_K)) = 2^{-s} \cdot |\det((\sigma_i(x_j)_{i,j}))| = 2^{-s}\sqrt{|d_K|}.$$

□

Corollary 4.2.5. *Let K be a number field with discriminant d_K and I be a nonzero ideal in $\mathcal{O}_K$. Then $\sigma(I)$ is a full rank lattice in $\mathbb{R}^n$ with volume*

$$\mathrm{vol}(\sigma(I)) = 2^{-s} N(I)\sqrt{|d_K|}.$$

Proof. The ideal I also is a free $\mathbb{Z}$-module of rank n. Hence $\sigma(I)$ is a full rank lattice. By the theorem for finitely generated modules we find a $\mathbb{Z}$-basis $\{x_1, \dots, x_n\}$ of $\mathcal{O}_K$, and suitable $a_i \in \mathbb{Z}$, so that simultaneously $\{a_1x_1, \dots, a_nx_n\}$ is a $\mathbb{Z}$-basis of I. Then we have $N(I) = |a_1 \cdots a_n|$, see Lemma 3.3.2. Hence it follows that

$$\begin{aligned} \mathrm{vol}(\sigma(I)) &= 2^{-s}|\det((\sigma_i(a_jx_j)_{i,j}))| \\ &= 2^{-s}|a_1 \cdots a_n| \cdot |\det((\sigma_i(x_j)_{i,j}))| \\ &= 2^{-s}N(I)\sqrt{|d_K|}. \end{aligned}$$

□

Now we can prove the following theorem, which will imply the finiteness of the class number.

Theorem 4.2.6. *Let K be a number field of degree n with discriminant d_K, and I be a nonzero ideal in $\mathcal{O}_K$. Then there is an $x \neq 0$ in I with*

$$|N_{K/\mathbb{Q}}(x)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}N(I).$$

Proof. Let us introduce the following abbreviations.

$$\begin{aligned} C_K &= \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s, \\ B_K &= C_K\sqrt{|d_K|} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}. \end{aligned}$$

The constant B_K is called *Minkowski bound*, and C_K is called the *Minkowski constant.*

Consider the canonical embedding $\sigma\colon K \hookrightarrow V_K$ in the Euclidean vector space $V_K = \mathbb{R}^r \times \mathbb{C}^s$, equipped with the norm

$$\|x\| = \sum_{i=1}^{r}|y_i| + 2\sum_{j=1}^{s}|z_j|$$

for $x = (y_1, \dots, y_r, z_1, \dots, z_s) \in V_K$. Let $t > 0$ be a real number and set

$$B_t = \{x \in V_K \mid \|x\| \leq t\}.$$

Our aim is to show that

$$\mu(B_t) = 2^r\left(\frac{\pi}{2}\right)^s\frac{t^n}{n!}. \tag{4.1}$$

Then the claim follows from Minkowski's lattice point theorem with a suitable choice of $t > 0$. The set B_t is compact, convex and centrally symmetric. We have to chose $\mu(B_t) \geq 2^n\mathrm{vol}(\sigma(I))$. By Corollary 4.2.5 this means

$$\begin{aligned} 2^r\left(\frac{\pi}{2}\right)^s\frac{t^n}{n!} &= \mu(B_t) \\ &\geq 2^n\mathrm{vol}(\sigma(I)) \\ &= 2^{n-s}\sqrt{|d_K|}N(I), \end{aligned}$$

so in other words

$$t^n \geq n!\,4^s\,\pi^{-s}\sqrt{|d_K|}N(I),$$

because of $n = r + 2s$. So if we chose t^n, so that we have equality above, then there exists by (2) of Theorem 4.1.12 an element $x \in I$ with $\sigma(x) \in B_t$ and $\sigma(x) \neq 0$, hence with $x \neq 0$. We can estimate the norm of x by the inequality

$$a_1 \cdots a_n \leq n^{-n}(a_1 + \cdots + a_n)^n$$

for $a_i > 0$ with the above formula for t^n. We obtain

$$\begin{aligned} |N_{K/\mathbb{Q}}(x)| &= |\sigma_1(x)| \cdots |\sigma_r(x)| \cdot |\sigma_{r+1}(x)|^2 \cdots |\sigma_{r+s}(x)|^2 \\ &\leq n^{-n}(|\sigma_1(x)| + \cdots + |\sigma_r(x)| + 2|\sigma_{r+1}(x)| + \cdots + 2|\sigma_{r+s}(x)|)^n \\ &= n^{-n}\|x\|^n \\ &\leq n^{-n}t^n \\ &= n^{-n}\,n!\,4^s\,\pi^{-s}\sqrt{|d_K|}N(I). \end{aligned}$$

This is exactly the claim. So it remains to prove the formula 4.1 for $\mu(B_t)$. We do this by induction over r and s. So let us write $V(r, s, t) = \mu(B_t)$. For the base case we compute the cases $(r,s)=(1,0)$ and $(r,s)=(0,1)$:

$$\begin{aligned} V(1,0,t) &= \mu(\{y_1 \in \mathbb{R} \mid |y_1| \le t\}) = 2t, \\ V(0,1,t) &= \mu(\{z_1 \in \mathbb{C} \mid 2|z_1| \le t\}) = \pi \left(\frac{t}{2}\right)^2, \end{aligned}$$

where $V(0,1,t)$ is the area of a circle with radius $t/2$. This coincides with the formula 4.1. The first induction step $r \mapsto r+1$ goes as follows, with $(y_0,\dots,y_r,z_1,\dots,z_s) \in B_t$:

$$\begin{aligned} V(r+1,s,t) &= \int_{\mathbb{R}} V(r,s,t-|y_0|)dy_0 \\ &= \int_{-t}^{t} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-|y_0|)^n}{n!} dy_0 \\ &= 2^r \left(\frac{\pi}{2}\right)^s \frac{2}{n!} \int_0^t (t-y_0)^n dy_0 \\ &= 2^{r+1} \left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n+1)!}, \end{aligned}$$

since

$$\int_0^t (t-y_0)^n dy_0 = \frac{-(t-y_0)^{n+1}}{n+1}\bigg|_0^t = \frac{t^{n+1}}{n+1}.$$

For the second induction step $s \mapsto s+1$ we write the new coordinate $z_0 \in \mathbb{C}$ in polar form $z_0 = \rho e^{i\theta}$, with $d\mu(z_0) = \rho\, d\rho\, d\theta$. We obtain

$$\begin{aligned} V(r,s+1,t) &= \int_{\mathbb{C}} V(r,s,t-2|z_0|)d\mu(z_0) \\ &= \int_{|z_0| \le t/2} V(r,s,t-2|z_0|)d\mu(z_0) \\ &= \int_0^{t/2} \int_0^{2\pi} 2^r \left(\frac{\pi}{2}\right)^s \frac{(t-2\rho)^n}{n!} \rho\, d\rho\, d\theta \\ &= 2^r \left(\frac{\pi}{2}\right)^s \frac{2\pi}{n!} \cdot \int_0^{t/2} (t-2\rho)^n \rho\, d\rho \\ &= 2^r \left(\frac{\pi}{2}\right)^{s+1} \frac{t^{n+2}}{(n+2)!}, \end{aligned}$$

because using the substitution $2\rho = x$ and using partial integration we have

$$\begin{aligned} \int_0^{t/2} (t-2\rho)^n \rho\, d\rho &= \frac{1}{4} \int_0^x (t-x)^n x\, dx \\ &= \frac{1}{4} \left(\frac{-(t-x)^{n+1}}{n+1} x \bigg|_0^t - \int_0^x \frac{-(t-x)^{n+1}}{n+1} dx \right) \\ &= \frac{1}{4} \frac{t^{n+2}}{(n+1)(n+2)}. \end{aligned}$$

□

Corollary 4.2.7. *Every ideal class in $Cl(K)$ contains an integral ideal J of $\mathcal{O}_K$ with*

$$N(J) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

Proof. Let J' be a fractional ideal in K. Then there exists a $d \in K^\times$, so that $I = d(J')^{-1}$ is an integral ideal of $\mathcal{O}_K$, with $I = (d)(J')^{-1}$ and $I \sim (J')^{-1}$. By Theorem 4.2.6 there exists a $y \in I$, $y \neq 0$ with $|N_{K/\mathbb{Q}}(y)| \leq B_K N(I)$. Because of $y\mathcal{O}_K \subseteq I$ we have $(y) = JI$ for an integral ideal J with $J \sim I^{-1} \sim J'$. By Lemma 3.3.3 and Lemma 3.3.4 we have

$$N(J)N(I) = N(JI) = N((y)) = |N_{K/\mathbb{Q}}(y)| \leq B_K N(I).$$

Canceling by $N(I)$ yields $N(J) \leq B_K$. □

We obtain an important corollary.

Corollary 4.2.8 (Dirichlet). *The ideal class group $Cl(K)$ of a number field K is finite.*

Proof. Every ideal class of K contains an integral ideal J with $N(J) \leq B_K$ by Corollary 4.2.7. However, there are only finitely many such ideals with a bounded norm. Indeed, if $N(J) = \#\mathcal{O}_K/J = q$ for a fixed q, it follows that $q \in J$. The ideals J of $\mathcal{O}_K$ with $q \in J$ correspond to the ideals of the finite ring $\mathcal{O}_K/(q)$, which has only finitely many ideals. □

Example 4.2.9. *The ideal class group of $K = \mathbb{Q}(i)$ is trivial.*

We have $(r, s) = (0, 1)$ and $n = 2$. So we have $d_K = -4$, see Example 2.4.19. Therefore the Minkowski bound is given by $B_K = 4/\pi = 1.273239$ and $N(J) \leq B_K < 2$, so that $N(J) = 1$. Hence every fractional ideal I is equivalent to an integral ideal J of norm 1, hence equivalent to $J = \mathbb{Z}[i]$, the trivial element of $Cl(K)$. Only $\mathbb{Z}[i]$ can have have norm 1. So the group $Cl(K)$ is trivial.

Of course there are other arguments to see this. We already know that $\mathbb{Z}[i]$ together with the norm $N(z) = z\overline{z}$ is a Euclidean ring and hence a PID. So its class group, i.e., the class group of $\mathbb{Q}(i)$, is trivial.

Example 4.2.10. *The ideal class group of $K = \mathbb{Q}(\sqrt{-5})$ is isomorphic to $\mathbb{Z}/2$.*

We have $(r, s) = (0, 1)$ and $n = 2$. We have $d_K = -20$, see example 2.4.19. The Minkowski bound is given by $B_K = 2.8470501736687$. Therefore every fractional ideal I is equivalent to an integral ideal J with $N(J) \leq \frac{4}{\pi}\sqrt{5} < 3$, hence with $N(J) = 1$ or $N(J) = 2$. In the first case we have $J = \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, which represents the trivial element in $Cl(K)$. In the second case, the ideal corresponds to an ideal in $\mathcal{O}_K/(2)$ with $(2) = P^2$, where $P = (2, 1 + \sqrt{-5})$ is the unique prime ideal of norm 2, e.g., $N(P)N(P) = N(P^2) = N(2) = 4$, hence $N(P) = 2$. Hence $Cl(K) =< P >$ and P has order at most 2, because $P^2 \sim \mathcal{O}_K$. On the other hand, P cannot have order 1, because P is not a principal ideal. It follows that the group $CL(K)$ has order 2.

Corollary 4.2.11. *Let K be a number field of degree $n \geq 2$ with discriminant d_K. Then we have*

$$|d_K| \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2s} \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

In particular,

$$\frac{n}{\log(|d_K|)} < \frac{117}{100}.$$

Proof. For the ideal $J = \mathcal{O}_K$ we have by Corollary 4.2.7

$$1 = N(J) \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

This is equivalent to

$$\sqrt{|d_K|} \ge \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}.$$

By squaring we obtain the first estimate. Using $2s \le n$ and $\pi/4 < 1$ we obtain $\left(\frac{\pi}{4}\right)^{2s} \ge \left(\frac{\pi}{4}\right)^n$, so that the estimate only depends on n. So we obtain $|d_K| \ge a_n$ with

$$a_n := \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}.$$

This sequence starts with $a_2 = \frac{\pi^2}{4}$, $a_3 = \frac{81\pi^3}{256}$ and satisfies

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{\pi}{4} \cdot \frac{(n+1)^2(n+1)^{2n}(n!)^2}{((n+1)!)^2 n^{2n}} \\ &= \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} \\ &\ge \frac{3\pi}{4},\end{aligned}$$

since $(1+1/n)^{2n} = 1+2+\cdots > 3$, because there are only further positive terms in the binomial formula. So we obtain $a_n \ge \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$ for all $n \ge 2$ by induction. This implies $|d_K| \ge \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. Taking logarithms we obtain

$$1.166796 \sim \frac{1}{\log(3\pi/4)} \ge \frac{n}{\log(|d_K|)}.$$

□

Example 4.2.12. *For every imaginary-quadratic number field K we have $|d_K| \ge 3$. For $K = \mathbb{Q}(\sqrt{-3})$ we have equality, i.e., $|d_K| = 3$.*

Indeed, both estimates in Corollary 4.2.11 give $|d_K| \ge \frac{\pi^2}{4} > 2$, since $s = 1$ and $n = 2$.

Example 4.2.13. *For every real-quadratic number field K we have $|d_K| \ge 4$. The smallest value is $|d_K| = 5$, for $K = \mathbb{Q}(\sqrt{5})$.*

This time the first estimate in Corollary 4.2.11 is better than the second one, because of $s = 0$. So we obtain $|d_K| \ge 4$. Equality cannot hold, which can be seen from the formulas in Example 2.4.19.

Proposition 4.2.14 (Hermite-Minkowski). *Let K be a number field different from $\mathbb{Q}$. Then we have $|d_K| > 1$.*

Proof. We have $|d_K| \ge \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$ for $n \ge 2$ by Corollary 4.2.11. □

Proposition 4.2.15 (Hermite). *For every $d \in \mathbb{Z}$ there are only finitely many number fields K with $d_K = d$.*

Proof. By Corollary 4.2.11 we have $[K:\mathbb{Q}] = n \le C \cdot \log(d)$ for a constant $C > 0$. Hence the degree of such number fields is bounded. So it suffices to show that there are only finitely many number fields to given fixed integers d, r, s. For $r > 0$ let B be the set of vectors $(y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s$ with

$$\begin{aligned} |y_1| &\le 2^n \left(\frac{\pi}{2}\right)^{-s} \sqrt{|d|}, \\ |y_i| &\le \frac{1}{2},\ i = 2, \dots, r, \\ |z_j| &\le \frac{1}{2},\ j = 1, \dots, s. \end{aligned}$$

For $r = 0$ let B be the set of vectors $(z_1, \dots, z_s) \in \mathbb{C}^s$ with

$$\begin{aligned} |z_1 - \overline{z_1}| &\le 2^n \left(\frac{\pi}{2}\right)^{1-s} \sqrt{|d|}, \quad |z_1 + \overline{z_1}| \le \frac{1}{2}, \\ |z_j| &\le \frac{1}{2},\ j = 2, \dots, s. \end{aligned}$$

Then B is convex, compact and centrally symmetric with volume

$$\operatorname{vol}(B) = 2^{n-s}\sqrt{|d|} = 2^n \operatorname{vol}(\sigma(\mathcal{O}_K))$$

by Corollary 4.2.4. Therefore we can apply Minkowski's lattice point theorem and obtain an element $0 \ne x \in \mathcal{O}_K$ with $\sigma(x) \in B$. We claim that $K = \mathbb{Q}(x)$. Since there are only finitely many such elements x, there are also only finitely many such number fields with $K = \mathbb{Q}(x)$. For $r > 0$ we have by assumption $|\sigma_i(x)| \le 1/2$ for $i \ne 1$. Now

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} |\sigma_i(x)| \ge 1$$

implies that $|\sigma_1(x)| \ge 1$, and hence $\sigma_1(x) \ne \sigma_i(x)$ for $i \ne 1$. We have $x \in \mathcal{O}_K \subseteq K$, so that $\mathbb{Q}(x) \subseteq K$. Suppose that K is not contained in $\mathbb{Q}(x)$. Then $\sigma_1 \mid_{\mathbb{Q}(x)} \mathbb{Q}(x) \to \mathbb{C}$ has an extension σ on K, which is different from σ_1. But this embedding must be one of the embeddings $\sigma_1, \dots, \sigma_n$. This is impossible. Hence we have $K = \mathbb{Q}(x)$.

For $r = 0$ we see similarly that $|\sigma_1(x)| = \overline{|\sigma_1(x)|} \ge 1$ and hence $\sigma_1(x) \ne \sigma_j(x)$, except for $\sigma_j = \sigma_1$ or $\sigma_j = \overline{\sigma_1}$. It follows from the definition of B that $\Re(\sigma_1(x)) \le 1/4$. Hence σ_1 cannot be real, i.e., we have $\sigma_1(x) \ne \overline{\sigma_1(x)}$. As before we obtain $K = \mathbb{Q}(x)$.

Thus in both cases the conjugates $|\sigma_i(x)|$ of x are bounded. Hence the minimal polynomial $m(x)(t) \in \mathbb{Z}[t]$ of degree n has bounded coefficients. Since there are only finitely many polynomials $f \in \mathbb{Z}[t]$ of degree n with bounded coefficients, there are only finitely many elements x with $K = \mathbb{Q}(x)$. So we are done. □

4.3. Class number 1

The number field K with class number $h_K = 1$ are exactly those where the ring of integers $\mathcal{O}_K$ is a PID. Is it possible to classify such number fields? This seems hopeless. We even don't know whether or not there are infinitely many real-quadratic number fields of class number 1. Gauss has conjectured that this is indeed the case. The Cohen–Lenstra heuristics are a set of more precise conjectures about the structure of class groups of quadratic number fields. For real-quadratic number fields they predict that about 75.446% of the fields obtained by adjoining the square root of a prime will have class number 1. This agrees so far with computations. For imaginary-quadratic number fields of class number 1 a classification is indeed possible.

We already know that the Minkowski bound gives a criterion for K having class number 1.

Example 4.3.1. *Every number field K with Minkowski bound $B_K < 2$ has class number* 1.

Indeed, this follows as in Example 4.2.9. What does this yield for quadratic number fields? Let $K = \mathbb{Q}(\sqrt{d})$ with squarefree $d \in \mathbb{Z}$. Then $B_K < 2$ for $d < 0$ just says that $|d_K| < \pi^2$, hence $d = -1, -2, -3, -7$. For $d > 0$ is says that $|d_K| < 16$, hence $d = 2, 3, 5, 13$. So the following number fields have class number 1 for this reason:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(\sqrt{13}).$$

On the other hand, there are much more quadratic number fields of class number 1, which do not satisfy the Minkowski bound $B_K < 2$.

As mentioned. for *imaginary-quadratic* number fields there is a classification, see 2.2.6:

Proposition 4.3.2 (Baker, Stark 1967). *There are exactly* 9 *imaginary-quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ with class number* 1 *for squarefree $d < 0$, namely for*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

It is not difficult to show that these number fields have class number 1, but it is more difficult to show that there is no tenth imaginary-quadratic number field of class number 1.

There are also classification results for imaginary-quadratic number fields of higher class numbers $h > 1$. The result for $h = 2$ is as follows.

Proposition 4.3.3 (Baker 1971). *There are exactly* 18 *imaginary-quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ with class number* 2 *for squarefree $d < 0$, namely for*

$$\begin{aligned} d = &-5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115,\\ &-123, -187, -235, -267, -403, -427. \end{aligned}$$

Indeed, the list of imaginary-quadratic number fields of class number h is finite for each $h \geq 1$.

Proposition 4.3.4 (Heilbronn 1934). *For every positive integer $h \geq 1$ there are only finitely many imaginary-quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ with class number h.*

There are also classification results for all $1 \leq h \leq 100$. The next table shows the number of imaginary-quadratic number fields having class number h for all $1 \leq h \leq 100$. This is due to Mark Watkins.

h	#	h	#	h	#	h	#	h	#	h	#	h	#
1	9	16	322	31	73	46	268	61	132	76	1075	91	214
2	18	17	45	32	708	47	107	62	323	77	216	92	1248
3	16	18	150	33	101	48	1365	63	216	78	561	93	262
4	54	19	47	34	219	49	132	64	1672	79	175	94	509
5	25	20	350	35	103	50	345	65	164	80	2277	95	241
6	51	21	85	36	668	51	159	66	530	81	228	96	3283
7	31	22	139	37	85	52	770	67	120	82	402	97	185
8	131	23	68	38	237	53	114	68	976	83	150	98	580
9	34	24	511	39	115	54	427	69	209	84	1715	99	289
10	87	25	95	40	912	55	163	70	560	85	221	100	1736
11	41	26	190	41	109	56	1205	71	150	86	472		
12	206	27	93	42	339	57	179	72	1930	87	222		
13	37	28	457	43	106	58	291	73	119	88	1905		
14	95	29	83	44	691	59	128	74	407	89	192		
15	68	30	255	45	154	60	1302	75	237	90	801		

A computation of the class number of quadratic number fields is also possible by Dirichlet's *analytic class number formula*, see section 5.2. There are also algorithms for computing a system of representatives for the ideal class group. We want to mention such an algorithm for imaginary-quadratic number fields.

Proposition 4.3.5. *Let K be an imaginary-quadratic number field with discriminant d_K. A complete system of representatives of the ideal class group is given by the ideals*

$$I = a\mathbb{Z} + \frac{b+\sqrt{d_K}}{2}\mathbb{Z}$$

for $a, b \in \mathbb{Z}$ with

$$\begin{gathered} a \geq 1, \\ 4a \mid d_k - b^2, \\ |b| \leq a, \\ 4a^2 \leq b^2 - d_K, \end{gathered}$$

where in case of equality $|b| = a$ or $4a^2 = b^2 - d_K$ it is required in addition that $b \geq 0$.

Clearly this result yields again, that the class number of $\mathbb{Q}(\sqrt{-d})$ is finite. Indeed, $|b| \leq a$ and $4a^2 \leq b^2 - d_K$ imply that $3a^2 \leq -d_K = |d_K|$, so that there are only finitely many values are possible for a. Because of $|b| \leq a$ then there are only finitely many pairs (a, b) satisfying the requirements of the proposition.

Example 4.3.6. *The class number of $K = \mathbb{Q}(\sqrt{-67})$ is equal to 1.*

This follows from the above proposition. We have $d_K = -67$. First, $3a^2 \leq -d_K = 67$ implies that $a \leq 4$. Since we have $|b| \leq a \leq 4$ and $4 \mid d_k - b^2$ it follows that $|b| = 1$ or 3. For $|b| = 1$ we have $4a \mid d_k - 1^2 = -68$, i.e., $a \mid 17$. Then $a \leq 4$ implies $a = 1$. For $|b| = 3$ we obtain $4a \mid d_k - 3^2 = -76$, so that $a \mid 19$, hence $a = 1$ and $3 = |b| \leq a = 1$. This is a contradiction. Now we have equality $a = |b| = 1$, so that $a = b = 1$. Hence there is only one class in $Cl(K)$, namely

$$\mathbb{Z} + \frac{1+\sqrt{-67}}{2}\mathbb{Z} = \mathcal{O}_K.$$

Here is a table of all squarefree integers $0 < d < 1000$ with class number $h_{\mathbb{Q}(\sqrt{d})} = 1$, using the CAS *pari-gp*:

```
1,2,3,5,6,7,11,13,14,17,19,21,22,23,29,31,33,37,38,41, 43,46,47,
53,57,59,61,62,67,69,71,73,77,83,86,89,93,94, 97,101,103,107,109,
113,118,127,129,131,133,134,137,139,141,149,151,157,158,161,163,
166,167,173,177,179,181,191,193,197,199,201,206,209,211,213,214,
217,227,233,237,239,241,249,251,253,262,263,269,271,277,278,281,
283,293,301,302,307,309,311,313,317,329,331,334,337,341,347,349,
353,358,367,373,379,381,382,383,389,393,397,398,409,413,417,419,
421,422,431,433,437,446,449,453,454,457,461,463,467,478,479,487,
489,491,497,501,502,503,509,517,521,523,526,537,541,542,547,553,
557,563,566,569,571,573,581,587,589,593,597,599,601,607,613,614,
617,619,622,631,633,641,643,647,649,653,661,662,669,673,677,681,
683,691,694,701,709,713,717,718,719,721,734,737,739,743,749,751,
753,757,758,766,769,773,781,787,789,797,809,811,813,821,823,827,
829,838,849,853,857,859,862,863,869,877,878,881,883,886,887,889,
893,907,911,913,917,919,921,926,929,933,937,941,947,953,958,967,
971,973,974,977,983,989,991,997,998.
```

Gauß has conjectured that there are infinitely many real-quadratic number fields with class number 1. The table seems to support this. However, the conjecture is still open, as of April 2021.

