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[1] 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 $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[x]/(x^2 - d)$

[1]after John Pell (1611 - 1685), an English mathematician

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

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

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, $\mathrm{Tr}_{L/K} : L \to K$ is a K-linear map, as

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

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 $f(x) = x^n + c_1x^{n-1} + \cdots + c_n$ 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. How 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 $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$, $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$ 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

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

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.

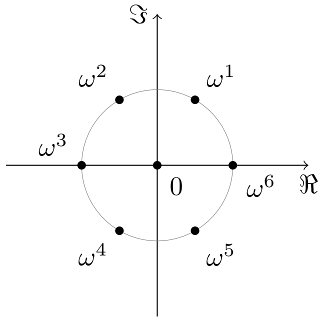
Example:

- 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[1] 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 $M = M'$.

[1] after Emmy Noether (1882 - 1935), a German mathematician

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[2] 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 $\gamma J \subseteq J$.

[2] after Richard Dedekind (1831 - 1916), a German mathematician

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 $P_1, \dots, P_r$ and this representation is unique up to ordering of $P_1, \dots, P_r$.

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 $1 \le i \le 3$. 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 $P_1, \dots, P_r$ are distinct prime ideals and $a_1, \dots, a_r, b_1, \dots, b_r \in \mathbb{Z}_{\ge 0}$. 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 (Ramification index, inertia degree)
We call

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

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 $K \subseteq L$. Lecture 8, 24.11.2023

Norms of ideals

Definition (Norm of an ideal)
Let K be a number field and $I \subseteq \mathcal{O}_K$ a non-zero ideal. Then we define the *norm* $N(I)$ of the ideal I as

$$N(I) := \Big|\mathcal{O}_K / I\Big|.$$

Lemma 2.13
Let $I, J \subseteq \mathcal{O}_K$ be non-zero ideals. Then

$$N(IJ) = N(I)N(J).$$

Proposition 2.14
Let K be a number field of degree $n = [K : \mathbb{Q}]$ and $p \in \mathbb{Z}$ a prime with prime ideal

factorisation

$$(p) = \prod_{i=1}^{r} P_i^{e_i}$$

in $\mathcal{O}_K$ *and* $f_i = f(P_i \mid p)$ *for* $1 \le i \le r$. *Then*

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

Next, we will look at general number field extensions $L \subseteq K$. We start with some preparations:

Lemma 2.15
Let $0 \neq B \subseteq A \subsetneq R$ *be ideals in a Dedekind domain* R. *Then there exists* $\alpha \in K = Quot(R)$, *such that*

$$\alpha B \subseteq R, \text{ but } \alpha B \subsetneq A.$$

Lemma 2.16
Let $I \neq 0$ *be an ideal in* $\mathcal{O}_K$ *and* $n = [L : K]$. *Then*

$$N(I\mathcal{O}_L) = N(I)^n.$$

Example: For $K = \mathbb{Q}$ we have already used this identity above, in which case it reduces to

$$N\big((p)\big) = p^n,$$

with $(p) \subseteq \mathcal{O}_L$ and p a rational prime.

Theorem 2.17
Let P *be a prime in* $\mathcal{O}_K$ *and* $P\mathcal{O}_L = \prod_{i=1}^{r} Q_i^{e_i}$ *the prime ideal factorisation in* $\mathcal{O}_L$ *with distinct ideals* $Q_1, \ldots, Q_r$ *and inertia degrees* $f_i = f(Q_i \mid P)$. *Then*

$$[L : K] = \sum_{i=1}^{r} e_i f_i.$$

Example: (a) Let p be a rational prime and $\omega = e^{\frac{2\pi i}{p^r}}$ for some $r \in \mathbb{N}$. By Lemma 1.31 we have

$$p = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} \Big(1 - \omega^k\Big).$$

We show on the exercise sheet that for $p \not| k$

$$(1-\omega^k) = u_k(1-\omega)$$

for some $u_k \in \mathbb{Z}[\omega]$. Hence in $\mathbb{Z}[\omega]$ we have

$$(p) = (1-\omega)^{\varphi(p^r)}.$$

By Theorem 2.17, we deduce that $(1-\omega)$ is a prime ideal in $\mathbb{Z}[\omega]$ and

$$f\Big((1-\omega) \mid (p)\Big) = 1$$

(b) Let α be a root of $\alpha^3 = \alpha + 1$. Then $\mathbb{Q}(\alpha)/\mathbb{Q}$ is an extension of degree 3. One can compute $\operatorname{disc}(1, \alpha, \alpha^2) = -23$. As 23 is square-free, we find that $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$ with integral basis $(1, \alpha, \alpha^2)$. Moreover, in $\mathbb{Z}[\alpha]$, we have

$$23 \cdot \mathbb{Z}[\alpha] = (23, \alpha - 10)^2 (23, \alpha - 3), \tag{2.2}$$

where $(23, \alpha - 10)$ and $(23, \alpha - 3)$ are coprime. Hence (2.2) is the prime ideal factorisation of (23) in $\mathbb{Z}[\alpha]$ and

$$f\Big((23, \alpha - 10) \mid 23\Big) = f\Big((23, \alpha - 3) \mid 23\Big) = 1.$$

Remark: In these examples we have found ramification indices $e > 1$, which however is not the "typical" case, as we will see below.

