Algebraic Number Theory
代数的整数論

Topics in Mathematical Science IV (数理科学特論 IV), Nagoya University, Fall 2021

Henrik Bachmann (Math. Building Room 457, henrik.bachmann@math.nagoya-u.ac.jp)
Lecture notes and exercises are available at: https://www.henrikbachmann.com/algnt_2021.html

---

注意：These notes are under construction and therefore may contain mistakes and change without notice. If you find any typos/errors or have any suggestions, please let me know! Often just the statements of theorems etc. are given. The proofs can be found in the handwritten lecture notes on the homepage.

Already a big thanks to Vic Austen, John Ashley Capellan and Li He for helping to prepare these notes and for correcting some typos. The main reference for this lecture is the book [N] by Neukirch. In addition, these notes were also inspired by the (german) lecture notes of Schweigert [Sch], which are also based on Neukirch's book, but which also include the necessary algebraic background in an excellent way. We also include a lot of basic notions from algebra since we assume that most of the students attending this lecture are Japanese students who attended Japanese algebra courses. We hope that some parts of these notes can not only serve as a compact overview but also as some kind of Japanese-English dictionary for algebra & algebraic number theory. This is why we also provide the Japanese translation for the main objects in these notes.

Contents

1 Introduction & Basics of algebra

We will start by giving a short answer to the question **"What is Algebraic number theory?"**. There are several possible answers to this question. As the name suggests, it is number theory with the help of algebraic methods. Algebraic number theory is the study of **algebraic number fields** [代数体], which are field extensions $K/\mathbb{Q}$ of finite degree. In these number fields, we will be in particular interested in the **ring of integers of** K [整数環], denoted by $\mathcal{O}_K$. This ring of integers takes the same place in K as the usual integers do in the rational numbers, i.e., in particular $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. The integers $\mathbb{Z}$ satisfy a lot of nice properties. For example, $\mathbb{Z}$ is a unique factorization domain (UFD) [一意分解環], i.e., any element can be written uniquely (up to units) as a product of irreducible elements, which are given by the prime numbers. As we will see, not every ring of integers $\mathcal{O}_K$ will be a UFD. This problem will be solved by considering ideals in $\mathcal{O}_K$. We will see that on the level of ideals, we will again have a kind of unique factorization property.

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathcal{O}_K \end{array}$$

Examples 1.1. Example of number fields K and their ring of integers $\mathcal{O}_K$.

(i) The field extension $K = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{C}\}$ has degree $[K : \mathbb{Q}] = \dim_{\mathbb{Q}} K = 2$ and is therefore a number field. Its ring of integers is $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{C}\}$. These are the so-called **Gaussian integers** and we will study their properties in the first section.

(ii) We will see that for the number field $K = \mathbb{Q}(\sqrt{5})$ the ring of integers is given by $\mathcal{O}_K = \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]$.

(iii) The ring of integers for $K = \mathbb{Q}(\sqrt{-5})$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. This ring is not a UDF, since for example in this ring we can write 6 in two different ways

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

and 2,3, $(1 + \sqrt{-5})$ and $(1 + \sqrt{-5})$ are all irreducible elements in this ring.

The next question one might ask is, why one should care about algebraic number field, and one could therefore ask **"Why is Algebraic number theory?"**. Algebraic number fields appear naturally when studying **Diophantine equations**. These are polynomial equations where one is interested in integer solutions.

Examples 1.2. Here are some examples of Diophantine equations. For a more detailed overview see [IR, Chapter 17] and [KKS, Chapter 1].

i) Linear Diophantine equation: Given $a, b, c \in \mathbb{Z}$ find all $x, y \in \mathbb{Z}$ with

$$ax + by = c\,.$$

It is an easy exercise to show that a solution for given a, b, c exists if and only if c divides the greatest common divisor of a and b, which we denote by $\gcd(a, b)$.

ii) Pell's equation: Given a non-square integer n we consider

$$x^2 - ny^2 = 1. \tag{1.1}$$

It was then shown by Lagrange (1768): For any non-saure n the equation (1.1) has infinitely many distincts solutions $x, y \in \mathbb{Z}$.

iii) Sum of four squares: For any positive integer $n \in \mathbb{N}$ one can ask if this integer can be written as a sum of four squares, i.e. if one can find $a, b, c, d \in \mathbb{Z}$ such that

$$a^2 + b^2 + c^2 + d^2 = n\,. \tag{1.2}$$

Again Lagrange (1770) showed: (1.2) has a solution for any n. For example, we have

$$2021 = 0^2 + 1^2 + 16^2 + 42^2 = 1^2 + 18^2 + 20^2 + 36^2\,.$$

In particular we see that there can be several different solutions for some n. The question of how many solutions there are for a given n was answered by Jacobi (1893): If $r_4(n) = \#\{a, b, c, d \in \mathbb{Z} \mid (1.2)\}$ then

$$r_4(n) = 8 \sum_{\substack{m|n \\ 4\nmid|m}} m\,.$$

This result can be proven by using modular forms for the congruence subgroup $\Gamma_0(4)$ (See Todo: add reference).

iv) Sum of two squares: Instead of the sum of four squares one can also consider the sum of two squares. Clearly not every number can be written as a sum of two squares, since 3 is already the first counter-example. We will discuss in detail how to determine if a prime is a sum of two squares in Section 1.1, by using methods of algebraic number theory.

v) Fermat's last theorem: For a given $n \geq 1$ consider the equation

$$x^n + y^n = z^n\,. \tag{1.3}$$

For $n = 1$ this equation is trivial to solve and for $n = 2$ one can find infinitely many integer solutions, the so-called **Pythagorean triples**. A few examples are given by $3^2 + 4^2 = 5^2$ or $5^2 + 12^2 = 13^2$. In 1637 Pierre de Fermat claimed that (1.3) has no non-trivial integer solutions (meaning $x \cdot y \cdot z \neq 0$) if $n \geq 3$. It took more than 300 years until Andrew Wiles gave a proof of this claim in 1994 (Todo: add reference).
Todo: Include timetable of events around FLT and add more history.

1.1 Primes as a sum of two squares and some ring theory

In this section we will answer the question when a prime is a sum of two squares. The first few examples are

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^3 + 3^2, \quad 17 = 1^2 + 4^2, \ldots\,.$$

For some primes, such as $3, 7$ or 11, this is not possible. This follows from the following simple observation: Any square is congruent to 0 or 1 modulo 4. Therefore if a prime is a sum of two squares, it can just be congruent to 0,1 or 2 modulo 4. But since it is prime, it can never be congruent to 0 modulo 4 and 2 is the only prime that can be congruent to 2 modulo 4. Therefore any prime $p \geq 3$, which is the sum for two squares, has to be congruent to 1 modulo 4. It was first shown by Fermat that also the converse is true:

Theorem 1.3. *A prime $p \geq 3$ can be written as a sum of two squares if and only if $p \equiv 1 \mod 4$.*

To prove this theorem, we will leave the ring of integers and work in a larger ring. Before doing this, we will recall some basic notations from algebra.

Definition 1.4. (i) A **ring** [環] is a triple $(R, +, \cdot)$ of a set R together with two binary operations $+$ (addition) and $\cdot$ (multiplication), such that

- $(R, +)$ is an abelian group [アーベル群].
  (i.e. $+$ is commutative and associative, there exists a neutral element $0 \in R$ and for each $a \in R$ an inverse $-a \in R$ with $a + (-a) = 0$.)
- $(R, \cdot)$ is a semigroup [半群].
  (i.e. $\cdot$ is associative)
- Addition and multiplication satisfy the distributive law [分配律]

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in R$. If $\cdot$ is commutative, we call R a **commutative ring** [可換環]. Instead of $(R, +, \cdot)$ we will usually just write R.

(ii) A ring R is **unitary** [単位環] if there exists a $1 \in R$ with $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. In other words $(R, \cdot)$ is a monoid [モノイド].

(iii) Let R, S be rings. A **ring homomorphism** [環準同型] is a map $\varphi : R \to S$, such that for all $a, b \in R$

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b). \tag{1.4}$$

If R, S are unitary one usually considers unitary ring homomorphisms which in addition satisfy $\varphi(1) = 1$.

(iv) A (non-zero) commutative ring R is called an **(integral) domain** [整域] if for all $a, b \in R$ the equation $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

Usually, all rings we consider in this course will be commutative and unitary if not stated otherwise.

Examples 1.5. (i) $\mathbb{Z}, \mathbb{R}[X], \mathbb{C}[X]$ are integral domains

(ii) $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain since $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

(iii) The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b, \in \mathbb{Z}\} \subset \mathbb{C}$ is a domain.

In the ring $\mathbb{Z}[i]$ the equation $p = x^2 + y^2$ can be written as

$$p = (x + iy)(x - iy)\,. \tag{1.5}$$

Definition 1.6. (i) An element $a \in R$ in an (unital) ring R is called a **unit** [可逆元] if there exists $b \in R$ with $a \cdot b = 1$.

(ii) $R^\times$ denotes the set of all units of R and $(R^\times, \cdot)$ is a group, the **unit group** [単元群].

(iii) If R is commutative, $1 \neq 0$ and $R^\times = R\backslash\{0\}$ then R is called a **field** [体].

Examples 1.7. (i) $\mathbb{Z} = \{1, -1\}$.

(ii) If R is a domain then $R[X]^\times = R^\times$. If R is not a domain there are also non-constant polynomials which can be units. For example, in the case $R = \mathbb{Z}/4\mathbb{Z}$ we have $(1 + 2X)^2 = 1$ in $R[X]$ and therefore $1 + 2X \in R[X]^\times$.

(iii) One can show (Exercise 3) that the units of the Gaussian integers are $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Definition 1.8. (i) An element $a \in R$ with $a \notin R^\times$ is called **irreducible** [既約元] if from $a = b \cdot c$ we obtain $b \in R^\times$ or $c \in R^\times$.

(ii) An element $p \in R\backslash\{0\}$ with $p \notin R^\times$ is called **prime** [素元] if whenever $p \mid a \cdot b$ then $p \,|\, a$ or $p \,|\, b$.

Notice that 0 in particular is not irreducible since $0 = 0 \cdot 0$ but $0 \notin \mathbb{R}^\times$. Since we will deal with prime elements in a ring and with prime numbers at the same time (which are the prime elements in $\mathbb{Z}$), we will refer to prime numbers often as **rational primes**.
In an (integral) domain, every prime element is irreducible (Exercise 1). However, the converse is not always true. For example, in the domain $R = \mathbb{Z}[\sqrt{-5}]$, 2 is irreducible, and

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

but $2 \nmid (1 - \sqrt{-5})$ and $2 \nmid (1 + \sqrt{-5})$, so 2 is not prime.

Until here in lecture 1 (8th October, 2021)

Definition 1.9. A domain R is called a **unique factorization domain (UFD)** [一意分解環], (often also just called **factorial ring**), if the following two conditions are satisfied:

(i) Any non-zero element $a \in R\backslash\{0\}$ can be written as

$$a = u p_1 \dots p_n \,, \tag{1.6}$$

where $p_1, \dots, p_r \in R$ are irreducible and $u \in R^\times$ is a unit.

(ii) The representation (1.6) is unique in the sente that whenever $a = u' p'_1 \dots p'_{n'}$ with irreducible $p'_i \in R$ and $u' \in R^\times$, then $n' = n$ and there exists a permutation $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ with $p_i = \epsilon_i p'_{\sigma(i)}$ for some $\epsilon_i \in R^\times$ and $i = 1, \dots, n$.

We will show that $\mathbb{Z}[i]$ is factorial, by showing that it is euclidean.

Definition 1.10. A domain R is called an **Euclidean domain/ring** [ユークリッド環] if there exists a function $N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$, such that for any $a, b \in R$ with $b \neq 0$ there exist $p, r \in R$ such that

$$a = b \cdot q + r \,, \tag{1.7}$$

with either $N(r) < N(b)$ or $r = 0$.

Proposition 1.11. *Euclidean rings are factorial.*

Proof. This is Exercise 1. □

Examples 1.12. (i) The standard example is $R = \mathbb{Z}$ with $N(x) = |x|$.

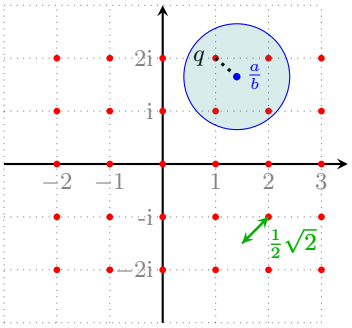
(ii) If K is a field then one can show that $R = K[X]$ is an Euclidean ring by taking $N(f) = \deg(f)$.

Proposition 1.13. *The ring $\mathbb{Z}[i]$ is factorial.*

Proof. We define the **norm** on $\mathbb{Z}[i]$ by $N(\alpha) = |\alpha|^2$. For $a, b, \in \mathbb{Z}[i]$ with $b \neq 0$ we want to find $q, r \in \mathbb{Z}[i]$ with $|r|^2 < |b|^2$, such that $a = q \cdot b + r$. Therefore, we want to find a $q \in \mathbb{Z}[i]$ with

$$\left| \frac{a}{b} - q \right| < 1 \,, \tag{1.8}$$

since then $r = a - q \cdot b$ satisfies $|r| < |b|$.



$\mathbb{Z}[i]$ as a lattice in $\mathbb{C}$

We can visualize $\mathbb{Z}[i]$ as a lattice in $\mathbb{C}$. It is easy to see that the maximal distance any complex number, such as $\frac{a}{b}$, can have to a lattice point is $\frac{\sqrt{2}}{2} < 1$. Therefore we can also find a $q \in \mathbb{Z}[i]$ which satisfies (1.8), by choosing the nearest point to $\frac{a}{b}$ on the lattice.