It is also interesting to compute class number for cyclotomic number fields $K = \mathbb{Q}(\zeta_n)$. As we have mentioned in the introduction, one can show that $x^n + y^n = z^n$ for $n > 2$ has no nontrivial integer solutions, if the class number of $\mathbb{Q}(\zeta_n)$ is equal to 1. Unfortunately this is only true for small n, see [**9**].

Proposition 4.3.7 (Montgomery, Masley 1976). *Let $n \not\equiv 2 \mod 4$. The class number of $\mathbb{Q}(\zeta_n)$ is equal to 1 if and only if*

$$\begin{aligned} n = {} & 1,3,4,5,7,8,9,11,12,13,15,16,17,19,20,21,24,25,27,28,\\ & 32,33,35,36,40,44,45,48,60,84. \end{aligned}$$

For $n \equiv 2 \mod 4$ the class number of $\mathbb{Q}(\zeta_n)$ is equal to 1 if and only if

$$n = 2,6,10,14,18,22,26,30,34,38,42,50,54,66,70,90.$$

In the second case, n is even, so that $\mathbb{Q}(\zeta_{n/2}) = \mathbb{Q}(\zeta_n)$. For $n = p$ be a prime number, the class number of $\mathbb{Q}(\zeta_p)$ is equal to 1 if and only if $p \leq 19$.

Remark 4.3.8. A prime number p is called *regular*, if it doesn't divide the class number of $\mathbb{Q}(\zeta_p)$. These prime numbers are important, because one can show Fermat's Last Theorem for them with an easy argument. Unfortunately, many primes are irregular. K.L. Jensen showed in 1915 that there are infinitely many irregular primes. There are even infinitely many irregular primes of the form $4n + 3$. Here is a table of all irregular primes p with $p \leq 2000$.

```
37,59,67,101,103,131,149,157,233,257,263,271,283,293,307,311,347,
353,379,389,401,409,421,433,461,463,467,491,523,541,547,557,577,
587,593,607,613,617,619,631,647,653,659,673,677,683,691,727,751,
757,761,773,797,809,811,821,827,839,877,881,887,929,953,971,1061,
1091,1117,1129,1151,1153,1193,1201,1217,1229,1237,1279,1283,1291,
1297,1301,1307,1319,1327,1367,1381,1409,1429,1439,1483,1499,1523,
1559,1597,1609,1613,1619,1621,1637,1663,1669,1721,1733,1753,1759,
1777,1787,1789,1811,1831,1847,1871,1877,1879,1889,1901,1933,1951,
1979,1987,1993,1997
```

Note that p is regular if and only if the class number of $\mathbb{Q}(\zeta_p))$ has no p-torsion. It is conjectures that there are also infinitely many regular primes. More precisely, Carl Ludwig Siegel conjectured in 1964, that $e^{-1/2}$, or roughly 60.65% of all primes are regular, asymptotically with respect to the natural density. These conjectures are still open.

The is a criterion by *Kummer*, which says, that a prime p is irregular if and only if it divides the nominator of a Bernoulli number B_k for $k = 2, 4, 6, \ldots, p-3$. Here

$$B_k = -k\zeta(1-k)$$

for $k = 2, 4, 6, \ldots$, and $B_{2k+1} = 0$. We have

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

The following table shows, that $p = 37, 59, 67, 101, 103, 131$ are irregular.

p	$h_{\mathbb{Q}(\zeta_p)}$
37	37
59	$41241 = 3 \cdot 59 \cdot 233$
67	$853513 = 67 \cdot 12739$
101	$3547404378125 = 5 \cdot 101 \cdot 601 \cdot 18701$
103	$9069094643165 = 5 \cdot 103 \cdot 1021 \cdot 17247691$
131	$28496379729272136525 = 3^3 \cdot 5^2 \cdot 53 \cdot 131 \cdot 1301 \cdot 4673706701$

For all primes $p \leq 19$ we have $h_{\mathbb{Q}(\zeta_p)} = 1$, and for all positive integers $n \leq 22$ we have $h_{\mathbb{Q}(\zeta_n)} = 1$. The next table shows the class numbers $h_{\mathbb{Q}(\zeta_p)}$ for all prime numbers $p < 150$. These numbers grow exponentially with p.

p	$h_{\mathbb{Q}(\zeta_p)}$
2	1
3	1
5	1
7	1
11	1
13	1
17	1
19	1
23	3
29	8
31	9
37	37
41	121
43	211
47	695
53	4889
59	41241
61	76301
67	853513
71	3882809
73	11957417
79	100146415
83	838216959
89	13379363737
97	411322824001
101	3547404378125
103	9069094643165
107	63434933542623
109	161784800122409
113	1612072001362952
127	2604529186263992195
131	28496379729272136525
137	646901570175200968153
139	1753848916484925681747
149	687887859687174720123201

CHAPTER 5

Dirichlet's unit theorem

In this chapter we will prove Dirichlet's unit theorem. It is a structure theorem for the group of units $\mathcal{O}_K^\times$ of the ring of integers $\mathcal{O}_K$ of a number field K, which determines the rank of $\mathcal{O}_K^\times$. More precisely, if K has r real embeddings and s pairs of complex embeddings, then we have

$$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r+s-1} \times T,$$

where T is a finite cyclic group. The proof uses Minkowski theory.

Recall that every finitely generated abelian group A is of the form $A \simeq \mathbb{Z}^t \times A_{\mathrm{tors}}$, where $t \geq 0$ is the *rank* of A, and A_{tors} denotes the finite group of torsion elements.

Dirichlet's result has many applications in number theory. It shows, for example, that the solutions to Pell's equation $x^2 - dy^2 = 1$, for $d > 1$ squarefree, form a free abelian group of rank 1.

5.1. The group of units

The group of units $A^\times$ of a ring A consists of the invertible elements of A. In other words, a is a unit in A if there exists a $b \in A$ with $ab = 1$.

Definition 5.1.1. The unit group if a number field K is $\mathcal{O}_K^\times$, the unit group of its ring of integers.

Example 5.1.2. *Let $K = \mathbb{Q}(\sqrt{3})$. Then we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. The element $x = 2 + \sqrt{3}$ is a unit with inverse element $2 - \sqrt{3}$. On the other hand, $y = 1 + \sqrt{3}$ is not a unit. By Dirichlet's unit theorem we have*

$$\mathcal{O}_K^\times = \{\pm(2+\sqrt{3})^k \mid k \in \mathbb{Z}\}.$$

Indeed, we have $(2+\sqrt{3})(2-\sqrt{3}) = 1$, so that $2 + \sqrt{3}$ is a unit. On the other hand, $(1+\sqrt{3})(a+b\sqrt{3}) = 1$ has no integer solution. Hence $1 + \sqrt{3}$ is not a unit. This also follows from the next lemma, because $N(1+\sqrt{3}) = -2$.

Lemma 5.1.3. *An element $x \in K$ is a unit in the ring of integers $\mathcal{O}_K$, if and only if $x \in \mathcal{O}_K$ and $N(x) = \pm 1$.*

Proof. If x is a unit, then

$$1 = N(1) = N(xx^{-1}) = N(x)N(x)^{-1}.$$

Since $N(x) \in \mathbb{Z}$ this implies $N(x) = \pm 1$. Conversely, let $x \in \mathcal{O}_K$ with $N(x) = \pm 1$. For the characteristic polynomial of x we have

$$P_x(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with $n = [K : \mathbb{Q}]$, $a_{n-1} = -\mathrm{tr}_{K/\mathbb{Q}}(x)$ and $a_0 = (-1)^n N_{K/\mathbb{Q}}(x) = \pm 1$, see the remark after Definition 2.4.2. So we have

$$\pm x(x^{n-1} + \cdots + a_1) = 1.$$

Hence x is a unit. □

The torsion subgroup of $\mathcal{O}_K^\times$ is exactly the group of roots of unity contained in K. We denote this group by μ_K. For imaginary-quadratic fields there is a short direct proof as follows.

Lemma 5.1.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary-quadratic number field with squarefree $d < 0$. Then we have $\mathcal{O}_K^\times = \mu_K$, and this finite cyclic group is given as follows:*

$$\mu_K = \begin{cases} \mathbb{Z}/4 = \{\pm 1, \pm i\} & \text{if } d = -1, \\ \mathbb{Z}/6 = \{\pm 1, \pm \zeta_3, \pm \zeta_3^2\} & \text{if } d = -3, \\ \mathbb{Z}/2 = \{\pm 1\} & \text{otherwise.} \end{cases}$$

In particular we have $\mathcal{O}_K^\times = \{\pm 1\}$, except for $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3}) \cong \mathbb{Q}(\zeta_3)$.

Proof. An element $x = a + b\sqrt{d}$ is a unit in $\mathcal{O}_K$ if $N(x) = \pm 1$. For $d \not\equiv 1 \mod 4$ we have $\mathcal{O}_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, so that $N(x) = \pm 1$ is equivalent to the Diophantine equation

$$a^2 - b^2 d = \pm 1.$$

For $d \equiv 1 \mod 4$ we have $\mathcal{O}_K = \{a + b(1 + \sqrt{d})/2 \mid a, b \in \mathbb{Z}\}$, so that x then is a unit if and only if

$$(2a + b)^2 - b^2 d = \pm 4.$$

For $d < 0$ these equations have only finitely many integer solutions. So we have already shown that $\mathcal{O}_K^\times = \mu_K$. A primitive m-th root of unity lies in K if and only if $\mathbb{Q}(\zeta_m) \subseteq K$. In this case, $\varphi(m) \mid [K : \mathbb{Q}] = 2$, so that $m \mid 4$ or $m \mid 6$. So $\mathcal{O}_K^\times$ can only contain roots of unity ζ_m for $m = 1, 2, 3, 4, 6$. However, we can solve the above Diophantine equations directly. For $d \le -2$ we have $a^2 - b^2 d = \pm 1$, so that $b = 0$ and $a = \pm 1$. For $d = -1$ we obtain in addition $a = 0$ and $b = \pm 1$. The solutions of the second equation can be determined in the same way. For $d \le -7$ we obtain $b = 0$ and $a = \pm 1$. Note that $d = -5$ is not congruent to $1 \mod 4$. For $d = -3$ we obtain in addition the solutions $b = \pm 1$ and $(2a \pm 1)^2 = 1$, so altogether the following 6 solutions

$$(a, b) = (\pm 1, 0),\ (0, \pm 1),\ (1, -1),\ (-1, 1).$$

□

Remark 5.1.5. In the real-quadratic case both equations may have infinitely many solutions and we cannot compute all solutions so easily. On the other hand, the only real roots of unity are ±1, so that we always have $\mu_K = \{\pm 1\}$. Since we have $(r, s) = (2, 0)$, Dirichlet's theorem then implies that

$$\mathcal{O}_K^\times \simeq \mathbb{Z} \times \{\pm 1\}.$$

Theorem 5.1.6 (Dirichlet). *The group of units $\mathcal{O}_K^\times$ of a number field K is isomorphic to*

$$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r+s-1} \times \mu_K,$$

where μ_K is a finite cyclic group.

Proof. Let

$$L\colon K^\times \to \mathbb{R}^{r+s},\ x \mapsto (\log(|\sigma_1(x)|), \ldots, \log(|\sigma_{r+s}(x)|)),$$

be the *logarithmic* embedding, which is the composition of the canonical embedding $\sigma\colon K^\times \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ with the multiplicative absolute value function, and the logarithm. Obviously we have

$L(xy) = L(x) + L(y)$ for all x, y, so that L is a group homomorphism. However, by the absolute value function we loose injectivity. Therefore the kernel of L is nontrivial. We claim that

$$\ker(L_{|\mathcal{O}_K^\times}) \simeq \mu_K.$$

Let $B \subseteq \mathbb{R}^{r+s}$ be a compact subset and $B_L = L^{-1}(B) \cap \mathcal{O}_K^\times$. Since B is bounded, so are the absolute values $|\sigma_i(x)|$ for $x \in B_L$. Thus the coefficients of the characteristic polynomial of x are bounded. Since they are integers, there are only finitely many such x, so that B_L is a finite set. Hence $\ker(L_{|\mathcal{O}_K^\times})$ is a finite subgroup of $\mathcal{O}_K^\times$, and therefore a cyclic group of roots of unity. So we have $\ker(L_{|\mathcal{O}_K^\times}) \subseteq \mu_K$. However, for a root of unity ζ_m we have $|\sigma_i(\zeta_m)|^m = |\sigma_i(\zeta_m^m)| = 1$, so that $\log(\sigma_i(\zeta_m)) = 0$ and $\ker(L_{|\mathcal{O}_K^\times}) = \mu_K$.

Since B_L is finite, the image $L(\mathcal{O}_K^\times)$ is a discrete subgroup of $\mathbb{R}^{r+s}$. So $L(\mathcal{O}_K^\times)$ is a free $\mathbb{Z}$-module of rank $t \leq r+s$ and

$$\mathcal{O}_K^\times \simeq L(\mathcal{O}_K^\times) \times \mu_K.$$

The proof is finished if we show that $t = r+s-1$, i.e., that the image is a lattice in a hyperplane of $\mathbb{R}^{r+s}$. It is easy to see that $t \leq r+s-1$. Indeed, $L(\mathcal{O}_K^\times)$ lies in the hyperplane

$$H := \left\{ (y_1, \ldots, y_{r+s}) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r} y_i + 2 \sum_{j=r+1}^{r+s} y_j = 0 \right\}$$

of codimension 1: for $x \in \mathcal{O}_K^\times$ we always have

$$\pm 1 = N(x) = \left(\prod_{i=1}^{r} \sigma_i(x) \right) \cdot \left(\prod_{j=r+1}^{r+s} \sigma_j(x) \overline{\sigma_j(x)} \right).$$

Taking the absolute value and the logarithm yields the claim.

So we are left to show the second inequality $t \geq r+s-1$, i.e., to show that $L(\mathcal{O}_K^\times) = H$. We may reformulate this as follows. Every linear form vanishing on $L(\mathcal{O}_K^\times)$ also vanishes on H. So for each nonzero $\mathbb{R}$-linear map $f \colon H \to \mathbb{R}$ we have to find a unit $u \in \mathcal{O}_K^\times$ with $f(L(u)) \neq 0$. We identify an element $(y_1, \ldots, y_{r+s}) \in H$ with $(y_1, \ldots, y_{r+s-1}) \in \mathbb{R}^{r+s-1}$. Then we write

$$f(y_1, \ldots, y_{r+s-1}) = c_1 y_1 + \cdots + c_{r+s-1} y_{r+s-1}$$

with $c_i \in \mathbb{R}$. For a given tuple of positive real numbers

$$\lambda = (\lambda_1, \ldots, \lambda_{r+s})$$

with

$$\alpha := \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 \geq 2^n (2\pi)^{-s} \sqrt{|d_K|}$$

we define a compact, convex and centrally symmetric set

$$B_\lambda = \{y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid |y_i| \leq \lambda_i,\ |z_j| \leq \lambda_{j+r}\}.$$

The volume of this set is given by

$$\begin{aligned} \operatorname{vol}(B_\lambda) &= \left(\prod_{i=1}^{r} 2\lambda_i \right) \cdot \left(\prod_{j=r+1}^{r+s} \pi \lambda_j^2 \right) \\ &= 2^r \pi^s \alpha \\ &\geq 2^{n-s} \sqrt{|d_K|}. \end{aligned}$$

Now by the lattice point theorem of Minkowski and Corollary 4.2.4 there exists an $x_\lambda \in \mathcal{O}_K$ with $\sigma(x_\lambda) \in B_\lambda$. We have $|\sigma_i(x_\lambda)| \leq \lambda_i$ for the real embeddings, and also for the conjugate pairs of complex embeddings, because of $|\sigma_j(x_\lambda)\sigma_{j+1}(x_\lambda)| = |\sigma_j(x_\lambda)\overline{\sigma_j(x_\lambda)}| = |\sigma_j(x_\lambda)|^2 \leq \lambda_j^2$. So we obtain

$$1 \leq |N_{K/\mathbb{Q}}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r} \lambda_i \prod_{j=r+1}^{r+s} \lambda_j^2 = \alpha$$

and therefore

$$|\sigma_i(x_\lambda)| = |N_{K/\mathbb{Q}}(x_\lambda)| \prod_{j\neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j\neq i} |\sigma_j(x_\lambda)|^{-1} \geq \frac{\lambda_i}{\alpha}.$$

In summary, we have

$$\lambda_i \alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i,$$

and taking the logarithm yields

$$0 \leq \log(\lambda_i) - \log(|\sigma_i(x_\lambda)|) \leq \log(\alpha).$$

Now for the given $f \in \operatorname{Hom}(H, \mathbb{R})$ we obtain

$$\begin{aligned} \left| f(L(x_\lambda)) - \sum_{i=1}^{r+s-1} c_i \log(\lambda_i) \right| &\leq \left| \sum_{i=1}^{r+s-1} c_i \big(\log(|\sigma_i(x_\lambda)|) - \log(\lambda_i)\big) \right| \\ &\leq \left(\sum_{i=1}^{r+s-1} |c_i| \right) \log(\alpha). \end{aligned}$$

Now let $\beta \geq \left(\sum_{i=1}^{r+s-1} |c_i|\right) \log(\alpha)$. For $h \in \mathbb{N}$ let $\lambda_{i,h}$ be positive real numbers for $i = 1, \ldots, r+s-1$, so that

$$\sum_{i=1}^{r+s-1} c_i \log(\lambda_{i,h}) = 2\beta h,$$

and choose $\lambda_{r+s,h} > 0$ so that

$$\prod_{i=1}^{r} \lambda_{i,h} \prod_{j=r+1}^{r+s} \lambda_{j,h}^2 = \alpha.$$

With $\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r+s,h})$ and $x_h := x_{\lambda(h)}$ we obtain for f by the above estimate

$$|f(L(x_h)) - 2\beta h| < \beta,$$

and therefore

$$(2h-1)\beta < f(L(x_h)) < (2h+1)\beta.$$

So we have $\beta < f(L(x_1)) < 3\beta < f(L(x_2)) < 5\beta < f(L(x_3)) < \cdots$, so that all values $f(L(x_h))$ are pairwise distinct for $h \in \mathbb{N}$. Consider the principal ideals $(x_h) \subseteq \mathcal{O}_K$. Because of $|N((x_h))| \leq \alpha$ there are only finitely many different ideals of the form (x_h), see the proof of Corollary 4.2.8. Hence there are different positive integers h_1 and h_2 with $(x_{h_1}) = (x_{h_2})$. Thus we have $(x_{h_1}^{-1} x_{h_2}) = \mathcal{O}_K$, so that $u = x_{h_1}^{-1} x_{h_2}$ is a unit. We obtain $f(L(u)) = f(L(x_{h_2})) - f(L(x_{h_1})) \neq 0$, and we are done. □

Remark 5.1.7. Dirichlet's unit theorem yields a short exact sequence of abelian groups

$$0 \to \mu_K \to \mathcal{O}_K^\times \to L(\mathcal{O}_K^\times) \to 0$$

with $L(\mathcal{O}_K^\times) \simeq \mathbb{Z}^{r+s-1}$. Choosing a $\mathbb{Z}$-basis $\overline{\varepsilon_1}, \dots, \overline{\varepsilon_{r+s-1}}$ of $L(\mathcal{O}_K^\times)$, the preimages $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ in $\mathcal{O}_K^\times$ are called a *system of fundamental units*. Every unit $\varepsilon \in \mathcal{O}_K$ has a unique representation

$$\varepsilon = \zeta \cdot \varepsilon_1^{n_1} \cdots \varepsilon_{r+s-1}^{n_{r+s-1}}$$

with a root of unity ζ in K and $n_i \in \mathbb{Z}$.

Example 5.1.8. *For a real-quadratic number field $K = \mathbb{Q}(\sqrt{d})$ we have $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \mathbb{Z}$, and every unit is of the form $\pm\varepsilon^k$ for a fundamental unit ε and $k \in \mathbb{Z}$.*

With ε also all $\pm\varepsilon^{\pm 1}$ are fundamental units. There is a convention to consider a unique fundamental unit for $K = \mathbb{Q}(\sqrt{d})$ by fixing an embedding

$$\sigma \colon K \hookrightarrow \mathbb{R}.$$

Then there is a *unique* fundamental unit ε with $\sigma(\varepsilon) > 0$. Let us call this *the* fundamental unit of K.

Let $d \not\equiv 1 \mod 4$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and the units in $\mathcal{O}_K^\times$ are given by $a + b\sqrt{d}$, where (a, b) are the integer solutions of the Pell equation $a^2 - db^2 = \pm 1$. Because of $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \mathbb{Z}$ these solutions are given by the fundamental unit $\varepsilon = a_1 + b_1\sqrt{d}$, namely by all pairs (a_n, b_n) with

$$a_n + b_n\sqrt{d} = \varepsilon^n = (a_1 + b_1\sqrt{d})^n.$$

A similar result holds for the case $d \equiv 1 \mod 4$ and a slightly different Pell equation. One can compute the fundamental unit for $\mathbb{Q}(\sqrt{d})$ by using continued fractions for $\sqrt{d}$. The following table lists some examples. The fundamental unit can be quite large even for small d.

d	ε
2	$1 + \sqrt{2}$
3	$2 + \sqrt{3}$
7	$8 + 3\sqrt{7}$
31	$1520 + 273\sqrt{31}$
46	$24335 + 3588\sqrt{46}$
94	$2143295 + 221064\sqrt{94}$
151	$1728148040 + 140634693\sqrt{151}$
331	$2785589801443970 + 153109862634573\sqrt{331}$
571	$181124355061630786130 + 7579818350628982587\sqrt{571}$

Let us compute the fundamental unit of $\mathbb{Q}(\sqrt{9199})$ by using PARI GP. The discriminant is given by $4 \cdot 9199$, since $9199 \equiv 3 \mod 4$.

```
? quadunit(4*9199)

%1 = 1053344927816119107196375157694929519417266
955491964582169476720418214485349747839063034640 +

109824769111439370223410310039186819141537351326
52023268221576527593244593149235240351449*sqrt(9199).
```

5.2. Analytic class number formula

If $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ in $\mathcal{O}_K^\times$ is a system of fundamental units for the number field K, then one defines the regulator of K by the volume of the full rank lattice $L(\mathcal{O}_K^\times)$ in $\mathbb{R}^{r+s-1}$.

Definition 5.2.1. Let $\mathcal{O}_K^\times$ be the group of units of a number field K and $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ in $\mathcal{O}_K^\times$ by a system of fundamental units. Then

$$R = |\det((\log|\sigma_i(\varepsilon_j)|)_{i,j=1}^{r+s-1})|$$

is called the *regulator* of K.

Example 5.2.2. *The regulator of an imaginary-quadratic number field is $R = 1$, and the regulator of a real-quadratic number field is $R = \log(|\varepsilon|)$, where ε is the fundamental unit.*

Indeed, the determinant of a 0×0-matrix is 1. Let us change the notation (r, s) for the field embeddings to (r_1, r_2) with $[K : \mathbb{Q}] = r_1 + 2r_2$. Then we can use s as a complex variable, as usual.

Definition 5.2.3. Let K be a number field and $s \in \mathbb{C}$ with $\Re(s) > 1$. Then

$$\zeta_K(s) := \sum_{I \subseteq \mathcal{O}_K} \frac{1}{N(I)^s}$$

is called the *Dedekind zeta function*.