Definition (Ramified prime)
Let P be a prime in $\mathcal{O}_K$. We say that P is *ramified in* $\mathcal{O}_L$, if there is a prime Q in $\mathcal{O}_L$, lying above P, with

$$e(Q \mid P) > 1.$$

Theorem 2.18
Let p be a rational prime (i.e. a prime number in $\mathbb{Z}$), which is ramified in $\mathcal{O}_K$. Then

$$p \mid \operatorname{disc}(\mathcal{O}_K).$$

Remark: One can even show, that $p \mid \operatorname{disc}(\mathcal{O}_K)$ imlies that p is ramified in $\mathcal{O}_K$.

Corollary 2.19
There are only finitely many primes P in $\mathcal{O}_K$ which are ramified in $\mathcal{O}_L$.

Lecture 9, 28.11.2023

Galois extensions

In the proof of Theorem 2.18 we noted that if $L/\mathbb{Q}$ is a Galois extension and Q a prime in $\mathcal{O}_L$ above $p \in \mathbb{Z}$, so is the ideal $\sigma(Q)$ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$.

Theorem 2.20
Let L/K be Galois and Q a prime in $\mathcal{O}_L$ lying above the prime P in $\mathcal{O}_L$. Then $\sigma(Q)$ is a prime above P for every $\sigma \in \mathrm{Gal}(L/K)$. Moreover, if Q' is another prime in $\mathcal{O}_L$ over P, then there exists an automorphism $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(Q) = Q'$.

Example: $K = \mathbb{Q},\ L = \mathbb{Q}(i),\ p \in \mathbb{Z}$ a prime with $p \equiv 1 \bmod 4$. Write $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$. In $\mathbb{Z}[i]$ we have $(p) = (a + ib)(a - ib)$.

Corollary 2.21
Let L/K be a Galois extension, P a prime in $\mathcal{O}_K$ and Q_1, Q_2 primes in $\mathcal{O}_L$ lying above P. Then

$$e(Q_1 \mid P) = e(Q_2 \mid P), \quad f(Q_1 \mid P) = f(Q_2 \mid P).$$

Remark: In the notation above, we hence obtain

$$P\mathcal{O}_L = (Q_1 \cdots Q_r)^e \text{ with } f(Q_i \mid P) = f(Q_j \mid P).$$

Question: Let L/K be any number fields (not necessarily Galois) and P a prime in $\mathcal{O}_K$. Find explicitly the factorisation

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

with $Q_1, \dots, Q_r$ prime.

Example: Let $m \in \mathbb{Z} \setminus \{1\}$ be odd and square-free and let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{m})$. Consider an odd prime $p \in \mathbb{Z}$ with $p \nmid m$. By Theorem 2.18, p is not ramified in $\mathcal{O}_K$ as $\mathrm{disc}(K) \in \{m, 4m\}$. Hence we either have $p\mathcal{O}_L = Q_i Q_2$ with distinct primes

Q_1, Q_2 and $f(Q_i \mid p) = 1$ for $i = 1, 2$, *or* $p\mathcal{O}_L$ is prime with $f(p\mathcal{O}_L \mid p) = 2$.

Let Q be a prime above p. Consider the polynomial $g(X) = X^2 - m$. Then $g(X)$ has a zero in $\mathcal{O}_L$ and hence a zero in $\mathcal{O}_L/Q$.

1. If m is not a square modulo p, then $X^2 - m$ has no zero in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_L/Q$ is a non-trivial field extension, i.e. $f(Q \mid p) = 2$.

2. Let $a \in \mathbb{Z}$ be a solution to $a^2 - m \equiv 0 \bmod p$. Then in $\mathcal{O}_L$ we have the factorisation $(a - \sqrt{m})(a + \sqrt{m}) \in p\mathcal{O}_L$ and in fact
$$(p, a - \sqrt{m})(p, a + \sqrt{m}) = p\mathcal{O}_L. \tag{2.3}$$
As neither of the factors $(p, a - \sqrt{m}), (p, a + \sqrt{m})$ contains 1, and $p\mathcal{O}_L$ factors into a product of at most two primes, we have already found in (2.3) the prime ideal factorisation of $p\mathcal{O}_L$ and
$$f\Big((p, a \pm \sqrt{m}) \mid p\Big) = 1.$$

More generally, let L/K be number fields, say of degree $n = [L : K]$. Fix an element $\alpha \in \mathcal{O}_L$, such that $L = K(\alpha)$. Note, that by Proposition 1.22 the quotient $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ is finite. Let $g(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K.