□

Lemma 1.14 (Wilson's theorem)**.** *For any prime number p we have*

$$(p-1)! \equiv -1 \mod p \,.$$

Proof. This is Exercise 2. □

Proof. of Theorem 1.3 We need to show that any prime p with $p \equiv 1 \mod 4$ can be written as a sum of two squares. Suppose that $p = 4n + 1$ and set $x = (2n)!$. In this case we obtain by Lemma 1.14:

$$\begin{aligned} -1 \equiv (p-1) &\equiv 1 \cdot 2 \ldots 2n \cdot (p-2n) \cdot (p-2n-1) \ldots (p-2) \cdot (p-1) \\ &\equiv (2n)!(-1)^{2n}(2n)! \\ &\equiv x^2 \mod p \,. \end{aligned}$$

Therefore $p \mid x^2+1 = (x+i)(x-i)$, but $p \nmid (x+i)$ and $p \nmid (x-1)$ since $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$. This shows that p is not prime in the factorial ring $\mathbb{Z}[i]$ and therefore also not irreducible. This means that we can find two non-units $\alpha, \beta \in \mathbb{Z}[i]$ with $p = \alpha \cdot \beta$. This implies the equation $p^2 = N(p) = N(\alpha \cdot \beta) = N(\alpha)N(\beta)$ in $\mathbb{Z}$. Since $\alpha, \beta \notin \mathbb{Z}[i]^\times$ we have $N(\alpha), N(\beta) \neq 1$, which leaves the only possibility that $N(\alpha) = N(\beta) = p$. But if $\alpha = a + bi$ this implies

$$N(\alpha) = a^2 + b^2 = p \,,$$

which is exactly what we wanted to show. □

Definition 1.15. Two elements $a, b \in R$ of a ring R are called **associated** [同伴], if there exists a unit $\epsilon \in R^\times$ with $a = \epsilon b$. In this case we write $a \sim b$.

Lemma 1.16. *If $a \in R$ is prime (resp. irreducible) then all elements $b \in R$ with $a \sim b$ are also prime (resp. irreducible).*

Theorem 1.17. *The prime elements π of $\mathbb{Z}[i]$ are, up to accociated elements, given by*

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

(ii) $\pi = a + bi$, *where* $a^2 + b^2 = p$ *is a rational prime,* $a > |b| > 0$ *and* $p \equiv 1 \mod 4$,

(iii) $\pi = p$, *where p is a rational prime and* $p \equiv 3 \mod 4$.

Proof. The elements in (i) and (ii) are prime since if $\pi = \alpha \cdot \beta$ for some $\alpha, \beta \in R$ we get $p = N(\pi) = N(\alpha)N(\beta)$ for a prime p ($p = 2$ in (i)). Therefore $N(\alpha) = 1$ or $N(\beta) = 1$, i.e. by Exercise 3 α or β has to be a unit which implies that π is irreducible. Since $\mathbb{Z}[i]$ is factorial π is therefore also prime. If $\pi = p$ for some rational prime p with $p \equiv 3 \mod 4$ then $p = \alpha \cdot \beta$ with non-units α, β would imply that $N(\alpha) = p$. But if $\alpha = a + bi$ this would give $p = a^2 + b^2$ which is not possible as we saw in Theorem 1.3. Therefore either α or β need to be a unit and therefore π is irreducible. It remains to show that nay prime element is associated to one of the ones in (i),(ii) or (iii). Let $\pi = a + bi$ be prime, then in $\mathbb{Z}$ we have $N(\pi) = \pi \cdot \overline{\pi} = p_1 \cdots p_r$, where $\overline{\pi} = a - bi$ is the complex conjugate of π and the $p_1, \ldots, p_r$ are rational primes. Since π is prime we get that π divides one of these rational primes, i.e. we can assume $\pi | p$ for some rational prime p. This implies $N(\pi) | N(p) = p^2$. From this we get $N(\pi) = p$ or $N(\pi) = p^2$. If $N(\pi) = p$ we have $p = a^2 + b^2$, i.e. π is associated to (i) or (ii). In the case $N(\pi) = p^2$ we obtain $\pi \sim p$. But then we need to have $p \equiv 3 \mod 4$ and therefore π is of the form (iii). □

Proposition 1.18. *The elements in $\mathbb{Z}[i]$ are exactly those in $\mathbb{Q}(i)$, which are a solution of*

$$X^2 + aX + b = 0 \tag{1.9}$$

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

Proof. We factor the polynomial as $X^2 + aX + b = (X - (c + di))(X - (c - di))$ for some $c, d \in \mathbb{Q}$. We want to show that if $a, b \in \mathbb{Z}$ then $c, d \in \mathbb{Z}$ and vice versa. Since $a = -2c, b = c^2 + d^2$ clearly $a, b \in \mathbb{Z}$ if $c, d \in \mathbb{Z}$. Conversely assume that $a, b \in \mathbb{Z}$. Then $2c \in \mathbb{Z}$ and if we write $d = \frac{p}{q}$ with $\gcd(p, q) = 1$ then $4b = (2c)^2 + \left(\frac{2p}{q}\right)^2$ implies $4\frac{p^2}{q^2} \in \mathbb{Z}$. Therefore $q^2 | 4$, which is just possible if $q = 1, 2$, which gives $2d \in \mathbb{Z}$. But $4b = (2c)^2 + (2d)^2 \equiv 0 \mod 4$ can just have a solution if $2c$ and $2d$ are even, which gives $c, d \in \mathbb{Z}$. □

In this section, we answered the general questions for the number field $\mathbb{Q}(i)$ and its ringer of integers $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ was factorial, it behaved quite similar to $\mathbb{Z}$. We will see that this in general will not be true for arbitrary number fields and their ring of integers. The problem of not having unique factorization in the ring of integers will be solved by going over to ideals instead of numbers.

Number field	$\mathbb{Q}$	$\mathbb{Q}(i)$	K
Ring of integers	$\mathbb{Z}$	$\mathbb{Z}[i]$	$\mathcal{O}_K$
Units	± 1	$\pm 1, \pm i$	Dirichlet's unit theorem (later)
Prime elements	Prime numbers	Theorem 1.17	?
UFD?	Yes	Yes	In general: No. ⇝ Ideals

Until here in lecture 2 (15th October, 2021)

1.2 Ideals

We already saw that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, since 6 can be factored into the product of two irreducible elements in two different ways

$$6 = \underbrace{2}_{a\cdot b} \cdot \underbrace{3}_{c\cdot d} = \underbrace{(1+\sqrt{-5})}_{a\cdot c} \cdot \underbrace{(1-\sqrt{-5})}_{b\cdot d} . \tag{1.10}$$

Kummer proposed the idea of "ideal numbers" to solve this problem by breaking the above equations into smaller pieces. Assume there exist ideal numbers a, b, c, d which divide the factors of 6 in the way as indicated in (1.10). Then the representation of $6 = a \cdot b \cdot c \cdot d$ into ideal numbers would become unique. Whatever these "ideal numbers" are, if p is an ideal number and $p|a$ and $p|b$ then we should also have $p|a \pm b$. Also if $p|a$ then $p|ax$ for any x. To deal with these type of object, Dedekind suggested representing an "ideal number" by the set of all numbers which are divisible by it. This leads to the following notion of ideals.

Definition 1.19. Let R be a commutative unitary ring. A non-empty subset $I \subset R$ is called an **ideal** [イデアル] of R, if

(i) for any $a, b \in I$ we have $a + b \in I$,

(ii) for any $a \in I$ and any $x \in R$ we have $a \cdot x \in I$.

Remark 1.20. Let $I \subset R$ be an ideal of a commutative and unitary ring R.

(i) If $1 \in I$ then we immediately obtain from the second condition that $I = R$.

(ii) $(I, +, \cdot)$ is a subring of R, which is non-unitary in the case $I \neq R$.

(iii) If $\varphi : R \to S$ is a ring homomorphism then the kernel of φ

$$\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$$

is an ideal in I.

(iv) We can define the **quotient ring** [剰余環]

$$R/I = \{\overline{a} \mid a \in R\}$$

given by the set of all **equivalence classes** [同値類] of $a \in R$ defined by

$$\overline{a} = \{b \in R \mid a - b \in I\} .$$

If $b \in \overline{a}$ we also write $a = b \mod I$ and $\overline{a}$ is sometimes also just denoted $a \mod I$. R/I is a ring with addition $\overline{a} + \overline{b} = \overline{a+b}$ and multiplication $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. The **canonical projection** [標準射影]

$$\begin{aligned} p : R &\longrightarrow R/I \\ a &\longmapsto \overline{a} \end{aligned}$$

is a surjective ring homomorphism with $\ker(p) = I$. In particular any ideal is the kernel of some ring homomorphism.

(v) We have the **isomorphism theorem** [同型定理]: Any ring homomorphism $\varphi : R \to S$ induces an isormophism

$$\widetilde{\varphi} : {}^{R}\!/_{\ker(\varphi)} \xrightarrow{\sim} \mathrm{im}(\varphi)\,.$$

If not stated otherwise, then R will always be a commutative unitary ring in the following.

Definition 1.21. (i) For $a \in R$ we define

$$(a) = Ra = \{ca \mid c \in R\}\,.$$

This is an ideal in R and it is called the **principal ideal** [単項イデアル] generated by a.

(ii) Let R be a domain. If every ideal in R is a principal ideal then R is called a **principal ideal domain (PID)** [単項イデアル整域].

Proposition 1.22. *Every Euclidean domain is a principal ideal domain.*

Proof. We just give a sketch of the proof. Let N be the Eucledian function in an Eucledian domain R. For an ideal $I \subset R$ choose an $a \in I$ such that $N(a) = \min_{x \in I}\{N(x)\}$. Using division by a with remainder one then sees immediately that $I = (a)$, i.e. I is a principal ideal. □

Lemma 1.23. *Let R be a commutative and unitary ring.*

(i) For all $a, b \in R$ we have $a|b \Leftrightarrow (b) \subset (a)$ and $a \sim b \Leftrightarrow (a) = (b)$.

(ii) If $\mathfrak{a}, \mathfrak{b}$ are ideals of R, then $\mathfrak{a} \cap \mathfrak{b}$ and

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

are ideals in R.

(iii) A $v \in R$ is a multiple of $a \in R$ and $b \in R$ if and only if $(v) \subset (a) \cap (b)$.

(iv) A $d \in R$ is a divisor of a and b if and only if $(a) + (b) \subset (d)$.

Proof. Todo: Give reference □

Definition 1.24. Let $a_1, \ldots, a_n \in R$ elements in some commutative and unitary ring R. We define a **greatest common divisor (gcd)** [最大公約数] (resp. a **least common multiple (lcm)** [最小公倍数]) of $a_1, \ldots, a_n$ by the following properties:

(i) $\gcd(a_1, \ldots, a_n) \mid a_i$ (resp. $a_i \mid \mathrm{lcm}(a_1, \ldots, a_n)$) for all $i = 1, \ldots, n$.

(ii) For all $t \in R$ with $t \mid a_i$ (resp. $a_i \mid t$) for all $i = 1, \ldots, n$ we obtain $t \mid \gcd(a_1, \ldots, a_n)$ (resp. $\mathrm{lcm}(a_1, \ldots, a_n) \mid t$.

A greatest common divisor and/or least common multiple do not always exist. But if they exist, then they are unique up to units.

Examples 1.25. In $R = \mathbb{Z}[\sqrt{-3}]$ the elements $a_1 = 4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and $a_2 = 2 \cdot (1 + \sqrt{-3})$ have no greatest common divisor. Both 2 and $1 + \sqrt{-3}$ are common divisors of a_1 and a_2 but they are not associated and they also do not divide another common divisor of a_1 and a_2.

Proposition 1.26. *Let R be a principal ideal domain.*

(i) For any $a, b \in R$ the gcd *and* lcm *exist and we have*

$$(\gcd(a,b)) = (a) + (b)\,,$$
$$(\mathrm{lcm}(a,b)) = (a) \cap (b)\,.$$

(ii) For $a_1, \dots, a_n \in R$ there exist $x_1, \dots, x_n \in R$ with

$$\gcd(a_1, \dots, a_n) = x_1 a_1 + \cdots + x_n a_n\,.$$

Proof. Todo: Can be shown by using Lemma 1.23. □

Proposition 1.27. *Principal ideal domains are factorial.*

Proof. Todo: Part of any algebra course (include reference or write out the proof). □

Todo: Include an overview of UFD, PID, and Eucledian domains.

Definition 1.28. Let $\mathfrak{a}, \mathfrak{b}$ ideals in R.

(i) $\mathfrak{a}$ and $\mathfrak{b}$ are called **coprime** [**互いに素**] if $\mathfrak{a} + \mathfrak{b} = R$.

(ii) We define the product of $\mathfrak{a}$ and $\mathfrak{b}$ by

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^{r} a_i b_i \mid r \geq 1, a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

This is again an ideal of R and we have $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.

Since $2 \cdot 3 - 5 = 1$ we have $1 \in (3) + (5) = R$, i.e. (3) and (5) are coprime ideals of $\mathbb{Z}$. In this case $(3) \cdot (5) = (15) = (3) \cap (5)$. The ideals (2) and (4) are not coprime since $(2) + (4) = (2)$. In this case we have $(2) \cdot (4) = (8) \subset (2) \cap (4) = (4)$.