For $K = \mathbb{Q}$ we obtain

$$\zeta_{\mathbb{Q}}(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s},$$

which is the *Riemann zeta function*, since I runs through the set of ideals (n) for $n \in \mathbb{N}$. Both $\zeta(s)$ and $\zeta_K(s)$ converge absolutely and locally uniformly for $\Re(s) > 1$. There is a holomorphic continuation to $\mathbb{C} \setminus \{1\}$ and there exists an Euler product

$$\zeta_K(s) = \prod_{P \in \operatorname{Spec}(\mathcal{O}_K)} \frac{1}{1 - \frac{1}{N(P)^s}}.$$

Also, $\zeta_K(s)$ has a functional equation

$$\zeta_K(1-s)\Gamma\left(\frac{1-s}{2}\right)^{r_1} \Gamma(1-s)^{r_2} = \zeta_K(s)\Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} (4^{-r_2}\pi^{-n}|d_K|)^{s-1}.$$

This can be used to show the holomorphic continuation to $\mathbb{C} \setminus \{1\}$and to show that $\zeta_K(s)$ has a simple pole at 1. We can compute the residue

$$\operatorname{res}_{s=1}\zeta_K(s) = \lim_{s \to 1}(s-1)\zeta_K(s).$$

It gives a formula for the class number h of K.

Theorem 5.2.4 (Analytic class number formula). *Let K be a number field with class number h and with r_1 real and r_2 complex embeddings. Denote by $w = w_K$ the number of roots of unity in K, and by R the regulator of K. Then we have*

$$\operatorname{res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R \cdot h}{w\sqrt{|d_K|}}.$$

This formula is widely used for the computation of the class number h. Indeed, all other terms of the formula can be computed more easily than h itself.

One can specialize this formula for quadratic number fields and cyclotomic fields. Let $\chi(n) = (d_K/n)$ be the quadratic Dirichlet character, given by the Legendre symbol. Then

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

is the L-series attached to χ. This series has a holomorphic continuation to $\mathbb{C}$. This yields $\zeta_K(s) = \zeta(s)L(s,\chi)$ and the following class number formula.

Corollary 5.2.5. *Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary–quadratic number field with discriminant d_K, class number h, and denote by w the number of roots of unity in K, i.e., $w = 2, 4, 6$. Then we have*

$$h = \frac{w\sqrt{|d_K|}}{2\pi} L(1,\chi).$$

Example 5.2.6. *For $K = \mathbb{Q}(i)$ we have $h = 1$.*

Indeed, then we have $w = 4$, $|d_K| = 4$, and $L(1,\chi)$ is the Leibniz series

$$L(1,\chi) = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \cdots = \frac{\pi}{4}.$$

So the formula in Corollary 5.2.5 yields

$$h = \frac{4 \cdot 2}{2\pi} L(1,\chi) = 1.$$

Let us take a more interesting example. Let $K = \mathbb{Q}(\sqrt{-15})$. This is the imaginary-quadratic number field with the smallest discriminant with class number $h > 1$.

Example 5.2.7. *For $K = \mathbb{Q}(\sqrt{-15})$ we have $h = 2$.*

Indeed, we have $w = 2$, $d_K = -15$, so that $h = \frac{\sqrt{15}}{\pi} L(1,\chi)$. Since

$$L(1,\chi) = \frac{2\pi}{\sqrt{15}} \sim 1.62231147038944475878 1184308$$

we obtain $h = 2$. Note that we only need an approximate value, since h is a positive integer.

In the real-quadratic case we obtain the following formula.

Corollary 5.2.8. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real-quadratic number field with discriminant d_K, class number h and fundamental unit ε. Then we have*

$$h = \frac{\sqrt{d_K}}{2\log(|\varepsilon|)} L(1,\chi).$$

Example 5.2.9. *For $K = \mathbb{Q}(\sqrt{5})$ we have $h = 1$.*

Indeed, we have $d_K = 5$, $\varepsilon = (1+\sqrt{5})/2$, and

$$\begin{aligned} L(1,\chi) &= \sum_{n=1}^{\infty} \left(\frac{1}{5n+1} - \frac{1}{5n+2} - \frac{1}{5n+3} + \frac{1}{5n+4} \right) \\ &= \int_0^1 (1-x-x^2+x^3)(1+x^5+x^{10}+x^{15}+\cdots)dx \\ &= \int_0^1 \frac{1-x-x^2+x^3}{1-x^5} dx \\ &= 0.4304089410\cdots \end{aligned}$$

Hence we obtain

$$h = \frac{\sqrt{5}}{2\log(\frac{1+\sqrt{5}}{2})} \cdot L(1,\chi) = 1.$$

CHAPTER 6

Splitting and ramification

Prime ideals in $\mathbb{Z}$ may not remain prime in extensions of $\mathbb{Z}$. For example, the ideals (2) and (3) are no longer prime in $\mathbb{Z}[\sqrt{-5}]$. See the example below for details. We study here prime ideals in rings of integers, or more generally in Dedekind domains, where we have a unique factorization of ideals in prime ideals. Given a prime ideal $\mathfrak{p}$ in a ring of integers $\mathcal{O}_K$ of a number field, and given an extension L/K of number fields, one considers the ideal $\mathfrak{p}$ as $\mathfrak{p}\mathcal{O}_L$ in the ring of integers $\mathcal{O}_L$ of L. Then the question is, how the ideal decomposes as product of prime ideals in $\mathcal{O}_L$. We have the decomposition

$$\mathfrak{p}\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$$

with different prime ideals P_i in $\mathcal{O}_L$ with exponents $e_i \geq 1$. If there is only one prime ideal in this decomposition with exponent 1, so $\mathfrak{p}\mathcal{O}_L$ is again a prime ideal in $\mathcal{O}_L$. Then $\mathfrak{p}$ is called *inert*. In general however, $\mathfrak{p}\mathcal{O}_L$ may "split" into several prime ideals, and it depends on how this splitting looks like. We will call $\mathfrak{p}$ *ramified*, $e_i \geq 2$ for some exponent.

We will study these decompositions in general for number field extensions L/K and their rings of integers. In case this extension is Galois, the situation becomes much easier. This is the case, for example, for quadratic number fields, i.e., for $[L : K] = 2$ with $K = \mathbb{Q}$. Then every prime ideal $\mathfrak{p}$ is of the form (p) for a rational prime p, and we have

$$\sum_{i=1}^{r} e_r \leq [L : K] = 2$$

for the exponents in the decomposition of $(p) = p\mathcal{O}_L$ in $\mathcal{O}_L$. So there are at most two exponents and we have, up to ordering, only three different cases:

$$\begin{aligned} &e_1 = 2, && \text{if } p\mathcal{O}_L = P^2 \text{ ramifies} \\ &e_1 = 1, e_2 = 1, && \text{if } p\mathcal{O}_L = P_1P_2 \text{ splits} \\ &e_1 = 1, && \text{if } p\mathcal{O}_L = P \text{ is inert} \end{aligned}$$

We will see in Proposition 6.2.7, that the splitting behavior of prime ideals (p) in quadratic number fields $\mathbb{Q}(\sqrt{d})$ is determined by the Legendre symbol (d/p). For example, a prime number $p > 2$ is inert if and only if $(d/p) = -1$, that is, if d and p are coprime and if d is not a square modulo p.

Example 6.0.1. *Let $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$ and $L = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$.*

(a) *For $\mathfrak{p} = (2)$ we have that $\mathfrak{p}\mathcal{O}_L = P^2$ ramifies.*
(b) *For $\mathfrak{p} = (3)$ we have that $\mathfrak{p}\mathcal{O}_L = P_1P_2$ splits.*
(c) *For $\mathfrak{p} = (11)$ we have that $\mathfrak{p}\mathcal{O}_L$ is inert.*

Indeed, we have $(2) = P^2$ with the prime ideal $P = (2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$, see Example 4.2.10. Furthermore we have $(3) = P_1P_2$ with the prime ideals $P_1 = (3, 1 + 2\sqrt{-5})$ and

$P_2 = (3, 1 - 2\sqrt{-5})$ in $\mathcal{O}_L$, see Example 3.2.14. Since we have

$$\left(\frac{-5}{11}\right) = -1,$$

it follows that -5 is not a square modulo 11. Hence (11) is inert, i.e., it stays prime in $\mathbb{Z}[\sqrt{-5}]$, see Proposition 6.2.7.

6.1. Localization

Let us review a few facts on localization's from commutative algebra. A subset $S \subset R$ of a ring R is called *multiplicatively closed*, if $1 \in S$ and $a, b \in S$ imply that $ab \in S$. For prime ideals this can be formulated as follows. An ideal P in R is prime, if $R \setminus P$ is multiplicatively closed. With such a set S we can form the ring of fractions $S^{-1}R$, which is called the *localization* of R, see Definition 1.2.11 in [**1**].

Example 6.1.1. *Let R be an integral domain. Then $S = R \setminus 0$ is a multiplicatively closed subset and $S^{-1}R = \mathrm{Quot}(R)$ is the quotient field of R.*

Example 6.1.2. *Let R be an integral domain and $\mathfrak{p}$ be a prime ideal in R. Then $S = R \setminus \mathfrak{p}$ is a multiplicatively closed set and $R_{\mathfrak{p}} := S^{-1}R$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.*

For details see Example 1.2.13 in [**1**]. We will need the following results on localization's.

Proposition 6.1.3. *The prime ideals P of the localization $S^{-1}R$ are in bijective correspondence to prime ideals $\mathfrak{p}$ in R, which do not meet S, i.e., with $\mathfrak{p} \cap S = \emptyset$.*

For a proof see Proposition 1.2.22, (4) in [**1**].

Proposition 6.1.4. *Let R be a Noetherian ring and S be a multiplicatively closed subset of R. Then the localization $S^{-1}R$ is again a Noetherian ring.*

For a proof see Proposition 1.3.5 in [**1**].

Proposition 6.1.5. *Let R be an integral domain, $A \subseteq R$ be a subring, $S \subseteq A$ be a multiplicatively closed subset, and B the integral closure of A in R. Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in $S^{-1}R$.*

For a proof see Lemma 4.2.8 in [**1**].

Corollary 6.1.6. *The localization of a Dedekind ring is again a Dedekind ring.*

Proof. Let A be a Dedekind ring. Then $S^{-1}A$ is a Noetherian ring by Proposition 6.1.4 and has Krull dimension 1 by Proposition 6.1.3. By Proposition 6.1.5, $S^{-1}A$ is integrally closed. Hence it is a Dedekind ring. □

Finally we have the following result.

Proposition 6.1.7. *Let R be an integral domain, $S \subseteq R$ be a multiplicatively closed subset, and $\mathfrak{m} \subseteq R$ be a maximal ideal in R with $\mathfrak{m} \cap S = \emptyset$. Then we have*

$$S^{-1}R/\mathfrak{m}S^{-1}R \simeq R/\mathfrak{m}$$

6.2. Degree theorem

We want to study the prime decomposition of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ in the ring $\mathcal{O}_L$ for a number field extension L/K. It turns out to be useful to consider a more general situation here.

Let $\mathfrak{p}$ be a prime ideal in a Dedekind ring A with $\mathrm{Quot}(A) = K$ and L/K be a finite field extension. Then we study the prime decomposition of $\mathfrak{p}$ as an ideal in B, which is the integral closure of A.

$$\begin{tikzcd}
L \arrow[r, phantom, "\supseteq"] \arrow[d] & B \arrow[d] & \mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r} \arrow[d] \\
K \arrow[r, phantom, "\supseteq"] & A & \mathfrak{p}
\end{tikzcd}$$

The case $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$ then is a special case. In general it follows that B is a Dedekind ring with $\mathrm{Quot}(B) = L$. We only prove it here for separable extensions.

Proposition 6.2.1. *Let A be a Dedekind ring with quotient field K, and let L be a finite, separable field extension of K. Then the integral closure B of A in L is a Dedekind ring with quotient field L.*

Proof. Since A is Noetherian, also B is Noetherian by Proposition 2.4.13, provided that $L \mid K$ is separable. Furthermore the integral closure is always integrally closed in an algebraic extension of of its quotient field. Indeed, if C is the integral closure of B in L, then C is integral over B, and B is integral over A, hence C is integral over A by transitivity, see Corollary 2.1.12. So we have $C \subseteq B$, and B is integrally closed. By Proposition 2.3.4 we have $\dim(B) = \dim(A) = 1$. Finally, $\mathrm{Quot}(B) = L$ by Corollary 2.2.9. □

So let A be a Dedekind ring with $\mathrm{Quot}(A) = K$, and L/K be a separable, finite field extension. Let B be the integral closure of A in L. Then every prime ideal $\mathfrak{p}$ of A has a factorization in B

$$\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$$

with different prime ideals P_i in B. We have $\mathfrak{p} \subseteq \mathfrak{p}B \subseteq P_i$, hence $P_i \mid B\mathfrak{p}$ in the sense of divisibility of ideals in Dedekind rings.

Lemma 6.2.2. *For nonzero prime ideals $\mathfrak{p}$ of A and P of B the following statements are equivalent.*

(1) *P lies over $\mathfrak{p}$, so $P \cap A = \mathfrak{p}$.*
(2) *$\mathfrak{p}B \subseteq P$.*
(3) *$P \mid \mathfrak{p}B$.*

Proof. (1) ⇒ (2): by assumption we have $\mathfrak{p} \subseteq P$, hence $\mathfrak{p}B \subseteq PB \subseteq P$.

(2) ⇔ (3): $I \mid J$ by definition is equivalent to $I \supseteq J$. Then there exists an ideal I' with $J = II'$.

(2) ⇒ (1): by assumption we have $\mathfrak{p} \subseteq P \cap A$. Since $\mathfrak{p}$ is a maximal ideal by Proposition 3.1.2, and $1 \notin P$, we obtain $P \cap A \neq A$ and $P \cap A = \mathfrak{p}$. □

For convenience we will always assume here that prime ideals are nonzero.

Lemma 6.2.3. *Let $\mathfrak{p}$ be a prime ideal of A, and P be a prime ideal of B lying over $\mathfrak{p}$. Then the canonical map $A/\mathfrak{p} \hookrightarrow B/P$ is an embedding of fields and B/P is a finite dimensional $A/\mathfrak{p}$-vector space.*

Proof. Because of $\mathfrak{p} = P \cap A$ the embedding $A \hookrightarrow B$ induces a map $A/\mathfrak{p} \to B/P$, $a + \mathfrak{p} \mapsto a + P$, which is a well-defined injective homomorphism of fields. Indeed, since B is by Proposition 2.4.13 a finitely generated A-module, B/P is a finitely generated $A/\mathfrak{p}$-module. Since both P and $\mathfrak{p}$ are maximal ideals, both quotients are fields. A finitely generated K-module for a field K just is a finite-dimensional K-vector space. □

Definition 6.2.4. Let $\mathfrak{p}$ be a prime ideal in A and

$$\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$$

be the prime ideal decomposition of $\mathfrak{p}B$ in B.

(1) The number $e_i = e(P_i/\mathfrak{p})$ is called the *ramification index* of P_i over $\mathfrak{p}$.
(2) The number $f_i = f(P_i/\mathfrak{p}) = [B/P_i : A/\mathfrak{p}]$ is called the *residue class degree* of P_i over $\mathfrak{p}$.
(3) $\mathfrak{p}$ is called *ramified*, if either $e_i \geq 2$ for some $i = 1, \dots, r$, or B/P_i is an inseparable extension of $A/\mathfrak{p}$ for some i.
(4) $\mathfrak{p}$ is called *totally ramified*, if $\mathfrak{p}$ is ramified and $f_i = 1$ for all $i = 1, \dots, r$.
(5) $\mathfrak{p}$ is called *non-split*, if $r = 1$, i.e., if there is only one prime ideal P over $\mathfrak{p}$.
(6) $\mathfrak{p}$ is called *inert*, if $r = 1$ and $e_1 = 1$, i.e., if $\mathfrak{p}B$ is a prime ideal in B.
(7) $\mathfrak{p}$ is called *completely split*, if $e_i = f_i = 1$ for all $i = 1, \dots, r$. In other words, if for every prime ideal P_i over $\mathfrak{p}$ we have $B/P_i = A/\mathfrak{p}$.

Note that the negation of (3) says that $\mathfrak{p}$ is *unramified*, if both $e_i = 1$ for all i *and* all field extensions B/P_i over $A/\mathfrak{p}$ are separable. In the case of rings of integers $B = \mathcal{O}_L$ and $A = \mathcal{O}_K$ these residue class fields are already *finite*, and therefore the extensions are never inseparable. So we may drop this condition in the definition of "ramified" for rings of integers.

We also can check that the names in Example 6.0.1 are consistent with the names from above. Let us now come to the degree theorem, which establishes a connection between the numbers e_i, f_i, r and $[L : K] = n$.

Theorem 6.2.5 (Degree Theorem). *Let A be a Dedekind ring with quotient field K and L be a finite separable field extension of K. Let B be the integral closure of A in L, and $\mathfrak{p}$ be a prime ideal in A with decomposition $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ in B. Then we have*

$$\sum_{i=1}^{r} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K].$$

Proof. By the CRT, the Chinese Remainder Theorem, we have

$$B/\mathfrak{p}B \simeq B/(P_1^{e_1} \cdots P_r^{e_r}) \simeq (B/P_1^{e_1}) \times \cdots \times (B/P_r^{e_r}).$$

Hence for the first equality it suffices to show $[B/P_i^{e_i} : A/\mathfrak{p}] = e_i f_i$. For each r_i we have that $P_i^{r_i}/P_i^{r_i+1}$ is a B/P_i-module. Since there lies no ideal between $P_i^{r_i}$ and $P_i^{r_i+1}$ we have $\dim_{B/P_i}(P_i^{r_i}/P_i^{r_i+1}) = 1$ as vector spaces over B/P_i. So we obtain

$$\dim_{A/\mathfrak{p}}(P_i^{r_i}/P_i^{r_i+1}) = f_i,$$

because $f_i = \dim_{A/\mathfrak{p}}(B/P_i)$. We obtain a chain of ideals

$$B \supseteq P_i \supseteq P_i^2 \supseteq \cdots \supseteq P_i^{e_i},$$

where each quotient $P_i^{r_i}/P_i^{r_i+1}$ has dimension f_i over $A/\mathfrak{p}$. Hence $B/P_i^{e_i}$ has dimension $e_i f_i$ over $A/\mathfrak{p}$.

To show that $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K] = n$ we first assume that A is a PID. Then B is a free A-module of rank n by Proposition 2.4.13. This yields an isomorphism $A^n \overset{\cong}{\to} B$, which induces an isomorphism $K^n \overset{\cong}{\to} L$ by tensoring with K. Tensoring by $A/\mathfrak{p}$ induces an isomorphism $(A/\mathfrak{p})^n \to B/\mathfrak{p}B$, so that $n = [B/\mathfrak{p}B : A/\mathfrak{p}]$.

Now we will reduce the general case to this case by localization. So let $S = A \setminus \mathfrak{p}$. This is a multiplicatively closed subset of A with local rings $A_\mathfrak{p} = S^{-1}A$ and $B_\mathfrak{p} = S^{-1}B$. By Proposition 6.1.3 the Krull dimension of $A_\mathfrak{p}$ is equal to 1, so that $A_\mathfrak{p}$ is a PID with maximal ideal $\mathfrak{p}A_\mathfrak{p}$. By Proposition 6.1.5, $B_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in L. Therefore $B_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of rank n, so that we obtain $[B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] = n$ as above. The factorization $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ yields by Proposition 6.1.3 and by using $P_i \cap S = \emptyset$ the factorization $\mathfrak{p}B_\mathfrak{p} = (P_1B_\mathfrak{p})^{e_1} \cdots (P_rB_\mathfrak{p})^{e_r}$. By Proposition 6.1.7 we obtain $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq A/\mathfrak{p}$ and $B_\mathfrak{p}/(P_iB_\mathfrak{p}) \simeq B/P_i$. Together we obtain

$$\begin{aligned} n &= [B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] \\ &= \sum_{i=1}^r e_i \cdot [B_\mathfrak{p}/(P_iB_\mathfrak{p}) : A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}] \\ &= \sum_{i=1}^r e_i \cdot [B/P_i : A/\mathfrak{p}] \\ &= \sum_{i=1}^r e_i f_i. \end{aligned}$$

□

Example 6.2.6. *Let $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $B = \mathcal{O}_L$, with $L = \mathbb{Q}(\sqrt{d})$. Then the degree theorem implies that we have only three possibilities for the indices. Hence a prime ideal (p) in $\mathbb{Z}$ has exactly the following possible factorizations as ideal in $\mathcal{O}_L$:*

$$\begin{aligned} p\mathcal{O}_L &= P^2, & r = 1, e_1 = 2, f_1 = 1, \\ p\mathcal{O}_L &= P_1P_2, & r = 2, e_1 = e_2 = f_1 = f_2 = 1 \\ p\mathcal{O}_L &= P, & r = 1, e_1 = 1, f_1 = 2. \end{aligned}$$

We can determine, which of the three cases holds for a given prime ideal (p).

Proposition 6.2.7. *Let $p > 2$ be a prime number in $\mathbb{Z}$ and $L = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with discriminant D.*

(a) *If $(D/p) = 0$, then $p\mathcal{O}_L = (p, \sqrt{d})^2$, and (p) is ramified.*
(b) *If $(D/p) = 1$, then $p\mathcal{O}_L = P_1P_2$ splits with two different prime ideals P_1 and P_2. So (p) splits.*
(c) *If $(D/p) = -1$, then $p\mathcal{O}_L = P$, and (p) is inert.*

Proof. In the first case we have $p \mid D$, and hence $p \mid d$ because of $p > 2$. Then we have

$$(p, \sqrt{d})^2 = (p^2, p\sqrt{d}, d) = (p)(p, \sqrt{d}, d/p) = (p),$$

because p and $\frac{d}{p}$ are coprime, so that $(p, \sqrt{d}, \frac{d}{p}) = (1) = \mathcal{O}_L$.

In the second case we have $D \equiv x^2 \mod p$ for some $x \in \mathbb{Z}$. With $P_1 = (p, x + \sqrt{d})$, $P_2 =$

$(p, x-\sqrt{d})$ we have

$$\begin{aligned} P_1P_2 &= (p^2, p(x \pm \sqrt{d}), x^2-d) \\ &= (p)(p, x \pm \sqrt{d}, (x^2-d)/p). \end{aligned}$$

Since $2\sqrt{d} = (x+\sqrt{d}) - (x-\sqrt{d})$, $4d = (2\sqrt{d})^2$ is contained in the second ideal. Since p and $4d$ are coprime , the second ideal is equal to (1) and we have $P_1P_2 = p\mathcal{O}_L$.

In the third case, assume that $p\mathcal{O}_L$ is not prime in $\mathcal{O}_L$. Then $p\mathcal{O}_L = Q_1Q_2$ with two prime ideals and $p^2 = N(p\mathcal{O}_L) = N(Q_1)N(Q_2)$ yields $N(Q_1) = N(Q_2) = p$. This is a contradiction to $(D/p) = -1$ as follows. Let Q be any prime ideal with $N(Q) = p$. Then we can write $Q = (p, a+\omega)$, with $a \in \mathbb{Z}$ and $\omega = \sqrt{d}$ or $\omega = (1+\sqrt{d})/2$, so that $p \mid N(a+\omega)$. Here $\{1, \omega\}$ is the usual integral basis for $\mathcal{O}_L = \mathbb{Z}[\omega]$. For $\omega = \sqrt{d}$ we obtain $a^2 - d \equiv 0 \mod p$, hence $(D/p) = (4d/p) = (d/p) = 1$, a contradiction. For $\omega = (1+\sqrt{d})/2$ we have $(2a+1)^2 \equiv d \mod p$, which is a again a contradiction. □

Remark 6.2.8. For the special case of $p = 2$ we can also find a criterion as in Proposition 6.2.7. In fact, for $d \equiv 2 \mod 4$ we have $2\mathcal{O}_L = (2, \sqrt{d})^2$, for $d \equiv 3 \mod 4$ we have $2\mathcal{O}_L = (2, 1+\sqrt{d})^2$, for $d \equiv 1 \mod 8$ we have $2\mathcal{O}_L = (2, (1+\sqrt{d})/2) \cdot (2, (1-\sqrt{d})/2)$, and for $d \equiv 5 \mod 8$, $2\mathcal{O}_L$ is prime.