Theorem 2.22
With notation as above, let P be a prime in $\mathcal{O}_K$ and factor $g(X)$ in $(\mathcal{O}_K/P)[X]$ as
$$g(X) \equiv g_1(X)^{e_1} \cdots g_r(X)^{e_r} \bmod P[X],$$
where $g_1(X), \dots, g_r(X) \in \mathcal{O}_K[X]$ are monic polynomials, pairwise distinct and irreducible in $(\mathcal{O}_K/P)[X]$. Let $(p) \in P \cap \mathbb{Z}$ and assume $p \nmid \Big|\mathcal{O}_L/\mathcal{O}_K[\alpha]\Big|$. Then we have the factorisation
$$P\mathcal{O}_L = \prod_{i=1}^{r} Q_i^{i_i},$$
where $Q_i = (P, g_i(\alpha))$ is a prime and $f(Q_i \mid P) = \deg g_i$ for $1 \le i \le r$.

Example: Let α be a root of $\alpha^3 - \alpha - 1 = 0$. We have from earlier that $\mathcal{O}_{\mathbb{Q}[\alpha]} = \mathbb{Z}[\alpha]$ and $\operatorname{disc}(\mathbb{Q}[\alpha]) = -23$. Modulo 23 we find that Lecture 10, 01.12.2023

$$X^3 - X - 1 \equiv (X - 10)^2(X - 3)$$

and hence by Theorem 2.22

$$23\mathbb{Z}[\alpha] = (23, \alpha - 10)^2(23, \alpha - 3).$$

3 Number fields - Dirichlet's unit theorem, class groups and lattices

3.1 Finiteness of the ideal class group

Let K be a number field with ring of integers $\mathcal{O}_K$. We will keep this notation throughout this chapter.

Recall: We call two non-zero ideals $I, J \subseteq \mathcal{O}_K$ equivalent, if $\exists\, \alpha, \beta \in \mathcal{O}_K \setminus \{0\}$, such that $\alpha I = \beta J$, and we write $Cl(\mathcal{O}_K)$ for the group of equivalence classes under multiplication.

Question: Is $Cl(\mathcal{O}_K)$ finite?

Theorem 3.1
For every number field K there is a constant C_K, such that every non-zero ideal I contains an element $\alpha \in I \setminus \{0\}$ with

$$\left|N_{K/\mathbb{Q}}(\alpha)\right| \leq C_K N(I).$$

Corollary 3.2
Let K and C_K be as in Theorem 3.1. Then every ideal class $C \in Cl(\mathcal{O}_K)$ contains an ideal I with $N(I) \leq C_K$.

Corollary 3.3
For every number field K we have $|Cl(\mathcal{O}_K)| < \infty$.

Example: Let $K = \mathbb{Q}[\sqrt{2}]$, i.e. $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. As in the proof of Theorem 3.1, we can take $C_K = (1+\sqrt{2})^2$ (using the integral basis $(1, \sqrt{2})$). Note that $(1+\sqrt{2})^2 < 6$. We consider the prime ideals in $\mathbb{Z}[\sqrt{2}]$, which lie above 2, 3, 5. Note that $2\mathbb{Z}[\sqrt{2}] = (\sqrt{2})^2$ and that (3), (5) are prime ideals (see Theorem 2.22, noting that $X^2 - 2$ remains irreducible modulo 3, 5). Hence $\left|Cl(\mathbb{Z}[\sqrt{2}])\right| = 1$.

Remark: In the example above and other examples, we would like to take C_K as small as possible.

Our next goal will be to find improvements for the value of C_K using results from the geometry of numbers.

Idea: Let K be a number field of degree n, $\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$ its real embeddings and $\tau_1, \bar{\tau}_1, \tau_2, \bar{\tau}_2, \dots, \tau_s, \bar{\tau}_s : K \hookrightarrow \mathbb{C}$ its different complex embedings, where we sort them into pairs $\tau_i, \bar{\tau}_i$, which differ by complex conjugations. Then $n = r + 2s$ and we can define an injective map

$$\varphi : K \to \mathbb{R}^n, \quad \alpha \mapsto \Big(\sigma_1(\alpha), \dots, \sigma_r(\alpha), \Re\tau_1(\alpha)\Im\tau_1(\alpha), \dots, \Re\tau_s(\alpha), \Im\tau_s(\alpha)\Big).$$

Let $(\alpha_1, \dots, \alpha_n)$ be an integral basis of $\mathcal{O}_K$. Then we can view $\varphi(\mathcal{O}_K) = \mathbb{Z}\varphi(\alpha_1) + \cdots + \mathbb{Z}\varphi(\alpha_n) \subseteq \mathbb{R}^n$ as an additive group. Also, if $I \subseteq \mathcal{O}_K$ is a non-zero ideal, then I is a free $\mathbb{Z}$-module of rank n, say with basis $(\beta_1, \dots, \beta_n)$. Then

$$\varphi(I) = \mathbb{Z}\varphi(\beta_1) + \cdots + \mathbb{Z}\varphi(\beta_n) \subseteq \mathbb{R}^n$$

and we can interpret $\varphi(I)$ as a *lattice* in $\mathbb{R}^n$. In order to improve upon C_K in Theorem 3.1, we would like to find a "small" non-zero element in this lattice.

