Analytic Number Theory III

Lecture notes

Prof. Dr. Damaris Schindler

LaTeX version by Alex Dalist Howl Sennewald

Mathematical Institute
Georg-August-University Göttingen

Winter term 2023/24

Contents

List of lectures

This script is not a substitute for Prof. Schindler's lecture notes and will not be reviewed by her again. Basically, these are just my personal notes, so I do not guarantee correctness or completeness and I might add further examples and notes if necessary. In general I will not include proofs (because this is no fun in LaTeX).

If you have any corrections, you can write to me at Stud.IP or make a pull request directly at the GitHub repository (which is much more convenient for me than the way via Stud.IP).

glhf,
Alex

1 Number Fields

Example (Pell equation)**:** Let $d > 1$ be an integer, which is not a square, and find all integer solutions to Lecture 1, 24.10.2023

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

Write $\mathbb{Z}[\sqrt{d}] = \{a + \sqrt{d}b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}[\sqrt{d}]$ with its natural ring structure. If $(x, y) \in \mathbb{Z}^2$ is a solution to (1.1), then

$$(x + \sqrt{d}y)(x - \sqrt{d}y) = x^2 - dy^2 = 1$$

and for every $k \in \mathbb{N}$

$$(x + \sqrt{d}y)^k(x - \sqrt{d}y)^k = x_k^2 - dy_k^2 = 1,$$

with $x_k, y_k \in \mathbb{Z}$. I.e. if $(x, y) \neq (\pm 1, 0)$ we can generate new solutions as above. Define the norm map $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z},\ a + \sqrt{d}b \mapsto a^2 - db^2$. Then solutions to (1.1) can be described as units $x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]^*$ in the ring $\mathbb{Z}[\sqrt{d}]$ with $N(x + \sqrt{d}y) = 1$.

Example (Gaussian integers)**:** The question is to find all primes p which can be written as a sum of two integer squares

$$p = a^2 + b^2.$$

I.e. we ask for primes p which factor as $p = (a + ib)(a - ib)$ in the ring $\mathbb{Z}[i]$.

1.1 Number fields and number rings, first definitions and examples

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

Example: a) For $d \in \mathbb{Z}$, where d is not a square, the fields $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[x]/(x^2 - d)$ are number fields (with degree 2 over $\mathbb{Q}$). We call $\mathbb{Q}[\sqrt{d}]$ a *real quadratic field* if $d > 0$ and an *imaginary quadratic field* if $d < 0$.

b) $\mathbb{Q}[\sqrt{d_1}, \sqrt{d_2}]$ are number fields for $d_1, d_2 \in \mathbb{Z}$, usually called *biquadratic fields*.

c) Let $m \in \mathbb{N}$ and $\omega = e^{\frac{2\pi i}{m}}$. Then $\mathbb{Q}[\omega]$ is a number field, called the *m-th cyclotomic field*.

?) What could be an analogue of the integers in a general number field?

$$Z \subset \mathbb{Q} \qquad ? \subset \mathbb{Q}[\sqrt{d}] \qquad ? \subset \mathbb{F}$$

Definition (Algebraic integer)
A complex number $\alpha \in \mathbb{C}$ is called an *algebraic integer*, if there is a monic polynomial $P(x) \in \mathbb{Z}[x]$ with $P(\alpha) = 0$.

Example:

- Every $n \in \mathbb{Z}$ is an algebraic integer.
- $\sqrt{d}$ for $d \in \mathbb{Z}$ is an algebraic integer (take $P(x) = x^2 - d$).
- $e^{\frac{2\pi i}{m}}$ is an algebraic integer for every $m \in \mathbb{N}$ (take $P(x) = x^m - 1$).

Theorem 1.1
Let α be an algebraic integer and $f(x) \in \mathbb{Z}[x]$ a monic polynomial with $f(x) = 0$. If $f(x)$ is of minimal degree with these properties, then f is irreducible.

Remark: Theorem 1.1 shows, that the minimal polynomial of an algebraic integer over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Lemma 1.2
Let $f \in \mathbb{Z}[x]$ be a monic polynomial and $g, k \in \mathbb{Q}[x]$ monic polynomials with $f = gh$. Then, $g, k \in \mathbb{Z}[x]$.

Corollary 1.3
If $\alpha \in \mathbb{Q}$ is an algebraic integer, then $\alpha \in \mathbb{Z}$.