With these results we can review Example 6.0.1, which is for $d = D = -5$.

(*a*) Because of $-5 \equiv 3 \mod 4$ the ideal $\mathfrak{p} = (2)$ is ramified, namely $2\mathcal{O}_L = P^2 = (2, 1+\sqrt{-5})^2$. So we have $e_1 = e(P \mid \mathfrak{p}) = 2$ and

$$f_1 = [\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) : \mathbb{Z}/2] = 1.$$

(*b*) Because of $\left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1$, the ideal $\mathfrak{p} = (3)$ splits with $3\mathcal{O}_L = P_1P_2$ and $e_1 = e_2 = 1$ and $f_1 = [\mathcal{O}_L/P_1 : \mathbb{Z}/3] = 1$, $f_2 = [\mathcal{O}_L/P_2 : \mathbb{Z}/3] = 1$, see also Example 3.2.14.

(*c*) Since $\left(\frac{-5}{11}\right) = -1$, the ideal $\mathfrak{p} = (11)$ stays prime in $\mathcal{O}_L$.

6.3. Decompositions in Galois extensions

Let A be a Dedekind ring with quotient field K and L/K be a finite extension, and B be the integral closure of A in L. A particular good case is when L/K is a *Galois extension.* Denote by G its Galois group. Then G acts on B, because for each element $b \in B$ and each $\sigma \in G$ the element $\sigma(b)$ is integral over A, hence belongs to $B = \overline{A}^L$. The Galois group also acts on the set of prime ideals P in B lying over an prime ideal $\mathfrak{p}$ of A. Indeed, $\sigma(P)$ is again a prime ideal in B for a prime ideal P, since σ induces an isomorphism $B/P \simeq B/\sigma(P)$ and therefore $B/\sigma(P)$ is again an integral domain. Moreover we have

$$\sigma(P) \cap A = \sigma(P \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p},$$

and $\sigma(P)$ lies again over $\mathfrak{p}$.

Definition 6.3.1. Let P in B be a prime ideal and $\sigma \in G = Gal(L/K)$. Then $\sigma(P)$ is called a *prime ideal conjugate to P.*

Proposition 6.3.2. *For each prime ideal $\mathfrak{p}$ of A, the Galois group G acts transitively on the set of prime ideals P of B lying over $\mathfrak{p}$. Hence each two prime ideals P and P' over $\mathfrak{p}$ of B are conjugated.*

Proof. We already have shown that G acts on the set of prime ideals of B lying over $\mathfrak{p}$. So we need to show the transitivity, namely that for each two prime ideals P and P' lying over $\mathfrak{p}$ there exists some $\sigma \in G$ with $P' = \sigma(P)$. Assume that we have $P' \neq \sigma(P)$ for all $\sigma \in G$. Then by the CRT there is an $x \in B$ with $x \equiv 0 \mod P'$ and $x \equiv 1 \mod \sigma(P)$ for all $\sigma \in G$. Thus

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in P' \cap A = \mathfrak{p} = P \cap A.$$

By assumption $x \notin \sigma(P)$ for all σ, hence $\sigma(x) \notin P$ for all σ, and therefore $\prod_{\sigma \in G} \sigma(x)$ is not in $P \cap A = \mathfrak{p}$. Since P is a prime ideal, $\prod_{\sigma \in G} \sigma(x) \in P$ implies that $\sigma(x) \in P$ for at least one σ. This is a contradiction. Hence the action is transitive. □

For Galois extensions we can simplify the degree theorem.

Theorem 6.3.3. *Let A be a Dedekind ring with quotient field K and L be a finite Galois extension of K. Let B be the integral closure of A in L, $\mathfrak{p}$ be a prime ideal in A with decomposition $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ in B. Then all ramification indices coincide and all residue degrees are equal, i.e., we have $e_i = e$ and $f_i = f$ for all $i = 1, \ldots, r$ and*

$$r \cdot e \cdot f = [B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K].$$

Proof. If P is a prime ideal in the factorization, then $P^k \mid \mathfrak{p}B$, so that $\sigma(P)^k \mid \sigma(\mathfrak{p}B) = \mathfrak{p}B$. Hence $\sigma(P)^k$ is again a factor in $\mathfrak{p}B$. By Proposition 6.3.2 there exists for each P_i some $\sigma \in G$ with $\sigma(P_i) = P_1$. Hence all e_i are equal to e_1. This σ then induces an isomorphism $B/P_1 \simeq B/P_i$, so that all f_i are equal to f_1. □

Remark 6.3.4. We already know that the indices are equal for quadratic number fields $L/\mathbb{Q}$. Indeed, quadratic extensions are automatically Galois extensions. So this is consistent with the above theorem.

Definition 6.3.5. Let P be a prime ideal of B and $G = Gal(L/K)$. Then

$$D_P := \{\sigma \in G \mid \sigma(P) = P\}$$

is called the *decomposition group* of P over K, and

$$Z_P := \{x \in L \mid \sigma(x) = x \ \ \forall\, \sigma \in D_P\}$$

is called the *decomposition field* of P in the extension L/K.

We have the following result.

Proposition 6.3.6. *Let A be a Dedekind ring with quotient field K, L/K be a finite Galois extension and B be the integral closure of A in L. Let $\mathfrak{p}$ be a prime ideal in A with decomposition $\mathfrak{p}B = P_1^{e_1} \cdots P_r^{e_r}$ in B. Then we have $r = (G : D_P)$, and for a prime ideal P over $\mathfrak{p}$ we have:*

(a) *$D_P = 1$ if and only if $Z_P = L$, so if $\mathfrak{p}$ is completely split.*
(b) *$D_P = G$ if and only if $Z_P = K$, so if $\mathfrak{p}$ is non-split.*
(c) *We have $D_{\sigma(P)} \simeq \sigma D_P \sigma^{-1}$ for all $\sigma \in G$.*

Proof. Since G acts transitively on the set $\mathcal{M}$ of prime ideals P of B lying over $\mathfrak{p}$, the map $G/D_P \to \mathcal{M}$, $\overline{\sigma} \mapsto \sigma P$ is a bijection. The set $\mathcal{M}$ has exactly r elements, and the statements are obvious. □

Definition 6.3.7. Let A be a Dedekind ring with quotient field K, L/K be a finite Galois extension and B be the integral closure der of A in L. Let $\mathfrak{p}$ be a prime ideal in A and P be a prime ideal in B lying over $\mathfrak{p}$.

(a) Denote by $k(P) = B/P$ and $k(\mathfrak{p}) = A/\mathfrak{p}$ the residue class fields.
(b) Denote by I_P the subgroup of D_P, given by

$$I_P = \{\sigma \in D_P \mid \sigma_{|k(P)} = \mathrm{id}\}.$$

It is called the *inertia group* of P in L/K.
(c) The fixed field $T_P = \{x \in L \mid \sigma(x) = x \;\; \forall\, \sigma \in I_P\}$ is called the *inertia field* of P in L/K.

Each $\sigma \in D_P$ satisfies $\sigma(P) \subseteq P$ and $\sigma(B) \subseteq B$ and hence induces an automorphism

$$\overline{\sigma}\colon k(P) = B/P \to B/P,\;\; x \mod P \mapsto \sigma(x) \mod P,$$

fixing $k(\mathfrak{p}) \subseteq k(P)$ elementwise. So we obtain an element $\overline{\sigma} \in \mathit{Gal}(k(P)/k(\mathfrak{p}))$, provided the field extension $k(P)/k(\mathfrak{p})$ is a Galois extension. However, this is not always the case. The extension is always normal, but it need not be separable in general. Of course, if $k(\mathfrak{p})$ is a *finite* field, it is separable. So in case of a Galois extension we obtain a map

$$\varphi\colon D_P \to \mathit{Gal}(k(P)/k(\mathfrak{p})),\; \sigma \mapsto \overline{\sigma}$$

with $\ker(\varphi) = I_P$.

Proposition 6.3.8. *Let A be a Dedekind ring with quotient field K, L/K be a finite Galois extension and B the integral closure of A in L. Let $\mathfrak{p}$ be a prime ideal in A and P be a prime ideal in B lying over $\mathfrak{p}$. Then the field extension $k(P)/k(\mathfrak{p})$ is normal.*

Proof. Let $y \in k(P)$ and choose an element $x \in B$ with $y \equiv x \mod P$. Let $p(t)$ be the minimal polynomial of x over K and $q(t)$ the minimal polynomial of y over $k(\mathfrak{p})$. For

$$\overline{p}(t) := p(t) \mod \mathfrak{p}$$

we have $\overline{p}(x) = 0$, hence $q(t) \mid p(t)$. Since L/K is normal, $p(t)$ splits into linear factors over L. Therefore also $\overline{p}(t)$ splits into linear factors over $k(P)$. Hence the same holds for $q(t)$ and the extension $k(P)/k(\mathfrak{p})$ is normal. □

Proposition 6.3.9. *Let A be a Dedekind ring with quotient field K, L/K be a finite Galois extension and B the integral closure of A in L. Let $\mathfrak{p}$ be a prime ideal in A and P be a prime ideal in B lying over $\mathfrak{p}$. Suppose that the extension $k(P)/k(\mathfrak{p})$ is separable. Then the map*

$$\varphi\colon D_P \to \mathit{Gal}(k(P)/k(\mathfrak{p}))$$

is a group homomorphism and we obtain a short exact sequence of groups

$$1 \to I_P \to D_P \xrightarrow{\varphi} \mathit{Gal}(k(P)/k(\mathfrak{p})) \to 1.$$

We have $\# I_P = e(P \mid \mathfrak{p})$, $\# D_P = e(P \mid \mathfrak{p}) f(P \mid \mathfrak{p})$ and

$$\mathit{Gal}(k(P)/k(\mathfrak{p})) \simeq D_P/I_P.$$

Proof. Let $e = e(P \mid \mathfrak{p})$ and $f = f(P \mid \mathfrak{p})$, and let r be the number of conjugates of P. Then by Theorem 6.3.3 we have

$$r = \frac{n}{\# D_P} = \frac{ref}{\# D_P},$$

and hence $\#D_P = ef$.

Let $E = T_P$ be the fixed field of D_P. By the fundamental theorem of Galois theory we have $Gal(L/E) \simeq D_P$. Define

$$\mathfrak{p}_E := P \cap (B \cap E).$$

By definition $\mathfrak{p}_E$ lies over $\mathfrak{p}$. The prime ideal P is fixed by all elements of D_P, hence the decomposition group of P in L/E is D_P. Therefore we have

$$ef = \#D_P = [L : E] = e(P \mid \mathfrak{p}_E) f(P \mid \mathfrak{p}_E) = e'f'.$$

For the tower of extensions $L/E/K$ the ramification degree and the residue degree are multiplicative, i.e., we have

$$\begin{aligned} e(P \mid \mathfrak{p}) &= e(P \mid \mathfrak{p}_E) \cdot e(\mathfrak{p}_E \mid \mathfrak{p}), \\ f(P \mid \mathfrak{p}) &= f(P \mid \mathfrak{p}_E) \cdot f(\mathfrak{p}_E \mid \mathfrak{p}). \end{aligned}$$

However, $ef = e'f'$ is equivalent to $e = e'$ and $f = f'$, since $e' \mid e$ and $f' \mid f$. This is equivalent to $e(\mathfrak{p}_E \mid \mathfrak{p}) = e/e' = 1$ and $f(\mathfrak{p}_E \mid \mathfrak{p}) = f/f' = 1$. In particular, the residue class fields $k(\mathfrak{p}_E)$ and $k(\mathfrak{p})$ are equal.

We will show that φ is surjective. By the primitive element theorem we have $k(P) = k(\mathfrak{p})(\overline{\alpha})$ for some $\alpha \in B$. Let $m \in (B \cap E)[t]$ be the monic minimal polynomial of α. It coincides with the characteristic polynomial of α. Therefore $\overline{m} \in k(\mathfrak{p}_E)[t]$ is a power of the minimal polynomial of $\overline{\alpha}$. Let $\overline{\sigma} \in Gal(k(P)/k(\mathfrak{p}_E))$, so that $\overline{\sigma}(\overline{\alpha})$ is a root of $\overline{m}$. Then there exists a $\sigma \in Gal(L/E) \simeq D_P$ with $\sigma(\alpha) = \overline{\sigma}(\overline{\alpha})$. It follows that $\overline{\sigma} = \varphi(\sigma)$, i.e., φ is surjective. Then it follows that

$$f = f(P \mid \mathfrak{p}_E) = \# \operatorname{im}(\varphi) = \frac{\#D_P}{\#I_P} = \frac{ef}{\#I_P},$$

so that $\#I_P = e$. □

Corollary 6.3.10. *A prime ideal $\mathfrak{p}$ of A is unramified in L/K if and only if $\#I_P = 1$ for a prime ideal P of B over $\mathfrak{p}$.*

We can consider a special case here, namely that for all prime ideals $\mathfrak{p} \neq 0$ in A the residue class field $k(\mathfrak{p}) = A/\mathfrak{p}$ is *finite*. Then $k(P)/k(\mathfrak{p})$ is a Galois extension, since finite fields are perfect. The Galois group of an extension of finite fields is cyclic, generated by the Frobenius automorphism.

Example 6.3.11. *Let L be a number field, and $B = \mathcal{O}_L$, $K = \mathbb{Q}$, $A = \mathbb{Z}$. Let P be a prime ideal over $\mathfrak{p} = (p)$ with a rational prime p. Then we have $k(\mathfrak{p}) = \mathbb{F}_p$, $k(P) = \mathcal{O}_L/P$ and*

$$Gal(k(P)/\mathbb{F}_p) \simeq \langle Frob_p \rangle,$$

with $Frob_p(x) = x^p$.

6.4. Ramification and discriminant

Let A be a PID and B/A be a ring extension so that B is a free A-module with basis $\{x_1, \dots x_n\}$. Then the discriminant of B/A is defined by

$$\mathcal{D}_{B/A} = (D(x_1, \dots, x_n)),$$

see Definition 2.4.9. In the special case $A = \mathbb{Z}$ and $B = \mathcal{O}_K$ with a number field K we call the positive generator of this ideal the *absolute discriminant d of K*. We have $d \in \mathbb{N}$ and the following important result.

Proposition 6.4.1. *Let K be a number field with absolute discriminant d, and p be a rational prime. Then the ideal $\mathfrak{p} = (p)$ is unramified in $K/\mathbb{Q}$, if and only if $p \nmid d$.*

Proof. We have $p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$ with distinct prime ideals P_i of $\mathcal{O}_K$. By the CRT we have

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_r^{e_r}.$$

The ideal $\mathfrak{p}$ is ramified in $K/\mathbb{Q}$ if and only if $e_i = 1$ for all i, i.e., if $\mathcal{O}_K/p\mathcal{O}_K$ is a product of fields. Let $A = \mathbb{Z}$, $B = \mathcal{O}_K$ and $\{x_1, \dots x_n\}$ be a basis of the free A-module B. For each ideal I of A then $\{\overline{x_1}, \dots \overline{x_n}\}$ is a basis of the free A/I-module B/IB, and

$$D(\overline{x_1}, \dots \overline{x_n}) \equiv D(x_1, \dots, x_n) \mod I.$$

With $I = \mathfrak{p}$ we see that the condition $p \mid d$ is equivalent to

$$\mathcal{D}_{B/A} \mod \mathfrak{p} = \mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = 0.$$

Hence we have to show that $B/\mathfrak{p}B$ is a product of fields if and only if

$$\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} \neq 0.$$

We have $A/\mathfrak{p} = \mathbb{F}_p$ and $B/\mathfrak{p}B = \mathcal{O}_K/(p)$.

Assume that $B/\mathfrak{p}B = \prod_i k_i$, where k_i are finite field extensions of $\mathbb{F}_p$. We have $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = \prod_i \mathcal{D}_{k_i/\mathbb{F}_p}$. Since every extension $k_i/\mathbb{F}_p$ is separable, no generator in the factors is equal to zero by Lemma 2.4.10. Hence also $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} \neq 0$.

Conversely assume that $B/\mathfrak{p}B = \prod_i B/P_i^{e_i}$ is not a product of fields. Then $B/\mathfrak{p}B$ contains a nilpotent element $x \neq 0$. Extend $x = x_1$ to a basis $\{x_1, \dots x_n\}$ of $B/\mathfrak{p}B$. Since then also the products x_1x_i are nilpotent, the multiplication with x_1x_i is a nilpotent endomorphism. Hence all of its eigenvalues are zero, and therefore we have $\operatorname{tr}(x_1x_j) = 0$. By the definition of a discriminant it follows that $\mathcal{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = 0$. □

Note that only *finitely many* prime ideals $\mathfrak{p}$ of $\mathbb{Z}$ can be ramified in K, since d has only finitely many prime divisors.

This result is also true for our general situation. The proof is similar, using Corollary 2.4.11.

Proposition 6.4.2. *Let A be a Dedekind ring with quotient field K, L/K be a finite field extension, and B the integral closure of A in L. Let B be a free A-module. Then the prime ideal $\mathfrak{p} = (p)$ of A is ramified in L/K, if and only if $\mathfrak{p} \supseteq \mathcal{D}_{B/A}$, which says that $\mathfrak{p} \mid \mathcal{D}_{B/A}$ in the sense of divisibility of ideals. In particular, only finitely many prime ideals of A are ramified.*

Since the discriminant is an ideal in A, only finitely many prime ideals of A contain this ideal.

Definition 6.4.3. A finite field extension L/K is called *unramified*, if all nonzero prime ideals of K, that is, of $\mathcal{O}_K$, are unramified in L.

Proposition 6.4.4. *Let K be a number field. If the extension $K/\mathbb{Q}$ is unramified then $K = \mathbb{Q}$.*

Proof. By Proposition 4.2.14 we have $|d_K| > 1$ for all number fields $K \neq Q$, and hence $d > 1$ for the absolute discriminant. So there is always a prime divisor $p \mid d$ of d. Hence the corresponding ideal $\mathfrak{p} = (p)$ is ramified by Proposition 6.4.1. So for $K \neq \mathbb{Q}$ the extension $K/\mathbb{Q}$ is always ramified. □

CHAPTER 7

Cyclotomic fields

A *cyclotomic field* is a number field $K = \mathbb{Q}(\zeta)$, where ζ is a primitive n-th root of unity. Such fields are interesting examples for the theory, but also have important applications, e.g., for a case of FLT. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n)^\times$, so it is abelian. Cyclotomic fields are also in the center of class field theory. For example, there is the famous theorem of *Kronecker-Weber*, which we will discuss in Chapter 9. It says that every number field with abelian Galois group is contained in some cyclotomic field.

7.1. Roots of unity

Let K be a field and $n \in \mathbb{N}$. Then $\zeta \in K$ is called a *n-th root of unity in K*, if $\zeta^n = 1$.

Definition 7.1.1. A n-th root of unity ζ in K is called *primitive*, if it has order n in the group $K^\times$, so if $\zeta^d \neq 1$ for all $d < n$. The group

$$\mu_n(K) = \{\zeta \in K^\times \mid \zeta^n = 1\}$$

is called the *group of roots of unities in K*.

Since every finite subgroup of $K^\times$ is cyclic, $\mu_n(K)$ is a finite cyclic group.

Example 7.1.2. *For $K = \mathbb{C}$ we have $\mu_n(\mathbb{C}) = \{e^{\frac{2\pi i m}{n}} \mid 0 \leq m \leq n-1\}$.*

Lemma 7.1.3. *Let ζ be a primitive n-th root of unity in K. Then ζ^m is a primitive n-th root of unity if and only if m and n are coprime.*

Proof. This holds in general, see for example Proposition 1.12 in [**7**]. Let G be a group and $\alpha \in G$ be an element of order n. Then α^m has order n, if and only if $\gcd(n, m) = 1$. Applying this for the group $G = \mu_n(K)$ we are done. □

Let us now restrict to roots of unity ζ in $K = \overline{\mathbb{Q}}$ in $\mathbb{C}$.

Definition 7.1.4. The minimal polynomial $\Phi_n(t) \in \mathbb{Q}[t]$ over $\mathbb{Q}$ of a primitive n-th root of unity ζ is called the *n-th cyclotomic polynomial.*

The following result is proved in a course of abstract algebra, see for example Chapter VI, 2 in [**7**].

Proposition 7.1.5. *Let ζ be a primitive n-th root of unity. Then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension of degree $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ with Galois group*

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n)^\times.$$

We have $\Phi_n(t) = \prod_{(n,m)=1}(t - \zeta^m)$ and

$$t^n - 1 = \prod_{d|n} \Phi_d(t).$$

EXAMPLE 7.1.6. *Let $n = 12$. Then the positive divisors of n are given by $d = 1, 2, 3, 4, 6, 12$, and*

$$\begin{aligned} \Phi_1(t) &= t - 1, \\ \Phi_2(t) &= t + 1, \\ \Phi_3(t) &= t^2 + t + 1, \\ \Phi_4(t) &= t^2 + 1, \\ \Phi_6(t) &= t^2 - t + 1, \\ \Phi_{12}(t) &= t^4 - t^2 + 1. \end{aligned}$$

Therefore $t^{12} - 1 \in \mathbb{Q}[t]$ has the following factorization into irreducible factors

$$t^{12} - 1 = (t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1)(t^4-t^2+1).$$

EXAMPLE 7.1.7. *For a prime $n = p$ we have $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$.*

Indeed, the degree of Φ_p is $\varphi(p) = p-1$, and $t^p - 1 = \prod_{d \mid p} \Phi_d(t) = \Phi_1(t)\Phi_p(t) = (t-1)\Phi_p(t)$. So we have

$$\Phi_p(t) = \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \cdots + t + 1.$$

For prime powers $n = p^r$ we have, because of $\Phi_{p^r}(t) = \Phi_p(t^{p^{r-1}})$,

$$\Phi_{p^r}(t) = \frac{t^{p^r} - 1}{t^{p^{r-1}} - 1} = t^{p^{r-1}(p-1)} + t^{p^{r-1}(p-2)} + \cdots + t^{p^{r-1}} + 1.$$

In particular we have $\Phi_{p^r}(1) = p$.

7.2. The ring of integers of a cyclotomic field

Let ζ be a complex primitive n-th root of unity. Then ζ is integral over $\mathbb{Z}$, so that

$$\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}.$$

Our aim is to show that equality holds.

LEMMA 7.2.1. *Let $n = p^r$ be a prime power, ζ be a primitive n-th root of unity, and $K = \mathbb{Q}(\zeta)$. Let $P = (1 - \zeta)$, $\mathfrak{p} = (p)$. Then P is a prime ideal in $\mathcal{O}_K$ and $p\mathcal{O}_K = P^e$ with*

$$e = e(P \mid \mathfrak{p}) = \varphi(p^r) = p^{r-1}(p-1)$$

and $f(P \mid \mathfrak{p}) = 1$. Hence $\mathfrak{p}$ is totally ramified in $K/\mathbb{Q}$.