Lecture 11, 05.12.2023

3.2 Geometry of numbers

Motivation: Consider a lattice L, e.g. $\mathbb{Z}^n \subseteq \mathbb{R}^n$, and a "nice" subset $C \subseteq \mathbb{R}^n$, e.g. a ball of radius r. When does C contain a point in $L \setminus \{0\}$?

Definition (Lattice)
Let $v_1, \dots, v_n \in \mathbb{R}^n$ be linearly independent vectors (over $\mathbb{R}$). Then we call the group

$$L = \{z_1 v_1 + \cdots + z_n v_n \mid z_1, \dots, z_n \in \mathbb{Z}\} \subseteq \mathbb{R}^n$$

a (full) *lattice* in $\mathbb{R}^n$ and $v_1, \dots, v_n$ a basis of L. We define the determinant $d(L)$ of the lattice L as

$$d(L) = |\det(v_1, \dots, v_n)|.$$

Remark: As additive groups we have $L \cong \mathbb{Z}^n$. If $x \in L$ and $v_1, \ldots, v_n$ as above, then there is exactly one way to write x as $\sum_{i=1}^n x_i v_i$ with $x_1, \ldots, x_n \in \mathbb{Z}$.

Notation: We write $M_{n\times n}(\mathbb{Z})$ for the set of $n \times n$ matrices with coefficients in $\mathbb{Z}$. and $GL(n, \mathbb{Z}) = \{A \in M_{n\times n}(\mathbb{Z}) \,|\, \det(M) = \pm 1\}$ for the group of invertible matrices in $M_{n\times n}(\mathbb{Z})$.

Lemma 3.4
Let $L \subseteq \mathbb{R}^n$ be a lattice and $\{v_1, \ldots, v_n\}$, $\{w_1, \ldots, w_n\}$ bases of L. Then there exists a matrix $A \in GL(n, \mathbb{Z})$, say $A = (a_{i,j})_{1\le i,j\le n}$, such that

$$w_i = \sum_{i=1}^n a_{i,j} v_j, \quad 1 \le i \le n.$$

Moreover,

$$|\det(v_1, \ldots, v_n)| = |\det(w_1, \ldots, w_n)|.$$

Remark: In particular, the determinant $d(L)$ of a lattice $L \subseteq \mathbb{R}^n$ is well-defined.

Next, we want to compare the relative "size" of two lattices $M \subseteq L \subseteq \mathbb{R}^n$. Let $L = \{\sum_{i=1}^n z_i v_i \,|\, z_1, \ldots, z_n \in \mathbb{Z}\}$ and $M = \{\sum_{i=1}^n t_i w_i \,|\, t_1, dotsc, t_n \in \mathbb{Z}\}$ with $M \subseteq L$. Then $w_i \in L \;\forall\, 1 \le i \le n$ and hence there exists an $a_{i,j} \in \mathbb{Z}$ with $w_i = \sum_{j=1}^n a_{i,j} v_j \;\forall\, 1 \le i \le n$. Let $A = (a_{i,j})_{1\le i,j\le n} \in M_{n\times n}(\mathbb{Z})$.

Definition (Index of a sublattice)
In the notation above, we define the *index* $[L : M]$ of M in L as

$$[L : M] = |\det(A)|.$$

Remark:

1. The index $[L : M]$ does not depend on the choice of bases of L, M. By $w_i = \sum_{j=1}^n a_{i,j} v_j$, we have

$$\underbrace{|\det(w_1, \ldots, w_n)|}_{d(M)} = |\det(A)| \underbrace{|\det(v_1, \ldots, v_n)|}_{d(L)},$$

and hence $[L : M] = \frac{d(M)}{d(L)}$.

2. One can show that $[L : M] = |L/M|$, where L/M is the quotient group.

Example: Let $e_1, \ldots, e_n$ be the unit vectors in $\mathbb{R}^n$, i.e. $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$.

1. $\mathbb{Z}^n = \{\sum_{i=1}^n e_i z_i \mid z_1, \ldots, z_n \in \mathbb{Z}\}$ is a lattice with $d(\mathbb{Z}^n) = 1$. Let $d_1, \ldots, d_n \in \mathbb{N}$ and set $w_i = d_i e_i$ for all $1 \leq i \leq n$. Then $M = \{\sum_{i=1}^n z_i w_i \mid z_1, \ldots, z_n \in \mathbb{Z}\} \subseteq \mathbb{Z}^n$ is a sublattice with $d(M) = |\det(d_1 e_1, \ldots, d_n e_n)| = d_1 \cdots d_n$ and $[Z^n : M] = d_1 \cdots d_n$. Hence, as abelian groups, $\mathbb{Z}^n / M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$.