Lemma 1.29. *(i) If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals then $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.*

(ii) If $\mathfrak{b}$ is coprime to $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ then $\mathfrak{b}$ is coprime to $\mathfrak{a}_1 \cdots \mathfrak{a}_n$.

Proof. If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime then there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a + b = 1$. Therefore if $c \in \mathfrak{a} \cap \mathfrak{b}$ then $c = ca + cb \in \mathfrak{ab}$, which shows i). For ii) we again can find $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$ for $i = 1, \dots, n$ with $a_i + b_i = 1$. There we have

$$1 = \prod_{i=1}^{n} (a_i + b_i) = \underbrace{b_1 \cdots b_n + \cdots}_{\in \mathfrak{b}} + \underbrace{a_1 \dots a_n}_{\in \mathfrak{a}_1 \cdots \mathfrak{a}_n} \in \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n$$

and therefore $R = \mathfrak{b} + \mathfrak{a}_1 \cdots \mathfrak{a}_n$. □

Theorem 1.30 (Chinese remainder theorem [中国の剰余定理])**.** *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be coprime ideals of R. Then the map*

$$\begin{aligned} R/\mathfrak{a}_1 \cdots \mathfrak{a}_n &\longrightarrow R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n \\ x \mod \mathfrak{a}_1 \cdots \mathfrak{a}_n &\longmapsto (x \mod \mathfrak{a}_1, \dots, x \mod \mathfrak{a}_n) \end{aligned}$$

is a ring isomorphism.

Proof. Due to Lemma 1.29 ii) it suffices to show the $n = 2$ case, since the general case then follows inductively by using the $n = 2$ case to obtain the isomorphism

$$R/\mathfrak{a}_1 \cdot \mathfrak{a}_2 \cdots \mathfrak{a}_n \longrightarrow R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \cdots \mathfrak{a}_n .$$

To prove the $n = 2$ case we first show that for coprime $\mathfrak{a}, \mathfrak{b}$ the ring homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow R/\mathfrak{a} \times R/\mathfrak{b} \\ x &\longmapsto (x \mod \mathfrak{a}, x \mod \mathfrak{b}) \end{aligned}$$

is surjective. Since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ with $a+b = 1$. For given $x_1, x_2 \in R$ we set $x = x_2 a + x_1 b$ and then obtain

$$\begin{aligned} x = x_2 a + x_1(1-a) = x_1 \mod \mathfrak{a}, \\ x = x_2(1-b) + x_1 b = x_2 \mod \mathfrak{b}, \end{aligned}$$

i.e. $\varphi(x) = (x_1 \mod \mathfrak{a}, x_2 \mod \mathfrak{b})$ which shows that φ is surjective. Now by Lemma 1.29 i) the kernel is given by $\ker \varphi = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ and therefore we obtain an isomorphism

$$\begin{aligned} \widetilde{\varphi} : R/\mathfrak{ab} &\longrightarrow R/\mathfrak{a} \times R/\mathfrak{b} \\ x \mod \mathfrak{ab} &\longmapsto (x \mod \mathfrak{a}, x \mod \mathfrak{b}) \end{aligned}$$

which proves the $n = 2$ case of the theorem. □

Definition 1.31. (i) An ideal $\mathfrak{p} \subset R$ with $\mathfrak{p} \neq R$ is called **prime ideal** [**素イデアル**] if $x \cdot y \in \mathfrak{p}$ for some $x, y \in R$ always implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

(ii) An ideal $\mathfrak{m} \subset R$ with $\mathfrak{m} \neq R$ is called **maximal ideal** [**極大イデアル**] if for any ideal $\mathfrak{a} \subset R$ with $\mathfrak{m} \subset \mathfrak{a}$ we have $\mathfrak{m} = \mathfrak{a}$ or $\mathfrak{a} = R$.

Proposition 1.32. *(i) An ideal $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is a domain.*

(ii) An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.

(iii) Every maximal ideal is prime.

(iv) An element $p \in R \backslash \{0\}$ is prime if and only if $(p) \neq (0)$ is prime.

Proof. Todo: include reference or give the proof. □

Notice that the converse of (iii) is not true, i.e., not every prime ideal is maximal. For example, if R is a domain that is not a field (e.g., $R = \mathbb{Z}$), then the zero ideal (0) is prime but not maximal.

Until here in lecture 3 (22nd October, 2021)

1.3 Modules

Definition 1.33. Let R be a commutative unitary ring. A **R-module** [加群] consists of an abelian group $(M, +)$ and a scalar multiplication

$$\begin{aligned} R \times M &\longrightarrow M \\ (\alpha, x) &\longmapsto \alpha x\,, \end{aligned}$$

such that for all $x, y \in M$ and $\alpha, \beta \in R$ we have

- $(\alpha\beta)x = \alpha(\beta x)$,
- $(\alpha + \beta)x = \alpha x + \beta x$,
- $\alpha(x + y) = \alpha x + \alpha y$,
- $1x = x$.

Remark 1.34. (i) If R is a field then R-modules are R-vector spaces.

(ii) We can define R-module homomorphism, submodules, quotient modules similar as linear maps, subspaces, and quotient spaces.

(iii) Every commutative unitary ring R is a R-module over itself by defining the scalar multiplication as the usual multiplication in the ring. Its submodules are exactly the ideals of R.

Definition 1.35. (i) Let $A \subset M$ be a subset of an R-module M. Then

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \mid n \geq 1, r_i \in R, a_i \in A \right\}$$

denotes the **submodule of M generated by A.** By convention we set $\langle \emptyset \rangle = \{0\}$.

(ii) If $\langle A \rangle = M$ then A is called a **generating set of M** [生成系]. If there exists a finite A with $\langle A \rangle = M$ then M is called **finitely generated** [有限生成].

(iii) A family $(m_\lambda)_{\lambda \in \Lambda}$ of elements $m_\lambda \in M$ is called **linearly independent** [線型独立] if

$$\sum_{\lambda \in \Lambda} r_\lambda = 0$$

with $r_\lambda \in R$ ($r_\lambda = 0$ for all but finitely many λ) implies $r_\lambda = 0$ for all $\lambda \in \Lambda$.

(iv) A linearly independent generating set is called a **basis** [基底].

(v) If a R-module M has a basis then M is called a **free module** [自由加群].

Remark 1.36. (i) If R is a field then every R-module is free.

(ii) The $\mathbb{Z}$-module $M = \mathbb{Z}/2\mathbb{Z}$, where the scalar multiplication is defined by $r\bar{m} = \overline{rm}$, is not free. The set $A = \{\overline{0}\}$ does not generate M and the sets $A = \{\overline{1}\}$ and $A = \{\overline{0}, \overline{1}\}$ are not linearly independent, since $2 \cdot \overline{1} = \overline{0}$.

Proposition 1.37. *Let R be a commutative unitary ring and M a R-module. Then the following two statements are equivalent*

(i) All submodules of M are finitely generated.

(ii) Any sequence $M_1 \subset M_2 \subset M_3 \subset \dots$ of submodules of M eventually stabilizes, i.e. there exists some n such that $M_n = M_{n+1} = M_{n+2} = \dots$.

Definition 1.38. (i) A R-module which satisfies one of the conditions in Proposition 1.37 is calles a **noetherian module** [ネーター加群]

(ii) A ring is called **noetherian** if it is a noetherian module over itself.

Examples 1.39. (i) Fields and in general principal ideal domains are noetherian.

(ii) The following ring is not noetherian

$$R = \{f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\} = \{f(x) = m + xg(x) \mid m \in \mathbb{Z}, g(x) \in \mathbb{Q}[x]\} \,.$$

Since we can define for $n \geq 1$ the following ideals of R

$$M_n := \left\{ax + h(x) \mid a = \frac{m}{2^n}, m \in \mathbb{Z}, h(x) \in x^2\mathbb{Q}[x]\right\},$$

which give a non-stabilizing sequences of ideals/submodules $M_1 \subset M_2 \subset \dots$.

(iii) The ring $R = \mathbb{Q}[x_1, x_2, \dots]$ is finitely generated as a R-module but it is not notherian since the $\langle x_1, x_2, \dots \rangle$ is not finitely generated.

Proposition 1.40. *Let R be a noetherian ring and M a R-module. Then M is a noetherian module if and only if M is finitely generated.*

Proof. This is Exercise 6 (ii). □

Corollary 1.41. *Finitely generated modules over principal ideal domains are noetherian.*

Proof. This is a direct consequence of Proposition 1.40 since principal ideal domains are noetherian rings. □

2 Integrality

We start by defining one of the main objects of this course.

Definition 2.1. (i) An **algebraic number field** [代数体] K is a finite field extension of $\mathbb{Q}$, i.e. $\mathbb{Q} \subset K$ and $\dim_{\mathbb{Q}} K < \infty$. The elements of K are called **algebraic numbers** [代数的数].

(ii) A number $x \in K$ of an algebraic number field is called an **algebraic integer** [代数的整数] if it is the zero of a monic polynomial with integer coefficients, i.e. there exist some $a_1, \dots, a_n \in \mathbb{Z}$ with

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \,.$$

We denote the set of all algebraic integers of a number field K by

$$\mathcal{O}_K = \{x \in K \mid x \text{ algebraic integer}\}$$

This is called the **ring of integers of** K [整数環].

By definition it is not clear that $\mathcal{O}_K$ is actually a ring. To prove this we will consider integrality in more generality in the following.

Definition 2.2. Let $A \subset B$ be an extension of rings. An element $b \in B$ is called **integral over** A [**A 上整である**], if it satisfies a monic equation

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

for some $n \geq 1$ and $a_1, \ldots, a_n \in A$. The ring B is called **integral over** A if all elements of B are integral over A.

Proposition 2.3. *Finitely many elements $b_1, \ldots, b_n \in B$ are all integral over A if and only if the ring $A[b_1, \ldots, b_n]$ viewed as an A-module is finitely generated.*

Proposition 2.4 (Laplace expansion/Row-Column expansion [余因子展開])**.** *Let $M = (m_{ij})$ be an $(r \times r)$-matrix with entries in a ring R, and let $M^* = (m^*_{ij})$ be the adjoint matrix, i.e.*

$$m^*_{ij} = (-1)^{i+j} \det(M_{ij})\,,$$

where M_{ij} is obtained from M by deleting the i-th column and the j-th row. Then we have

$$MM^* = M^*M = \det(M)E,$$

where E denotes the unit matrix. In particular, for $x \in R^r$ we get

$$Mx = 0 \implies \det(M)x = 0\,.$$

Proof of Proposition 2.3. Let b be integral over A, i.e. $f(b) = 0$ for some monic polynomial $f(x) \in A[x]$ of degree $m \geq 1$. Since f is monic we can write any $g(x) \in A[x]$ as

$$g(x) = q(x)f(x) + r(x)$$

for some $q(x), r(x) \in A[x]$ with $\deg(r) < m$. Since $f(0) = 0$ we obtain $g(b) = r(b) = a_0 + a_1 b + \cdots + a_{m-1} b^{m-1}$ for some $a_i \in A$. This shows that $A[b]$ is finitely generated by $1, b, \ldots, b^{m-1}$ as a A-module. If $b_1, \ldots, b_n$ are integral over A we then see by induction on n that $A[b_1, \ldots, b_n]$ is finitely generated. This shows one direction of the proposition.
For the other direction assume that $A[b_1, \ldots, b_n]$ is finitely generated by $\omega_1, \ldots, \omega_r$. Then for any $b \in A[b_1, \ldots, b_n]$ we can write

$$bw_i = \sum_{j=1}^{r} a_{ij}\omega_j$$

for some $a_{ij} \in A$ and $i = 1, \ldots, r$. This we can also write in terms of matrices as

$$\underbrace{\begin{pmatrix} a_{1,1} & \cdots & a_{1,r} \\ \vdots & \ddots & \vdots \\ a_{r,1} & \cdots & a_{r,r} \end{pmatrix}}_{S:=} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \begin{pmatrix} b\omega_1 \\ \vdots \\ b\omega_r \end{pmatrix}$$

In particular, setting $M = bE - S$, which is a $r \times r$-matrix with entries in A, we can use Proposition 2.4 to obtain $\det(M)w_i = 0$. Moreover since $1 \in A[b_1, \dots, b_n]$ we can write $1 = c_1\omega_1 + \cdots + c_r\omega_r$ with $c_i \in A$, which gives $0 = \sum_{i=1}^{r} c_i \det(M)w_i = \det(M)$. The determinant of $M = bE - S$ is a monic polynomial in b, i.e. for some $a_i \in A$ we obtain

$$\det(M) = b^r + a_1 b^{r-1} + \cdots + a_r = 0\,,$$

which shows that b is integral over A. And therefore all $b_1, \dots, b_n$ are integral over A since b was an arbitrary element in $A[b_1, \dots, b_n]$. □

As a direct consequence from the proof of Proposition 2.3 we obtain the following.

Corollary 2.5. *If b_1 and b_2 are integral over A, then $b_1 + b_2$ and $b_1 \cdot b_2$ are also integral over A.*

Proof. By the proof of Proposition 2.3 we see that $b_1 + b_2 \in A[b_1, b_2]$ and $b_1 b_2 \in A[b_1, b_2]$ are integral over A if b_1 and b_2 are integral. □

Definition 2.6. Let $A \subset B$ be an extensions of rings.

(i) The ring

$$\bar{A} = \{b \in B \mid b \text{ integral over } A\}$$

is called the **integral closure of A in B**.

(ii) If $\bar{A} = A$ then A is called **integrally closed in B**.