PROOF. For every other primitive p^r-th root of unity we have $\zeta' = \zeta^s$ with $p \nmid s$ by Lemma 7.1.3. Also $\zeta = (\zeta')^t$ with $p \nmid t$. This implies $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta')$ and $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta']$. We have

$$\frac{1 - \zeta'}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{s-1} \in \mathbb{Z}[\zeta]$$

and also

$$\frac{1 - \zeta}{1 - \zeta'} = 1 + \zeta' + \cdots + (\zeta')^{t-1} \in \mathbb{Z}[\zeta]$$

Hence both elements are invertible and thus units in $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}$. So we obtain

$$\begin{aligned} p &= \Phi_{p^r}(1) \\ &= \prod_{\mathrm{ord}\zeta'=p^r} (1-\zeta') \\ &= \prod_{\mathrm{ord}\zeta'=p^r} (1-\zeta')\frac{1-\zeta}{1-\zeta'} \\ &= u \cdot (1-\zeta)^e \end{aligned}$$

for a unit u in $\mathbb{Z}[\zeta]$. This means $p\mathcal{O}_K = (1-\zeta)^e = P^e$ as ideals. Now $p\mathcal{O}_K$ is the product of g distinct prime ideals in $\mathcal{O}_K$. By the degree theorem for Galois extensions 6.3.3 we have

$$e = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p^r) = gef.$$

But this implies $g = f = 1$. Hence P is a prime ideal with residue class degree $f(P \mid \mathfrak{p}) = [\mathcal{O}_K/(p) : \mathbb{Z}/p] = 1$ and ramification index $e(P \mid \mathfrak{p}) = \varphi(p^r)$. □

LEMMA 7.2.2. *Let $n = p^r$ be a prime power, ζ be a primitive n-th root of unity, and $K = \mathbb{Q}(\zeta)$. Then we have $N_{K/\mathbb{Q}}(1-\zeta) = p$.*

PROOF. Because of $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p^r)^\times$ the Galois conjugates are just the ζ^j, where j runs through a system of representatives of $(\mathbb{Z}/p^r)^\times$. So by Proposition 2.4.4 we have

$$N_{K/\mathbb{Q}}(1-\zeta) = \prod_{(j,p^r)=1} (1-\zeta^j) = \Phi_{p^r}(1) = p.$$

□

LEMMA 7.2.3. *Let $n = p^r$ be a prime power, ζ be a primitive n-th root of unity, and $K = \mathbb{Q}(\zeta)$. Then the $\mathbb{Q}$-basis $\{1, \zeta, \dots, \zeta^{e-1}\}$ with $e = \varphi(p^r)$ has the discriminant*

$$D(1, \zeta, \zeta^2, \dots, \zeta^{e-1}) = \pm p^m,$$

with $m = p^{r-1}(pr - r - 1)$. Hence of all prime ideals (ℓ) in $\mathbb{Z}$ only (p) is ramified, the others are unramified.

PROOF. By Proposition 2.4.23 we have

$$D(1, \zeta, \zeta^2, \dots, \zeta^{e-1}) = \pm N_{K/\mathbb{Q}}(\Phi_n'(\zeta)).$$

So we need to compute the norm of $\Phi_n'(\zeta)$. By differentiating the equation we obtain

$$\Phi_{p^r}(t) = \frac{t^{p^r}-1}{t^{p^{r-1}}-1},$$

where we substitute $t = \zeta$. Then we obtain,by using $\zeta^{p^r-1} = \zeta^{-1}$,

$$\zeta(\zeta^{p^{r-1}} - 1)\Phi_n'(\zeta) = p^r.$$

We take the norm on both sides. Then the RHS becomes $N_{K/\mathbb{Q}}(p^r) = (p^r)^e$, and the LHS becomes $N_{K/\mathbb{Q}}(\zeta) = \pm 1$ because of

$$1 = a_0 = (-1)^e N_{K/\mathbb{Q}}(\zeta).$$

Here a_0 is the constant term of the minimal polynomial of ζ, hence 1. So it remains to show

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

Then we obtain

$$\begin{aligned} p^{re} &= N_{K/\mathbb{Q}}(p^r) = N_{K/\mathbb{Q}}(\zeta) \cdot N_{K/\mathbb{Q}}(\zeta^{p^{r-1}} - 1) \cdot N_{K/\mathbb{Q}}(\Phi'_n(\zeta)) \\ &= \pm 1 \cdot p^{p^{r-1}} \cdot N_{K/\mathbb{Q}}(\Phi'_n(\zeta)), \end{aligned}$$

and hence

$$N_{K/\mathbb{Q}}(\Phi'_n(\zeta)) = \pm \frac{p^{re}}{p^{p^{r-1}}} = \pm p^{rp^r - rp^{r-1} - p^{r-1}}.$$

So let p^s be a p-power with $0 \le s < r$. We will show that

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

For $s = 0$ this follows from Lemma 7.2.2, namely $N_{K/\mathbb{Q}}(1 - \zeta) = p$. Since ζ^{p^s} is a primitive p^{r-s}-th root of unity, one can apply the lemma again for p^{r-s}. This yields $N_{\mathbb{Q}(\zeta^{p^s})/\mathbb{Q}}(1 - \zeta^{p^s}) = p$. The norm is transitive for field extensions $K/M/\mathbb{Q}$. So we have $N_{K/\mathbb{Q}}(\alpha) = N_{K/M}(N_{M/\mathbb{Q}}(\alpha))$ for $\alpha \in K$. For $\alpha \in M$ we have $N_{K/M}(\alpha) = \alpha^{[K:M]}$. So we put $M = \mathbb{Q}(\zeta^{p^s})$. The by the degree theorem we have

$$[K : M] = \frac{\varphi(p^r)}{\varphi(p^{r-s})} = p^s.$$

This implies

$$\begin{aligned} N_{K/\mathbb{Q}}(1 - \zeta^{p^s}) &= N_{K/M}(N_{M/\mathbb{Q}}(1 - \zeta^{p^s})) \\ &= N_{K/M}(p) \\ &= p^{[K:M]} \\ &= p^{p^s}. \end{aligned}$$

Hence the discriminant is a proper p-power and the claim on the ramification directly follows from Proposition 6.4.1. □

THEOREM 7.2.4. *Let ζ be a primitive n-th root of unity and $K = \mathbb{Q}(\zeta)$. Then we have $\mathcal{O}_K = \mathbb{Z}[\zeta]$, and $\{1, \zeta, \dots, \zeta^{\varphi(n)-1}\}$ is an integral basis for $\mathcal{O}_K$ over $\mathbb{Z}$.*

PROOF. We will first prove the result for prime powers $n = p^r$. By Proposition 2.4.24 we have $d\mathcal{O}_K \subseteq \mathbb{Z}[\zeta]$ for the discriminant

$$d = D(1, \zeta, \dots, \zeta^{\varphi(p^r)-1}) = \pm p^m$$

by Lemma 7.2.3. Therefore we have

$$p^m \mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K.$$

By Lemma 7.2.1 we have $[\mathcal{O}_K/(\pi) : \mathbb{Z}/(p)] = 1$, with $\pi := 1 - \zeta$. So the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ induces an isomorphism $\mathbb{Z}/(p) \simeq \mathcal{O}_K/(\pi)$. So we may write $\mathcal{O}_K$ as $\{0, 1, \dots, p-1\} + \pi\mathcal{O}_K$, so that $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$, hence also

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi\mathcal{O}_K.$$

Multiplying with π yields $\pi\mathcal{O}_K = \pi\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K$, and hence

$$\begin{aligned} \mathcal{O}_K &= \mathbb{Z}[\zeta] + \pi\mathcal{O}_K \\ &= \mathbb{Z}[\zeta] + \pi\mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K \\ &= \mathbb{Z}[\zeta] + \pi^2\mathcal{O}_K. \end{aligned}$$

This yields iteratively

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^k\mathcal{O}_K$$

for all $k \geq 1$. Then $(\pi^{\varphi(p^r)}) = (p)$ implies

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + p^m \mathcal{O}_K \subseteq \mathbb{Z}[\zeta].$$

For the general case let $n = p_1^{r_1} \cdots p_g^{r_g}$ and ζ be a primitive n-th root of unity. Then we have

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{r_1}}) \cdots \mathbb{Q}(\zeta_{p_g^{r_g}})$$

and

$$\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta_{p_1^{r_1}}, \ldots, \zeta_{p_g^{r_g}}] = \mathbb{Z}[\zeta].$$

To see this, one needs the following argument. If K and L are two finite extensions of $\mathbb{Q}$ with $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$ and if d is the greatest common divisor of the generators of $\mathcal{D}_{\mathcal{O}_K/\mathbb{Z}}$ and $\mathcal{D}_{\mathcal{O}_L/\mathbb{Z}}$, then

$$\mathcal{O}_{KL} \subseteq d^{-1} \mathcal{O}_K \mathcal{O}_L.$$

For details see [**12**]. □

7.3. Fermat's equation

Kummer proved Fermat's Last Theorem (FLT) for regular primes. We will give the proof here for the so-called *first case* of Fermat's equation

$$x^p + y^p = z^p,$$

which assumes $p \nmid xyz$. The *second case* is $p \mid xyz$. For $p = 3$ we have proved both cases in Proposition 1.0.1. The first case for $p = 3$ was very easy, namely studying the equation modulo 9. The same is true for $p = 5$ by studying the equation modulo 25. However, more effort is necessary for $p > 5$.

Let us assume from now onward that $p > 5$ and $p \nmid xyz$. Furthermore we may assume that x, y, z are pairwise coprime. Let ζ be a primitive p-th root of unity. Then

$$t^p - 1 = \prod_{i=0}^{p-1} (t - \zeta^i)$$

yields, by substituting $t = -x/y$ and clearing denominators,

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta^i y).$$

Lemma 7.3.1. *The elements $x + \zeta^i y$ in $\mathbb{Z}[\zeta]$ are pairwise coprime.*

Proof. We will show that the ideals $(x + \zeta^i y)$ in $\mathbb{Z}[\zeta]$ are pairwise coprime for $i = 0, 1 \ldots, p-1$. Let $P = (\pi) = (1 - \zeta)$ be the unique prime ideal in $\mathbb{Z}[\zeta]$ lying over (p), see Lemma 7.2.1. We have $1 - \zeta^i = \left(\frac{1-\zeta^i}{1-\zeta}\right)(1 - \zeta) = u \cdot (1 - \zeta)$ with a unit u, so that $P = (1 - \zeta^k)$ for $1 \leq k \leq p - 1$. Suppose that Q is a prime ideal in $\mathbb{Z}[\zeta]$, which divides two different ideals $(x + \zeta^i y)$ and $(x + \zeta^j y)$. Then we have

$$Q \mid (x + \zeta^j y) - (x + \zeta^i y) = ((\zeta^i - \zeta^j) y) = (\varepsilon \cdot (1 - \zeta) y) = Py$$

for a unit ε. Since Q is a prime ideal, we have $Q = (1 - \zeta)$ or $Q \mid y$. Similarly we have

$$Q \mid \zeta^i (x + \zeta^j y) - \zeta^j (x + \zeta^i y) = ((\zeta^i - \zeta^j) x) = Px,$$

so either $Q = (1-\zeta)$ or $Q \mid x$. Since x and y are coprime, Q cannot divide both. Therefore we must have $Q = P$. It follows that

$$x + y \equiv x + \zeta^i y \equiv 0 \mod P,$$

and therefore $x + y \equiv 0 \mod p$, because of $x + y \in P \cap \mathbb{Z} = (p)$. This yields

$$z^p = x^p + y^p \equiv x + y \equiv 0 \mod p$$

and hence $p \mid z$. This is a contradiction to our assumption $p \nmid xyz$. □

Lemma 7.3.2. *Four each $\alpha \in \mathbb{Z}[\zeta]$ we have $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta]$. In other words, there is an integer $b \in \mathbb{Z}$ with $\alpha^p \equiv b \mod p$.*

Proof. Let $\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$ with $b_i \in \mathbb{Z}$. Then we have

$$\begin{aligned} \alpha^p &\equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-2}\zeta^{p-2})^p \mod p \\ &= b_0^p + b_1^p + \cdots + b_{p-2}^p \mod p \end{aligned}$$

So take $b = b_0^p + b_1^p + \cdots + b_{p-2}^p$. □

Lemma 7.3.3. *Let $\alpha = b_0 + b_1\zeta + \cdots + b_{p-1}\zeta^{p-1}$ with integer coefficients, such that at least one of them is zero. If $n \mid \alpha$, so $\alpha \in n\mathbb{Z}[\zeta]$ for some $n \in \mathbb{Z}$, then it follows that $n \mid b_j$ for all j.*

Proof. We have $1+\zeta+\cdots+\zeta^{p-1} = 0$, so that each subset of $\{1, \zeta, \ldots, \zeta^{p-1}\}$ with cardinality $p-1$ is a $\mathbb{Z}$-basis. Assume that $b_i = 0$. Then we write α in terms of a $\mathbb{Z}$-basis, which omits exactly ζ^i. Then the claim follows from the uniqueness of a basis representation. □

Definition 7.3.4. Let ζ be a primitive n-th root of unity and $n \geq 3$. Then

$$\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$$

is called the *maximal real* subfield of $\mathbb{Q}(\zeta)$.

Note that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^+] = 2$, because the minimal polynomial of ζ over $\mathbb{Q}(\zeta)^+$ is $t^2 - (\zeta + \zeta^{-1})t + 1$. This field is indeed totally real, since ζ^{-1} maps under all embeddings of $\mathbb{Q}(\zeta) \hookrightarrow \mathbb{C}$ to the complex conjugate of ζ^{-1}, so to $\overline{\zeta}$. Hence the image of $\mathbb{Q}(\zeta)^+$ under every embedding is invariant under complex conjugation and hence lies in $\mathbb{R}$. Here a number field is called *totally real*, if all of its embeddings to $\mathbb{C}$ already lie in $\mathbb{R}$. A number field is called *totally imaginary*, if none of the embeddings lies in $\mathbb{R}$. And a number field is called a *CM-field*, if it is a totally imaginary number field, which is a quadratic extension of a totally real number field. In this sense, $\mathbb{Q}(\zeta)$ is a CM-field, with maximal totally real subfield $\mathbb{Q}(\zeta)^+$.

Lemma 7.3.5. *Let $n = p > 2$ be a prime number and ζ be a primitive p-th root of unity. Then every unit u in $\mathbb{Z}[\zeta]$ can be written as $u = \zeta^r v$, with $r \in \mathbb{Z}$ and a real unit v in $\mathbb{Q}(\zeta)^+$.*

Proof. Let $\alpha = u/\overline{u}$. This is a unit in $\mathbb{Z}[\zeta]$, since u is a unit. Moreover all Galois conjugates of α have absolute value 1. Hence α is contained in the kernel of the logarithmic embedding, which consists of roots of unities, see the proof of Theorem 5.1.6. Indeed, every integral algebraic number $\alpha \in \mathbb{C}$, whose conjugates all have absolute value 1, is a root of unity. The reason is, that the minimal polynomial of each power of α has bounded coefficients in $\mathbb{Z}[x]$, so that there are only finitely many such polynomials, hence only finitely many different powers of α. All roots of unity are of the form $\pm\zeta^a$ with $a \in \mathbb{Z}$. Therefore we can also write

$$\alpha = u/\overline{u} = \pm\zeta^a.$$

We claim that the negative sign *cannot occur*. Let $u = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$ with $b_i \in \mathbb{Z}$. Then

$$\begin{aligned} u &\equiv b_0 + \cdots + b_{p-2} \mod (1-\zeta), \\ &\equiv b_0 + b_1\zeta^{-1} + \cdots + b_{p-2}\zeta^{-p+2} \mod (1-\zeta) \\ &\equiv \overline{u} \mod (1-\zeta). \end{aligned}$$

Assume that $u = -\zeta^a \overline{u}$. Then

$$\overline{u} \equiv u \equiv -\zeta^a\overline{u} \equiv -\overline{u} \mod (1-\zeta),$$

so that $1-\zeta \mid 2\overline{u}$ in $\mathbb{Z}[\zeta]$. Since $\overline{u}$ is a unit, it follows that $1-\zeta \mid 2$. Hence $(1-\zeta)$ lies over (2). But $(1-\zeta)\cap\mathbb{Z} = (p)$, with $p > 2$. This is a contraction. Hence we have the positive sign. Since p is odd, there exists an $r \in \mathbb{Z}$ with $2r \equiv a \mod p$. Hence we can write $\alpha = u/\overline{u} = +\zeta^{2r}$, and hence $u = \zeta^{2r}\overline{u}$. Then we have

$$\zeta^{-r}u = \zeta^r\overline{u} = \overline{\zeta^{-r}u}.$$

Setting $v := \zeta^{-r}u$, we have $u = \zeta^r v$ and $v = \overline{v}$. Hence v is a real unit in $\mathbb{Q}(\zeta)^+$. □

Now we can show Kummer's result for the first case of FLT.

THEOREM 7.3.6 (Kummer). *Let $p > 5$ be a prime number, which doesn't divide the class number h of $\mathbb{Q}(\zeta)$, where ζ is a primitive p-th root of unity. Then Fermat's equation*

$$x^p + y^p = z^p$$

has no integer solutions with $p \nmid xyz$.

PROOF. We may assume that x, y, z are coprime with $p \nmid x - y$. Indeed, suppose that $x \equiv y \equiv -z \mod p$, then also $-2z \equiv z \mod p$ and hence $p \mid 3z$. Since $p > 3$ and $p \nmid z$, this is impossible. So one of the congruences $x \equiv y \equiv -z \mod p$ cannot hold. So by a possible rearranging $x^p + (-z)^p = (-y)^p$ we may assume that $p \nmid x - y$.

Now consider Fermat's equation as an equation of ideals in $\mathbb{Z}[\zeta]$, by using the identity of Lemma 7.3.1,

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

Since $\mathbb{Z}[\zeta]$ is a Dedekind ring, and the ideals $(x+\zeta^i y)$ are pairwise coprime by Lemma 7.3.1, one can write every ideal, by the unique factorization of ideals, on the RHS as a p-th power of an ideal in $\mathbb{Z}[\zeta]$, so as

$$(x+\zeta^i y) = \mathfrak{a}_i^p.$$

In the class group of $\mathbb{Q}(\zeta)$ we have $p\cdot[\mathfrak{a}_i] = [\mathfrak{a}_i^p] = [(x+\zeta^i y)] = [0]$, because $(x+\zeta^i y)$ is a principal ideal. Since the class group is finite, whose order is not divisible by p by assumption, the multiplication with p is a group isomorphism. So there is no p-torsion. Hence $[\mathfrak{a}_i] = [0]$, and thus each $\mathfrak{a}_i$ is a principal ideal. We write $\mathfrak{a}_i = (\alpha_i)$ with some $\alpha_i \in \mathbb{Z}[\zeta]$ and focus on $i = 1$, setting $\alpha = \alpha_1$. So we have

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

for a unit u in $\mathbb{Z}[\zeta]$. By Lemma 7.3.5 we can write $u = \zeta^r v$ for a unit v with $\overline{v} = v$. By Lemma 7.3.2 there is a $b \in \mathbb{Z}$ with $\alpha^p \equiv b \mod p$. Hence we have

$$\begin{aligned} x + \zeta y &= u\alpha^p = \zeta^r v\alpha^p \equiv \zeta^r vb \mod p, \\ x + \overline{\zeta}y &= \overline{x+\zeta y} = \zeta^{-r}v(\overline{\alpha})^p \equiv \zeta^{-r}vb \mod p. \end{aligned}$$

Together we have

$$\zeta^{-r}(x+\zeta y) \equiv \zeta^{r}(x+\zeta^{-1}y) \mod p,$$

which says

$$x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y \equiv 0 \mod p. \tag{7.1}$$

Now we want to apply Lemma 7.3.3 with $n = p$. Clearly p divides the LHS above. Suppose that all powers of ζ are different in this expression. Then, because of $p > 5$, at least one coefficient is zero with respect to the representation in the $\mathbb{Z}$-basis. Hence the Lemma yields that *all* coefficients are divisible by p, so in particular $p \mid x$ and $p \mid y$. This is a contradiction. So we are done, if we show that really all numbers $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are pairwise distinct. Here we have to consider different cases. Because of $\zeta \neq 1$ and $\zeta^{2r} \neq \zeta^{2r-1}$ there are the following 3 cases.

Case 1: Let $\zeta^{2r} = 1$. Then (7.1) is given by $\zeta y - \zeta^{-1}y \equiv 0 \mod p$, and Lemma 7.3.3 yields again a contradiction, namely $p \mid y$.

Case 2: Let $\zeta^{2r-1} = 1$. Then $\zeta^{2r} = \zeta$ and (7.1) is given by $(x-y)-(x-y)\zeta \equiv 0 \mod p$. So we have $p \mid x-y$, which is a contradiction.

Case 3: Let $\zeta^{2r-1} = \zeta$. Then (7.1) is given by $x - \zeta^2 x \equiv 0 \mod p$, and Lemma 7.3.3 yields $p \mid x$, hence a contradiction. □

Remark 7.3.7. One can similarly prove the second case of Kummer's result. It is, however, more complicated, see [**12**]. Modern proofs refer to Iwasawa theory for a proof. Kummer proved FLT only for **regular** prime powers, but we know that there are infinitely many irregular primes, see 4.3.8. So there is a lot more to do for the general proof. Nevertheless Kummer's proof is a great contribution to the solution of Fermat's equation and has initiated many interesting developments in algebraic number theory.

CHAPTER 8

Valuations and local fields

8.1. Valuations

Definition 8.1.1. Let K be a field. A function $K \to \mathbb{R}$, $x \mapsto |x|$ is called an *absolute value* over K, if it satisfies following properties.

(a) We have $|x| > 0$, except for $|0| = 0$.
(b) $|xy| = |x||y|$.
(c) $|x + y| \leq |x| + |y|$.

The usual absolute value $\mathbb{C} \to \mathbb{R}$, $z \mapsto |z| = \sqrt{z\overline{z}}$ is an absolute value on the field $\mathbb{C}$. Also its restriction to $\mathbb{R}$ is an absolute value in the above sense.

The conditions (a) and (b) also say that an absolute value is a group homomorphism $K^\times \to \mathbb{R}_+$. Since the group $\mathbb{R}_+$ is torsion-free, we have $|\zeta| = 1$ for all roots of unity ζ in $K^\times$, in particular $|-1| = 1$ and $|-x| = |x|$ for all $x \in K$.

Example 8.1.2. *Let K be a number field and $\sigma\colon K \hookrightarrow \mathbb{C}$ be an embedding of K to $\mathbb{C}$. Then $|a|_\sigma = |\sigma(a)|$ defines an absolute value on K.*

Definition 8.1.3. By $|a| = 1$ for all $a \neq 0$ in K an absolute value is defined, the so-called *trivial valuation* on K.

Lemma 8.1.4. *Let K be a finite field. Then every absolute value on K is trivial.*

Proof. In a finite field all elements $a \neq 0$ are roots of unity. Since

$$| \cdot |\colon K^\times \to \mathbb{R}_+$$

is a group homomorphism, we have $1 = |1| = |a^n| = |a|^n$ in $\mathbb{R}_+$. So we have $|a| = 1$. □

Definition 8.1.5. An absolute value on a field K is called *non-archimedean*, if (c) is replaced by (c'), which is

$$(c') \quad |x + y| \leq \max\{|x|, |y|\}.$$

Otherwise the absolute value is called *Archimedian.*

The inequality (c') is called the *ultrametric inequality.* It is obviously stronger than the usual triangle inequality (c). We always have equality in (c'), except for the case of $|x| = |y|$. Indeed, suppose that $|x| < |y|$ and $|x + y| < \max\{|x|, |y|\} = |y|$. Then

$$|y| = |y + x - x| \leq \max\{|y + x|, |x|\} < |y|,$$

a contradiction.

Example 8.1.6. *Let p be a prime. Then $|a|_p := (1/p)^{\mathrm{ord}_p(a)}$ defines a non-archimedean norm on $\mathbb{Q}$, the so-called p-adic absolute value.*

If $a = a_0 p^r$ with $\operatorname{ord}_p(a_0) = 0$, so $a_0 = \frac{m}{n}$ with $(m,p) = (n,p) = 1$, then we have $|a|_p = p^{-r}$. Obviously $a \mapsto |a|_p$ defines an absolute value on $\mathbb{Q}$. Note that the values $|n|_p$ are bounded for all $n \in \mathbb{Z}$, because we have $|n|_p \leq 1$ for all $n \in \mathbb{Z}$. Hence it follows by the next Proposition, that the p-adic absolute value is is non-archimedean.