2. $L = \left\{ \frac{a_1}{2} e_1 + \cdots + \frac{a_n}{2} e_n \,\middle|\, a_1, \ldots, a_n \in \mathbb{Z},\ a_1 \equiv \cdots \equiv a_n \bmod 2 \right\}$ is a lattice in $\mathbb{R}^n$ with basis $e_1, \ldots, e_{n-1}, \frac{e_1 + \cdots + e_n}{2}$.

Convex bodies

Definition (Convex set)
We call a subset $C \subseteq \mathbb{R}^n$ *convex* if for all $x, y \in C$ the line segment

$$\{tx + (1-t)y \mid 0 \leq t \leq 1\}$$

is contained in C as well.

Definition (Central symmetric convex body)
A subset $C \subseteq \mathbb{R}^n$ ´is called a *central symmetric convex body* if it has the following properties:

(a) C is compact (i.e. closed and bounded) and convex. (convex body)

(b) 0 is in the interior of C. (central)

(c) If $x \in C$, then $-x \in C$. (symmetric)

Example:

1. Let $C \subseteq \mathbb{R}^n$ be a central symmetric convex body and $A : \mathbb{R}^n \to \mathbb{R}^n$ an invertible linear map. Then $A(C)$ is a central symmetric convex body.

2. The norm $\|x\|_2 = (\sum_{i=1}^n |x_i|^2)^{\frac{1}{2}}$ leads to the n-dimensional unit ball

$$B_n = \{x \in \mathbb{R}^n \mid \|x\|_2 \leq 1\}.$$

$\|x\|_\infty = \max_{1 \leq i \leq n} |x_i|$ induces the n-dimensional unit cube

$$K_n = \left\{ x \in \mathbb{R}^n \,\middle|\, \max_{1 \leq i \leq n} |x_i| \leq 1 \right\}.$$

$\|x\|_1 = \sum_i^n |x_i|$ give the n-dimensional unit octahedron

$$O_n = \left\{ x \in \mathbb{R}^n \,\middle|\, \sum_{i=1}^n |x_i| \leq 1 \right\}.$$

Lemma 3.5
Let $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}^n_{\geq 0}$ be a norm. Then $B_{\|\cdot\|} = \{x \in \mathbb{R}^n \,|\, \|x\| \leq 1\}$ is a central symmetric convex body.

So far we have found that every norm on $\mathbb{R}^n$ "produces" a central symmetric convex body in $\mathbb{R}^n$. Is there a one-to-one correspondence, i.e. are these all the different classes of central symmetric convex bodies?

Remark: Let $C \subseteq \mathbb{R}^n$ be a central symmetric convex body. For $\lambda \geq 0$, set $\lambda C = \{\lambda x \,|\, x \in C\}$. If $\lambda > 0$, then λC is again a central symmetric body. For $x \in \mathbb{R}^n$, we define $\|x\|_C = \min \{\lambda \in \mathbb{R}_{\geq 0} \,|\, x\lambda \in C\}$.

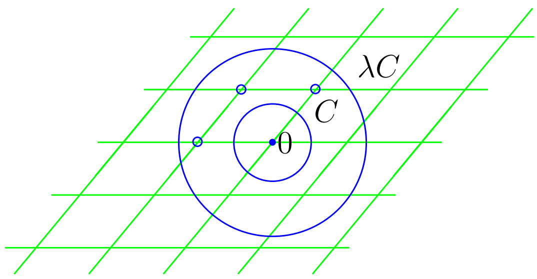
Lemma 3.6
Using the same notation as above, the following statements hold:

1. *$\|\cdot\|_C$ is well-defined.*
2. *$\|\cdot\|_C$ defines a norm on $\mathbb{R}^n$.*
3. *$\lambda C = \{x \in \mathbb{R}^n \,|\, \|x\|_C \leq \lambda\}$ for $\lambda > 0$.*

In particular, we recover C via $C = \{x \in \mathbb{R}^n \,|\, \|x\|_C \leq 1\}$.

Minkowski's[1] first convex body theorem

Let $L \subseteq \mathbb{R}^n$ be a lattice and $C \subseteq \mathbb{R}^n$ a central symmetric convex body. When is $C \cap L \neq \{0\}$, i.e. when does C contain more lattice points than just 0?



Theorem 3.7 (Minkowski's first convex body theorem, 1896)
With the same notation as above, let $\mathrm{vol}(C) \geq 2^n d(L)$. Then $C \cap L \neq \{0\}$, i.e. there exists a $x \in L \setminus \{0\}$ with $x \in C$.

[1] after Hermann Minkowski (1864 - 1909), a German mathematician

Lecture 12, 08.12.2023

Notation: For a lattice $L \subseteq \mathbb{R}^n$ with basis $v_1, \ldots, v_n$, we define

$$F = \left\{ \sum_{i=1}^{n} x_i v_i \,\middle|\, 0 \leq x_i \leq 1 \;\forall\, 1 \leq i > n \right\}$$

as the *fundamental parallelepiped* for L. This is the fundamental domain for $\mathbb{R}^n/L$. (see below)

Example: $[0,1)^n$ is the fundamental parallelepiped for $\mathbb{Z}^n$.