Theorem 1.4 (Characterization of algebraic integers)
Let $\alpha \in \mathbb{C}$. Then the following statements are equivalent:

(i) α is an algebraic integer.

(ii) $\mathbb{Z}[\alpha]$ *is a finitely generated group (under addition).*

(iii) There exists a subring $R \subset \mathbb{C}$ *with* $\alpha \in R$ *and such that* $(R, +)$ *is a finitely generated group.*

(iv) There is a non-trivial finitely generated subgroup $(A, +)$ *of* $\mathbb{C}$*, such that* $\alpha A \subseteq A$.

Corollary 1.5
The set of algebraic integers in $\mathbb{C}$ *is a ring.*

Lecture 2, 27.10.2023

Definition (Ring of algebraic integers)
Let K be a number field. Then we write $\mathcal{O}_K$ for the set of algebraic integers contained in K and we call $\mathcal{O}_K$ the ring of integers of K.

Example: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

Proposition 1.6
Let $d \in \mathbb{Z}$ *be a squarefree integer.*

- *If* $d \equiv 2, 3 \bmod 4$ *then* $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \left\{ a + \sqrt{d}b \,\middle|\, a, b \in \mathbb{Z} \right\}$.
- *If* $d \equiv 1 \bmod 4$*, then* $\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \left\{ \frac{a+\sqrt{d}b}{2} \,\middle|\, a \equiv b \bmod 2 \right\}$.

1.2 Embeddings, Norm and Trace

Recall: Let L/K be a finite field extension. If $char K = 0$, then L/K is separable. Let $\bar{K}$ be an algebraic closure of K. If L/K is seperable, them $[L : K] = \# \operatorname{Hom}_K(L, \bar{K})$.

Theorem
Let L/K *be a finite separable field extension. Then there exists an element* $\alpha \in L$ *such that* $L = K(\alpha)$*. In particular, for number fields* $Q \subseteq K \subseteq L$ *we obtain the following:*

- *There exists* $\alpha \in L$ *such that* $L = K(\alpha)$
- *If there is an embedding* $\hat{\imath} : K \hookrightarrow \mathbb{C}$*, then there exist* $[L : K]$ *embeddings* $L \hookrightarrow \mathbb{C}$*, which extend* $\hat{\imath}$*. If* $g(x)$ *is a minimal polynomial of* α *over* K *then the embeddings are given by* $\sigma_i : \alpha \mapsto \beta_i$*, where* $\beta_1, \ldots, \beta_{[L:K]}$ *are the* $[L : K]$ *distinct conjugates of* α.

Example: 1. Let $d \in \mathbb{Z}$ be not a square. Then there are exactly two embeddings of $\mathbb{Q}[\sqrt{d}]$ into $\mathbb{C}$, namely $\sigma_1 : a + \sqrt{d}b \mapsto a + \sqrt{d}b$ and $\sigma_2 : a + \sqrt{d}b \mapsto a - \sqrt{d}b$.

2. We have $[\mathbb{Q}[\sqrt[3]{2} : \mathbb{Q}]] = 3$ and the three embeddings are given by

$$\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2},\ \sigma_2(\sqrt[3]{2}) = e^{\frac{2\pi i}{3}} \sqrt[3]{2},\ \sigma_3(\sqrt[3]{2}) = e^{\frac{4\pi i}{3}} \sqrt[3]{2}.$$

Note that $\sigma_1(\mathbb{Q}[\sqrt[3]{2}]) \subseteq \mathbb{R}$, whereas σ_2 and σ_3 are "complex embeddings". $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is not a normal extension.

Definition (Trace and norm)
Let K be a field and V an n-dimensional K-vector space. For $\varphi : V \to V$ a K-endomorphism, we define the characteristic polynomial

$$\chi_\varphi(x) = \det(xI_n - \varphi) = \sum_{i=0}^{n} c_i x^{n-i}$$

for some $c_0, \ldots, c_n \in K$. We define the determinant and trace of φ by $\det \varphi = (-1)^n c_n$ and $\operatorname{trace} \varphi = -c_1$

Note that if $\varphi, \psi : V \to V$ are both K-endomorphisms of V, then $\det(\varphi \circ \psi) = \det(\varphi) \det(\psi)$ and $\operatorname{trace}(a\varphi + b\psi) = a \operatorname{trace}(\varphi) + b \operatorname{trace}(\psi)\ \forall\, a, b \in K$.