Proposition 8.1.7. *An absolute value $|\ |$ on K is non-archimedean if and only if it takes bounded values on $\{m1 \mid m \in \mathbb{Z}\}$.*

Proof. Let $|\ |$ be non-archimedean and $m \in \mathbb{N}$. Then we have by (c')

$$|m1| = |1 + 1 + \cdots + 1| \leq |1| = 1,$$

and $|-1| = 1$, $|-m1| = |m1| \leq 1$.

Conversely assume that $|m1| \leq N$ for all $m \in \mathbb{Z}$ and some $N \in \mathbb{N}$. Because of $|\binom{n}{r}| \leq N$ we have,

$$\begin{aligned} |x+y|^n &= \left| \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r} \right| \leq \sum_{r=0}^{n} \left| \binom{n}{r} \right| |x|^r |y|^{n-r} \\ &\leq (n+1)N \cdot \max\{|x|^n, |y|^n\} \\ &\leq (n+1)N \cdot \max\{|x|, |y|\}^n. \end{aligned}$$

Taking the n-th root one obtains

$$|x+y| \leq \sqrt[n]{N(n+1)} \cdot \max\{|x|, |y|\}.$$

For $n \to \infty$ this yields the ultrametric triangle inequality. □

Corollary 8.1.8. *Let K be a field of prime characteristic. Then K admits only non-archimedean absolute values.*

Proof. Because the characteristic of K is positive, the set $\{m1 \mid m \in \mathbb{Z}\}$ is finite. So the claim follows from Proposition 8.1.7. □

Example 8.1.9. *Let K be a number field and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then*

$$|a|_{\mathfrak{p}} = (1/N(\mathfrak{p}))^{\operatorname{ord}_{\mathfrak{p}}(a)}$$

defines a non-archimedean absolute value on K, the $\mathfrak{p}$-adic absolute value.

Obviously the p-adic absolute value of Example 8.1.6 is a special case, where $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$.

Definition 8.1.10. A *valuation on K*, or an exponential valuation on K is a map $\nu\colon K \to \mathbb{R} \cup \{\infty\}$ with the following properties.

(a) We have $\nu(x) < \infty$, except for $\nu(0) = \infty$.
(b) $\nu(xy) = \nu(x) + \nu(y)$.
(c) $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$.

An exponential valuation is the additive version of a non-archimedean absolute value. Indeed, given a valuation ν we can consider the aboslute value defined by $|x|_\nu := a^{-\nu(x)}$ for some $a > 1$. So we have the following result.

Proposition 8.1.11. *If $|\ |$ is a non-archimedean absolute value on K, then $\nu(x) = -\log(|x|)$ for $x \neq 0$ and $\nu(0) = \infty$ defines a valuation on K. This assignment induces a bijection between non-archimedean absolute values and valuations on K.*

Definition 8.1.12. Two valuations ν and μ on K are called *equivalent*, if there exists a $t > 0$ with $\nu(x) = t\mu(x)$ for all $x \in K$. Two absolute values $|\ |_1$ and $|\ |_2$ are called *equivalent*, if there exists a $t > 0$ with $|x|_1 = |x|_2^t$ for all $x \in K$.

For a given absolute value $|\ |$ on K, $d(x, y) = |x - y|$ defines a metric and hence a topology on K. In fact, for $a \in K$ the open sets

$$U(a, \varepsilon) = \{x \in K \mid |x - a| < \varepsilon\}$$

with $\varepsilon > 0$ form a basis of the topology.

Proposition 8.1.13. *Let $|\ |_1$ and $|\ |_2$ be two absolute values on K, and $|\ |_1$ be nontrivial. Then the following statements are equivalent.*

(a) *$|\ |_1$ and $|\ |_2$ define the same topology on K.*
(b) *$|x|_1 < 1 \Rightarrow |x|_2 < 1$.*
(c) *$|\ |_1$ and $|\ |_2$ are equivalent.*

Proof. $(a) \Rightarrow (b)$: Because of $|x^n| = |x|^n$ we have $|x| < 1$ if and only if $x^n \to 0$ for $n \to \infty$. So (a) implies that $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$.

$(b) \Rightarrow (c)$: Since $|\ |_1$ is nontrivial there exists a $y \in K$ with $|y|_1 > 1$. Then $a := \log(|y|_2)/\log(|y|_1)$ is well-defined and we have $\log(|y|_2) = a\log(|y|_1)$, and hence

$$|y|_2 = |y|_1^a.$$

Let $x \neq 0$ in K. Then there exists a real number b with $|x|_1 = |y|_1^b$. To show (c), it suffices to show $|x|_2 = |y|_2^b$, because

$$|x|_2 = |y|_2^b = |y|_1^{ab} = |x|_1^a.$$

So let $\frac{m}{n} > b$ be a rational number with $n > 0$. Then we have

$$|x|_1 = |y|_1^b < |y|_1^{\frac{m}{n}},$$

and hence

$$|x^n/y^m|_1 < 1.$$

So (b) implies that $|x^n/y^m|_2 < 1$. Since this holds for all rational numbers $\frac{m}{n} > b$, we obtain

$$|x|_2 \leq |y|_2^b.$$

The other inequality $|x|_2 \geq |y|_2^b$ follows the same way, with rational numbers $\frac{m}{n} < b$. So we have equality.

$(c) \Rightarrow (a)$: By assumption an ε-neighborhood with respect to $|\ |_2$ is an ε^t-neighborhood with respect to $|\ |_1$. Hence the two topologies coincide. □

8.2. Ostrowski's theorem

Alexander Markowich Ostrowski was a Ukrainian mathematician, who lived from 1893 to 1986. He began to study mathematics at Marburg University under Hensel's supervision in 1912. His result of 1916 states that every nontrivial absolute value on the rational numbers $\mathbb{Q}$ is equivalent to either the usual real absolute value $|\ |_\infty$ on $\mathbb{R}$, or a p-adic absolute value $|\ |_p$.

THEOREM 8.2.1 (Ostrowski). *Let $| \ |$ be a nontrivial absolute value on $\mathbb{Q}$.*

(a) *If $| \ |$ is Archimedian then $| \ |$ is equivalent to $| \ |_\infty$.*

(b) *If $| \ |$ is non-archimedean then $| \ |$ is equivalent to $| \ |_p$ for exactly one prime number p.*

PROOF. Let $n, m > 1$ be integers. Then one can write

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

with integers $0 \le a_i < n$ and $n^r \le m$. Let $N = \max\{1, |n|\}$. Then the triangle inequality yields

$$|m| \le \sum_{i=0}^{r} |a_i||n|^i \le (r+1)N^r \sum_{i=0}^{r} |a_i|.$$

Similarly we have

$$|a_i| = |1 + \cdots + 1| \le a_i|1| = a_i \le n.$$

Together we obtain by using $r \le \log(m)/\log(n)$,

$$|m| \le (1+r)nN^r \le \left(1 + \frac{\log(m)}{\log(n)}\right) nN^{\frac{\log(m)}{\log(n)}}.$$

Replacing m here by m^k with $k \in \mathbb{N}$ and taking the k-th root we obtain

$$|m| \le \left(1 + \frac{k\log(m)}{\log(n)}\right)^{\frac{1}{k}} n^{\frac{1}{k}} N^{\frac{\log(m)}{\log(n)}}.$$

For $k \to \infty$ we obtain

$$|m| \le N^{\frac{\log(m)}{\log(n)}}. \tag{8.1}$$

Case 1: We have $|n| > 1$ for all $n > 1$. Then $N = |n|$, and (8.1) yields

$$|m|^{\frac{1}{\log(m)}} \le |n|^{\frac{1}{\log(n)}}.$$

By symmetry we have even equality and there exists a $c > 1$ with

$$c = |m|^{\frac{1}{\log(m)}} = |n|^{\frac{1}{\log(n)}}$$

for all positive integers $n, m > 1$. So we have

$$|n| = c^{\log(n)} = e^{\log(c)\cdot\log(n)} = n^{\log(c)} = n^a$$

for all $n > 1$. It follows that $|n| = |n|_\infty^a$, where $| \ |_\infty$ is the usual absolute value on $\mathbb{Q}$. Since both $| \ |$ and $| \ |_\infty^a$ are group homomorphisms of $\mathbb{Q}^\times$ to $\mathbb{R}_+$, and these coincide on a generating set of $\mathbb{Q}$, namely on the primes and on -1, it follows that $| \ | = | \ |_\infty^a$.

Case 2: There *is* a $n > 1$ with $|n| \le 1$. Then we have $N = 1$, and (8.1) yields $|m| \le 1$ for all $m > 1$. Hence the absolute value is non-archimedean by Proposition 8.1.7. It is easy to see that for each non-archimedean absolute value on K the set

$$A := \{a \in K \mid |a| \le 1\}$$

is a subring of K, with exactly one maximal ideal

$$\mathfrak{m} := \{a \in K \mid |a| < 1\}.$$

Hence A is a local ring - see section 5.3 in my notes [**1**]. We have $\mathbb{Z} \subseteq A$. If $ab \in \mathfrak{m}$, so $|a||b| = |ab| < 1$, then it follows either $|a| < 1$ or $|b| < 1$, hence either $a \in \mathfrak{m}$ or $b \in \mathfrak{m}$. Therefore $\mathfrak{m}$ is a prime ideal in A, and hence $\mathfrak{m} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. It is nonzero, because otherwise the absolute value is trivial, a contradiction. So we have $\mathfrak{m} \cap \mathbb{Z} = (p)$ for a rational prime p. If m is not divisible by p, then $m \notin \mathfrak{m}$, and therefore $|m| = 1$. With $a = \log_{|p|}(\frac{1}{p})$ we have $|p|^a = \frac{1}{p}$. Then

$$|mp^r|^a = |m|^a |p|^{ar} = |p|^{ar} = \frac{1}{p^r} = |mp^r|_p.$$

So we have $|\ |^a = |\ |_p$ on $\mathbb{Z}$, and hence also on $\mathbb{Q}$ by multiplicativity. Thus $|\ |$ and $|\ |_p$ are equivalent. □

There is a generalization of Ostrowski's result from $\mathbb{Q}$ to any number field K as follows. For a proof, see for example Keith Conrad's notes.

Theorem 8.2.2 (Number field Ostrowski). *Any nontrivial absolute value on K is equivalent to a $\mathfrak{p}$-adic absolute value for a unique prime $\mathfrak{p}$ in $\mathcal{O}_K$ or is equivalent to an absolute value coming from a real or complex embedding of K.*

There is also an interesting product formula for absolute values on $\mathbb{Q}$.

Theorem 8.2.3. *For every nonzero rational number a we have*

$$\prod_p |a|_p = 1.$$

where the product runs over all primes $p = 2, 3, 5, 7, \ldots$ and $p = \infty$.

Proof. Let $\alpha = \frac{a}{b}$ with integers a, b and $b \neq 0$. Then $|\alpha|_p = 1$ unless $p \mid a$ or $p \mid b$. Therefore $|\alpha|_\nu = 1$ for all but finitely many ν, and so the product is really finite. Let $\pi(a) = \prod_\nu |a|_\nu$. Then $\pi \colon \mathbb{Q}^\times \to \mathbb{R}^\times$ is a group homomorphism, and so it suffices to show that $\pi(-1) = 1$ and $\pi(p) = 1$ for each prime number p. The first is obvious since $|-1| = 1$ for all absolute values $|\ |$. For the second, let $q \neq p$ be a prime. Then we have

$$|p|_p = \frac{1}{p},\ |p|_q = 1,\ |p|_\infty = p.$$

But the product of these numbers is equal to 1. □

The product formula also can be generalized to number fields K, where in each equivalence class of absolute values on K one selects a normalized absolute value in a certain way.

Theorem 8.2.4 (Product Formula). *For any $\alpha \neq 0$ in K, we have*

$$\prod_\nu |\alpha|_\nu = 1,$$

where the product runs over a canonical set of non-equivalent valuations on K.

All but finitely many of the $|\alpha|_\nu$'s are 1, so their formally infinite product is really a finite product, and thus the product makes algebraic sense.

8.3. Discrete valuations

Definition 8.3.1. A valuation ν on K is called *discrete*, if $\nu(K^\times) \subseteq \mathbb{R}$ is discrete. An absolute value $|\ |$ on K is called *discrete*, if $|K^\times| \subseteq \mathbb{R}_+$ is discrete.

So if ν is discrete then $\nu \colon K^\times \to \mathbb{Z}$ is a nonzero group homomorphism, such that $\nu(K^\times)$ is discrete in $\mathbb{R}$. Hence it is a lattice in $\mathbb{R}$, of the form $\mathbb{Z}c$ for some $c \in \mathbb{R}_+$. Actually, c is the smallest positive element in the lattice. We may normalize the valuation by considering the equivalent valuation $\nu' = \frac{1}{c}\nu$ instead of ν. Then ν' is called *normalized*, and $\nu' \colon K^\times \to \mathbb{Z}$ is a surjective group homomorphism.

Example 8.3.2. *The p-adic valuation $|\ |_p$ on $\mathbb{Q}$ is discrete, and the corresponding valuation ν_p, defined by*

$$\nu_p\Bigl(\pm \prod_{q\in\mathbb{P}} q^{n_q}\Bigr) = n_p$$

is discrete and normalized.

We associate to each non-archimedean valuation a local valuation ring, in the same way as in the proof of Proposition 8.2.1.

Definition 8.3.3. Let $|\ |$ be a non-archimedean absolute value on K, and ν be the associated valuation. Then define

$$\begin{aligned}
A &= \{a \in K \mid |a| \le 1\} = \{a \in K \mid \nu(a) \ge 0\} \\
U &= \{a \in K \mid |a| = 1\} = \{a \in K \mid \nu(a) = 0\} \\
\mathfrak{m} &= \{a \in K \mid |a| < 1\} = \{a \in K \mid \nu(a) > 0\}.
\end{aligned}$$

Here A is called the *valuation ring* of $|\ |$, or of ν, U is called the *group of units* of A, and $A/\mathfrak{m}$ dis called the *residue class field* of A.

The names are justified, because A is a local ring with maximal ideal $\mathfrak{m}$, and U really consists of units in A. The ideal $\mathfrak{m}$ is maximal, because it consists of the non-units. Indeed, for $a \in A$ with $a \notin \mathfrak{m}$ we have $|a| = 1$, and therefore $|1/a| = 1/|a| = 1$, and thus $1/a \in A$. So a is a unit in A.

Remark 8.3.4. There also exist *non-discrete* non-archimedean valuations on a number field K. For example, let $K = \overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. The p-adic absolute value $|\ |_p \colon \mathbb{Q} \to \mathbb{R}$ can be extended in many ways to $\overline{\mathbb{Q}}$. Then we have

$$|\overline{\mathbb{Q}}^{\times}|_p = \{p^r \mid r \in \mathbb{Q}\},$$

and this is not discrete in $\mathbb{R}_+$. Indeed, consider $p^{1/n} \in \overline{\mathbb{Q}}^{\times}$ for all n, hence $1/\sqrt[n]{p} \in |\overline{\mathbb{Q}}^{\times}|$ with $\lim_{n\to\infty} 1/\sqrt[n]{p} = 1$.

Lemma 8.3.5. *Let $|\ |$ be a non-archimedean absolute value on a field K. Then $|\ |$ is discrete if and only if $\mathfrak{m}$ is a principal ideal.*

Proof. Let $|\ |$ be discrete. Choose a $\pi \in \mathfrak{m}$ with $|\pi|$ maximal. This exists since $|K^{\times}|$ is discrete, and bounded from above. Let $a \in \mathfrak{m}$. Then we have

$$\left|\frac{a}{\pi}\right| = \frac{|a|}{|\pi|} \le 1,$$

so that $a/\pi \in A$. Hence $a = \pi \cdot \frac{a}{\pi} \in \pi A$ and $\mathfrak{m} = \pi A$ is a principal ideal in A.

Conversely let $\mathfrak{m} = (\pi)$ be a principal ideal. Then $|K^{\times}| \le \mathbb{R}_+$ is the subgroup generated by $|\pi|$ and hence isomorphic to $\mathbb{Z}$. □

Example 8.3.6. *The p-adic valuation $|\ |_p$ on $\mathbb{Q}$ is discrete, and its valuation ring A and its group of units U are given by*

$$\begin{aligned}
A =&\mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} \mid (n,p) = 1\}, \\
U =&\mathbb{Z}_{(p)}^{\times} = \{m/n \in \mathbb{Q} \mid p \nmid mn\},
\end{aligned}$$

with maximal ideal $\mathfrak{m} = pA$ and residue class field $A/pA \simeq \mathbb{F}_p$.

More generally let K be a number field with ring of integers $\mathcal{O}_K$, and $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then the map $\nu_{\mathfrak{p}}\colon K^\times \to \mathbb{Z}$ with $\nu_{\mathfrak{p}}(a) = n_{\mathfrak{p}}$ and

$$a\mathcal{O}_K = \prod_{\mathfrak{q} \text{ prim}} \mathfrak{q}^{n_{\mathfrak{q}}}$$

is a valuation and

$$|a|_{\mathfrak{p}} = N(\mathfrak{p})^{-\nu_{\mathfrak{p}}(a)} = (\#\mathcal{O}_K/\mathfrak{p})^{-\nu_{\mathfrak{p}}(a)}$$

is the corresponding absolute value on K with valuation ring

$$A = (\mathcal{O}_K)_{\mathfrak{p}} = \left\{ \frac{a}{b} \in K \mid a \in \mathcal{O}_K,\, b \in \mathcal{O}_K \setminus \mathfrak{p} \right\}.$$

This ring coincides with the localization of $\mathcal{O}_K$ by $\mathfrak{p}$. The maximal ideal of A is the principal ideal $\mathfrak{p}A$, and the residue class field is $A/\mathfrak{p}A$, which is isomorphic by Proposition 6.1.7 to the usual residue class field $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ of $\mathfrak{p}$, see Definition 6.3.7. So we have

$$(\mathcal{O}_K)_{\mathfrak{p}}/\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}} \simeq \mathcal{O}_K/\mathfrak{p}.$$

Definition 8.3.7. A *discrete valuation ring* is an integral domain A, which is the valuation ring of a discrete valuation on the quotient field K of A.

We have proved in Theorem 5.3.16 of [**1**] the following charactzerizations of such a ring.

Theorem 8.3.8. *Let A be an integral domain, which is not a field. Then the following statements are equivalent.*

(1) *A is a discrete valuation ring.*
(2) *A is a local PID.*
(3) *A is a factorial ring with, up to associates, a unique irreducible element.*
(4) *A is a Noetherian local ring, whose maximal ideal is a principal ideal.*
(5) *A is a local Dedekind ring.*

8.4. Completions

Let K be a field with a non-trivial absolute value $|\ |$. Then $d(a, b) = |a - b|$ is a metric on K, and a sequence (a_n) of elements from K is called a *Cauchy sequence*, if there is for each $\varepsilon > 0$ an N such that

$$d(a_n, a_m) < \varepsilon$$

for all $n, m > N$.

Example 8.4.1. *Let $K = \mathbb{Q}$ equipped with the 5-adic metric. Then the sequence $a_n = \frac{1}{2^n}$ is not a Cauchy sequence. On the other hand,*

$$4, 34, 334, 3334, 33334, \ldots$$

is a Cauchy sequence.

Indeed, we have $d(a_n, a_{n+1}) = |2^{-(n+1)}|_5 = 5^0 = 1$, so that (a_n) is not a Cauchy sequence. For the second sequence we have for all $m > n$,

$$d(b_m, b_n) = 5^{-n}.$$

Hence it is a Cauchy sequence, which converges to $\frac{2}{3} \in \mathbb{Q}$, because

$$3 \cdot 4 = 12,\ 3 \cdot 34 = 102,\ 3 \cdot 334 = 1002,\ 3 \cdot 3334 = 10002, \ldots$$

and hence $3 \cdot a_n - 2 \to 0$ for $n \to \infty$ in the 5-adic topology.

Definition 8.4.2. A field K with a valuation $|\ |$ on it is called a *valued field.* A valued field $(K, |\ |)$ is called *complete*, if every Cauchy sequence has a limit in K.

We know that $\mathbb{Q}$ with respect to the real absolute value is not complete. The same is true for every p-adic absolute value on $\mathbb{Q}$. By Ostrowski's theorem we obtain the following result.

Proposition 8.4.3. *The field $\mathbb{Q}$ is not not complete with respect to any of its absolute values.*

Proof. Let $|\ |$ be an absolute value on $\mathbb{Q}$. By Ostrowski's Theorem 8.2.1 we need to show that $(\mathbb{Q}, |\ |_\infty)$ and all $(\mathbb{Q}, |\ |_p)$ are not complete. In the first case we construct a sequence $(a_n)$with rational a_n recursively by $a_1 = 1$ and

$$a_{n+1} = \frac{a_n}{2} + \frac{1}{a_n}.$$

This is a Cauchy sequence in $\mathbb{Q}$ with respect to $|\ |_\infty$, which doesn't converge to a rational number. Indeed, a limit x would necessarily satisfy $x^2 = 2$ in $\mathbb{Q}$.

In the second case we consider $\mathbb{Q}$ equipped with the p-adic metric. Let $a \in \mathbb{Z}$ with $1 < a < p-1$. Then the sequence

$$a_n = a^{p^n}$$

is a Cauchy sequence having no limit in $\mathbb{Q}$. Indeed, we have

$$a_{n+1} - a_n = a^{p^{n+1}} - a^{p^n} = a^{p^n}(a^{\varphi(p^{n+1})} - 1),$$

and by Fermat's little theorem we have $p^{n+1} \mid a^{\varphi(p^{n+1})} - 1$. Hence

$$|a_{n+1} - a_n|_p < p^{-n-1},$$

so that (a_n) is a Cauchy sequence. The reason is, that for a non-archimedean absolute value $|\ |$ the sequence (a_n) is a Cauchy sequence if and only if

$$\lim_{n\to\infty} |a_{n+1} - a_n| = 0.$$

Now assume this sequence has a limit $x \in \mathbb{Q}$. Then

$$\begin{aligned} |x - a|_p &= |x - a^{p^n} + a^{p^n} - a|_p \\ &\le \max\{\{|x - a^{p^n}|_p, |a^{p^n} - a|_p\} \\ &= |a^{p^n} - a|_p \\ &\le |a^{p^n - 1} - 1|_p \\ &< 1. \end{aligned}$$

Furthermore $x = \lim_{n\to\infty} a_n = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} a_n^p = x^p$. Since $x \neq 0$ we have $x^{p-1} = 1$ and $x \in \mathbb{Q}$, hence $x = 1$. However, $|x - a|_p < 1$ implies that $p \mid (x - a)$, and hence $p \mid (1 - a)$. Then we have $1 - a = pk$ for some $k \in \mathbb{Z}$, i.e., $a = pk + 1$. For $k > 0$ we have $a > p$, and for $k < 0$ we have $a < 1$. Both is a contraction to $1 < a < p - 1$. □

So both the metric space $(\mathbb{Q}, |\ |_\infty)$ and the ultrametric space $(\mathbb{Q}, |\ |_p)$ are not complete. However, they can be completed as every metric space can be completed. Before doing so we want to illustrate, why the p-adic metric differs very much from the Euclidean metric.

Lemma 8.4.4. *Let $|\ |$ be a non-archimedean absolute value on K. Suppose that $x, a, b \in K$ satisfy $|x-b| < |x-a|$. Then it follows that $|b-a| = |x-a|$. So every triangle in the ultrametric space $(K; |\ |)$ is an isosceles triangle.*

PROOF. Indeed, we have

$$\begin{aligned}|b-a| &= |b-x+x-a| = \max\{|b-x|, |x-a|\}\\ &= |x-a|.\end{aligned}$$

□

REMARK 8.4.5. A strange fact is also the following. Every point inside a ball

$$B(x,r) = \{y \in K \mid |x-y| < r\}$$

is its center. So if $d(x,y) < r$ then $B(x,r) = B(y,r)$. Moreover intersecting balls are contained in each other, i.e. if $B(x,r) \cap B(y,s)$ is non-empty then either $B(x,r) \subseteq B(y,s)$ or $B(y,s) \subseteq B(x,r)$.