Until here in lecture 4 (29th October, 2021)

Proposition 2.7. *Let $A \subset B \subset C$ be extension of rings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $c \in C$ with $c^n + b_1 c^{n-1} + \cdots + b_n = 0$ for some $b_1, \dots, b_n \in B$. Since $b_1, \dots, b_n$ are integral over A, we have by Proposition 2.3 that $R = A[b_1, \dots, b_n]$ is a finitely generated A-module. But $R[c]$ is a finitely generated R-module and therefore also a finitely generated A-module. Again by Proposition 2.3 we get that c is integral over A. □

Corollary 2.8. *If $A \subset B$ is an extension of rings, then the integral closure $\bar{A}$ of A in B is integrally closed in B.*

Proof. Let $\bar{\bar{A}}$ be the integral closure of $\bar{A}$. Then $A \subset \bar{A} \subset \bar{\bar{A}} \subset B$. Since $\bar{A}$ is integral over A and $\bar{\bar{A}}$ is integral over $\bar{A}$ we get by Proposition 2.7 that $\bar{\bar{A}}$ is integral over A. This implies $\bar{\bar{A}} \subset \bar{A}$ and therefore $\bar{A} = \bar{\bar{A}}$. □

Definition 2.9. Let R be a commutative unitary ring and let $S \subset R$ be a **multiplicative set**, i.e. $1 \in S$ and whenever $x, y \in S$ then $x \cdot y \in S$. On $R \times S$ we define the following equivalence relation

$$(r, s) \sim (r', s') :\Leftrightarrow \exists t \in S : t(rs' - r's) = 0\,.$$

The **localization of R by S** [環 R の部分集合 S による局所化] is defined as the set of equivalences classes

$$S^{-1}R := R \times S \big/ \sim .$$

We write the class of (r, s) in $S^{-1}R$ as a fraction $\frac{r}{s}$. $S^{-1}R$ is a commutative unitary ring with addition and multiplication defined by

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}, \qquad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

The neutral elements with respect to these operations are given by $0 = \frac{0}{1}$ and $1 = \frac{1}{1}$.

Remark 2.10. (i) The map

$$\begin{aligned} \varphi_S : R &\longmapsto S^{-1}R \\ r &\longmapsto \frac{r}{1} \end{aligned}$$

is an ring homomorphism, which is injective if and only if S does not contain any zero divisors.

(ii) We have $\varphi_S(S) \subset (S^{-1}R)^\times$ since $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$. But in general there are more units than just the elements coming from S, e.g. if $S = \{1, 4, 4^2, \dots\}$ then $2 \notin S$ but $\frac{2}{1} \in (S^{-1}\mathbb{Z})^\times$.

(iii) If R is a domain then $S = R\backslash\{0\}$ is a multiplicative set. In this case $S^{-1}R$ is a field, called the **field of fractions of R** [商体] and denoted by $\mathrm{Frac}(R) := S^{-1}R$. In particular φ_S is injective in this case and we can view R as a subring of $\mathrm{Frac}(R)$. For example we have $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(iv) If $\mathfrak{p} \subset R$ is a prime ideal, then $S_\mathfrak{p} := R\backslash\mathfrak{p}$ is multiplicative, since $1 \notin \mathfrak{p}$ and the condition $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ implies $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p} \implies xy \notin \mathfrak{p}$. The localization is then denoted by $R_\mathfrak{p} = S_\mathfrak{p}^{-1}R$. This is a so-called **local ring** [局所環], which means hat it has exaclty one maximal ideal given by $\mathfrak{m} = \left\{\frac{r}{s} \mid s \notin \mathfrak{p}, r \in \mathfrak{p}\right\}$.

Definition 2.11. Let A be a domain with field of fractions $K = \mathrm{Frac}(A)$.

(i) The integral closure $\bar{A}$ of A in K is called the **normalization of** A.

(ii) A is called **integrally closed** if $A = \bar{A}$.

Proposition 2.12. *Every factorial ring is integrally closed.*

Proof. Let A be a factorial ring and $K = \mathrm{Frac}(A)$. If $\frac{a}{b} \in K$ is integral over A, then

$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \dots + a_n = 0$$

for $a_1, \dots, a_n \in A$. Therefore multiplying with b^n gives

$$a^n + a_1 b a^{n-1} + \dots + a_n b^n = 0 .$$

If $\pi \in A$ is prime and $\pi | b$ then since A is factorial the above equations implies that $\pi | a$. Assuming that $\frac{a}{b}$ is reduced we therefore obtain $b \in A^\times$ and $\frac{a}{b} \in A$. □

3 Trace, Norm, and Discriminant

We recall some basic notions and facts about fields and their extensions.

Remark 3.1. (i) Let R be a ring and $K \subset R$ a field. An element $x \in R$ is called **algebraic over** K if it is the zero of a polynomial in $K[X]$. Otherwise, it is called **transcendental**. R is called algebraic over K if all elements in R are algebraic over K.

(ii) Let $K \subset L$ be a field extension, which we will denote L/K, read "L over K" in the following. The field L is a K-vector space and we call $[L : K] := \dim_K L$ the **degree** of the extension L/K. If the degree is finite, then L/K is called finite, and it is easy to see that L/K is algebraic in this case. Given two finite field extensions L/K and M/L, the extension M/K is also finite, and we have

$$[M : K] = [M : L][L : K] .$$

(iii) Let R again be a ring and $K \subset R$ a field. For any $\alpha \in R$ we have the ring homomorphism

$$\begin{aligned} \psi_\alpha : K[X] &\longrightarrow R \\ f &\longmapsto f(\alpha) . \end{aligned}$$

An element $\alpha \in R$ is algebraic if and only if $\ker(\psi_\alpha) \neq (0)$. Since $K[X]$ is a principal ideal domain we can find for any algebraic $\alpha \in R$ a monic polynomial, the **minimal polynomial of** α [**最小多項式**], $\min(\alpha) \in K[X]$ with $\ker(\psi_\alpha) = (\min(\alpha))$. We get

$$K[X]/(\min(\alpha)) = K(\alpha) .$$

(iv) A field K is called **algebraically closed** [**代数的閉体**], if any non-constant $f(X) \in K[X]$ splits into linear factors

$$f(X) = k(X - \alpha_1) \cdots (X - \alpha_n)$$

for some $k, \alpha_1, \ldots, \alpha_n \in K$. An **algebraic closure** $\bar{K}$ of a field K is an algebraic extension $\bar{K}/K$ which is algebraically closed. An algebraic closure always exists and is unique up to K-isomorphisms.

Proposition 3.2. *Let K be a field with $\mathrm{char}(K) = 0$ or $|K| < \infty$.*

(i) If $f \in K[X]$ is irreducible and $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ with $\alpha_i \in L$ in some extension L/K then the α_i are pairwise distinct.

(ii) If L/K is a finite extension with $[L : K] = n$ then there exist exactly n different homomorphisms $\sigma : L \to \bar{K}$, with $\sigma(x) = x$ for all $x \in K$. These type of homomorphisms between extensions of K are called K-homomorphisms.

(iii) If $[L : K] = n$ then there exists an element $\alpha \in L$ with $L = K(\alpha)$. This α is called a **primitive element**.

Examples 3.3. (i) For $K = \mathbb{Q}$ and $L = \mathbb{Q}(i) = \mathbb{Q}[X]/(X^2 + 1)$ we have $[L : K] = 2$. In this case the two different embeddings $\sigma_i : L \to \bar{K}$ are given by $\sigma_1(a + bi) = a + bi$ and $\sigma_2(a + bi) = a - bi$.

(ii) In general if $L = \mathbb{Q}(\alpha)$ for some algebraic number α with $[L : K] = n$ any element in L can be written as a sum $\sum_{j=0}^{n-1} c_j \alpha^j$ for some $c_j \in K$. If the minimal polynomial of α is $\min_K(\alpha) = \prod_{j=1}^{n}(X - \alpha_j)$ with $\alpha_j \in \bar{K}$ then the n embeddings of L into $\bar{K}$ are given for $i = 1, \ldots, n$ by

$$\begin{aligned} \sigma_i : L &\longrightarrow \bar{K} \\ \sum_{j=0}^{n-1} c_j \alpha^j &\longmapsto \sum_{j=0}^{n-1} c_j \alpha_i^j \,. \end{aligned}$$

(iii) For $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ a primitive element is given by $\alpha = \sqrt{2} + \sqrt{3}$ since clearly $\mathbb{Q}(\alpha) \subset L$ and due to $\sqrt{3} = \frac{11\alpha - \alpha^2}{2}$ and $\sqrt{2} = -\frac{9\alpha - \alpha^3}{2}$ we also have $L \subset \mathbb{Q}(\alpha)$, i.e. $L = \mathbb{Q}(\alpha)$.

Definition 3.4. Let L/K be a finite field extension with $[L : K] = n$. For $x \in L$ define the K-linear map on the n-dimensional K-vector space L by

$$\begin{aligned} T_x : L &\longrightarrow L \\ \alpha &\longmapsto x \cdot \alpha. \end{aligned}$$

Then we define the **trace** [跡] and **norm** [ノルム] of x by

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(T_x), \qquad \mathrm{N}_{L/K}(x) = \det(T_x)\,.$$

These are coefficients in the **characteristic polynomial** [固有多項式] of T_x

$$f_x(\lambda) = \det(\lambda \,\mathrm{id} - T_x) = \lambda^n - a_1\lambda^{n-1} + \cdots + (-1)^n a_n \in K[\lambda]$$

since we have $a_1 = \mathrm{Tr}_{L/K}(x)$ and $a_n = \mathrm{N}_{L/K}(x)$.

By definition we have for $x, y \in L$

$$\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)\,, \quad \text{and} \quad \mathrm{N}_{L/K}(x \cdot y) = \mathrm{N}_{L/K}(x)\,\mathrm{N}_{L/K}(y)\,,$$

and therefore the trace and norm can also be seen as group homomorphisms

$$\begin{aligned} \mathrm{Tr}_{L/K} &: (L, +) \longrightarrow (K, +), \\ \mathrm{N}_{L/K} &: (L^\times, \cdot) \longrightarrow (K^\times, +)\,. \end{aligned}$$

Examples 3.5. For $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$ we have $n = 2$ and $B = \{1, i\}$ is a basis of L as a K-vector space. For $x = a + bi \in L$ the matrix of T_x with respect to this basis is given by

$$[T_x]_B = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\,.$$

Therefore we obtain $\mathrm{Tr}_{L/K}(x) = 2a$ and $\mathrm{N}_{L/K}(x) = a^2 + b^2$.

Until here in lecture 5 (5th November, 2021)

Proposition 3.6. *Let L/K be a finite field extension with $[L:K]=n$ and $\mathrm{char}(K)=0$ or $|K|<\infty$. If $\sigma_i : L \to \bar{K}$ for $i=1,\dots,n$ denotes the n embeddings of L in $\bar{K}$, then for $x \in L$ we have*

$$\begin{aligned} f_x(\lambda) &= \prod_{i=1}^{n} (\lambda - \sigma_i(x)) \,, \\ \mathrm{Tr}_{L/K}(x) &= \sum_{i=1}^{n} \sigma_i(x) \,, \\ \mathrm{N}_{L/K}(x) &= \prod_{i=1}^{n} \sigma_i(x) \,. \end{aligned}$$

Proof. Let $p_x(t) = t^m + c_1 t^{m-1} + \cdots + c_m = \prod_{i=1}^{m}(t-x_i) \in K[t]$ be the minimal polynomial of x, i.e. $[K(x):K]=m$. Here the $x_i \in \bar{K}$ denote the, pairwise different, zeros of p_x, which are called the conjugates of x. Then $1, x, \dots, x^{m-1}$ is a basis of $K(x)/K$ and if $\alpha_1, \dots, \alpha_d$ is a basis of $L/K(x)$, then

$$B = (\alpha_1, \alpha_1 x_1, \dots, \alpha_1 x^{m-1}, \dots, \alpha_d, \alpha_d x, \dots, \alpha_d x^{m-1})$$

is a basis of L/K. The matrix of the k-linear map T_x with respect to the basis B is given by the diagonal block matrix

$$[T_x]_B = \begin{pmatrix} M & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & M \end{pmatrix}$$

which has d copies of the the $m \times m$-matrix

$$M = \begin{pmatrix} 0 & 0 & \dots & -c_m \\ 1 & \ddots & & -c_{m-1} \\ \vdots & 1 & \ddots & \vdots \\ 0 & \dots & 1 & -c_1 \end{pmatrix}$$

on the diagonal. Since $\det(tE - M) = p_x(t)$ we get that the characteristic polynomial of T_x is given by $f_x(t) = \det(tE - [T_x]_B) = p_x(t)^d$. We have n embeddings $\sigma \in \mathrm{Hom}_K(L, \bar{K})$, which can be divide into m classes of size d by the equivalence relation $\sigma \sim \tau :\Leftrightarrow \sigma(x) = \tau(x)$. Let $\tau_1, \dots, \tau_m$ be a system of representatives. Since for each embedding the image of x needs to be one of its conjugates, we get $p_x(t) = \prod_{j=1}^{m}(t - \tau_j(x))$ and therefore

$$f_x(t) = p_x(t)^d = \prod_{j=1}^{m} (t - \tau_j(x))^d = \prod_{j=1}^{m} \prod_{\sigma \sim \tau_j} (t - \sigma(x)) = \prod_{i=1}^{n} (t - \sigma_i(x)) \,,$$

which is the first statement we wanted to show. The second and third follow immediately by multiplying the product out and then use that the trace and norm are given by the first and last coefficients of f_x. □

Corollary 3.7. *Let $K \subset L \subset M$ be finite field extensions with $\mathrm{char}(K) = 0$ or $|K| < \infty$. Then we have*

$$\begin{aligned} \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} &= \mathrm{Tr}_{M/K} \\ \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L} &= \mathrm{N}_{M/K} \end{aligned}$$

Proof. This is Exercise 8. □

Definition 3.8. Let L/K be a finite field extension with $[L : K] = n$, $\mathrm{char}(K) = 0$ or $|K| < \infty$ and let $\sigma_i : L \to \bar{K}$ for $i = 1, \dots, n$ denote the n embeddings of L in $\bar{K}$. Then the **discriminant** [判別式] of a basis $\alpha_1, \dots, \alpha_n$ of L is defined by

$$d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

Remark 3.9. (i) Since $\mathrm{Tr}_{L_K}(\alpha_i\alpha_j) = \sum_{l=1}^{n} \sigma_l(\alpha_i)\sigma_l(\alpha_j)$ the matrix $(\mathrm{Tr}_{L_K}(\alpha_i\alpha_j))_{1\le i,j\le n}$ is given by the product of the transposed matrix $(\sigma_l(\alpha_i))^T$ and $(\sigma_l(\alpha_i))$. Therefore we get

$$d(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_{L_K}(\alpha_i\alpha_j)). \tag{3.1}$$

In particular this shows that $d(\alpha_1, \dots, \alpha_n) \in K$.

