Number Theory I und II

Prof. Richard Pink

Summary
Fall Semester 2023
Spring Semester 2024
ETH Z"urich

Preliminary Version

October 6, 2023

This summary contains the definitions and results covered in the lecture course, but no proofs, examples, explanations, or exercises.

Content

1 Some commutative algebra

1.1 Integral ring extensions

All rings are assumed to be commutative and unitary. Consider a ring extension $A \subset B$.

Definition 1.1.1: (a) An element $b \in B$ is called *integral over* A if there exists a monic $f \in A[X]$ with $f(b) = 0$.

(b) The ring B is called *integral over* A if every $b \in B$ is integral over A.

(c) The *integral closure of* A *in* B is the set $\tilde{A} := \{b \in B \mid b \text{ integral over } A\}$.

Definition-Example 1.1.2: (a) An element $z \in \mathbb{C}$ is integral over $\mathbb{Q}$ if and only if z is an *algebraic number*.

(b) An element $z \in \mathbb{C}$ is integral over $\mathbb{Z}$ if and only if z is an *algebraic integer*.

Proposition 1.1.3: The following statements for an element $b \in B$ are equivalent:

(a) b is integral over A.

(b) The subring $A[b] \subset B$ is finitely generated as an A-module.

(c) b is contained in a subring of B which is finitely generated as an A-module.

Proposition 1.1.4: (a) For any integral ring extensions $A \subset B$ and $B \subset C$ the ring extension $A \subset C$ is integral.

(b) The subset $\tilde{A}$ is a subring of B that contains A.

(c) The subring $\tilde{A}$ is its own integral closure in B.

1.2 Prime ideals

Consider an integral ring extension $A \subset B$.

Proposition 1.2.1: For every prime ideal $\mathfrak{q} \subset B$ the intersection $\mathfrak{q} \cap A$ is a prime ideal of A.

Definition 1.2.2: We say that $\mathfrak{q}$ *lies over* $\mathfrak{q} \cap A$.

Theorem 1.2.3: For any prime ideals $\mathfrak{q} \subset \mathfrak{q}' \subset B$ over the same $\mathfrak{p}$ we have $\mathfrak{q} = \mathfrak{q}'$.

Theorem 1.2.4: For every prime ideal $\mathfrak{p} \subset A$ there exists a prime ideal $\mathfrak{q} \subset B$ over $\mathfrak{p}$.

1.3 Normalization

From now on we assume that A is an integral domain with quotient field K.

Definition 1.3.1: (a) The integral closure of A in K is called the *normalization of* A.

(b) The ring A is called *normal* if this normalization is A.

Proposition 1.3.2: (a) The normalization of A is normal.

(b) Any unique factorization domain is normal.

1.4 Localization

Definition 1.4.1: A subset $S \subset A \setminus \{0\}$ is called *multiplicative* if it contains 1 and is closed under multiplication.

Definition-Proposition 1.4.2: For any multiplicative subset $S \subset A$ the subset

$$S^{-1}A \ := \ \bigl\{ \tfrac{a}{s} \bigm| a \in A,\ s \in S \bigr\}$$

is a subring of K that contains A and is called the *localization of A with respect to S*.

Example 1.4.3: For every prime ideal $\mathfrak{p} \subset A$ the subset $A \setminus \mathfrak{p}$ is multiplicative. The ring $A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1}A$ is called the *localization of A at* $\mathfrak{p}$.

Proposition 1.4.4: For every multiplicative subset $S \subset A$ we have:

(a) $S^{-1}\tilde{A} = \widetilde{S^{-1}A}$.

(b) If A is normal, then so is $S^{-1}A$.

1.5 Field extensions

In the following we consider a normal integral domain A with quotient field K, and an algebraic field extension L/K, and let B be the integral closure of A in L.

Proposition 1.5.1: For any homomorphism $\sigma\colon L \to M$ of field extensions of K, an element $x \in L$ is integral over A if and only if $\sigma(x)$ is integral over A.

Proposition 1.5.2: An element $x \in L$ is integral over A if and only if the minimal polynomial of x over K has coefficients in A.

Proposition 1.5.3: We have $(A \setminus \{0\})^{-1}B = L$.