THEOREM 8.4.6. *Let K be a field with absolute value $|\ |$. Then there exists a complete valued field $\widehat{K}$ containing K as a dense subfield and extending the valuation on K to $\widehat{K}$. It has a universal property, namely every homomorphism $K \to L$ to a complete valued field L extending the valuation on K, can be uniquely extended to a homomorphism $\widehat{K} \to L$.*

PROOF. The result is a special case of a general result on the completion of metric spaces. So we may restrict the proof to the points we need. Let R be the ring of Cauchy sequences in K, and

$$\mathcal{M} = \{(a_n) \in R \mid a_n \to 0\}$$

the ideal Cauchy sequences converging to zero. It is easy to see that $\mathcal{M}$ is a maximal ideal. So we obtain a field

$$\widehat{K} = R/\mathcal{M},$$

consisting of equivalence classes of such Cauchy sequences. There is a canonical embedding $K \hookrightarrow \widehat{K}$ by mapping each $a \in K$ to the constant Cauchy sequence $(a) = (a, a, a, \ldots)$, i.e., to their equivalence class a in $\widehat{K}$. The absolute value $|\ |$ on K can be extended to $\widehat{K}$ by defining for the class a of the Cauchy sequence (a_n)

$$|a| = \lim_{n\to\infty} |a_n|.$$

This limit exists because of the completeness of $\mathbb{R}$, since the sequence $(|a_n|)$ is a Cauchy sequence in $\mathbb{R}$. Indeed, $||a_m| - |a_n|| \le |a_m - a_n|$. Now one can show easily that $\widehat{K}$ is complete with respect to its absolute value. By the universal property $\widehat{K}$ is unique up to a canonical isomorphism. The image of K is dense in $\widehat{K}$, because the closure $\overline{K}$ in $\widehat{K}$ is complete and satisfies the universal property like $\widehat{K}$ does. Hence we have $\overline{K} \simeq \widehat{K}$. □

COROLLARY 8.4.7. *An absolute value on K is non-archimedean if and only if it is non-archimedean on $\widehat{K}$. In this case we have $|K| = |\widehat{K}|$.*

PROOF. The absolute value $|\ |$ on K is non-archimedean if and only if it has bounded values on $\{m1 \mid m \in \mathbb{Z}\}$, see Proposition 8.1.7. Since $|K|$ extends the absolute value on K, and all $m1$ lie in K, this criterion also holds in $\widehat{K}$.

Let $b \neq 0$ in $\widehat{K}$. Then there exists a $c \in K$ with $|b-c| < |c|$. By Lemma 8.4.4 it follows $|b| = |c|$, and therefore $|K| = |\widehat{K}|$. □

EXAMPLE 8.4.8. *The completion of $\mathbb{Q}$ with respect to $|\ |_\infty$ equals $\mathbb{R}$.*

Definition 8.4.9. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\ |_p$ is denoted by $\mathbb{Q}_p$. It is called the *field of p-adic numbers.* Its valuation ring A is denoted by $\mathbb{Z}_p$. It is called the *ring of p-adic integers.*

In other words, $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \le 1\}$. Note that $\mathbb{Q}_p$ is a field of characteristic zero. One may view p-adic numbers in $\mathbb{Q}_p$ as equivalence classes of Cauchy sequences of the form

$$a_{-n}p^{-n} + \cdots + a_{-1}p^{-1} + a_0 + a_1p + a_2p^2 + \cdots$$

with integers $0 \le a_i < p$. If the coefficients with negative index vanish, then $a \in \mathbb{Z}_p$. The ring $\mathbb{Z}_p$ is a discrete valuation ring (DVR), hence a PID with maximal ideal $p\mathbb{Z}_p$ and quotient field $\mathbb{Q}_p$. We have $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$. One can introduce $\mathbb{Q}_p$ and $\mathbb{Z}_p$ also by inverse limits of projective systems, see Example 5.3.20 in my notes [**1**].

8.5. Local fields

A local field is the completion of a global field with respect to a canonical absolute value. There are several equivalent definitions of a local field. Let us consider the following definition.

Definition 8.5.1. A *local field* is a field, which is a complete metric space with respect to a discrete valuation, and has a finite residue class field.

For example, $\mathbb{R}$ and $\mathbb{C}$ are local fields, called *archimedean local fields.* They are the only archimedean local fields. If the valuation is non-archimedean, we call the fields non-archimedean local fields. Examples are $\mathbb{Q}_p$ and finite extensions of $\mathbb{Q}_p$.

Example 8.5.2. *Let K be a number field, $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, and $K_\mathfrak{p}$ be the completion of $K$with respect to the $\mathfrak{p}$-adic norm. Then $K_\mathfrak{p}$ is a non-archimedean local field.*

We denote by $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$ the completion of the ring $\mathcal{O}_K$ with respect to the $\mathfrak{p}$-adic metric. One can show the following result.

Proposition 8.5.3. *Let K be a global field with ring of integers $\mathcal{O}_K$, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring with quotient field $K_\mathfrak{p}$ and finite residue class field $\mathcal{O}_K/\mathfrak{p}$. The ring $\mathcal{O}_\mathfrak{p}$ is compact for the $\mathfrak{p}$-adic metric, and the field $K_\mathfrak{p}$ is locally compact.*

Here a metric space is called *locally compact*, if every bounded sequence has a convergent subsequence. The compactness of $\mathcal{O}_\mathfrak{p}$ can be seen by representing this ring as inverse limit of $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^n$, which is compact as a closed subset of the infinite product $\prod_n \mathcal{O}_\mathfrak{p}/\mathfrak{p}^n$. This follows, since the product is compact by Tychonoff's theorem, because all factors are compact. Indeed, all rings $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^n$ are finite, hence compact. Let $a \in K_\mathfrak{p}$. Then $a + \mathcal{O}_\mathfrak{p}$ is an open and compact neighborhood. Hence $K_\mathfrak{p}$ is locally compact. There is also the following result.

Proposition 8.5.4. *Let K be a valued field of characteristic zero. Then the following statements are equivalent.*

(1) *K is a local field.*
(2) *K is a finite extension of $\mathbb{Q}_p$.*
(3) *K is complete, locally compact and not discrete.*
(4) *K is a completion $K_\mathfrak{p}$ as in Example* 8.5.2.

Remark 8.5.5. There is a similar result for fields of characteristic p. Then K is a local field if and only if K is a finite extension of some $\mathbb{F}_q((t))$ over a finite field $\mathbb{F}_q$, where $q = p^n$.

Helmut Hasse's *local-global principle*, also known as the Hasse principle, is the idea that certain types of equations have a rational solution if and only if they have a solution in the real numbers and in the p-adic numbers for each prime p. This works particularly well for quadratic forms. We have the following theorem.

THEOREM 8.5.6 (Hasse-Minkowski). *Let K be a global field and*

$$f(x) = a_1 x_1^2 + \cdots + a_n x_n^2$$

a quadratic form with coefficients in $K^\times$. Then f has a nontrivial root in K, if and only if f has a nontrivial root in each local field arising as completion of K with respect to an absolute value on K.

Hasse proved this result for $K = \mathbb{Q}$ in his thesis, in 1921. He generalized it to all number fields in 1924. His result over $\mathbb{Q}$ is as follows.

COROLLARY 8.5.7. *Let $Q(x_1, \dots, x_n)$ be a quadratic form over $\mathbb{Q}$. Then the equation $Q(x_1, \dots, x_n) = 0$ has a nontrivial solution over $\mathbb{Q}$ if and only if it has a nontrivial solution over $\mathbb{R}$ and over all p-adic fields $\mathbb{Q}_p$.*

The *trivial* solution is $(x_1, \dots, x_n) = 0$. One direction of Hasse-Minkowski is not difficult. A nontrivial solution in a global field K yields a nontrivial solution in the local field $K_{\mathfrak{p}}$. The converse direction is more difficult. The proof also needs the *Hensel Lemma.*

LEMMA 8.5.8 (Hensel). *Let K be a complete and discretely valued field with discrete valuation ring A, and maximal ideal $\mathfrak{m}$ of A. Let $f(t) \in A[t]$ be a polynomial, and a_0 be a simple root of f modulo $\mathfrak{m}$, so*

$$\begin{aligned} f(a_0) &\equiv 0 \mod \mathfrak{m}, \\ f'(a_0) &\not\equiv 0 \mod \mathfrak{m}. \end{aligned}$$

Then there exists a unique $a \in A$ with $f(a) = 0$ and $a \equiv a_0 \mod \mathfrak{m}$.

PROOF. Let $\mathfrak{m} = (\pi)$. We inductively construct roots of f modulo π^n for all $n \in \mathbb{N}$, that is, $a_n \in A$ with

$$f(a_n) \equiv 0 \mod \pi^{n+1}.$$

For $n = 0$ this is the assumption. For the induction step we use the Taylor series of f, and obtain

$$\begin{aligned} f(a_n + h\pi^{n+1}) &= f(a_n) + h\pi^{n+1} f'(a_n) + \frac{1}{2!}(h\pi^{n+1})^2 f''(a_n) + \cdots \\ &= f(a_n) + h\pi^{n+1} f'(a_n) \mod \pi^{n+2} \\ &\equiv 0 \mod \pi^{n+2}, \end{aligned}$$

where

$$h := -\frac{f(a_n)}{\pi^{n+1}} \cdot \frac{1}{f'(a_n)}.$$

Note that h is well-defined because of $f'(a_n) \not\equiv 0 \mod \pi$. We define

$$a_{n+1} = a_n + h\pi^{n+1}$$

and obtain, because of $f(a_n) \equiv 0 \mod \pi^{n+1}$,

$$f(a_{n+1}) = f(a_n + h\pi^{n+1}) \equiv 0 \mod \pi^{n+2}.$$

So we have shown the induction step. By construction this sequence converges. Let $a \in A$ be the limit. Since $a \equiv a_n \mod \pi^n$ we obtain $f(a) \equiv f(a_n) \equiv 0 \mod \pi^{n+1}$ for all $n \in \mathbb{N}$, and therefore $f(a) = 0$. □

In the special case of $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p$, $\mathfrak{m} = (p) = p\mathbb{Z}_p$ and $A/\mathfrak{m} \simeq \mathbb{F}_p$ we obtain the following version.

Corollary 8.5.9. *Let f be a polynomial in $\mathbb{Z}_p[t]$ and $a_0 \in \mathbb{Z}_p$ with $f(a_0) \equiv 0 \mod p\mathbb{Z}_p$, but $f'(a_0) \not\equiv 0 \mod p\mathbb{Z}_p$. Then there exists a unique $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a \equiv 0 \mod p\mathbb{Z}_p$.*

If f in $\mathbb{Z}[t] \subseteq \mathbb{Z}_p[t]$, then the assumption in the corollary says that $f(a_0) = 0$ and $f'(a_0) \neq 0$ in the finite field $\mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. Then there exists a unique $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a_0 = a$ in $\mathbb{F}_p$. So we can *lift* a root of f in a finite field to a root in $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. However, for roots over finite fields we have the following result.

Proposition 8.5.10 (Chevalley-Warning). *Let $K = \mathbb{F}_{p^r}$ be a finite field and $f \in K[x_1, \ldots, x_n]$ be a polynomial of total degree $\deg(f) < n$. Then $V_K := \{x \in K^n \mid f(x) = 0\}$ satisfies the congruence $\#V_K \equiv 0 \mod p$.*

Corollary 8.5.11. *Every quadratic form over a finite field in at least three variables has a nontrivial root.*

Proof. Since $0 \in V_K$ we have $\#V_K \geq p$ by Chevalley-Warning, provided that $n > \deg(Q) = 2$. □

Example 8.5.12. *The quadratic form*

$$Q(x, y, z) = 5x^2 + 7y^2 - 13z^2$$

has a nontrivial root in $\mathbb{R}$ and in every p-adic field $\mathbb{Q}_p$.

Proof: Obviously

$$5x^2 + 7y^2 - 13z^2 = 0$$

has a nonzero root in $\mathbb{R}$. By Chevalley-Warning every quadratic form in at least three variables has a nontrivial root in every finite field. Hence there are $a, b, c \in \mathbb{Z}$

$$5a^2 + 7b^2 - 13c^2 \equiv 0 \mod p,$$

so that at least one of these numbers a, b, c is not divisible by p, since the solution is nontrivial. We may assume that $p \nmid a$. However, to satisfy the assumption that the quadratic form really has at least three variables we have to assume in addition that

$$p \neq 5, 7, 13$$

Now we apply Hensel's lemma in the form of Corollary 8.5.9. The polynomial $f(t) = 5t^2 + 7b^2 - 13c^2$ has by Chevalley-Warning a root a with $f(a) \equiv 0 \mod (p)$. Then we have

$$f'(a) = 10a \not\equiv 0 \mod (p)$$

if $p \neq 2, 5$. We also assumed that $p \nmid a$. Now Henssel's lemma yields the existence of an $\overline{a} \in \mathbb{Z}_p \subseteq \mathbb{Q}_p$ with $f(\overline{a}) = 0$. This yields a nontrivial solution $(\overline{a}, b, c)$ of $5x^2 + 7y^2 - 13z^2 = 0$ over $\mathbb{Q}_p$ for every prime number different from $2, 5, 7, 13$. For the primes $2, 5, 7, 13$ we can apply the same idea, with suitable polynomials f. So we have found nontrivial solutions of $5x^2 + 7y^2 - 13z^2 = 0$ over every $\mathbb{Q}_p$ and over $\mathbb{R}$. □

Note that by Hasse-Minkowski, $5x^2 + 7y^2 - 13z^2 = 0$ has a nontrivial rational solution. A quadratic form has a nontrivial rational solution if and only if it has a nontrivial *integer* solution. And indeed,

$$(x, y, z) = (3, 1, 2)$$

is an integer solution. There is a criterion by Lagrange for the existence of nontrivial integer roots.

THEOREM 8.5.13 (Lagrange). *Let a, b, c be positive, squarefree, pairwise coprime integers. Then $ax^2 + by^2 = cz^2$ has a nontrivial integral root if and only if*

$$\left(\frac{bc}{a}\right) = \left(\frac{ac}{b}\right) = \left(\frac{-ab}{c}\right) = 1.$$

It is better to use the notation $bc \,\square\, a$, $ac \,\square\, b$ and $-ab \,\square\, c$, because it is not the Jacobi symbol in general. For the example $5x^2 + 7y^2 = 13z^2$ we have

$$\left(\frac{7 \cdot 13}{5}\right) = \left(\frac{5 \cdot 13}{7}\right) = \left(\frac{-5 \cdot 7}{13}\right) = 1$$

so that there is a nontrivial integer solution.

EXAMPLE 8.5.14. *The quadratic form*

$$Q(x, y, z) = x^2 + y^2 - 3z^2$$

has no non-trivial integer root.

How do we find a nontrivial root for a ternary quadratic form, if there exists one? Here is an example of an algorithm, based on the following result by Holzer.

PROPOSITION 8.5.15 (Holzer 1950). *Let a, b, c be squarefree integers. Suppose that the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integer solution, then there exists a nontrivial solution with*

$$|x| \le \sqrt{|bc|},\ |y| \le \sqrt{|ca|},\ |z| \le \sqrt{|ab|}.$$

The algorithm then is as follows. Search for a nontrivial solution in the indicated range. Either one finds a solution there, or there is none. However, the size of the search space is exponential in the length of the input, which is $O(\log(|abc|))$. So we need more efficient algorithms in general. For such algorithms, see for example [**5**]. Here is an example from [**5**]:

EXAMPLE 8.5.16. *The equation*

$$x^2 - 310146482690273725409y^2 + 113922743z^2 = 0$$

has a nontrivial integer solution. Here is such a solution satisfying Holzer's condition:

$$(x, y, z) = (70647575606369,\ 5679,\ 6632499416).$$

8.6. Failure of the Hasse Principle

Unfortunately, a general polynomial equation of higher degree having nontrivial solutions in $\mathbb{R}$ and all p-adic fields, by no means needs to have a nontrivial solution in $\mathbb{Q}$. So the Hasse principle fails in general. Here is a very simple counterexample.

PROPOSITION 8.6.1. *The equation*

$$f = (X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

has a nontrivial root in $\mathbb{R}$ and every $\mathbb{Q}_p$, but has no nontrivial rational root.

Proof. Obviously, $2, 17, 34$ have no square root in $\mathbb{Q}$, so that f has no rational root at all. So it remains to show that f has a root in every $\mathbb{Q}_p$. For $p = 17$ we have $f(6) \equiv 0 \bmod 17$ and $f'(6) \equiv 12 \not\equiv 0 \bmod 17$. So by Hensel's Lemma, there is a root in $\mathbb{Q}_{17}$. For $p = 2$ we have $17 \equiv 1 \bmod 8$, and one can show that 17 is a 2-adic square. Finally, let $p \neq 2, 17$. If $\left(\frac{2}{p}\right) = 1$ or $\left(\frac{17}{p}\right) = 1$, then $x^2 = 2$ or $x^2 = 17$ has a solution a in $\mathbb{F}_p$ with $f(a) \equiv 0 \bmod p$ and $f'(a) \not\equiv\equiv 0 \bmod p$. So by Hensel's Lemma, there is a solution in $\mathbb{Q}_p$. Otherwise we have $\left(\frac{2}{p}\right) = \left(\frac{17}{p}\right) = -1$, so that

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = (-1) \cdot (-1) = 1.$$

So again there is a solution in $\mathbb{Q}_p$. □

The first counterexample actually is due to Selmer in 1951.

Theorem 8.6.2 (Selmer). *The homogeneous polynomial equation*

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a nontrivial solution over every p-adic field $\mathbb{Q}_p$ and over $\mathbb{R}$, but not over $\mathbb{Q}$.

A proof can be found in the note *Counterexample to the local-global principle* by K. Conrad. The existence of nontrivial local solutions follows from the Hasse-Weil bound for finite fields. They can be named also explicitly. Indeed,

$$\begin{aligned}(x, y, z) = (-1, \sqrt[3]{3/4}, 0),\ (0, \sqrt[3]{5/4}, -1),\\ (5, -2\sqrt[3]{15/4}, -3),\ (-1, 0, \sqrt[3]{3/5})\end{aligned}$$

are always solutions in $\mathbb{R}$, and at least one exists in a given field $\mathbb{Q}_p$.

The harder part is to show that Selmer's equation has no rational solution except for $(x, y, z) = (0, 0, 0)$. Here one can pass to the curve $a^3 + 6b^3 = 10c^3$ via $a = 2y$, $b = x$, $c = -z$ and view this equation as a norm equation

$$N_{K/\mathbb{Q}}(a + b\sqrt[3]{6}) = 10c^3$$

in the field $K = \mathbb{Q}(\sqrt[3]{6})$ and its ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{6}]$. In fact, the class number is $h_K = 1$.

We also want to mention another counterexample.

Proposition 8.6.3 (Lind, Reichardt). *The polynomial equation*

$$X^4 - 2Y^2 - 17Z^4 = 0$$

has a nontrivial solution over every p-adic field $\mathbb{Q}_p$ and over $\mathbb{R}$, but not over $\mathbb{Q}$.

Finally, let us give a positive result, namely an application of Hasse-Minkowski.

Proposition 8.6.4 (Three-square theorem). *Let n be a positive integer. Then the following statements are equivalent.*

(1) *$n = a^2 + b^2 + c^2$ for integers a, b, c.*
(2) *n is not of the form $4^\ell(8k + 7)$ for $k, \ell \in \mathbb{Z}_{\geq 0}$.*
(3) *$-n$ is not a square in the 2-adic field $\mathbb{Q}_2$.*

Proof. We only give a few ideas on the proof, in particular how to apply Hasse-Minkowski.

(1) ⇒ (2): Let us show the negation, i.e., if n is of the form $4^\ell(8k-1)$, then n *cannot* be the sum of three squares. First note the following fact. If $4n = x_1^2 + x_2^2 + x_3^2$ is the sum of three squares, so must be n, namely $n = (x_1/2)^2 + (x_2/2)^2 + (x_3/2)^2$, because all x_i are even. So it is enough to show that $n = 8k+7$ is not the sum of three squares. Indeed, since a square is congruent to $0, 1, 4 \mod 8$, the sum of three squares cannot be congruent to $7 \mod 8$ and we are done.

(2) ⇒ (1) First note that if n is the sum of three rational squares, then n is also the sum of three integer squares. Now consider the nondegenerate quadratic form

$$Q(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 - nx_4^2.$$

The equation $Q(x) = 0$ certainly has a nontrivial solution in $\mathbb{R}$, but also in every p-adic field $\mathbb{Q}_p$. For example, if p is an odd prime, then at least three of the coefficients of the diagonal quadratic form are p-adic units. Then we always have a nontrivial root in $\mathbb{Q}_p$. For $p = 2$ one needs an additional argument with quadratic residues. The point is that we may apply Hasse-Minkowski to obtain a nontrivial rational root with $x_4 \neq 0$. So we may divide by x_4^2 and obtain a representation of n as a sum of three rational squares, and then also of three integer squares. □

CHAPTER 9

The Theorem of Kronecker-Weber

The Kronecker-Weber Theorem says that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. Here an extension is called *abelian*, if it is a Galois extension with abelian Galois group. This result was first formulated by Kronecker in 1853, but not completely proved. In fact, there was a gap for the case, where the number field degree is a power of two. Weber published a proof in 1886, but again there was a gap. A complete proof was finally given by Hilbert 1896.

The result nowadays belongs to *class field theory*, which studies abelian extensions of global fields. This theory is an important branch of number theory. There are at least three topics which have stimulated the development of class field theory at the end of the 19-th century. Firstly, the relationship between abelian extensions and ideal class groups, secondly density results for primes and L-series, and thirdly reciprocity laws.

The Kronecker-Weber Theorem follows directly from the results of general class field theory, which are not available here. So we want to give an elementary proof relying on the local-global principle. We first prove the result for all p-adic fields $\mathbb{Q}_p$ and for $\mathbb{R}$. Then we conclude it for $\mathbb{Q}$. For a reference see the book [**12**].

9.1. Preparations

Let K and L be finite extensions of a field k. Then the smallest field containing K and L is called the *composite* of K and L, and is denoted by KL. For the following lemma see for example [**7**].

Lemma 9.1.1. *Let K and L be finite Galois extensions of a field k. Then $K \cap L$ and KL are also finite Galois extensions of k, and the group* $\mathrm{Gal}(KL/k)$ *is isomorphic to the subgroup*

$$\{(\varphi, \psi) \in \mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k) \mid \varphi_{|K\cap L} = \psi_{|K\cap L}\}$$

of $\mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k)$.

Corollary 9.1.2. *Let K and L be finite Galois extensions of a field k with $K \cap L = k$. Then we have*

$$\mathrm{Gal}(KL/k) \simeq \mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k).$$

Let L/K be an extension of fields. If $\mathbb{R} \subseteq K$, then we only have the three possibilities

$$\mathbb{R}/\mathbb{R},\ \mathbb{C}/\mathbb{R},\ \mathbb{C}/\mathbb{C}.$$

For the extension $\mathbb{C}/\mathbb{R}$ we define the ramification index by $e(\mathbb{C}/\mathbb{R}) = 2$, and the residue class degree by $f(\mathbb{C}/\mathbb{R}) = 1$. So let us assume from now on that we have $\mathbb{Q}_p \subseteq K$ for some fixed prime p. We call the field K then a p-adic field.