(ii) If θ is a primitive element of L/K, then $\{1, \theta, \dots, \theta^{n-1}\}$ is a basis of L/K. Setting $\theta_i := \sigma_i(\theta)$ we get the Vandermonde matrix

$$(\sigma_i(\theta^{j-1})) = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \ddots & & \theta_2^{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & \theta_n & \dots & & \theta_n^{n-1} \end{pmatrix}$$

which gives the discriminant $d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_j - \theta_i)^2$.

Proposition 3.10. *Let $\mathrm{char}(K) = 0$ or $|K| < \infty$ and let L/K be a finite field extensions with basis $\alpha_1, \dots, \alpha_n$. Then*

$$d(\alpha_1, \dots, \alpha_n) \neq 0$$

and $(x, y) = \mathrm{Tr}_{L/K}(xy)$ is a nondegenerate bilinear form on the K-vector space L.

Proof. Todo: See handwritten lecture notes. □

Situation 3.11. From now on we will consider the situation, where A is an integrally closed ring (e.g. $\mathbb{Z}$) with field of fractions $K = \mathrm{Frac}\, A$ (e.g. $\mathbb{Q}$). L/K will be a finite field extension (e.g. algebraic number field) and B is the integral closure of A in L (e.g. $\mathcal{O}_L$).

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & B \end{array}$$

Proposition 3.12. *With the notation as in Situation 3.11 we have the following.*

(i) Every element $\beta \in L$ has the form

$$\beta = \frac{b}{a}, \qquad \text{with } b \in B, a \in A.$$

In particular $L = \operatorname{Frac} B$.

(ii) $\beta \in L$ is integral over A if and only if $\min_K(\beta) \in A[X]$.

(iii) If $b \in B$ then $\operatorname{Tr}_{L/K}(b), \operatorname{N}_{L/K}(b) \in A$.

(iv) We have $b \in B^\times$ if and only if $\operatorname{N}_{L/K}(b) \in A^\times$.

Proof. Todo: See handwritten lecture notes for (i) and Homework 3 for (ii)-(iv). □

Lemma 3.13. *With the notation as in Situation 3.11. Let $\alpha_1, \dots, \alpha_n$ be a basis of L/K which is contained in B of discriminant $d = d(\alpha_1, \dots, \alpha_n)$. Then*

$$dB \subset A\alpha_1 + \cdots + A\alpha_n\,.$$

Proof. Todo: See handwritten lecture notes. □

Definition 3.14. An **integral basis** [整基底] of B over A (A-basis of B) is a system of elements $\omega_1, \dots, \omega_n \in B$, such that each $b \in B$ can be written uniquely as a linear combination

$$b = a_1\omega_1 + \cdots + a_n\omega_n,$$

with $a_1, \dots, a_n \in A$.

Remark 3.15. (i) An integral basis of B over A is automatically also a basis of L/K as a K-vector space, i.e. $n = [L : K]$. This follows from Proposition 3.12 i). In this case we say that L/K as an integral basis.

(ii) If B has an integral basis over A then B is a free A-module of rank $[L : K]$.

Proposition 3.16. *Let A be a principal ideal domain and consider again the Situation 3.11. Then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank $[L : K]$. In particular, B admits an integral basis over A.*

Proof. [N, Proposition 2.10]. □

Corollary 3.17. *Let K be a number field. Then every finitely generated $\mathcal{O}_K$-module $\mathfrak{a}$ in K has a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$, i.e.*

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

with $n = [K : \mathbb{Q}]$. The discriminant $d(\alpha_1, \dots, \alpha_n)$ is independent of the choice of the basis.

Proof. Todo: See handwritten lecture notes. □

Definition 3.18. With the same notation as in Corollary 3.17 we call $d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n)$ the **discriminant of the $\mathcal{O}_K$-module $\mathfrak{a}$**. In particular,

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \ldots, \omega_n),$$

where $\omega_1, \ldots, \omega_n$ is an integral basis of $K/\mathbb{Q}$,is called the **discriminant of the number field K**.

Until here in lecture 6 (12th November, 2021)

Proposition 3.19. *If $\mathfrak{a} \subset \mathfrak{a}'$ are two nonzero finitely generated $\mathcal{O}_K$-submodules of K, then the index $[\mathfrak{a}' : \mathfrak{a}]$ is finite and we have*

$$d(\mathfrak{a}) = [\mathfrak{a}' : \mathfrak{a}]^2 d(\mathfrak{a}')\,. \tag{3.2}$$

Proof. See [N, Proposition 2.12]. □

4 Dedekind domains

Proposition 4.1. *Let K be a number field. In $\mathcal{O}_K$ every non-unit $\alpha \neq 0$ can be factored into a product of irreducible elements.*

Proof. If α is not irreducible, then $\alpha = \beta\gamma$ with non-units $\beta, \gamma \in \mathcal{O}_K$. By the multiplicativity of the norm, $N_{L/K}(\beta)N_{L/K}(\gamma) = N_{L/K}(\alpha) \in \mathbb{Z}$. Since $\beta, \gamma \notin \mathcal{O}_K^\times, N_{L/K}(\beta), N_{L/K}(\gamma) \notin \{\pm 1\}$. This implies $1 < |N_{L/K}(\beta)|, |N_{L/K}(\gamma)| < |N_{L/K}(\alpha)|$. □

Definition 4.2. A domain R is called a **Dedekind domain** [デデキント環] if

(i) R is noetherian,

(ii) R is integrally closed,

(iii) every non-zero prime ideal in R is maximal.

Proposition 4.3. *The ring of integers $\mathcal{O}_K$ of an algebraic number field K is a Dedekind domain.*

Proof. (i) $\mathcal{O}_K$ is Noetherian since it is a finitely generated $\mathbb{Z}$-module, where $\mathbb{Z}$ is Noetherian.

(ii) $\mathcal{O}_K$ is integrally closed since it is the integral closure of $\mathbb{Z}$ in K which is integrally closed.

(iii) Let $\mathfrak{p} \neq (0)$ be a prime ideal in $\mathcal{O}_K$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. This ideal is nonzero, since for a nonzero $y \in \mathfrak{p}$, we have:

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0, a_j \in \mathbb{Z}.$$

We see that $a_0 \neq 0$ and $a_0 \in \mathfrak{p} \cap \mathbb{Z} \neq 0$. Hence, there is a prime ideal $\mathfrak{p}$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$.
We want now to show that $\overline{O} = \mathcal{O}_K/\mathfrak{p}$ is a field.
Note that $\overline{O}$ has the subring $\overline{K} = \mathbb{Z}/(p)$ and all $x \in \overline{O} - \{0\}$ are algebraic over $\overline{K}$. This means:

$$x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_0 = 0, \beta_j \in \overline{K}$$

with $\beta_0 \neq 0$, implies that $x \cdot ((-\beta_0)^{-1}(x^{n-1} + \cdots + \beta_1)) = 1$. Hence, x is invertible in $\overline{O}$, and so $\overline{O}$ is a field, and so $\mathfrak{p}$ is also a maximal ideal.

□

Theorem 4.4. *Let $\mathcal{O}$ be a Dedekind domain. Every ideal $\mathfrak{a}$ of $\mathcal{O}$, which differs from* (0) *and* (1)*, admits a factorization*

$$\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_i$ of $\mathcal{O}$, which is unique up to the order of the factors.

Lemma 4.5. *Let $\mathcal{O}$ be a Dedekind domain. For every ideal $\mathfrak{a} \neq (0)$ of $\mathcal{O}$ there exist nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that*

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{a}\,. \tag{4.1}$$

Proof. Let M be the set of $\mathfrak{a} \neq (0)$ such that there are no prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ with $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}$.

O is Noetherian, so that $M \neq \emptyset$ we can find a maximal element $\mathfrak{a} \in M$ with respect to inclusion $\subset$.

Certainly, $\mathfrak{a}$ is not a prime ideal (otherwise, the prime ideal itself is the $\mathfrak{p}_1$). By definition, there is $b_1, b_2 \notin \mathfrak{a}$ with $b_1 b_2 \in \mathfrak{a}$.

Setting $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$ and $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$. We have, $\mathfrak{a} \subset \mathfrak{a}_1 \notin M$, $\mathfrak{a} \subset \mathfrak{a}_2 \notin M$, and $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$.

Because $\mathfrak{a}_1, \mathfrak{a}_2 \notin M$, then $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}_1$, and $\mathfrak{p}'_1 \cdots \mathfrak{p}'_r \subset \mathfrak{a}_2$, for some prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{p}'_1, \cdots, \mathfrak{p}'_r$. Then, $\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}'_1 \cdots \mathfrak{p}'_r \subset \mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$. Thus, $\mathfrak{a} \notin M$. Contradiction.

Thus, $M = \emptyset$. □

Lemma 4.6. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K = \operatorname{Frac} \mathcal{O}$. Let $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal and set*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}\}\,.$$

Then we have $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ for any nonzero ideal $\mathfrak{a}$.

Proof. Let $\mathfrak{p} \neq (0)$ and $a \in \mathfrak{p}$ with $a \neq 0$, then $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$, for some prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ (with r as small as possible).

Then for some j, we have $\mathfrak{p}_j \subset \mathfrak{p}$, say $\mathfrak{p}_1 \subset \mathfrak{p}$. We set $\mathfrak{p} = \mathfrak{p}_1$ since $\mathfrak{p}_1$ is maximal.

Since r is minimal, we get $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a)$, so that we can choose $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r - (a)$, so $a^{-1}b \notin O$.

On the other hand, $b\mathfrak{p} \subset (a)$, then $a^{-1}b\mathfrak{p} \subset O$, then $a^{-1}b \in \mathfrak{p}^{-1}$, then $O \neq \mathfrak{p}^{-1}$.

Now let $\mathfrak{a} \subset O$ be a nonzero ideal. Because O is Noetherian, then $\mathfrak{a}$ is generated by the elements $\alpha_1, \cdots, \alpha_n$.

Suppose now that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, then for all $x \in \mathfrak{p}^{-1}$, we have:

$$x\alpha_i = \Sigma_{j=1}^{n} a_{ij}\alpha_j, a_{ij} \in O$$

Then $A(\alpha_1, \cdots, \alpha_n)^T = 0$ with $A = xE - (a_{ij})$.
Hence, $0 = det(A) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then x is integral over O.

But because O is integrally closed, then $x \in O$, then $\mathfrak{p}^{-1} = O$, contradiction. In conclusion, $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. □

Proof of Theorem 4.4. (i) (Existence)

Let M be the set of ideals not either (0) or (1) which do not admit a prime ideal decompositon.

If $M \neq \emptyset$, then there is a maximal element under inclusion ($\subset$), which we denote $\mathfrak{a} \subset M$ (because O is Noetherian).

Since $\mathfrak{a}$ is not prime (otherwise, the ideal itself is the decomposition), there exists a maximal ideal $\mathfrak{p}$ with $\mathfrak{a} \subset \mathfrak{p}$.

The previous lemma implies $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1}, \mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset O$.

Since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1} = O$, and with $O \subset \mathfrak{p}^{-1}$. We get $\mathfrak{a}\mathfrak{p}^{-1} \neq O$, otherwise, $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ (which is a contradiction).

Since $\mathfrak{a}$ is a maximal element in M, we see that $\mathfrak{a}\mathfrak{p}^{-1} \notin M$, so that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$.

Then $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}$, then $\mathfrak{a} \notin M$ (again, a contradiction). Hence, $M = \emptyset$.

(ii) (Uniqueness)

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

For a prime ideal $\mathfrak{p}, \mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \to \mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$ if and only if $\mathfrak{p}|\mathfrak{a}\mathfrak{b} \to \mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$.

Now we get that $\mathfrak{p}_1|\mathfrak{q}_j$, for some j, say $\mathfrak{p}_1|\mathfrak{q}_1$.

But because $\mathfrak{q}$ is maximal, $\mathfrak{q}_1 = \mathfrak{p}_1$. Then, $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$. Repeating the steps inductively, we can conclude that $r = s$ (at one point we will end with $\mathfrak{p}_i \cdots \mathfrak{p}_j = 1$ or $\mathfrak{q}_i \cdots \mathfrak{q}_j = 1$). Hence, $\mathfrak{p}_j = \mathfrak{q}_j$ after renaming.