1.6 Norm and Trace

Assume that L/K is finite separable. Let $\bar{K}$ be an algebraic closure of K.

Definition 1.6.1: For any $x \in L$ we consider the K-linear map $T_x\colon L \to L$, $u \mapsto ux$.

(a) The *norm of x for L/K* is the element $\mathrm{Nm}_{L/K}(x) := \det(T_x) \in K$.

(b) The *trace of x for L/K* is the element $\mathrm{Tr}_{L/K}(x) := \mathrm{tr}(T_x) \in K$.

Proposition 1.6.2: (a) For any $x, y \in L$ we have $\mathrm{Nm}_{L/K}(xy) = \mathrm{Nm}_{L/K}(x)\cdot\mathrm{Nm}_{L/K}(y)$.

(b) The map $\mathrm{Nm}_{L/K}$ induces a homomorphism $L^\times \to K^\times$.

(c) The map $\mathrm{Tr}_{L/K}\colon L \to K$ is K-linear.

Proposition 1.6.3: For any $x \in L$ we have

$$\mathrm{Nm}_{L/K}(x) \;=\; \prod_{\sigma\in\mathrm{Hom}_K(L,\bar{K})} \sigma(x) \qquad\text{and}\qquad \mathrm{Tr}_{L/K}(x) \;=\; \sum_{\sigma\in\mathrm{Hom}_K(L,\bar{K})} \sigma(x).$$

Proposition 1.6.4: The map $\mathrm{Tr}_{L/K}\colon L \to K$ is non-zero.

Proposition 1.6.5: For any two finite separable field extensions $M/L/K$ we have:

(a) $\mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{M/L} = \mathrm{Nm}_{M/K}$.

(b) $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$.

Proposition 1.6.6: For any $x \in B$ we have:

(a) $\mathrm{Nm}_{L/K}(x) \in A$.

(b) $\mathrm{Nm}_{L/K}(x) \in A^\times$ if and only if $x \in B^\times$.

(c) $\mathrm{Tr}_{L/K}(x) \in A$.

1.7 Discriminant

Proposition 1.7.1: The map

$$L \times L \longrightarrow K, \quad (x,y) \mapsto \mathrm{Tr}_{L/K}(xy)$$

is a non-degenerate symmetric K-bilinear form.

Lemma 1.7.2: Write $\mathrm{Hom}_K(L, \bar{K}) = \{\sigma_1, \ldots, \sigma_n\}$ with $[L/K] = n$ and consider the matrix $T := (\sigma_i(b_j))_{i,j=1,\ldots,n}$. Then

$$T^T \cdot T \;=\; \big(\mathrm{Tr}_{L/K}(b_i b_j)\big)_{i,j=1,\ldots,n}.$$

Definition 1.7.3: The *discriminant* of any ordered basis $(b_1, \ldots, b_n)$ of L over K is the determinant of the associated *Gram matrix*

$$\mathrm{disc}(b_1, \ldots, b_n) \;:=\; \det\big(\mathrm{Tr}_{L/K}(b_i b_j)\big)_{i,j=1,\ldots,n} \;=\; \det(T)^2 \;\in\; K.$$

Proposition 1.7.4: If $L = K(b)$ and $n = [L/K]$, then $\operatorname{disc}(1, b, \ldots, b^{n-1})$ is the discriminant of the minimal polynomial of b over K.

Proposition 1.7.5: (a) We have $\operatorname{disc}(b_1, \ldots, b_n) \in K^\times$.

(b) If $b_1, \ldots, b_n \in B$, then $\operatorname{disc}(b_1, \ldots, b_n) \in A \setminus \{0\}$ and

$$B \subset \frac{1}{\operatorname{disc}(b_1, \ldots, b_n)} \cdot \big(Ab_1 + \ldots + Ab_n\big).$$

Proposition 1.7.6: If A is a principal ideal domain, then:

(a) B is a free A-module of rank $[L/K]$.

(b) For any basis $(b_1, \ldots, b_n)$ of B over A, the number $\operatorname{disc}(b_1, \ldots, b_n)$ is independent of the basis up to the square of an element of $A^\times$.

Definition 1.7.7: This number is called the *discriminant of B over A* or *of L over K* and is denoted $\operatorname{disc}_{B/A}$ or $\operatorname{disc}_{L/K}$.