Definition 9.1.3. Let E/F be an extension of p-adic fields with local ring of integers $\mathcal{O}_{\mathfrak{p}_E}$ and $\mathcal{O}_{\mathfrak{p}_F}$, maximal ideals $\mathfrak{p}_E$ and $\mathfrak{p}_F$, and residue class fields $\kappa(\mathfrak{p}_E) = \mathcal{O}_{\mathfrak{p}_E}/\mathfrak{p}_E$ and $\kappa(\mathfrak{p}_F) = \mathcal{O}_{\mathfrak{p}_F}/\mathfrak{p}_F$. Then

$$f(E/F) := [\kappa(\mathfrak{p}_E) : \kappa(\mathfrak{p}_F)]$$

is called the *residue class degree* of E/F. The *ramification degree* $e = e(E/F)$ is defined by

$$\mathfrak{p}_F \mathcal{O}_E = \mathfrak{p}_E^e.$$

The extension E/F is called *unramified*, if $e(E/F) = 1$. The extension is called *tamely ramified*, if $p \nmid e(F/E)$ for $p = \operatorname{char}(\kappa(\mathfrak{p}_F))$. It is called *totally ramified*, if $f(E/F) = 1$.

We have the local degree theorem, saying that $[E : F] = e(E/F)f(E/F)$.

Lemma 9.1.4. *Let L/K be an extension of number fields, P be a prime ideal of $\mathcal{O}_L$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Let L_P and $K_\mathfrak{p}$ be the completions of L and K with respect to the P-adic and the $\mathfrak{p}$-adic metric. Denote the completions of $\mathcal{O}_L$ and $\mathcal{O}_K$ by $\mathcal{O}_P$ and $\mathcal{O}_\mathfrak{p}$. Then the residue class fields of L_P and L are isomorphic, as well as those of $K_\mathfrak{p}$ and K, and we have*

$$e(L_P \mid K_\mathfrak{p}) = e(P \mid \mathfrak{p}),$$
$$f(L_P \mid K_\mathfrak{p}) = f(P \mid \mathfrak{p}).$$

Proof. The residue class fields $\kappa(P) = \mathcal{O}_P/\mathfrak{p}_L \simeq \mathcal{O}_L/P = k(P)$ and $\kappa(\mathfrak{p}) = \mathcal{O}_\mathfrak{p}/\mathfrak{p}_K \simeq \mathcal{O}_K/\mathfrak{p} = k(\mathfrak{p})$ are isomorphic, see Proposition 8.5.3. Therefore the residue class degrees are the same. The local degree theorem yields

$$[L_P : K_\mathfrak{p}] = e(L_P \mid K_\mathfrak{p}) \cdot f(L_P \mid K_\mathfrak{p}).$$

This implies the second claim. □

Lemma 9.1.5. *Let E/F be a Galois extension of p-adic fields. Then* $\operatorname{Gal}(E/F)$ *acts on $\mathcal{O}_{\mathfrak{p}_E}$ and induces a surjective group homomorphism*

$$\operatorname{Gal}(E/F) \to \operatorname{Gal}(\kappa(\mathfrak{p}_E)/\kappa(\mathfrak{p}_F))$$

with kernel $I(E/F)$. We have

$$\#I(E/F) = e(E/F),$$
$$\# \operatorname{Gal}(\kappa(\mathfrak{p}_E)/\kappa(\mathfrak{p}_F)) = f(E/F).$$

The subextension $E^{I(E/F)}/F$ is unramified.

Proof. The proof goes like in the number field case, see Proposition 6.3.9, and is even easier. □

Finally we need the following tow lemmas.

Lemma 9.1.6. *Let L/K be a finite extension of number fields, $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ and P be a prime ideal in $\mathcal{O}_L$ lying over $\mathfrak{p}$. Then we have*

$$Gal(L_P/K_\mathfrak{p}) \simeq D_P,$$
$$I(L_P/K_\mathfrak{p}) \simeq I_P.$$

Lemma 9.1.7. *Let L_1/K and L_2/K be Galois extensions of p-adic local fields with $L = L_1L_2$ and $e(L_1/K) = 1$. Then we have $e(L/K) = e(L_2/K)$. In particular, if L_2/K is unramified, so is L/K.*

9.2. Reduction to the local version

The aim of this section is to conclude the global version of Kronecker-Weber from the local version. This is a nice example of the local-global principle. Let us first state the exact versions for the local and global Kronecker-Weber.

THEOREM 9.2.1 (Local Kronecker-Weber). *Let $K/\mathbb{Q}_p$ be a finite abelian field extension of p-adic fields. Then there exists a primitive n-th root of unity with $K \subseteq \mathbb{Q}_p(\zeta_n)$.*

This will be proved in section 9.3. Note that also the local version holds for $\mathbb{Q}_\infty = \mathbb{R}$, which is not saying much, because we only have the finite extensions $\mathbb{R}/\mathbb{R}$ and $\mathbb{C}/\mathbb{R}$ over $\mathbb{R}$.

THEOREM 9.2.2 (Global Kronecker-Weber). *Let $K/\mathbb{Q}$ be a finite abelian field extension. Then there exists a primitive n-th root of unity with $K \subseteq \mathbb{Q}(\zeta_n)$.*

PROOF. Let $K/\mathbb{Q}$ be a finite abelian extension and let S be the set of rational primes, for which $\mathfrak{p} = (p)$ ramifies in K. We have $S = \{p \in \mathbb{P} \mid p \mid d\}$ for the absolute discriminant d of K, see Proposition 6.4.1. Let P over $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and consider the completions K_P and $\mathbb{Q}_p$. Then $\mathrm{Gal}(K_P/\mathbb{Q}_p) \simeq D_P \subseteq \mathrm{Gal}(K/\mathbb{Q})$ is also abelian and $K_P/\mathbb{Q}_p$ is an abelian extension. By Theorem 9.2.1 the exists a primitive n_p-th root of unity ζ_{n_p} with $K_P \subseteq \mathbb{Q}_p(\zeta_{n_p})$. Let p^{e_p} be the exact p-power in n_p. We define

$$n := \prod_{p\in S} p^{e_p}.$$

We want to show that $K \subseteq \mathbb{Q}(\zeta_n)$. So let

$$L := K(\zeta_n)$$

and we show that $L = \mathbb{Q}(\zeta_n)$. By Lemma 9.1.1, $\mathrm{Gal}(L/\mathbb{Q})$ is a subgroup of the abelian group $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, hence also abelian. Thus $L/\mathbb{Q}$ is a finite abelian extension. It is unramified outside of S. Indeed, if (p) is ramified over L, it is ramified over K and hence $p \in S$. Let L_Q be the completion at a suitable prime ideal Q over (p), so with

$$\mathbb{Q}_p \subseteq K_P \subseteq L_Q.$$

Then, with $(m,p) = 1$, we have

$$L_Q = K_P(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{p^{e_p}m}) = \mathbb{Q}_p(\zeta_{p^{e_p}})\mathbb{Q}_p(\zeta_m).$$

Here the extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified and $\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p$ is totally ramified.
Since $\mathbb{Q}(\zeta_{p^{e_p}})/\mathbb{Q}$ is purely ramified over p, with $e = \varphi(p^{e_p})$ by Lemma 7.2.1, Lemma 9.1.4 implies that

$$e(\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p) = e = \varphi(p^{e_p}).$$

Hence the inertia group

$$I_p = I(L_Q/\mathbb{Q}_p)$$

has exactly $\varphi(p^{e_p})$ elements by Lemma 9.1.5. Now let I be the subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ generated by all I_p with $p \in S$. Since these groups are abelian, I is the image of $\prod_p I_p$ under the natural map. We have

$$\#I \le \prod_{p\in S} \#I_p = \prod_{p\in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

By construction of I the extension $L^I/\mathbb{Q}$ is unramified, where L^I is the fixed field. Therefore we have $L^I = \mathbb{Q}$ by Proposition 6.4.4, namely by Hermite-Minkowski. So we obtain

$$[L : \mathbb{Q}] = \#I \le \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Now $\mathbb{Q}(\zeta_n) \subseteq L$ implies that $L = \mathbb{Q}(\zeta_n)$. □

9.3. Proof of the local version

Let $K/\mathbb{Q}_p$ be a finite abelian extension of p-adic fields. We need again some lemmas.

LEMMA 9.3.1. *Let L/K be an unramified extension of p-adic fields of degree n. Then we have $L = K(\zeta_{q-1})$, where $q = p^n$ is the cardinality of the residue class field of L.*

PROOF. Let $e = e(L/K)$ and $f = f(L/K)$. Since L/K is unramified, we have $e = 1$ and $n = [L : K] = f$. The extension L/K is a Galois extension if and only if the extension of the residue class fields $k(\mathfrak{p}_L)/k(\mathfrak{p}_E)$ is a Galois extension. This is the case, since the latter is a finite extension of finite fields, which is of course a Galois extension. It has cyclic Galois group. By Lemma 9.1.5 we have the isomorphism

$$Gal(L/K) \simeq \mathrm{Gal}(k(\mathfrak{p}_L)/k(\mathfrak{p}_E)).$$

The Galois extension $k(\mathfrak{p}_L)/k(\mathfrak{p}_E)$ has a primitive element $\alpha \in k(\mathfrak{p}_L)$, with $k(\mathfrak{p}_L) = k(\mathfrak{p}_E)(\alpha)$. This element α is a primitive $(q-1)$-th root of unity with $\gcd(q-1, p) = 1$, and hence it is a root of $f(t) = t^n - 1$. Since $q - 1$ and p are coprime we have $f'(\alpha) \not\equiv 0 \mod \mathfrak{p}_L$. So we can apply Hensel's Lemma on f. So there exists a root $\beta \in \mathcal{O}_{\mathfrak{p}_L}$ with $f(\beta) \equiv 0 \mod \mathfrak{p}_L$ and $\beta \equiv \alpha \mod \mathfrak{p}_L$. Then β is a root of unity and

$$[K(\beta) : K] \geq [k(\mathfrak{p}_E)(\alpha) : k(\mathfrak{p}_E)] = [k(\mathfrak{p}_L) : k(\mathfrak{p}_E)] = [L : K].$$

It follows that $L = K(\beta) = K(\zeta_{q-1})$. □

LEMMA 9.3.2. *Let L/K be a totally and tamely ramified extension of finite extensions of $\mathbb{Q}_p$ with $[L : K] = e$. Then there exists a generator π of the maximal ideal $\mathfrak{p}_K$ in the valuation ring of K with $L = K(\pi^{1/e})$.*

PROOF. By assumption we have $f = f(E/F) = 1$ and

$$e(L/K) = [L : K] = ef = e$$

with $p \nmid e$. Let π_L and π_K be prime elements generating the maximal ideals $\mathfrak{p}_L$ and $\mathfrak{p}_K$. Then we have $K(\pi_L) = L$, because of $K(\pi_L) \subseteq L$, and since the extension $K(\pi_L)/K$ also has ramification index e. So we have

$$[L : K(\pi_L)] = 1.$$

By definition we have

$$\pi_L^e = u \cdot \pi_K$$

for a unit $u \in \mathcal{O}_{\mathfrak{p}_L}^\times$. Because of $f = 1$ we have $\kappa(\mathfrak{p}_L) = \kappa(\mathfrak{p}_K)$ for the residue class fields. Hence there is a unit $v \in \mathcal{O}_{\mathfrak{p}_K}^\times$ with $\overline{u} = \overline{v}$ for the cosets. The element $x = v\pi_k/\pi_L^e$ has coset $\overline{x} = \overline{1} \in \kappa(\mathfrak{p}_L)$. We can apply Hensel's Lemma to $f(t) = t^e - x$, which has a root at $\overline{1} \in \kappa(\mathfrak{p}_L)$. This root is simple, because the derivative $\overline{e}\overline{t}^{e-1}$ doesn't vanish outside of $\overline{0}$, since $p \nmid e$. Hence there is a $y \in \mathcal{O}_{\mathfrak{p}_L}^\times$ with $y^e = x$. Setting $\pi = v\pi_K$ we obtain

$$L = K(y\pi_L) = K(\sqrt[e]{v\pi_K}) = K(\sqrt[e]{\pi}).$$

□

LEMMA 9.3.3. *The extension $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally ramified with ramification index $e = p-1$. It can be written as $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p((-p)^{1/(p-1)})$.*

Proof. Let $L = \mathbb{Q}_p(\zeta_p)$ and $K = \mathbb{Q}_p$. Then the maximal ideal of $\mathcal{O}_{\mathfrak{p}_L}$ is given by $\mathfrak{p}_L = (\pi_L)$ with $\pi_L = 1-\zeta_p$. We have $\mathfrak{p}_K = (p) = (1-\zeta_p)^{p-1}$. The proof is analogous to the one in Lemma 9.3.2. We have

$$u^{-1} = \frac{\pi_K}{\pi_L^e} = \frac{p}{(1-\zeta_p)^{p-1}}.$$

We claim that $u^{-1} \equiv -1 \mod \mathfrak{p}_L$. Then we can take $v = -1$ and we obtain $L = K(\sqrt[e]{v\pi_K}) = K(\sqrt[p-1]{-p})$ as above. The claim follows by Wilson's Theorem and by $\zeta_p \equiv 1 \mod \mathfrak{p}_L$. Indeed, u^{-1} satisfies

$$\frac{p}{(1-\zeta_p)^{p-1}} = \prod_{i=1}^{p-1} \frac{1-\zeta_p^i}{1-\zeta_p} = \prod_{i=1}^{p-1} \left(\sum_{j=0}^{i-1} \zeta_p^j \right) \equiv (p-1)! \equiv -1 \mod \mathfrak{p}_L.$$

□

Proof of the local Kronecker-Weber Theorem:

Since the abelian group $\mathrm{Gal}(K/\mathbb{Q}_p)$ is a product of cyclic groups of prime power, we can write K as composite of extensions of $\mathbb{Q}_p$, whose Galois group is cyclic of prime power degree, see Lemma 9.1.1. Therefore we may assume that $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r$ for a prime q and some $r \in \mathbb{N}$.

Case 1: $q \neq p$.

Let L be the maximal unramified subextension of K. It is given by the fixed field of the inertia group. By Lemma 9.3.1 we have

$$L = \mathbb{Q}_p(\zeta_n)$$

for some $n \in \mathbb{N}$. Let $e = [K : L]$. Since e is a power of q, we have $p \nmid e$. Hence K is totally and tamely ramified over L. Therefore by Lemma 9.3.2 there exist a $\pi \in \mathcal{O}_{\mathfrak{p}_L}$ with $\mathfrak{p}_L = (\pi)$ and $K = L(\pi^{1/e})$. Since $L/\mathbb{Q}_p$ is unramified, also p generates the maximal ideal $\mathfrak{p}_L = (\pi)$. So we can write $\pi = -pu$ with a unit $u \in \mathcal{O}_{\mathfrak{p}_L}^\times$. Furthermore $L(u^{1/e})/L$ is unramified because of $(e,p) = 1$ and since u is a unit and therefore the discriminant of $f(t) = t^e - u$ is not divisible by p. In particular, the extension $L(u^{1/e})/\mathbb{Q}_p$ is unramified and hence abelian. Then $K(u^{1/e})/\mathbb{Q}_p$ is the composite of two abelian extensions $K/\mathbb{Q}_p$ and $L(u^{1/e})/\mathbb{Q}_p$, hence abelian itself. It follows that every subextension is abelian, in particular that $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is abelian.

Since the extension $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is a Galois extension, it contains all e-th roots of $-p$, hence also all e-th roots of unity. Note that we may divide two roots to obtain an e-th root of unity. However, $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is totally ramified, while $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is unramified. This is a contradiction, except for the case that $\mathbb{Q}_p(\zeta_e) = \mathbb{Q}_p$, i.e., if $\zeta_e \in \mathbb{Q}_p$. But this can only hold for $e \mid p-1$, since the residue class field $\mathbb{F}_p$ of $\mathbb{Q}_p$ only contains the $(p-1)$-th roots of unity.

We have, as mentioned above, $K \subseteq L((-p)^{1/e}, u^{1/e})$. On the one hand $L(u^{1/e})$ is unramified over L, so $L(u^{1/e}) = L(\zeta_m)$ for some m by Lemma 9.3.1; on the other hand we have, because of $e \mid p-1$,

$$\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$$

by Lemma 9.3.3. Together this yields

$$K \subseteq L((-p)^{1/e}, u^{1/e}) \subseteq \mathbb{Q}_p(\zeta_n, \zeta_p, \zeta_m) \subseteq \mathbb{Q}_p(\zeta_{mnp}),$$

and we are done.

Case 2: $q = p \neq 2$.

Let $K/\mathbb{Q}_p$ be a finite abelian extension. As said above, we may assume that

$$Gal(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r = \mathbb{Z}/p^r.$$

We consider two further extensions of $\mathbb{Q}_p$ with this Galois group, namely an unramified extension $K_u/\mathbb{Q}_p$ of degree p^r, and a totally ramified extension $K_r/\mathbb{Q}_p$ of degree p^r. Indeed, $K_u = \mathbb{Q}_p(\zeta_{p^{p^r}-1})$ is unramified of degree p^r, and therefore has a cyclic Galois group of order p^r. Let K_r be the subfield of index $p-1$ of $\mathbb{Q}_p(\zeta_{p^{r+1}})$. The extension $\mathbb{Q}_p(\zeta_{p^{r+1}})/\mathbb{Q}_p$ has degree $p^r(p-1)$. Since $p > 2$, the Galois group is cyclic. Hence the extension $K_r/\mathbb{Q}_p$ is totally ramified with cyclic Galois group $\mathbb{Z}/p^r$. Because of $K_r \cap K_u = \mathbb{Q}_p$ we have by Corollary 9.1.2,

$$Gal(K_rK_u/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^r)^2.$$

So we have either $K \subseteq K_rK_u \subseteq \mathbb{Q}_p(\zeta_{p^{r+1}(p^{p^r}-1)})$, or $K \not\subseteq K_rK_u$. In the second case we have

$$Gal(K(\zeta_{p^{p^r}-1}, \zeta_{p^{r+1}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^r)^2 \times \mathbb{Z}/p^s$$

for some $s > 0$. This group has $(\mathbb{Z}/p)^3$ as a quotient, so that we obtain an extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p)^3$. This is impossible by Lemma 9.3.5. So the first case arises and we are done, after having proved this lemma. Unfortunately this requires another lemma, from Kummer theory.

Lemma 9.3.4. *Let K be a field of characteristic ℓ with coprime ℓ and n, let $L = K(\zeta_n)$, and $M = L(a^{1/n})$ for some $a \in L^\times$. Define a homomorphism $\omega : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by the relation $\zeta_n^{\omega(g)} = \zeta_n^g$. Then M/K is a Galois extension. It is abelian if and only if*

$$a^g/a^{\omega(g)} \in (L^\times)^n \qquad \forall g \in \mathrm{Gal}(M/K). \tag{9.1}$$

Here is the lemma we need.

Lemma 9.3.5. *Let $p > 2$ be a prime. There exists no Galois extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p)^3$.*

Proof. Let $\pi = \zeta_p - 1$ be the uniformizing element of $\mathbb{Q}_p(\zeta_p)$. Assume that $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p)^3$. Then $\mathrm{Gal}(K(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p)^3$, and $K(\zeta_p)$ is abelian over $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p)^\times \times (\mathbb{Z}/p)^3$. Applying "Kummer theory" to $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$ we obtain a subgroup $B \subseteq \mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$, which is isomorphic to $(\mathbb{Z}/p)^3$. This implies $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, B^{1/p})$. Let $\omega\colon \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^\times$ be the canonical map. By Lemma 9.3.4 we have

$$b^g/b^{\omega(g)} \in (\mathbb{Q}_p(\zeta_p)^\times)^p \qquad \forall b \in B, g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p),$$

since $\mathbb{Q}_p(\zeta_p, b^{1/p}) \subseteq K(\zeta_p)$ is also abelian over $\mathbb{Q}_p$. Let us recall the structure of $\mathbb{Q}_p(\zeta_p)^\times$. The maximal ideal of $\mathbb{Z}_p[\zeta_p]$ is generated by π, and each unit of $\mathbb{Z}_p[\zeta_p]$ is congruent to a $(p-1)$-th root of unity modulo π. Hence we have

$$\mathbb{Q}_p(\zeta_p)^\times = \pi^{\mathbb{Z}} \times (\zeta_{p-1})^{\mathbb{Z}} \times U_1,$$

where U_1 is the set of all units of $\mathbb{Z}_p[\zeta_p]$, which are congruent to 1 modulo π, and similarly

$$(\mathbb{Q}_p(\zeta_p)^\times)^p = \pi^{p\mathbb{Z}} \times (\zeta_{p-1})^{p\mathbb{Z}} \times U_1^p.$$

Choose a representative $a \in L^\times$ of a nonzero element in B. We may assume that $a = \pi^m u$ for some $m \in \mathbb{Z}$ and some $u \in U_1$. Then we have

$$\frac{a^g}{a^{\omega(g)}} = \frac{(\zeta_p^{\omega(g)} - 1)^m}{\pi^{m\omega(g)}} \frac{u^g}{u^{\omega(g)}};$$

but $v_\pi(\pi) = v_\pi(\zeta_p^{\omega(g)} - 1) = 1$. Hence the valuation on the right hand side equals $m(1-\omega(g))$, which can only be a multiple of p for all g if $m \equiv 0 \pmod{p}$. Here we have used that p is *odd*. In other words, we could have chosen $m = 0$ and $a = u \in U_1$.

Concerning $u^g/u^{\omega(g)}$ it is easy to see that U_1^p is the set of units, which are congruent to 1 modulo π^{p+1}. Because of $\zeta_p = 1 + \pi + O(\pi^2)$ we may write $u = \zeta_p^b(1 + c\pi^d + O(\pi^{d+1}))$, with $c \in \mathbb{Z}$ and $d \geq 2$. Since $\pi^g/\pi \equiv \omega(g) \pmod{\pi}$, we obtain

$$\begin{aligned} u^g &= \zeta_p^{b\omega(g)}(1 + c\omega(g)^d\pi^d + O(\pi^{d+1})), \\ u^{\omega(g)} &= \zeta_p^{b\omega(g)}(1 + c\omega(g)\pi^d + O(\pi^{d+1})). \end{aligned}$$

Both expressions must be congruent modulo π^{p+1}. Hence we either have $d \geq p+1$ or $d \equiv 1 \pmod{p-1}$. The latter can only arise for $d = p$. Together this implies that the set of possible elements u is generated by ζ_p and $1+\pi^p$. However, these two elements only generate a subgroup of U_1/U_1^p, which is isomorphic to $(\mathbb{Z}/p)^2$, while $B \cong (\mathbb{Z}/p)^3$. This is a contradiction. □

Case 3: $p = q = 2$**.**

This case is proved similarly, but it is more difficult since among other things $\mathbb{Q}_2$ may indeed have a Galois extension with Galois group $(\mathbb{Z}/2)^3$. However, it can be shown that $\mathbb{Q}_2$ does not admit a Galois extension with Galois group $(\mathbb{Z}/2)^4$ or $(\mathbb{Z}/4)^3$. This suffices to finish the proof as in the previous case. All details are given in [**12**].

Bibliography

[1] D. Burde: *Commutative Algebra.* Vorlesungsskript (2009), 1–87.

[2] L. Claborn, *Every abelian group is a class group.* Pacific J. Math. **18**, No. 2 (1966), 219–222.

[3] H. Cohen, *A course in computational algebraic number theory.* Graduate Texts in Mathematics, **138** (1993). Springer-Verlag, Berlin.

[4] T. Coquand T, H. Lombardi: *A short proof for the Krull dimension of a polynomial ring.* American Math. Monthly. **112** (2005), no. 9, 826–829.

[5] J. E. Cremona, D. Rusin: *Efficient solution of rational conics.* Math. Comp. **72** (2003), no. 243, 1417–1441.

[6] K. Ireland, M. Rosen: *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics **84** (1990). Springer-Verlag, New York.

[7] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).

[8] H. Koch: *Zahlentheorie.* Vieweg-Verlag (1997).

[9] J. M. Masley, H. L. Montgomery: *Cyclotomic fields with unique factorization.* J. Reine Angew. Math. **287** (1976), 248–256.

[10] J. Neukirch: *Algebraische Zahlentheorie.* Grundlehren der mathematichen Wissenschaften (1992). Springer-Verlag, Berlin.

[11] H. M. Stark: *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. Journal **14** (1967), 1–27.

[12] L. C. Washington: *Introduction to cyclotomic fields.* Springer-Verlag (1997).