□

By Theorem 4.4 any ideal $\mathfrak{a} \neq (0)$ of a Dedekind domain $\mathcal{O}$ can be (uniquely up to reordering) written as

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}$$

with $\nu_1, \dots, \nu_r \geq 1$ and pairwise distinct prime ideals $\mathfrak{p}_i$.

Examples 4.7. In Homework 2, we saw that in $R = \mathbb{Z}[\sqrt{-5}]$ we have the non-unique factorization of 6 into irreducible elements as $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. There are prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \subset R$ such that the ideals generated by these elements can be written as

$$(2) = \mathfrak{p}_1^2\,, \quad (3) = \mathfrak{p}_2\mathfrak{p}_3\,, \quad (1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2\,, \quad (1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$$

and thus, $(6) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ is the factorization in terms of prime ideals.

Until here in lecture 7 (19th November, 2021)

Definition 4.8. Let $\mathcal{O}$ be a Dedekind domain with field of fractions $K = \operatorname{Frac}\mathcal{O}$.

(i) A **fractional ideal** of K is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq \{0\}$ of K.

(ii) Fractional ideals in $\mathcal{O}$ are called **integral ideals** of K.

(iii) For $a \in K^\times$ the module $(a) := a\mathcal{O}$ is a fractional ideal, called a **fractional principal ideal**.

Proposition 4.9. *A $\mathcal{O}$-submodule $\mathfrak{a} \neq \{0\}$ of K is a fractional if and only if there exits a $c \in \mathcal{O}$, $c \neq 0$ with $c\mathfrak{a} \subset \mathcal{O}$.*

Proof. Suppose an O-submodule $\mathfrak{a} \neq (0)$ of K is a fractional ideal, then $\mathfrak{a}$ is generate by $\alpha_1, \alpha_2, \cdots, \alpha_r \in K$, then we can choose c to be the product of their denominators so that $c\mathfrak{a} \subset O$.

Suppose there is some $c \in O, c \neq 0$ such that $c\mathfrak{a} \subset O$. Then, $c\mathfrak{a}$ is an ideal in O, but because O is Noetherian, $c\mathfrak{a}$ is finitely generated by $\beta_1, \beta_2, \cdots, \beta_r$. Then $\beta_1/c, \beta_2/c, \cdots, \beta_r/c$ generate $\mathfrak{a}$. □

Proposition 4.10. *The fractional ideals form an abelian group, the* **ideal group** *J_K of K. The identity is $(1) = \mathcal{O}$, and the inverse of a fractional ideal $\mathfrak{a}$ is*

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathcal{O}\}\,.$$

Proof. The associativity, commutativity, and existence of identity (which is $\mathcal{O}$) is clear. For prime ideals $\mathfrak{p} \subset O$, we have $\mathfrak{p}\mathfrak{p}^{-1} = O$. For an integral ideal $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ the inverse is given by $\mathfrak{b} = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\cdots\mathfrak{p}_r^{-1}$. Since $\mathfrak{a}\mathfrak{b} = O, \mathfrak{b} \subset \mathfrak{a}^{-1}$ and if $x \in \mathfrak{a}^{-1}$ (so that $x\mathfrak{a} \subset O$), we have $x\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$ (note here: $xa \in O$ and $\mathfrak{a}\mathfrak{b} = O$), thus, $x \in \mathfrak{b}$. Hence, $\mathfrak{b} = \mathfrak{a}^{-1}$. If $\mathfrak{a}$ is fractional, i.e. $c\mathfrak{a} \subset O$ for some $c \in O, c \neq 0$, then $(c\mathfrak{a})^{-1} = c^{-1}\mathfrak{a}^{-1} \to (c\mathfrak{a})(c^{-1}\mathfrak{a}^{-1}) = O$. □

Corollary 4.11. *Every fractional ideal $\mathfrak{a}$ admits a unique representation as a product*

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p}\subset\mathcal{O}\\ \text{prime ideal}}} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$$

with $\nu_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$ and $\nu_\mathfrak{p}(\mathfrak{a}) = 0$ for almost all $\mathfrak{p}$.

Proof. For some $c \in O, c \neq 0, \mathfrak{a}$ is an integral ideal, which has a prime decomposition.
$\mathfrak{a} = (c\mathfrak{a})(c^{-1})$, since any fractional ideal is the quotient of integral ideals. □

Remark 4.12. The exponents $\nu_\mathfrak{p}$ satisfy the following properties for fractional ideals $\mathfrak{a}, \mathfrak{b} \subset K$ and all prime ideals $\mathfrak{p}$.

(i) $\nu_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = \nu_\mathfrak{p}(\mathfrak{a}) + \nu_\mathfrak{p}(\mathfrak{b})$.

(ii) $\mathfrak{a} \subset \mathcal{O} \Leftrightarrow \nu_\mathfrak{p}(\mathfrak{a}) \geq 0$.

(iii) $\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow \nu_\mathfrak{p}(\mathfrak{a}) \geq \nu_\mathfrak{p}(\mathfrak{b})$.

(iv) $\nu_\mathfrak{p}(\mathfrak{a}+\mathfrak{b}) = \min(\nu_\mathfrak{p}(\mathfrak{a}), \nu_\mathfrak{p}(\mathfrak{b}))$.

These properties are the data needed to define the so-called 'discrete valuation rings' (DVR). See section 11 of [N] for details. In fact, the Dedekind domains and DVRs are almost the same except that DVRs are mostly defined for local rings.

Definition 4.13. (i) By P_K we denote the subgroup of J_K generated by all fractional principal ideals $(a) = a\mathcal{O}$ with $a \in K^\times$.

(ii) The quotient

$$\mathrm{Cl}_K = {}^{J_K}\!/_{P_K}$$

is called the **(ideal) class group** [**イデアル類群**] of K.

Remark 4.14. (i) A Dedekind domain $\mathcal{O}$ is a PID if and only if Cl_K is trivial.

(ii) One can show that a Dedekind domain is a UFD if and only if it is a PID.

(iii) We have the exact sequence

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow K^\times \longrightarrow J_K \longrightarrow \mathrm{Cl}_K \longrightarrow 1\,.$$

5 Lattices

Definition 5.1. Let V be an n-dimensional $\mathbb{R}$-vector space.

(i) A **lattice** in V is a subgroup of the form

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

with linearly independent $v_1, \ldots, v_m \in V$. The $(v_1, \ldots, v_m)$ is called a **basis** of Γ and the set

$$\Phi = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

a **fundamental mesh** of the lattice Γ.

(ii) Γ is called **complete** if $m = n$.

Definition 5.2. A subgroup $G \subset V$ is called **discrete subgroup** if all $\gamma \in G$ are isolated points in V (with respect to the topology V obtains from an isomorphism $V \cong \mathbb{R}^n$).

Proposition 5.3. *A subgroup $\Gamma \subset V$ is a lattice if and only if it is discrete.*

Proof. [N, Proposition 4.2]. □

Lemma 5.4. *A lattice $\Gamma \subset V$ is complete if and only if there exist a bounded subset $M \subset V$ whose translates cover V, i.e.*

$$V = \bigcup_{\gamma \in \Gamma} (M + \gamma)\,.$$

Proof. Todo: See handwritten lecture notes. □

Definition 5.5. (i) A **euclidean vector space** is a finite dimensional $\mathbb{R}$-vector space V equipped with a symmetric, positive definite bilinear form

$$\langle , \rangle : V \times V \longrightarrow \mathbb{R}\,.$$

(ii) On a euclidean vector space V we have a notion of volume. Let $e_1, \dots, e_n$ be a orthonormal basis of V. For linear independent $v_1, \dots, v_n \in V$ with $v_i = \sum_{j=1}^{n} a_{ij} e_j$ we define the volume of the parallelepiped

$$\Phi(v_1, \dots, v_n) = \{x_1 v_1 + \cdots + x_n v_n \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

by

$$\mathrm{vol}(\Phi(v_1, \dots, v_n)) = |\det(a_{ij})| = |\det(A)|\,.$$

Definition 5.6. A subset $X \subset V$ is called

(i) **centrally symmetric** if for all $x \in X$ we also have $-x \in X$.

(ii) **convex** if for all $x, y \in X$ the line segment $\{ty + (1-t)x \mid 0 \leq t \leq 1\}$ is contained in X.

Theorem 5.7. *Let Γ be a complete lattice in the n-dimensional euclidean vector space V and X a centrally symmetric, convex subset of V. Suppose that*

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

Then X contains at least one nonzero lattice point $\gamma \in \Gamma$.

Proof. Todo: See handwritten lecture notes. Would be nice to include also an example and a nice picture with Tikz. □

Until here in lecture 8 (26th November, 2021)

6 Minkowski Theory

From now on K is again a number field. We will recall some facts on the embeddings of K. Let $[K : \mathbb{Q}] = n$ and let θ be a primitive element, i.e. $K = \mathbb{Q}[\theta]$, and denote the minimal polynomial of θ by $p_\theta(X) = \prod_{i=1}^{n}(X - \theta_i)$, where $\theta_i \in \bar{K} \subset \mathbb{C}$ are the conjugates of θ. Any $a \in K$ can then uniquely be written as $a = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$ for some $a_0, \dots . a_{n-1} \in \mathbb{Q}$. Each conjugate θ_i for $i = 1, \dots, n$ gives an embedding of K by

$$\begin{aligned} \tau_i : K &\longrightarrow \mathbb{C} \\ \sum_{j=0}^{n-1} a_j \theta^j &\longmapsto \sum_{j=0} a_j \theta_i^j\,. \end{aligned}$$

Some of the θ_j might be real and therefore $\tau_i(K) \subset \mathbb{R}$. These embeddings τ_i are called **real embeddings**. The other zeros of p_θ come in pairs of complex conjugates $\theta_i = \overline{\theta_{i'}} \in \mathbb{C}\backslash\mathbb{R}$ with $1 \leq i < i' \leq n$. The corresponding embeddings $\tau_i, \tau_{i'}$ are called **complex embeddings**. We will usually denote the number of real embeddings by r and the number of pairs of complex embeddings by s, i.e. we have $n = r + 2s$.

We want to embed K into some euclidean vector space in order to use the results of the previous section. For this we will first embed it into a complex vector space. Consider all embeddings $\tau_i : K \to \mathbb{C}$ at the same time and define the map

$$\begin{aligned} j : K &\longrightarrow K_{\mathbb{C}} := \prod_\tau \mathbb{C} \\ a &\longmapsto j(a) = (\tau(a))_\tau =: (a_\tau)_\tau \,. \end{aligned}$$

Here and in the following we denote by $\prod_\tau$ (resp. $\sum_\tau$) alway the product (resp. the sum) over all embeddings $\tau_i : K \to \mathbb{C}$.
The space $K_{\mathbb{C}}$ can be equipped with the hermitian scalar product

$$\langle x, y\rangle = \sum_\tau x_\tau \overline{y_\tau}\,,$$

i.e. $\langle \cdot, y\rangle$ is linear, $\overline{\langle x, y\rangle} = \langle y, y\rangle$ and $\langle x, x\rangle > 0$ for $x \neq 0$. The complex conjugation $F : z \to \bar{z}$ generates the Galois group $G(\mathbb{C}/\mathbb{R})$, which acts on $\mathbb{C}$ and also on $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ by

$$\begin{aligned} F : \tau \mapsto (\overline{\tau} : K &\to \mathbb{C}) \\ x &\mapsto \bar{\tau}(x) := \overline{\tau(x)}\,. \end{aligned}$$

This gives an involution $F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ with $(F(z))_\tau = \bar{z}_{\bar{\tau}}$. Then one checks that the hermitian scalar product satisfies

$$\langle F(x), F(y)\rangle = F\left(\langle x, y\rangle\right)\,.$$

We see that the image of j in $K_{\mathbb{C}}$ is invariant under the action of F, which leads to the following.

Definition 6.1. Let $K_{\mathbb{R}}$ denote the F-invariant subspace of $K_{\mathbb{C}}$, i.e.

$$K_{\mathbb{R}} = \{z \in K_{\mathbb{C}} \mod z_{\bar{\tau}} = \overline{z_\tau}\}\,.$$

The restriction of $\langle , \rangle$ on $K_{\mathbb{R}}$ gives a scalar product $\langle , \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ on the $\mathbb{R}$-vector space $K_{\mathbb{R}}$, since for $x, y \in K_{\mathbb{R}}$ we have $F\langle x, y\rangle = \langle F(x), F(y)\rangle = \langle x, y\rangle = \langle y, y\rangle \in \mathbb{R}$.
The euclidean vector space $(K_{\mathbb{R}}, \langle , \rangle)$ is called **Minkowski space**. $\langle , \rangle$ is called the **canonical metric** and the associated measure (Definition 5.5) is called **canonical measure**. We denote for $X \subset K_{\mathbb{R}}$ its volume by $\mathrm{vol}(X)$.