1.8 Linearly disjoint extensions

Definition 1.8.1: Two finite separable field extensions $L, L'/K$ are called *linearly disjoint* if $L \otimes_K L'$ is a field.

Proposition 1.8.2: For any two finite separable field extensions $L, L'/K$ within a common overfield M the following statements are equivalent:

(a) L and L' are linearly disjoint over K.

(b) $[LL'/K] = [L/K] \cdot [L'/K]$

(c) $[LL'/L] = [L'/K]$

(d) $[LL'/L'] = [L/K]$

If at least one of L/K and L'/K is galois, they are also equivalent to

(e) $L \cap L' = K$.

Theorem 1.8.3: Consider linearly disjoint finite separable field extensions $L, L'/K$. Assume that A is a principal ideal domain and that $d := \operatorname{disc}_{L/K}$ and $d' := \operatorname{disc}_{L'/K}$ are relatively prime in A. Let $B, B', \tilde{B}$ be the integral closures of A in L, L', LL'. Then:

(a) $B \otimes_A B' \xrightarrow{\sim} \tilde{B}$.

(b) $\operatorname{disc}_{LL'/K} = d^{[L'/K]} \cdot d'^{[L/K]}$ up to the square of a unit in A.

1.9 Dedekind Rings

Definition 1.9.1: (a) A ring A is *noetherian* if every ideal is finitely generated.

(b) An integral domain A has *Krull dimension* 1 if it is not a field and every non-zero prime ideal is a maximal ideal.

(c) A noetherien normal integral domain of Krull dimension 1 is called a *Dedekind ring.*

Proposition 1.9.2: Any principal ideal domain that is not a field is a Dedekind ring.

Examples 1.9.3: Take $A = \mathbb{Z}$ or $A = \mathbb{Z}[i]$ or $A = k[t]$ or $A = k[[t]]$ for a field k.

In the following we assume that $A \subset K$ is Dedekind and that $B \subset L$ is as above.

Proposition 1.9.4: (a) For every multiplicative subset $S \subset A$ the ring $S^{-1}A$ is Dedekind or a field.

(b) For every prime ideal $0 \neq \mathfrak{p} \subset A$ the localization $A_\mathfrak{p}$ is a discrete valuation ring.

Theorem 1.9.5: The ring B is Dedekind and finitely generated as an A-module.

1.10 Fractional Ideals

Let A be a Dedekind ring with quotient field K.

Definition 1.10.1:

(a) A non-zero finitely generated A-submodule of K is called a *fractional ideal of A.*

(b) A fractional ideal of the form $(x) := Ax$ for some $x \in K^\times$ is called *principal.*

(c) The *product* of two fractional ideals $\mathfrak{a}, \mathfrak{b}$ is defined as

$$\mathfrak{a}\mathfrak{b} \;:=\; \Big\{\textstyle\sum_{i=1}^r a_i b_i \;\Big|\; r \geqslant 0,\; a_i \in \mathfrak{a},\; b_i \in \mathfrak{b}\Big\}.$$

(d) The *inverse* of a fractional ideal $\mathfrak{a}$ is defined as

$$\mathfrak{a}^{-1} \;=\; \Big\{x \in K \;\Big|\; x \cdot \mathfrak{a} \subset A\Big\}.$$

Proposition 1.10.2: For any fractional ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ we have:

(a) There exist $a, b \in A \smallsetminus \{0\}$ with $(a) \subset \mathfrak{a} \subset (\frac{1}{b})$.

(b) $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}^{-1}$ are fractional ideals.

(c) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ and $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ and $(1)\mathfrak{a} = \mathfrak{a}$.

(d) $\mathfrak{a} \subset A$ if and only if $A \subset \mathfrak{a}^{-1}$.

Lemma 1.10.3: For every non-zero ideal $\mathfrak{a} \subset A$ there exist an integer $r \geqslant 0$ and maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{a}$.

Lemma 1.10.4: For every maximal ideal $\mathfrak{p} \subset A$ and every fractional ideal $\mathfrak{a}$ we have

(a) $A \subsetneqq \mathfrak{p}^{-1}$.