Definition
Let $\mathbb{Q} \subseteq K \subseteq L$ be number fields and $\alpha \in L$. We write $\varphi_\alpha : L \to L,\ x \mapsto \alpha x$ and define the (relative) norm and trace of α by

$$N_{L/K}(\alpha) = \det \varphi_\alpha, \quad \operatorname{Tr}_{L/K}(\alpha) = \operatorname{trace}(\varphi_\alpha).$$

Remark: The map $N_{L/K} : L^* \to K^*$ is a grouphomomorphism as $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)\ \forall\, \alpha, \beta \in L \setminus \{0\}$. Similarly, $\operatorname{Tr}_{L/K} : L \to K$ is a K-linear map, as

$$\operatorname{Tr}_{L/K}(u\alpha + v\beta) = u \operatorname{Tr}_{L/K}(\alpha) + v \operatorname{Tr}_{L/K}(\beta)\ \forall\, u, v \in K,\ \alpha, \beta \in L.$$

Example: Let $K = \mathbb{Q},\ L = \mathbb{Q}(i)$ and $\alpha = a + ib \in \mathbb{Q}(i)$. Then φ_α can be represented with respect to the basis $1,\ i$ by

$$\varphi_\alpha = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

and hence

$$N_{L/\mathbb{Q}}(a+ib) = a^2 + b^2, \quad \mathrm{Tr}_{L/\mathbb{Q}}(a+ib) = 2a.$$

Lemma 1.7
Let L/K is an extension of number fields with $[L:K]=n$. For $a \in K$ we have

$$N_{L/K}(a) = a^n, \quad \mathrm{Tr}_{L/K} = na.$$

Lemma 1.8
Let L/K be an extension of number fields with $L = K(\alpha)$ and $[L:K]=n$. Let $f(x) = x^n + c_1 x^{n-1} + \cdots + c_n$ be the minimal polynomial of α over K. Then

$$N_{L/K}(\alpha) = (-1)^n c_n, \quad \mathrm{Tr}_{L/K}(\alpha) = -c_1.$$

Lemma 1.9
Let L/K be a number field extension, $\alpha \in L$, $[L:K(\alpha)] = r$. Then we have

$$N_{L/K}(\alpha) = \left(N_{K(\alpha/K)}(\alpha)\right)^r, \quad \mathrm{Tr}_{L/K}(\alpha) = r\,\mathrm{Tr}_{K(\alpha)/K}(\alpha).$$

Corollary 1.10
Let L/K be number fields and $\alpha \in \mathcal{O}_L$. Then $N_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$. In particular $N_{L/\mathbb{Q}}(\alpha), \mathrm{Tr}_{L/\mathbb{Q}} \in \mathbb{Z}$.

Theorem 1.11
Let L/K be number fields, $[L:K]=n$ and $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \mathbb{C}$ be the n distinct K-linear embeddings of L into $\mathbb{C}$. Then, for $\alpha \in L$, we have

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Corollary 1.12
Let L/K be a Galois extension of number fields. Then, for $\alpha \in L$ and $\sigma \in \mathrm{Gal}(L/K)$, we have

$$N_{L/K}(\sigma(\alpha)) = N_{L/K}(\alpha), \quad \mathrm{Tr}_{L/K}(\sigma(\alpha)) = \mathrm{Tr}_{L/K}(\alpha).$$

Theorem 1.13
Let $K \subseteq L \subseteq M$ be a tower of number fields and $\alpha \in M$. Then

$$N_{M/K} = N_{L/K}(N_{M/L}(\alpha)), \quad \mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)).$$

Lecture 3, 03.11.2023

An application of the norm map

Given a number field K with ring of integers $\mathcal{O}_K$, how can we find $\mathcal{O}_K^*$, i.e. the units in $\mathcal{O}_K$?

- If $\alpha \in \mathcal{O}_K^*$, $\alpha^{-1} \in \mathcal{O}_K$ and $1 = N_{K/\mathbb{Q}}(\alpha\alpha^{-1}) = N_{K/\mathbb{Q}}(\alpha) \cdot N_{K/\mathbb{Q}}(\alpha^{-1})$. By Corollary 1.10, $N_{K/\mathbb{Q}}(\alpha),\ N_{K/\mathbb{Q}}(\alpha^{-1}) \in \mathbb{Z} \implies N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

- If $\alpha \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, then $\alpha \in \mathcal{O}_K^*$.

