
Analytic Number Theory III

Lecture notes

Prof. Dr. Damaris Schindler

L^AT_EX version by Alex Dalist Howl Sennewald

Mathematical Institute
Georg-August-University Göttingen
Winter term 2023/24

Contents

1	Number Fields	1
1.1	Number fields and number rings	1
1.2	Embeddings, Norm and Trace	3
	Definitions	7

List of lectures

Lecture 1 from 24.10.2023	1
Lecture 2 from 27.10.2023	3

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

$$x^2 - dy^2 = 1. \quad (1.1)$$

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 $N : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}$, $a + \sqrt{d}b \mapsto a^2 - db^2$. 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?

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

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 $f(\alpha) = 0$. 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 $\alpha \in \mathbb{C}$ 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.

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

1.2 Embeddings, Norm and Trace

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

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 $\hat{\iota} : K \hookrightarrow \mathbb{C}$, then there exist $[L : K]$ embeddings $L \hookrightarrow \mathbb{C}$, which extend $\hat{\iota}$. If $g(x)$ is a minimal polynomial of α over K then the embeddings are given by $\sigma_i : \alpha \mapsto \beta_i$, where $\beta_1, \dots, \beta_{[L:K]}$ 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

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

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 $\varphi : V \rightarrow V$ 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 $c_0, \dots, c_n \in K$. We define the determinant and trace of φ by $\det \varphi = (-1)^n c_n$ and $\text{trace } \varphi = -c_1$

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

Definition

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

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

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

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

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

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

Lemma 7

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

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

Lemma 8

Let L/K be an extension of number fields with $L = K(\alpha)$ and $[L : K] = n$. Let $f(x) = x^n + c_1x^{n-1} + \cdots + c_n$ be the minimal polynomial of α over K . Then

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

Lemma 9

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

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

Corollary 10

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

Theorem 11

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

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

Corollary 12

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

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

Theorem 13

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

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

Definitions

Algebraic integer, [2](#)

Norm, [4](#)

Number field, [1](#)

Trace, [4](#)