(b) $\mathfrak{a} \subsetneqq \mathfrak{p}^{-1}\mathfrak{a}$.

(c) $\mathfrak{p}^{-1}\mathfrak{p} = (1)$.

Theorem 1.10.5: Any non-zero ideal of A is a product of maximal ideals and the factors are unique up to permutation. *(Unique factorization of ideals)*

Theorem 1.10.6: (a) The set J_A of fractional ideals is an abelian group with the above product and inverse and the unit element $(1) = A$.

(b) The group J_A is the free abelian group with basis the maximal ideals of A.

1.11 Ideals

Consider any non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset A$.

Definition 1.11.1: We write $\mathfrak{b}|\mathfrak{a}$ and say that $\mathfrak{b}$ *divides* $\mathfrak{a}$ if and only if $\mathfrak{a} \subset \mathfrak{b}$.

Proposition 1.11.2: For any $a, b \in A \setminus \{0\}$ we have $b|a$ if and only if $(b)|(a)$.

Proposition 1.11.3: We have $\mathfrak{b}|\mathfrak{a}$ if and only if there is a non-zero ideal $\mathfrak{c} \subset A$ with $\mathfrak{b}\mathfrak{c} = \mathfrak{a}$.

Definition 1.11.4: Ideals $\mathfrak{a}, \mathfrak{b} \subset A$ with $\mathfrak{a} + \mathfrak{b} = A$ are called *coprime*.

Proposition 1.11.5: For any non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset A$ the following are equivalent:

(a) $\mathfrak{a}$ and $\mathfrak{b}$ are coprime.

(b) Their factorizations in maximal ideals do not have a common factor.

(c) $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Chinese Remainder Theorem 1.11.6: For any pairwise coprime ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \subset A$ we have a ring isomorphism

$$\begin{aligned} A/\mathfrak{a}_1 \cdots \mathfrak{a}_r &\stackrel{\sim}{\longrightarrow} A/\mathfrak{a}_1 \times \ldots \times A/\mathfrak{a}_r, \\ a + \mathfrak{a}_1 \cdots \mathfrak{a}_r &\longmapsto (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_r). \end{aligned}$$

Proposition 1.11.7: For any fractional ideals $\mathfrak{a} \subset \mathfrak{b}$ there exists $b \in \mathfrak{b}$ with $\mathfrak{b} = \mathfrak{a} + (b)$.

Proposition 1.11.8: Every fractional ideal of A is generated by 2 elements.

Proposition 1.11.9: For any non-zero ideal $\mathfrak{a}$ and any fractional ideal $\mathfrak{b}$ of A there exists an isomorphism of A-modules $A/\mathfrak{a} \cong \mathfrak{b}/\mathfrak{a}\mathfrak{b}$.

1.12 Ideal class group

Definition 1.12.1: The factor group

$$\mathrm{Cl}(A) \;:=\; \big\{\text{fractional ideals}\big\} \,/\, \big\{\text{principal ideals}\big\}$$

is called the *ideal class group of* A. Its order $h(A) := |\,\mathrm{Cl}(A)|$ is called the *class number of* A.

Proposition 1.12.2: Any ideal class is represented by a non-zero ideal of A.

Proposition 1.12.3: There is a fundamental exact sequence

$$1 \longrightarrow A^\times \longrightarrow K^\times \longrightarrow J_A \longrightarrow \mathrm{Cl}(A) \longrightarrow 1.$$

2 Minkowski's lattice theory

2.1 Lattices

Fix a finite dimensional $\mathbb{R}$-vector space V.

Proposition 2.1.1: There exists a unique topology on V such that for any basis $v_1, \ldots, v_n$ of V the isomorphism $\mathbb{R}^n \to V$, $(x_i)_i \mapsto \sum_{i=1}^n x_i v_i$ is a homeomorphism.

Definition 2.1.2: A subset $X \subset V$ is called ...

(a) ... *bounded* if and only if the corresponding subset of $\mathbb{R}^n$ is bounded.

(b) ... *discrete* if and only if the corresponding subset of $\mathbb{R}^n$ is discrete, that is, if its intersection with any bounded subset is finite.

Now we are interested in an (additive) subgroup $\Gamma \subset V$.