Example: Let $d \in \mathbb{Z}$, d squarefree. Then, for $a, b \in \mathbb{Q}$, $N_{\mathbb{Q}[\sqrt{d}]/\mathbb{Q}}(a + \sqrt{d}b) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$. For $d \equiv 2, 3 \bmod 4$, we find that

$$\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \left\{ a + b\sqrt{d} \,\middle|\, a, b \in \mathbb{Z},\ a^2 - db^2 = \pm 1 \right\}.$$

The trace as a bilinear form

Let L/K be number fields. Then $\mathrm{Tr}_{L/K}$ induces a bilinear form

$$\mathrm{Tr}_{L/K} : L \times L \to K,\ (x, y) \mapsto \mathrm{Tr}_{L/K}(x \cdot y). \tag{1.2}$$

Write L^* for the dual vector space of L, i.e. the set of all K-linear vector space homomorphisms.

Theorem 1.14
The bilinear form (1.2) induces an isomorphism of K-vector spaces

$$\psi : L \to L^*,\ x \to \mathrm{Tr}_{L/K}(x, \cdot).$$

Corollary 1.15
Let L/K be number fields and $(v_1, \ldots, v_n)$ a K-basis with $n = [L : K]$. Then there exists a unique K-basis $(w_1, \ldots, w_n)$ of L, such that $\mathrm{Tr}_{L/K}(v_i w_j) = \delta_{ij},\ 1 \leq i, j, \leq n$.

1.3 Discriminant

Let $K/\mathbb{Q}$ be a number field of degree $n = [K : \mathbb{Q}]$ and $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ its embeddings.

Definition (Discriminant)
For $\alpha_1, \ldots, \alpha_n \in K$, we define the *discriminant* as

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det\Big((\sigma_i(\alpha_j))_{1\le i,j\le n}\Big)^2.$$

Theorem 1.16
Let $\alpha_1, \ldots, \alpha_n \in K$. Then $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent if and only if $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Lemma 1.17
Let $\alpha_1, \ldots, \alpha_n \in K$. Then

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det\Big(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\Big)_{1\le i,j\le n}.$$

Corollary 1.18
Let $\alpha_1, \ldots, \alpha_n \in K$. Then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. *If moreover $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then* $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Theorem 1.19
Let α be algebraic over $\mathbb{Q}$ with $\Big[\mathbb{Q}[\alpha] : \mathbb{Q}\Big] = n$, and $\alpha_1, \ldots, \alpha_n$ the n different conjugates of α. Then

$$\operatorname{disc}\Big(1, \alpha, \ldots, \alpha^{n-1}\Big) = \prod_{1\le i,j\le n} (a_i - a_j)^2.$$

If moreover $f(x)$ is the minimal polynomial of α over $\mathbb{Q}$, then

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

Question: Let K be a number field with ring of integers $\mathcal{O}_K$ and of degree $n = [K : \mathbb{Q}]$. Then K is an n-dimensional $\mathbb{Q}$-vector space. Hpw can we describe the structure of the group $(\mathcal{O}_K, +)$?

Example: For $d \in \mathbb{Z}$ squarefree and $K = \mathbb{Q}\left[\sqrt{d}\right]$, the ring of integers $\mathcal{O}_K$ is a free abelian group of rank 2, where a $\mathbb{Z}$-basis is given by $(1,\ \omega)$, with

$$\omega = \begin{cases} \sqrt{d} & d \equiv 2, 3 \bmod 4, \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \bmod 4. \end{cases}$$

Theorem 1.20
Let $K/\mathbb{Q}$ be a number field of degree $n = [K : \mathbb{Q}]$. Then $\mathcal{O}_K$ is a free abelian group of rank n, i.e. there exists $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, such that every $\beta \in \mathcal{O}_K$ can be uniquely written in the form

$$\beta = m_1\alpha_1 + \cdots + m_n\alpha_n$$

with $m_1, \dots, m_n \in \mathbb{Z}$.

Remark: In the notation of Theorem 1.20, we call $(\alpha_1, \dots, \alpha_n)$ and integral basis of $\mathcal{O}_K$ (over $\mathbb{Z}$).

Lecture 4, 07.11.2023

Lemma 1.21
Let K be a number field as above. Then there exists a $\mathbb{Q}$-basis of the number field, say $(\alpha_1, \dots, \alpha_n)$, with $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$.

Proposition 1.22
Let $(\alpha_1, \dots, \alpha_n)$ be a $\mathbb{Q}$-basis of a number field K with $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, $d = \mathrm{disc}(\alpha_1, \dots, \alpha_n)$ and $\beta \in \mathcal{O}_K$. Then there exist $m_1, \dots, m_n \in \mathbb{Z}$, such that

$$\beta = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

and $d \mid m_i^2$ for $1 \le i \le n$.