Remark: A fundamental parallelepiped depends on the choice of basis $v_1, \ldots, v_n$, but we have $\mathrm{vol}(F) = |\det(v_1, \ldots, v_n)| = d(L)$.

Lemma 3.8
Using the notation as above and for $u \in \mathbb{R}^n$ we write $u + F = \{u + x \,|\, x \in F\}$. Then

$$\mathbb{R}^n = \bigcup_{u \in L} (u + F)$$

is a disjunction.

Remark: Recall Landau's O-notation: Let $f, g, h : \mathbb{R}_{\geq x_0} \to \mathbb{R}$ for some $x_0 \in \mathbb{R}$. We write $f(x) = g(x) + = (h(x))$ if there exists $x_1 \geq x_0$ and $C \geq 0$, such that

$$|f(x) - g(x)| \leq Ch(x) \quad \forall\, x > x_1.$$

Example: $x^{-1} = O(1)$, $\lfloor x \rfloor = x + O(1)$, $(x+a)^n = x^n + O(x^{n-1})$ for any $a \in \mathbb{R}$, $n \in \mathbb{N}$, $(x+1)^{\frac{1}{2}} = x^{\frac{1}{2}} + O(x^{-\frac{1}{2}})$

Lemma 3.9
Let $L \subseteq \mathbb{R}^n$ be a lattice and $C \subseteq \mathbb{R}^n$ a central symmetric convex body. Then, as $\lambda \to \infty$, we have

$$|\lambda C \cap L| = \frac{\mathrm{vol}(C)}{d(L)} \lambda^n + O\!\left(\lambda^{n-1}\right).$$

Question: Do we need C to be central symmetric or convex in Minkowski's theorem?

Minkowski's second convex body theorem

Let $L \subseteq \mathbb{R}^n$ be a lattice and $C \subseteq \mathbb{R}^n$ a central symmetric convex body. When is $L \cap C \neq \{0\}$?

Definition (Successive minima)
We let
$$\lambda_1 = \min \{\lambda > 0 \,|\, \lambda C \cap L \neq \{0\}\}$$
and for $2 \leq i \leq n$ we define
$$\lambda_i = \min \{\lambda \in \mathbb{R}_{\geq 0} \,|\, \lambda C \cap L \text{ contains at least } i \text{ linearly independent points}\}.$$
We call $\lambda_1, \dots, \lambda_n$ the *successive minima* of L with respect to C.

Lemma 3.10
Let $L, C \subseteq \mathbb{R}^n$ be as above. The successive minima $\lambda_1, \dots, \lambda_n$ of L with respect to C are well defined and we have $0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n < \infty$. Moreover, there exist linearly independent elements $v_1, \dots, v_n \in L$ with $v_i \in \lambda_i C \;\forall\, 1 \leq i \leq n$.

Caveat: The vectors $v_1, \dots, v_n$ from Lemma 3.10 may not be a basis of L. Let
$$L = \left\{ \frac{x_1 e_1 + \cdots + x_n e_n}{2} \,\middle|\, x_i \in \mathbb{Z},\; x_1 \equiv \cdots \equiv x_n \bmod 2 \right\}.$$
For $n > 4$ and $C = B_n$ the unit ball, we have
$$\left\| \frac{e_1 + \cdots + e_n}{2} \right\| = \frac{1}{2}\sqrt{n} > 1,$$
but $\|e_1\|_2 = \cdots = \|e_n\|_2 = 1$.

Question: Is there a relation between $d(L)$ and the product $\lambda_1 \cdots \lambda_n$?

Example: The lattice $L = \mathbb{Z}d_1e_1 \oplus \cdots \oplus \mathbb{Z}d_ne_n$ with $0 < d_1 \leq \cdots \leq n_n$ has with respect to $\|\cdot\|_\infty$ the successive minima $d_1 \leq \cdots \leq d_n$ and $d_1 \cdots d_n = d(L)$.

Theorem 3.11 (Minkowski's second convex body theorem, 1910)
Let $L \subseteq \mathbb{R}^n$ be a lattice, $C \subseteq \mathbb{R}^n$ a central symmetric convex body and $\lambda_1, \dots, \lambda_n$

successive minima of L with respect to C. Then

$$\frac{1}{n!}\frac{2^n d(L)}{\mathrm{vol}(C)} \leq \lambda_1 \cdots \lambda_n \leq \frac{2^n d(L)}{\mathrm{vol}(C)}$$

Lecture 13, 12.12.2023

Remark: The upper bound is sharp. Take for example $L = \mathbb{Z}^n$ and $C = \{x \in \mathbb{R} \,|\, \|x\|_\infty \leq 1\}$, then $\mathrm{vol}(C) = 2^n$, $d(L) = 1$, $\lambda_1 = \cdots = \lambda_n = 1$. The following example shows that the lower bound is sharp as well.

