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

Lemma 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 3
If $\alpha \in \mathbb{Q}$ is an algebraic integer, then $\alpha \in \mathbb{Z}$.

Theorem 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 5
The set of algebraic integers in $\mathbb{C}$ *is a ring.*

Lecture 2, 27.10.2023

Definition
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 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 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 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 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 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 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 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 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 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 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 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 $\mathrm{Tr}_{L/K}(v_i w_j) = \delta_{ij},\ 1 \le i, j, \le n$.

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

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

Theorem 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 17
Let $\alpha_1, \ldots, \alpha_n \in K$. Then

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

Corollary 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 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

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

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 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 $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, 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 $m_1, \ldots, m_n \in \mathbb{Z}$.

Remark: In the notation of Theorem 20, we call $(\alpha_1, \ldots, \alpha_n)$ and integral basis of $\mathcal{O}_K$ (over $\mathbb{Z}$).

Lecture 4, 07.11.2023

Lemma 21
Let K be a number field as above. Then there exists a $\mathbb{Q}$-basis of the number field, say $(\alpha_1, \ldots, \alpha_n)$, with $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$.

Proposition 22
Let $(\alpha_1, \ldots, \alpha_n)$ be a $\mathbb{Q}$-basis of a number field K with $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ and $\beta \in \mathcal{O}_K$. Then there exist $m_1, \ldots, m_n \in \mathbb{Z}$, such that

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

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

Lemma 23
Let K be a number field with integral bases $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$. Then

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

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

$\operatorname{disc}(K)$ of K as

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

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

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

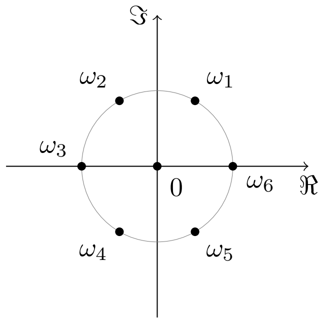
1.4 Cyclotomic fields

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 24
The extension $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ is Galois with degree equal to $\varphi(m)$. 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 25
The conjugates of ω are exactly given by ω^k with $\gcd(m, k) = 1$.

Corollary 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 27

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

Theorem 28

Let $m = p^r$ for some prime p. Then $\mathcal{O}_{Q[m]} = \mathbb{Z}[\omega]$.

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

Lemma 29

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

Definitions