Lemma 1.23
Let K be a number field with integral bases $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$. Then

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = \mathrm{disc}(\beta_1, \dots, \beta_n).$$

Definition (Discriminant of K)
Let K be a number field and $(\alpha_1, \dots, \alpha_n)$ a $\mathbb{Z}$-basis for $\mathcal{O}_K$. We define the *discriminant*

disc(K) of K as

$$\operatorname{disc}(K) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

Example: Let $d \in \mathbb{Z}$ be squarefree. Then

$$\operatorname{disc}\left(\left[\sqrt{d}\right]\right) = \begin{cases} 4d & d \equiv 2,3 \mod 4, \\ d & d \equiv 1 \mod 4. \end{cases}$$

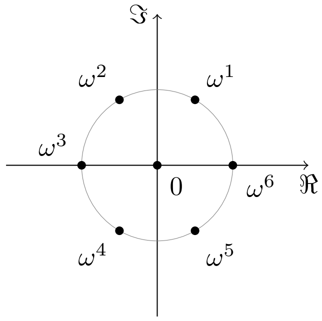
1.4 Cyclotomic fields

Definition
For $m \in \mathbb{N}$ we call $\mathbb{Q}\left[e^{\frac{2\pi i}{m}}\right]$ the m-th cyclotomic field.

Example:

- The first two cyclotomic fields are equal to $\mathbb{Q}$.
- Let $m = 6$ and write $\omega = e^{\frac{2\pi i}{6}}$. Then $\omega^5 = -\omega^2$, i.e. $\omega = -\omega^4$ and $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^2]$. This means that the third and sixth cyclotomic fields are equal.

In the following let $m \in \mathbb{N}$ and write $\omega = e^{\frac{2\pi i}{m}}$.



Theorem 1.24
The extension $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is Galois with degree equal to $\varphi(m)$, where φ is Euler's totient function. Moreover, the Galois group is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^* = \{k \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(k, m) = 1\}$.

For $k \in (\mathbb{Z}/m\mathbb{Z})^*$ the corresponding automorphism is given by $\omega \mapsto \omega^k$.

Proposition 1.25
The conjugates of ω are exactly given by ω^k with $\gcd(m, k) = 1$.

Corollary 1.26
Let $m \in \mathbb{N}$ be even. Then the roots of unity contained in $\mathbb{Q}(e^{\frac{2\pi i}{m}})$ are exactly the m-th roots of unity.

Corollary 1.27
The m-th cyclotomic fields, for m even, are all non-isomorphic.

Theorem 1.28
Let $m = p^r$ for some prime p and $\omega = e^{\frac{2\pi i}{m}}$. Then $\mathcal{O}_{Q[\omega]} = \mathbb{Z}[\omega]$.

Remark: More generally, $Z[\omega] = \mathcal{O}_{Q[\omega]}$ for *every* cyclotomic field.

Notation: We write $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \dots, \alpha^{n-1})$.

Lemma 1.29
For $m \in \mathbb{N}$ we have $\operatorname{disc}(\omega) \mid m^{\varphi(m)}$.

Lecture 5, 10.11.2023

Lemma 1.30
For $m \geq 3$ we have $\operatorname{disc}(1-\omega) = \operatorname{disc}(\omega)$.

Lemma 1.31
Let $m = p^r$ be a prime power, $r \in \mathbb{N}$. Then

$$\prod_{\substack{1 \leq k \leq m \\ \gcd(k,m)=1}} \left(1 - \omega^k\right) = p.$$

Remark: In particular for $m = p^r$ we have $\frac{p}{(1-\omega)^{\varphi(m)}} \in \mathbb{Z}[\omega]$.

2 Prime ideal factorisation

2.1 Unique prime ideal factorisation

Motivation: If K is a number field with ring of integers $\mathcal{O}_K$, then we may not have a unique factorisation in $\mathcal{O}_K$ into irreducible elements (up to units and ordering).

Example: Let $K = \mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In $\mathbb{Z}[\sqrt{-5}]$ we have $2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, where 2 and 3 are irreducible elements.

Our next goal is to replace factorisation into irreducible elements by prime *ideal* factorisation. Instead of number fields, we consider more generally *Dedekind domains*.