Example: Let $0 < \lambda_1 \leq \cdots \leq \lambda_n$, $L = \mathbb{Z}^n$, $C = \{x \in \mathbb{R}^n \,|\, \sum_{i=1}^n \lambda_i |x_i| \leq 1\}$. Then L has successive minima $\lambda_1, \dots, \lambda_n$ with respect to C and $\mathrm{vol}(C) = \frac{2^n}{n!}(\lambda_1 \cdots \lambda_n)^{-1}$.

Minkowski's second convex body theorem implies Minkowski's first convex body theorem. Let L, C be as above and assume that $\mathrm{vol}(C) \geq 2^n d(L)$. Then

$$\lambda_1^n \leq \lambda_1 \cdots \lambda_n \leq \frac{2^n d(L)}{\mathrm{vol}(C)} \leq 1\,,$$

i.e. $\lambda_1 \leq 1$ and $C \cap L \neq \{0\}$.

Remark: Theorem 3.11 is invariant under linear transformation. Let $L, C, \lambda_1, \dots, \lambda_n$ be as above and $\phi : \mathbb{R}^n \to \mathbb{R}^n$ a linear invertible map. Then $\phi(L)$ is a lattice, $\phi(C)$ is a central symmetric convex body and one can show that $\lambda_1, \dots, \lambda_n$ are the successive minima of $\phi(L)$ with respect to $\phi(C)$ as for $x \in \mathbb{R}^n$ we have $\|x\|_C = \|\phi(x)\|_{\phi(C)}$. We note that

$$\frac{d(\phi(L))}{\mathrm{vol}(\phi(C))} = \frac{|\det \phi| d(L)}{|\det \phi| \,\mathrm{vol}(C)} = \frac{d(L)}{\mathrm{vol}(C)}\,.$$

This means it suffices to prove Theorem 3.11 for $L = \mathbb{Z}^n$.

Lemma 3.12
Let $v_1, \dots, v_r \in \mathbb{R}^n$. Then $S = \{\sum_{i=1}^r x_i v_i \,|\, x_i \in \mathbb{R},\ \sum_{i=1}^r |x_i| \leq 1\}$ is the smallest convex subset in $\mathbb{R}^n$ that is symmetric about 0 and contains $v_1, \dots, v_r$. I.e. S is symmtric about 0 and if $R \subseteq \mathbb{R}^n$ is convex, symmetric about 0 and $v_1, \dots, v_r \in R$, then $S \subseteq R$.

Theorem 3.13
Let $L \subseteq \mathbb{R}^n$ be a lattice. Then there exist $v_1, \dots, v_n \in L$, such that $v_1, \dots, v_n$ are a

basis of L and

$$\|v_1\|_2 \cdots \|v_n\|_2 \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} d(L)\,.$$

Remark: This is a weaker version of the upper bound in Theorem 3.11. Our constant $\left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}}$ is in general larger than 2^n (and is for large n actually pretty far off, as the exponent grows in n^2), and each successive minimum λ_i is bounded above by $\|v_i\|_2$, so they might be even smaller.

Corollary 3.14
Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of a lattice $L \subseteq \mathbb{R}^n$ with respect to B_n. Then

$$\lambda_1 \cdots \lambda_n \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} d(L)\,.$$

Corollary 3.15
Let $E \subseteq \mathbb{R}^n$ be an ellipsoid, symmetric about 0 and $L \subseteq \mathbb{R}^n$ a lattice. Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of L ´with respect to E. Then

$$\lambda_1 \cdots \lambda_n \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} V(n) \frac{d(L)}{\mathrm{vol}(E)}\,,$$

where we write $V(n) = \mathrm{vol}(B_n)$.

Theorem (Jordan's[2] theorem)
Let $C \subseteq \mathbb{R}^n$ be a central symmetric convex body. Then there exists and ellipsoid $E \subseteq \mathbb{R}^n$ with

$$E \subseteq C \subseteq \sqrt{n} E\,.$$

Corollary 3.16
For all $n \in \mathbb{N}$ there exists a constant $c(N) > 0$ with the following property: Let $L \subseteq \mathbb{R}^n$ be a lattice, $C \subseteq \mathbb{R}^n$ a central symmetric convex body, and $\lambda_1, \ldots, \lambda_n$ the successive minima of L with respect to C. Then

$$\lambda_1 \cdots \lambda_n \leq c(n) \frac{d(L)}{\mathrm{vol}(C)}\,.$$

[2] after M. E. Camille Jordan (1838 - 1922), a French mathematician

Let $v_1 \in L \setminus \{0\}$ be such that $\|v_1\|_2 = \lambda_1$, where λ_1 is the first successive minimum of L with respect to B_n. Fix an orthonormal basis $\{e_1, \dots, e_n\}$ of $\mathbb{R}^n$, such that $e_1 = \lambda_1^{-1} v_1$. Consider the projection $\rho : \mathbb{R}^n \to \mathbb{R}^{n-1}$, $\sum_{i=1}^n x_i e_i \mapsto (x_2, \dots, x_n)$. Let $L' = \rho(L)$, e.g. if $L = \mathbb{Z}d_1e_1 \oplus \cdots \oplus \mathbb{Z}d_ne_n$, then $L' = \mathbb{Z}d_2e_2 \oplus \cdots \oplus \mathbb{Z}d_ne_n$.