Example 6.2. If $K = \mathbb{Q}[\sqrt[3]{2}]$ then with $\theta = \theta_1 = \sqrt[3]{2}$ we have $p_\theta(X) = X^3 - 2 = (X - \theta_1)(X - \theta_2)(X - \theta_3)$, where $\theta_2 = -\frac{1}{\sqrt[3]{4}} + \frac{\sqrt{3}}{\sqrt[3]{4}}$ and $\theta_3 = -\frac{1}{\sqrt[3]{4}} - \frac{\sqrt{3}}{\sqrt[3]{4}}$. In this case there is one real embedding τ_1 and one pair of complex embeddings τ_2, τ_3. If we indentify $K_{\mathbb{C}}$ with $\mathbb{C}^3$ such that that the first entry corresponds to the real embedding, then the involution F is given by

$$F\left(\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}\right) = \begin{pmatrix} \overline{z_1} \\ \overline{z_3} \\ \overline{z_2} \end{pmatrix} .$$

Therefore the Minkowski space in this case is given by

$$K_{\mathbb{R}} = \left\{ \begin{pmatrix} z_1 \\ z_2 \\ \overline{z_2} \end{pmatrix} \mid z_1 \in \mathbb{R}, z_2 \in \mathbb{C} \right\} .$$

Denote the real embeddings of K by $\rho_1, \dots, \rho_r : K \to \mathbb{R}$ and the complex ones by $\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$. Then the Minkowski space can be written as

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} \mid z_\rho \in \mathbb{R}, z_{\bar{\sigma}} = \overline{z_\sigma}\}$$

here we use the notation $z_\rho \in \mathbb{R}$ for $z_{\rho_i} \in \mathbb{R}$ for all $i = 1, \dots, r$ and similarly $z_{\bar{\sigma}} = \overline{z_\sigma}$ means that $z_{\overline{\sigma_j}} = \overline{z_{\sigma_j}}$ for $j = 1, \dots, s$. This space is isomorphic to $\mathbb{R}^{r+2s} = \mathbb{R}^n$ by the following isomorphism

$$\begin{aligned} f : K_{\mathbb{R}} &\longrightarrow \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s} \\ z_\tau &\longmapsto x_\tau, \end{aligned}$$

where $x_\rho = z_\rho$, $x_\sigma = \mathrm{Re}(z_\sigma)$ and $x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma)$. This isomorphism transforms the canonical metric into the scalar product

$$(x, y) = \sum_\tau a_\tau x_\tau y_\tau$$

on $\mathbb{R}^n$, where $a_\tau = 1$ if τ is real and $a_\tau = 2$ if τ is complex (See [N, Proposition 5.1]).Therefore the canonical measure and the Lebesgue measure on $\mathbb{R}^n$ differ by a factor of 2^s, i.e. for $X \subset K_{\mathbb{R}}$ we have

$$\mathrm{vol}(X) = 2^s \, \mathrm{vol}_{\mathrm{Lebesgue}}(f(X)) .$$

Proposition 6.3. *If $\mathfrak{a} \neq 0$ is an ideal of $\mathcal{O}_K$, then $\Gamma = j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$. Its fundamental mesh has volume*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}] .$$

Proof. Todo: See handwritten lecture notes. (See also [N, Proposition 5.2]) □

Now we can use Minkowskis lattice point theorem (Theorem 5.7) to obtain the following:

Theorem 6.4. *Let $\mathfrak{a} \neq (0)$ be an ideal of $\mathcal{O}_K$, and let $c_\tau > 0$ be real numbers for each embedding $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, such that $c_\tau = c_{\overline{\tau}}$ and*

$$\prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}] . \tag{6.1}$$

Then there exists an $a \in \mathfrak{a}$, $a \neq 0$ with

$$|\tau(a)| < c_\tau$$

for all $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

Proof. Todo: See handwritten lecture notes. □

Until here in lecture 9 (3rd December, 2021)

7 The class number

In this section, K will always denote a number field.

Definition 7.1. Let $\mathfrak{a} \neq (0)$ be an ideal in $\mathcal{O}_K$. Then

$$\mathfrak{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = \left|\mathcal{O}_K/\mathfrak{a}\right|$$

is called the **absolute norm** of $\mathfrak{a}$.

Remark 7.2. (i) By Proposition 3.19 the absolute norm is always finite.

(ii) For principal ideals $\mathfrak{a} = (a)$ with $a \in \mathcal{O}_K \backslash \{0\}$ we have

$$\mathfrak{N}(\mathfrak{a}) = |\,\mathrm{N}_{K/\mathbb{Q}}(a)|.$$

Proposition 7.3. *If $\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}$ is the prime factorization of an ideal $\mathfrak{a} \neq (0)$ then*

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{\nu_1} \dots \mathfrak{N}(\mathfrak{p}_r)^{\nu_r}\,.$$

Proof. Todo: See handwritten lecture notes. □

Corollary 7.4. *For ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ with $\mathfrak{a}, \mathfrak{b} \neq (0)$ we have*

$$\mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})\,.$$

Lemma 7.5. *In every ideal $\mathfrak{a} \neq (0)$ of $\mathcal{O}_K$ there exists an $a \in \mathfrak{a}$, $a \neq 0$, with*

$$|\,\mathrm{N}_{K/\mathbb{Q}}(a)| \leq \left(\frac{2}{\pi}\right)^2 \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a})\,.$$

Proof. Todo: See handwritten lecture notes. □

Theorem 7.6. *The ideal class group $\mathrm{Cl}_K = {}^{J_K}\!/_{P_K}$ is finite. Its order*

$$h_k = |\,\mathrm{Cl}_K\,|$$

is called the **class number** [類数] *of K.*

Proof. Todo: See handwritten lecture notes. □

Until here in lecture 10 (10th December, 2021)

Example 7.7. Let $K = \mathbb{Q}(\sqrt{-5})$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ has integral basis $\{1, \sqrt{-5}\}$ and $r = 0, s = 1$, $\tau_{1,2} : a + b\sqrt{-5} \mapsto a \pm b\sqrt{-5}$.

$$d_K = \det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-2\sqrt{-5})^2 = -20\,,$$
$$\left(\frac{2}{\pi}\right)^2 \sqrt{|d_K|} = \frac{2}{\pi}\sqrt{20} \approx 2.85\,.$$

Every class of Cl_K therefore contains an ideal $\mathfrak{a}$ with $\mathfrak{N}(\mathfrak{a}) \leq 2$. If $\mathfrak{N}(\mathfrak{a}) = 1$ then $\mathfrak{a} = \mathcal{O}_K$. If $\mathfrak{N}(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a}$, i.e. $\mathfrak{a}|(2)$. The prime factorization of (2) is

$$(2) = (2, 1 + \sqrt{-5})^2 =: \mathfrak{p}^2$$

and $\mathfrak{N}(\mathfrak{p}) = 2$. This shows that $(2, 1 + \sqrt{-5})$ is the only ideal of norm 2. This shows $h_K \leq 2$ and since $\mathbb{Z}[\sqrt{-5}]$ is not a PID we have $h_K > 1$ from which we get $h_K = 2$.

A better bound for the norm is given by the following:

Theorem 7.8 (Minkowski's bound)**.** *Every class of* Cl_K *contains an ideal* $\mathfrak{a} \subset \mathcal{O}_K$ *with*

$$\mathfrak{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^2 \sqrt{|d_K|}\,.$$

Proof. This can be shown by proving a refinement of Theorem 6.4, Lemma 7.5 and the proof of Theorem 7.6. □

Definition 7.9. The **Dedekind zeta function** of a number field K is defined for $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$ by

$$\zeta_K(z) = \sum_{(0)\neq\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{\mathfrak{N}(\mathfrak{a})^z}\,.$$

Remark 7.10. (i) The Dedekind zeta functions converges absolutely for $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$ and it has an analytic continuation to $\mathbb{C}$ with a simple pole only at $z = 1$.

(ii) Due to the unique prime ideal factorization in $\mathcal{O}_K$ we have the **Euler product** ($\mathrm{Re}(z) > 1$)

$$\zeta_K(z) = \prod_{\substack{(0)\neq\mathfrak{p}\subset\mathcal{O}_K \\ \mathfrak{p}\text{ prime ideal}}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-z}}\,.$$

(iii) In the case $K = \mathbb{Q}$ we have for $\mathrm{Re}(z) > 1$

$$\zeta_K(z) = \zeta(z) = \sum_{m>0} \frac{1}{m^z} = \prod_{p\text{ prime}} \frac{1}{1 - p^{-z}}\,.$$

Theorem 7.11 (Analytic class number formula)**.** *The residue of* ζ_K *at* $z = 1$ *is given by*

$$\lim_{z\to 1}(1 - z)\zeta_K(z) = \frac{2^r(2\pi)^s h_K R_K}{\omega_K\sqrt{|d_K|}}\,,$$

where R_K *is the regulator of* K *and* ω_K *is the number of roots of unity in* K*. (Both will appear in Section 9).*

8 Fermat's Last Theorem

Recall that for $n \geq 1$ the Fermat equation is

$$x^n + y^n = z^n \,. \tag{8.1}$$

We are interest in **non-trivial solutions** $(xyz \neq 0)$ for (8.1) with $x, y, z \in \mathbb{Z}$.

(i) The case $n = 1$ is clear and for $n = 2$ there are infinitely many non-trivial solutions (Exercise 4).

(ii) For $n \geq 3$ Fermat claimed (Fermat's Last Theorem): There are no non-trivial solutions for (8.1).

Theorem 8.1. *There are no nonzero solutions $x, y, z \in \mathbb{Z}$ for*

$$x^4 + y^4 = z^2 \,.$$

Proof. This is Exercise 12 □

Definition 8.2. A prime p is called **regular** if p does not divide $h_{\mathbb{Q}(\zeta_p)}$.

Theorem 8.3 (Kummer 1850)**.** *(i) If $n = p \geq 3$ is a regular prime then there are no non-trivial solutions to* (8.1)*.*

(ii) A prime p is regular if and only if it does not divide the numerator of the Bernoulli numbers B_k for $k = 2, 4, \ldots, p-3$. Here the **Bernoulli numbers** *B_k are defined by their exponential generating series*

$$\sum_{k \geq 0} \frac{B_k}{k!} X^k := \frac{X}{e^X - 1} \,.$$

Remark 8.4. (i) Setting $h_p := h_{\mathbb{Q}(\zeta_p)}$ we have $h_p = 1$ for $p \leq 19$ and $h_{23} = 3$, $h_{37} = 37$, $h_{59} = 3 \cdot 59 \cdot 233$, $h_{67} = 67 \cdot 12739$. All primes ≤ 100 are regular except for 37, 59 and 67.

(ii) Conjecturally there are infinitely many ($\sim 60\%$ of all primes) regular primes. We just know that there are infinitely irregular primes.

Lemma 8.5. *Let $K = \mathbb{Q}(\zeta_p)$ and let $\mathfrak{a} \subset \mathcal{O}_K$ be an idea. If p is regular and $\mathfrak{a}^p$ is principal, then $\mathfrak{a}$ is also principal.*

Proof. Todo: See handwritten lecture notes. □

Lemma 8.6. *We write $\zeta = \zeta_p$ for a fixed prime p.*

(i) In $\mathbb{Z}[\zeta]$ the numbers $1 - \zeta, 1 - \zeta^2, \ldots, 1 - \zeta^{p-1}$ are all associated and $1 + \zeta$ is a unit.

(ii) $p = u(1 - \zeta)^{p-1}$ for some unit $u \in \mathbb{Z}[\zeta]^\times$ and $(1 - \zeta)$ is the only prime ideal in $\mathbb{Z}[\zeta]$ dividing (p).

Proof. See [C]. □

Until here in lecture 11 (17th December, 2021)

9 Dirichlet's Unit Theorem

Denote by $\mu(K)$ the set of roots of unities contained in a number field K and define $\gamma = (l \circ j)(\mathcal{O}_K) = \lambda(\mathcal{O}_K)$. Todo: See details in the handwritten lecture notes.

Proposition 9.1. *The sequence*

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \longrightarrow 0$$

is exact.

Proof. Todo: See handwritten lecture notes. □

Lemma 9.2. *For a given $a \in \mathbb{Z}$, there are, up to associates, only finitely many elements $\alpha \in \mathcal{O}^\times$ with $N_{K/\mathbb{Q}}(\alpha) = a$.*

Proof. Todo: See handwritten lecture notes. □

Proposition 9.3. *The group Γ is a complete lattice in the $(r+s-1)$-dimensional vector space H, i.e $\Gamma \cong \mathbb{Z}^{r+s-1}$.*

Proof. Todo: See handwritten lecture notes. □

Theorem 9.4 (Dirichlet's unit theorem)**.** *The unit group $\mathcal{O}_K^\times$ is given by a direct product of the cyclic group $\mu(K)$ and a free abelian group of rank $r+s-1$, i.e.*

$$\mathcal{O}_K^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}\,.$$

Proof. Todo: See handwritten lecture notes. □

Until here in lecture 12 (14th January, 2022)

Remark 9.5. (i) By Theorem 9.4 there exist units $\epsilon_1, \ldots, \epsilon_t$ $(t = r+s-1)$ called the **fundamental units**, such that any unit $\epsilon \in \mathcal{O}_K^\times$ can be written as

$$\epsilon = \zeta \epsilon_1^{\nu_1} \cdots \epsilon_t^{\nu_t}$$

with $\zeta \in \mu(K)$ and $\nu_1, \ldots, \nu_t \in \mathbb{Z}$.

(ii) Todo: See handwritten lecture notes for unit the unit groups of quadratic fields $K = \mathbb{Q}(\sqrt{d})$

10 Extensions of Dedekind domains

In this section, we consider again the general case, where A is a Dedekind domain, $K = \operatorname{Frac} A$ its field of fractions, L/K a finite extension and $\mathcal{O}$ the integral closure of A in L.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \uparrow & & \uparrow \\ A & \hookrightarrow & \mathcal{O} \end{array}$$

Proposition 10.1. *(i) $\mathcal{O}$ is a Dedekind domain.*

(ii) Every ideal of $\mathcal{O}$ is a finitely generated A-module.