Definition (Integrally closed ring)
Let R be an integral domain and $K = \left\{ \frac{a}{b} \,\middle|\, a, b \in R,\ b \neq 0 \right\}$ its field on fractions. We call R *integrally closed*, if every element $\frac{a}{b} \in K$, which is a zero of a monic polynomial with coefficients in R is contained in R.

Example: Let K be a number field with ring of integers $\mathcal{O}_K$. Then $\mathcal{O}_K$ is integrally closed. Indeed let $\alpha \in K$ satisfy $\alpha^n + b_1\alpha^{n-1} + \cdots + b_n = 0$, with $b_1, \ldots, b_n \in \mathcal{O}_K$. Then $\mathbb{Z}[\alpha, b_1, \ldots, b_n]$ is finitely generated as an additive group and we have $\alpha \in \mathcal{O}_K$.

Definition (Noetherian ring)
We call a commutative ring R *noetherian* if every ideal is finitely generated.

Remark: The following statements about a commutative ring R are equivalent:

1. R is noetherian.
2. Every increasing sequence of ideals is eventually constant, i.e. if $I_1 \subseteq I_2 \subseteq \ldots$, then there is some $n_0 \in \mathbb{N}$, such that $I_n = I_{n_0}$ for every $n > n_0$.
3. Every non-empty set S of ideals has a maximal element, i.e. there is some $M \in S$, such that if $M' \in S$ with $M \subseteq M'$, then $M = M'$.

Example: Principal ideal domains and polynomial rings $\mathbb{Z}[x_1, \ldots, x_n]$ or $K[x_1, \ldots, x_n]$ for any field K are noetherian.

Definition (Dedekind domain)
A *Dedekind domain* is a noetherian integrally closed domain, in which every non-zero prime ideal is maximal.

Theorem 2.1
Let K be a number field. Then its ring of integers $\mathcal{O}_K$ is a Dedekind domain.

Example: Coordinate rings of irreducible smooth curves over an algebraically closed field, e.g. $\mathbb{C}[T]$ is a Dedekind domain.

First properties of Dedekind domains

Lemma 2.2
Let R be a Dedekind domain, which is not a field, and $0 \neq I \subseteq R$ an ideal. Then I contains a product of non-zero prime ideals $P_1 \cdots P_k \subseteq I$.

Lemma 2.3
Let R be a Dedekind domain with field of fractions K and $0 \neq I \subsetneq R$ a ideal. Then there exists $\alpha \in K \setminus R$ with $\alpha I \subseteq R$.

Lecture 6, 17.11.2023

Theorem 2.4
Let R be a Dedekind domain and $0 \neq I \subseteq R$ an ideal. Then there is an ideal $0 \neq J \subseteq R$, such that IJ is principal.

Example: Let $R = \mathbb{Z}\left[\sqrt{-5}\right]$ and $I = \left(2, 1+\sqrt{-5}\right)$. Then I is not principal, but $\left(2, 1+\sqrt{-5}\right)\left(2, 1-\sqrt{-5}\right) = (2)$ is principal.

Observation: Note that $\alpha \in I$ implies that $J \subset A = \frac{1}{\alpha} IJ$. Hence $\gamma JI = \gamma\alpha\left(\frac{1}{\alpha} JI\right) = \alpha\gamma A \subseteq (\alpha)$. As $\gamma J \subseteq \gamma A \subseteq R$, we find that $\gamma J \subseteq J$.

The ideal class group

Definition (Equivalence of ideals)
Let R be an integral domain. We say that two non-zero ideals I, J are equivalent if and only if there exist $\alpha, \beta \in R \setminus \{0\}$ with $\alpha I = \beta J$.

Remark:
1. This really is an equivalence relation. We call the equivalence classes under this relation *ideal classes*.
2. We can define a multiplication on the set of ideal classes by multiplication of representatives, $[I][J] = [IJ]$, with the neutral element $[R]$.
3. All principal ideals form one ideal class.

Corollary 2.5
Let R be a Dedekind domain. Then the ideal classes form a group under multiplication.

Definition (Ideal class group)
We call the group given by ideal classes under multiplication in the Dedekind domain R the *ideal class group* of R, denoted by $Cl(R)$.

Example: $\mathbb{Z}$ is a principal ideal domain, hence $|Cl(\mathbb{Z})| = 1$.

Remark: There are only finitely many imaginary quadratic fields K with $|Cl(\mathcal{O}_K)| = 1$.

Question (Gauss)**:** Do there exist as many real quadratic number fields K with $|Cl(\mathcal{O}_K)| = 1$?