Lemma 3.17
Using the same notation as above, $L' \subseteq \mathbb{R}^{n-1}$ is a lattice and if $v_1, \dots, v_n$ is a basis of L then $\rho(v_2), \dots, \rho(v_n)$ is a bsis of L'.

Lecture 14, 15.12.2023

Lemma 3.18
Let $\{v_2', \dots, v_n'\}$ be a basis of L' and $v_2, \dots, v_n \in L$ with $\rho(v_i) = v_i'$ for $2 \leq i \leq n$. Then $\{v_1, \dots, v_n\}$ is a basis of L.

Lemma 3.19

$$d(L) = \lambda_1 d(L')\,.$$

Lemma 3.20
Let $v' \in L'$. Then there exists $v \in L$, such that $\rho(v) = v'$ and

$$\|v\|_2^2 \leq \frac{4}{3}\|v'\|_2^2\,.$$

Remark: We always have $\prod_{i=1}^n \|v_i\|_2 \geq d(L)$.

3.3 Bounds for class numbers

For the rest of this section, let K be a number field with ring of integers $\mathcal{O}_K$.

Question: Can we improve upon our earlier upper bounds on $|Cl(\mathcal{O}_K)|$?

Idea: We could interpret the non-zero ideal $I \subseteq \mathcal{O}_K$ as a lattice and apply Minkowski's first convex body theorem to find an element $\alpha \in I \setminus \{0\}$ of small norm.

More concretely, let $\sigma_1, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$ be the real embeddings and $\tau_1, \bar{\tau}_1, \dots, \tau_s, \bar{\tau}_s$:

$K \hookrightarrow \mathbb{C}$ be the complex embeddings of K. Note that $r + 2s = n$, where $n = [K : \mathbb{Q}]$. Define the map

$$\varphi : K \to \mathbb{R}^n, \quad \alpha \mapsto \Big(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \Re\tau_1(\alpha), \Im\tau_1(\alpha), \ldots, \Re\tau_s(\alpha), \Im\tau_s(\alpha)\Big)\,.$$

Lemma 3.21
The image $\varphi(\mathcal{O}_K) =: \Lambda$ is a (full) lattice in $\mathbb{R}^n$ with determinant

$$d(\Lambda) = \frac{1}{2^s}\sqrt{|\operatorname{disc}\mathcal{O}_K|}\,.$$

Remark: If I is a non-zero ideal, then the same argument shows that $\varphi(I)$ is a sublattice of $\mathcal{O}_K$. More precisely, $d\big(\varphi(I)\big) = d\big(\varphi(\mathcal{O}_K)\big)\underbrace{\big|\varphi(\mathcal{O}_K)/\varphi(I)\big|}_{=|\mathcal{O}_K/I|}$, i.e.

$$d\big(\varphi(I)\big) = \frac{1}{2^s}\sqrt{|\operatorname{disc}\mathcal{O}_K|}N(I)\,.$$

Corollary 3.22
$\varphi(K)$ is dense in $\mathbb{R}^n$.

Our next goal is for a non-zero ideal $I \subseteq \mathcal{O}_K$ to find a $\alpha \in I \setminus \{0\}$, such that $|N_{K/\mathbb{Q}}(\alpha)|$ is small. We write $\varphi(\alpha) = (y_1, \ldots, y_n) \in \mathbb{R}^n$. Then

$$N_{K/\mathbb{Q}}(\alpha) = y_1 \cdot y_2 \cdots y_r \cdot \left(y_{r+1}^2 + y_{r+2}^2\right) \cdots \left(y_{n-1}^2 + y_n^2\right).$$

The problem here is that the function $N : \mathbb{R}^n \to \mathbb{R}$ is not a norm on $\mathbb{R}^n$.

Idea: Construct a central symmetric convex body $A \subseteq \mathbb{R}^n$, such that $x \in A$ implies that $|N(x)| \leq 1$.

We define

$$A = \left\{x \in \mathbb{R}^n \,\middle|\, |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n\right\}$$

Lemma 3.23
A is a central symmetric convex body with the property that $x \in A$ implies $|N(x)| \leq 1$. Moreover,

$$\operatorname{vol}(A) = \frac{n^n}{n!}2^r\left(\frac{\pi}{2}\right)^s\,.$$

Theorem 3.24
Let $I \subseteq \mathcal{O}_K$ be a non-zero ideal. Then there exists an $\alpha \in I \setminus \{0\}$ with

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc} \mathcal{O}_K|} N(I) \,.$$

Definitions