Proof. Todo: See handwritten lecture notes. □

Proposition 10.2. *Let $\mathfrak{p}$ be a prime ideal of A ($\mathfrak{p} \neq (0)$) then $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.*

Proof. Todo: See handwritten lecture notes. □

A prime ideal $\mathfrak{p} \neq (0)$ of A decomposes in $\mathcal{O}$ in a unique way into a product of prime ideals,

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} . \tag{10.1}$$

Definition 10.3. (i) The exponent e_i in (10.1) is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$.

(ii) The degree of the field extension

$$f_i = \left[{}^{\mathcal{O}}\!/_{\mathfrak{P}_i} : {}^{A}\!/_{\mathfrak{p}} \right]$$

is called the **inertia degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$.

Theorem 10.4 (Fundamental identity)**.** *Let* $\mathrm{char}(K) = 0$ *or* $|K| < \infty$, $n = [L/K]$ *and let $\mathfrak{p}$ be a prime ideal of A which has the factorization* (10.1)*. Then we have*

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

Proof. Todo: See handwritten lecture notes. □

Until here in lecture 13 (21th January, 2022)

Example 10.5. In the case $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathcal{O} = \mathcal{O}_L = \mathbb{Z}[i]$ we have the following different situations for the factorization of prime ideals $\mathfrak{p} \subset A$ in $\mathcal{O}$:

- $\mathfrak{p} = (2)$: It is $(2) = (1+i)^2$, i.e. $r = 1, e_1 = 2$ and $f_1 = [{}^{\mathbb{Z}[i]}\!/_{(1+i)} : {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}] = 1$.
- $\mathfrak{p} = (p)$ for prime $p \equiv 1 \mod 4$: In this case we saw that there exist $a, b \in \mathbb{Z}$ with $p = a^2 + b^2$ and $(p) = (a+bi)(a-bi)$. Therefore, $r = 2, e_1 = e_2 = 1$ and $f_{1,2} = [{}^{\mathbb{Z}[i]}\!/_{(a \pm bi)} : {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}] = 1$.
- $\mathfrak{p} = (p)$ for prime $p \equiv 3 \mod 4$: In this case (p) is prime in $\mathbb{Z}[i]$ and $r = 1, e_1 = 1$ and $f_1 = [{}^{\mathbb{Z}[i]}\!/_{(p)} : {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}] = 2$.

Let $\theta \in L$ be a primitive element, i.e. $L = K(\theta)$. We can choose $\theta \in \mathcal{O}$ and write $p(X) \in A[X]$ for its minimal polynomial.

Definition 10.6. The ideal

$$\mathfrak{F} = \{\alpha \in \mathcal{O} \mid \alpha\mathcal{O} \subset A[\theta]\} \subset \mathcal{O}$$

is called the **conductor** of the ring $A[\theta]$.

Proposition 10.7. *Let $\mathfrak{p} \subset A$ be a prime ideal which is coprime to the conductor $\mathfrak{F}$ of $A[\theta]$ (i.e. $\mathfrak{p}\mathcal{O} + \mathfrak{F} = \mathcal{O}$). Let*

$$\overline{p}(X) = \overline{p}_1(X)^{e_1} \cdots \overline{p}_r(X)^{e_r}$$

be the factorization of $\overline{p}(X) \equiv p(x) \mod \mathfrak{p}$ into irreducibles $\overline{p}_i(X) \equiv p_i(x) \mod \mathfrak{p}$ over $A/\mathfrak{p}$. Then for $i = 1, \ldots, r$ the

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$$

are the different prime ideals of $\mathcal{O}$ above $\mathfrak{p}$. The inertia degrees are $f_i = \deg p_i$ and we have

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} . \tag{10.2}$$

Proof. Todo: See handwritten lecture notes. □

Example 10.8. Again we consider the the case $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathcal{O} = \mathcal{O}_L = \mathbb{Z}[i]$. Let $\mathfrak{p} = (p)$ for a prime p. We have the following factorization of the minimal polynomial $p(X) = X^2 + 1$ modulo the ideal $\mathfrak{p}$:

- $p = 2$: $X^2 + 1 \equiv (X + 1)^2 \mod \mathfrak{p}$.
- $p = 4n + 1$ for $n \geq 1$: $X^2 + 1 \equiv (X - (2n)!)(X + (2n)!) \mod \mathfrak{p}$. (see proof of Theorem 1.3)
- $p = 4n + 3$ for $n \geq 1$: $X^2 + 1$ is irreducible modulo $\mathfrak{p}$.

Definition 10.9. Let $\mathfrak{p} \subset A$ be a prime ideal with the following factorization in $\mathcal{O}$

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} . \tag{10.3}$$

(i) $\mathfrak{p}$ is said to **split completely** (or **totally split**) in L, if $r = n = [L : K]$, i.e. $e_i = f_i = 1$ for all $i = 1, \ldots, r$.

(ii) $\mathfrak{p}$ is called **nonsplit** (or **indecomposed**) if $r = 1$, i.e. there is just one prime ideal in $\mathcal{O}$ over $\mathfrak{p}$.

(iii) $\mathfrak{P}_i$ is called **unramified** over A (or K) if $e_i = 1$ and if the extension $\mathcal{O}/\mathfrak{P}_i / A/\mathfrak{p}$ is separable. Otherwise $\mathfrak{P}_i$ is called **ramified**. If $e_i > 1$ and $f_i = 1$ then $\mathfrak{P}_i$ is called **totally ramified**.

(iv) $\mathfrak{p}$ is called **unramified** if all $\mathfrak{P}_i$ over $\mathfrak{p}$ are unramified. Otherwise, $\mathfrak{p}$ is called **ramified**. In particular, if $\mathfrak{p}$ split completely then it is unramified.

(v) The extension L/K is called unramified if all prime ideals $\mathfrak{p} \subset A$ are unramified.

Example 10.10. Again we consider the the case $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathcal{O} = \mathcal{O}_L = \mathbb{Z}[i]$.

- $(2) = (1 + i)^2$ is ramified.
- $\mathfrak{p} = (p)$ for prime $p \equiv 1 \mod 4$: In this case we saw that there exist $a, b \in \mathbb{Z}$ with $p = a^2 + b^2$ and $(p) = (a + bi)(a - bi)$. Therefore $\mathfrak{p}$ split completely and is unramified.
- $\mathfrak{p} = (p)$ for prime $p \equiv 3 \mod 4$: $\mathfrak{p}$ is **inert** (it is also a prime ideal in $\mathcal{O}$) and therefore unramified.

Proposition 10.11. *There are just finitely many prime ideals of A which are ramified over L.*

Definition 10.12. The **discriminatn** $d_{\mathcal{O}/A}$ of the ring extension $\mathcal{O}/A$ is the ideal generated by the discriminants $d(\omega_1, \ldots, \omega_n)$ of all bases $\omega_1, \ldots, \omega_n$ of L/K contained in $\mathcal{O}$

One can show that $\mathfrak{p}$ is ramified in L if and only if $\mathfrak{p}$ divides $d_{\mathcal{O}/A}$. In the example $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\mathcal{O} = \mathcal{O}_L = \mathbb{Z}[i]$ we have $d_{\mathcal{O}/A} = (4)$ and therefore (2) is the only ramified prime ideal.

Until here in lecture 14 (28th January, 2022)

Exercises

The following gives the collection of all homework exercises.

Exercise 1. Recall some algebra. For this show the following basic facts for rings:

(i) In an integral domain, every prime element is irreducible.

(ii) In a unique factorization domain, every irreducible element is prime.

(iii) Any Euclidean ring is factorial.

Exercise 2. Wilson's theorem, i.e. show that for any prime number p we have

$$(p-1)! \equiv -1 \mod p\,.$$

Exercise 3. Show the following facts for the Gaussian integers $\mathbb{Z}[i]$:

(i) The group of units is $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. For this show that an element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$, where N is the norm defined by $N(\alpha) = |\alpha|^2$.

(ii) Show that, in the ring $\mathbb{Z}[i]$, the relation $\alpha\beta = e\gamma^n$, for relatively prime[1] numbers $\alpha, \beta \in \mathbb{Z}[i]$ and a unit $e \in \mathbb{Z}[i]^\times$ implies $\alpha = e_1 a^n$ and $\beta = e_2 b^n$ with $a, b \in \mathbb{Z}[i]$ and units $e_1, e_2 \in \mathbb{Z}[i]^\times$.

Exercise 4. Find all pythagorean triples, i.e. find all integers $a, b, c \in \mathbb{Z}$ satisfying

$$a^2 + b^2 = c^2\,.$$

For this proceed as follows:

(i) First focus on the case where $a, b, c > 0$ and $\gcd(a, b, c) = 1$ and then explain afterwards how you can obtain the remaining solutions from this.

(ii) Show that in this case, up to permutation, the solutions are all given by

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2\,,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $\gcd(u, v) = 1$ and u, v are not both odd. To show that these are indeed all solutions, factor $a^2 + b^2$ in $\mathbb{Z}[i]$ and then use Exercise 3 (ii).

Exercise 5. We saw that in $R = \mathbb{Z}[\sqrt{-5}]$ we have the non-unique factorization of 6 into irreducible elements as $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Find prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \subset R$ such that the ideals generated by these elements can be written as

[1] Relatively prime here means that there exists no irreducible element which divides both of them.

$$(2) = \mathfrak{p}_1^2\,, \quad (3) = \mathfrak{p}_2\mathfrak{p}_3\,, \quad (1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2\,, \quad (1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3$$

and conclude $(6) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$.

Exercise 6.

(i) Let R be a commutative unitary ring and M a R-module. Show that the following two statements are equivalent definitions for M being noetherian

   (a) All submodules of M are finitely generated.

   (b) Any sequence $M_1 \subset M_2 \subset M_3 \subset \dots$ of submodules of M eventually stabilizes, i.e. there exists some n such that $M_n = M_{n+1} = M_{n+2} = \dots$.

(ii) Let R be a noetherian ring and M a R-module. Show that M is a noetherian module if and only if M is finitely generated.

Exercise 7. Let $d \neq 1, 0$ be a square-free integer. Show that the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ is

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 1 \mod 4 \\ \mathbb{Z}\left[\frac{\sqrt{d}+1}{2}\right] & d \equiv 2,3 \mod 4 \end{cases},$$

i.e. show that the above set give exactly those elements in K which are integral over $\mathbb{Z}$.

Exercise 8. Let $K \subset L \subset M$ be finite field extensions with $\mathrm{char}(K) = 0$ or $|K| < \infty$. Show that

$$\begin{aligned} \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} &= \mathrm{Tr}_{M/K} \\ \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L} &= \mathrm{N}_{M/K} \end{aligned}$$

Exercise 9. Let A be an integrally closed ring with field of fractions $K = \mathrm{Frac}(A)$. L/K a finite field extension and B is the integral closure of A in L. Show the following:

(i) $\beta \in L$ is integral over A if and only if $\min_K(\beta) \in A[X]$.

(ii) If $b \in B$ then $\mathrm{Tr}_{L/K}(b), \mathrm{N}_{L/K}(b) \in A$.

(iii) We have $b \in B^\times$ if and only if $\mathrm{N}_{L/K}(b) \in A^\times$.

Exercise 10. Let d_1, d_2 be two coprime square-free integers and $d_1 \equiv 1 \mod 4$. Determine the discriminant d_K of the number field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

Exercise 11. Show that for any number field K the discriminant satisfies $d_K \equiv 0, 1 \mod 4$.

Exercise 12. Show that there are no nonzero solutions $x, y, z \in \mathbb{Z}$ for

$$x^4 + y^4 = z^2 .$$

(Hint: Use Exercise 4).

Exercise 13. Let ζ be a primitive n-th root of unity for $n \geq 3$. Show that the numbers $\epsilon = \frac{1-\zeta^k}{1-\zeta}$ for $(k, n) = 1$ are units in the ring of integers of the field $\mathbb{Q}(\zeta)$.

Exercise 14. Calculate the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$ for the cases $d = 2, 5, 10$.

Exercise 15. In $\mathbb{Z}[\sqrt[4]{2}]$, show $u = 1 + \sqrt[4]{2}$ and $v = 1 + \sqrt{2}$ are units and they are multiplicatively independent: if $u^a v^b = 1$ for $a, b \in \mathbb{Z}$ then $a = 0$ and $b = 0$.

References

[C] Keith Conrad, Fermat' s Last Theorem for Regular Primes. Available at`http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/fltreg.pdf`.

[IR] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, *Graduate Texts in Mathematics*, Second Edition, Springer-Verlag, Berlin.

[KKS] Kazuya Kato (加藤 和也), Nobushige Kurokawa (黒川 信重), Takeshi Saito (斎藤 毅), 数論〈*1*〉*Fermat* の夢と類体論 単行本, Tankobon Hardcover 2005/1/7.
English version: *Number Theory 1: Fermat's Dream*, Translations of Mathematical Monographs, Vol 186, First Edition.

[N] Jürgen Neukirch, Algebraic Number Theory, *Grundlehren der Mathematischen Wissenschaften* 322. Springer-Verlag.

[ST] Ian Stewart, David Tall, Algebraic Number Theory and Fermat's Last Theorem, *Chapman and Hall/CRC* 4th edition.

[Sch] Christoph Schweigert, Zahlentheorie, *Lecture notes, WS 2004/05, Universität Hamburg.* `http://www.math.uni-hamburg.de/home/schweigert/skripten/zskript.pdf`.