Corollary 2.6
Let R be a Dedekind domain and A, B, C ideals with $A \neq 0$.

1. *If $AB = AC$ then $B = C$.*
2. *We have $B \mid A$, i.e. $A = BJ$ for some ideal J, if and only if $A \subseteq B$.*

Theorem 2.7 (Unique prime ideal factorisation)
Every ideal $I \neq 0$ in a Dedekind domain R can be written as a product $I = P_1 \cdots P_r$

with non-zero prime ideals $P_1, \ldots, P_r$ and this representation is unique up to ordering of $P_1, \ldots, P_r$.

Example: In $\mathbb{Z}\left(\sqrt{-5}\right)$ we don't have unique factorisation into reducible elements, e.g. $2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$, but in terms of ideals we have $(2) = \left(2, 1+\sqrt{-5}\right)^2 = P_1^2$, $(3) = \left(3, 1+\sqrt{-5}\right)\left(3, 1-\sqrt{-5}\right) = P_2 \cdot P_3$. Note that P_1, P_2, P_3 are all prime ideals as $\left|\mathbb{Z}\left[\sqrt{-5}\right]/P_i\right| \in \{2, 3\}$ for $1 \leq i \leq 3$. In the ideal class group we find that

$$\begin{aligned}(2) \cdot (3) &= P_1^2 P_2 P_3 \\ &= P_1 P_2 P_1 P_3 \\ &= \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right).\end{aligned}$$

Definition (Greatest common divisor, least common multiple)
Let R be a Dedekind domain and $I, J \neq 0$ ideals with prime factorisation

$$I = \prod_{i=1}^{r} P_1^{a_i}, \ J = \prod_{i=1}^{r} P_i^{b_i},$$

where $P_1, \ldots, P_r$ are distinct prime ideals and $a_1, \ldots, a_r, b_1, \ldots, b_r \in \mathbb{Z}_{\geq 0}$. We define the *greatest common divisor* $\gcd(I, J)$ and *least common multiple* $\operatorname{lcm}(I, J)$ by

$$\gcd(I, J) = \prod_{i=1}^{r} P_i^{\min(a_i, b_i)}, \quad \operatorname{lcm}(I, J) = \prod_{i=1}^{r} P_i^{\max(a_i, b_i)}.$$

Exercise
Show that

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

Question: Given the ring of integers $\mathcal{O}_K$ in a number field K, we know that every ideal is finitely generated. Can we say something about the numbers of generators we need? E.g. in $\mathbb{Z}[\sqrt{-5}]$, the prime ideal $(2, 1+\sqrt{-5})$ is not a principal idea, but generated by two elements.

Lecture 7, 21.11.2023

Remark: Chinese Remainder Theorem: Let R be a commutatiove ring with 1 and

$a_1, \dots, a_n$ coprime ideals, i.e. $a_i + a_j = R \; \forall\, i \neq j$. Then there is an isomorphism

$$R / \bigcap_{i=1}^{n} a_i \to R/a_1 \times \cdots \times R/a_n.$$

Theorem 2.8
Let R be a Dedekind domain, $I \subseteq R$ a non-zero ideal and $\alpha \in I \setminus \{0\}$. Then there exists $\beta \in I$ with $I = (\alpha, \beta)$.

Corollary 2.9
A Dedekind domain is a unique factorisation domain (UFD) if and only if is is a principal ideal domain (PID).

Remark: In general, a PID is a UFD but the reverse implication does not hold. For example $\mathbb{Z}[x]$ is a UFD, but not a PID.

2.2 Splitting of primes

Let p be a (rational) prime number. Then (p) is a prime ideal in $\mathbb{Z}$, but the ideal $(p) = p\mathcal{O}_K$ need not be a prime ideal in $\mathcal{O}_K$. For example, let $p \equiv 1 \bmod 4$, then in $\mathbb{Z}[i]$ we have

$$(p) = (a + ib)(a - ib), \tag{2.1}$$

where $a^2 + b^2 = p$ with $a, b \in \mathbb{Z}$. Note that $N_{\mathbb{Q}[i]/\mathbb{Q}}(a + ib) = p$ and hence $a + ib$ is a prime element in the PID $\mathbb{Z}[i]$, and (2.1) is the prime ideal factorisation of (p). Moreover, $a + ib$ and $a - ib$ do not differ by multiplication with one of the units $\pm 1, \pm i$, and hence

$$P_1 = (a + ib) \neq (a - ib) = P_2$$

in $\mathbb{Z}[i]$. The ideal (2) splits in $\mathbb{Z}[i]$ as $2 = (1 + i)^2$, where $(1 + i)$ is a prime ideal. If $p \equiv 3 \bmod 4$ is a rational prime, then (p) remains a prime ideal in $\mathbb{Z}[i]$. (check!)

