
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
	Definitions	5

List of lectures

Lecture 1 from 24.10.2023	1
-------------------------------------	---

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 1.0.1 (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 1.0.2 (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 1.1.1

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

Lemma 1.1.2

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 1.1.3

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

Theorem 1.1.4 (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 1.1.5

The set of algebraic integers in \mathbb{C} is a ring.

Definitions

Algebraic integer, [2](#)

Number field, [1](#)