Question: More generally, let $K \subseteq L$ be number fields with rings of integers $\mathcal{O}_K, \mathcal{O}_L$. Given a non-zero prime ideal P in $\mathcal{O}_K$, how does $P\mathcal{O}_L$ split into prime ideals in $\mathcal{O}_L$?

Notation: In the following, we keep the notation $K \subseteq L,\ \mathcal{O}_K \subseteq \mathcal{O}_L$ as above.

Definition (Primes)
We say that $P \subseteq \mathcal{O}_K$ or $Q \subseteq \mathcal{O}_L$ is a *prime* if P or respectively Q is a non-zero

prime ideal in $\mathcal{O}_K$ or respectively $\mathcal{O}_L$. Moreover, we say that Q *lies above* P or P *lies under* Q if $Q \mid P\mathcal{O}_L$.

Lemma 2.10
Let P resp. Q be primes in $\mathcal{O}_K$ resp. $\mathcal{O}_L$. Then Q lies above P if and only if one of the following equivalent conditions holds:

1. $P\mathcal{O}_L \subseteq Q$.
2. $P \subseteq Q$.
3. $Q \cap \mathcal{O}_K = P$.
4. $Q \cap K = P$.

Theorem 2.11
Every prime Q in $\mathcal{O}_L$ lies above a unique prime P in $\mathcal{O}_K$ and for every prime P in $\mathcal{O}_K$ there is some prime Q in $\mathcal{O}_L$, which lies above P.

Lemma 2.12
Let Q be a prime in $\mathcal{O}_L$ lying above P in $\mathcal{O}_K$. Then $\mathcal{O}_L/Q$ and $\mathcal{O}_K/P$ are finite fields with $\mathcal{O}_K/P \hookrightarrow \mathcal{O}_L/Q$.

Let P be a prime in $\mathcal{O}_K$ and consider in $\mathcal{O}_L$ the prime ideal factorisation

$$P\mathcal{O}_L = \prod_{i=1}^{r} Q_i^{e_i}$$

with distinct primes $Q_1, \ldots, Q_r$.

Definition
We call

$$e_1 = e(Q_i \mid P)$$

the *ramification index* of Q_i above P and

$$f_i = f(Q_i \mid P) = \left[\mathcal{O}_L/Q_i : \mathcal{O}_K/P\right]$$

the *inertia degree* of Q_i over P. Moreover, we call $\mathcal{O}_L/Q_i$ and $\mathcal{O}_K/P$ *residue fields* of Q_i or respectively P.

Remark: Let $K \subseteq L \subseteq M$ be number fields with primes $P \subseteq Q \subseteq R$. Then

$$e(R \mid P) = e(R \mid Q)e(Q \mid P), \quad f(R \mid P) = f(R \mid Q)f(Q \mid P).$$

Example: Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$. If p is a rational prime with $p \equiv 1 \bmod 4$, then $(p) = P_1 \cdot P_2$, $P_1 = (a + ib)$, $P_2 = (a - ib)$ for some $a, b \in \mathbb{Z}$. We have

$$e\Big(P_i \mid (p)\Big) = 1, \quad f\Big(P_i \mid (p)\Big) = 1.$$

For a rational prime $p \equiv 3 \bmod 4$ we obtain

$$e\Big(\underbrace{(p)}_{\subseteq \mathbb{Z}[i]} \mid \underbrace{(p)}_{\subseteq \mathbb{Z}}\Big) = 1, \quad f\Big((p) \mid (p)\Big) = 2.$$

For $p = 2$ note that $(2) = (1+i)^2$ and $\Big|\mathbb{Z}[i] \mid (1+i)\Big| = 2$, hence

$$e\Big((1+i) \mid (2)\Big) = 2, \quad f\Big((1+i) \mid (2)\Big) = 1.$$

In this example, independent of the rational prime p we find that

$$\sum_{i=1}^{r} e_i f_i = \Big[\mathbb{Q}(i) : \mathbb{Q}\Big].$$

Our goal now is to show the above statement for number fields $K \subseteq L$.

Definitions