Definition-Proposition 2.1.3: The following are equivalent:

(a) Γ is discrete.

(b) $\Gamma = \bigoplus_{i=1}^m \mathbb{Z}v_i$ for $\mathbb{R}$-linearly independent elements $v_1, \ldots, v_m$.

Such a subgroup is called a *lattice*.

Definition-Proposition 2.1.4: The following are equivalent:

(a) Γ is discrete and there exists a bounded subset $\Phi \subset V$ such that $\Gamma + \Phi = V$.

(b) Γ is discrete and V/Γ is compact.

(c) $\Gamma = \bigoplus_{i=1}^n \mathbb{Z}v_i$ for an $\mathbb{R}$-basis $v_1, \ldots, v_n$ of V.

Such a subgroup is called a *complete lattice*.

In the following we consider a lattice $\Gamma \subset V$.

Definition 2.1.5: Any measurable subset $\Phi \subset V$ such that $\Phi \to V/\Gamma$ is bijective is called a *fundamental domain for* Γ. (With respect to the measure from §2.2.)

Example 2.1.6: If $\Gamma = \bigoplus_{i=1}^n \mathbb{Z}v_i$ for an $\mathbb{R}$-basis $v_1, \ldots, v_n$ of V, a fundamental domain is:

$$\Phi := \left\{ \sum_{i=1}^n x_i v_i \;\middle|\; \forall i\colon\ 0 \leqslant x_i < 1 \right\}.$$

Caution 2.1.7: If $V \neq 0$, there does not exist a compact fundamental domain, because there is a problem with the boundary.

2.2 Volume

Now we fix a scalar product $\langle\ ,\ \rangle$ on V.

Proposition 2.2.1: (a) There exists a unique Lebesgue measure $d\mathrm{vol}$ on V such that for any measurable function f on V and any orthonormal basis $(e_1, \ldots, e_n)$ of V we have

$$\int_V f(v)\ d\mathrm{vol}(v) \ = \ \int_{\mathbb{R}^n} f\big(\textstyle\sum_{i=1}^n x_i e_i\big)\, dx_1 \ldots dx_n.$$

(b) For any $\mathbb{R}$-basis $(v_1, \ldots, v_n)$ of V we then have

$$\mathrm{vol}\big(\{\textstyle\sum_{i=1}^n x_i v_i \,\big|\, \forall i\colon\ 0 \leqslant x_i < 1\}\big) \ = \ \sqrt{\det\big(\langle v_i, v_j\rangle\big)_{i,j=1}^n}$$

and

$$\int_V f(v)\ d\mathrm{vol}(v) \ = \ \int_{\mathbb{R}^n} f\big(\textstyle\sum_{i=1}^n y_i v_i\big)\, dy_1 \ldots dy_n \cdot \sqrt{\det\big(\langle v_i, v_j\rangle\big)_{i,j=1}^n}.$$

Definition-Proposition 2.2.2: Consider any fundamental domain $\Phi \subset V$.

(a) For any measurable function f on V/Γ this integral is independent of Φ:

$$\int_{V/\Gamma} f(\bar{v})\ d\mathrm{vol}(\bar{v}) \ := \ \int_\Phi f(v+\Gamma)\ d\mathrm{vol}(v).$$

(b) In particular we obtain

$$\mathrm{vol}(V/\Gamma) \ := \ \int_{V/\Gamma} 1\ d\mathrm{vol}(\bar{v}) \ = \ \mathrm{vol}(\Phi).$$

Fact 2.2.3: We have $\mathrm{vol}(V/\Gamma) < \infty$ if and only if Γ is a complete lattice.

2.3 Lattice Point Theorem

Let Γ be a complete lattice in a finite dimensional euclidean vector space V.

Definition 2.3.1: A subset $X \subset V$ is *centrally symmetric* if and only if

$$X = -X := \{-x \mid x \in X\}.$$

Theorem 2.3.2: Let $X \subset V$ be a centrally symmetric convex subset which satisfies

$$\mathrm{vol}(X) \ > \ 2^{\dim(V)} \cdot \mathrm{vol}(V/\Gamma).$$

Then $X \cap \Gamma$ contains a non-zero element.

Remark 2.3.3: The theorem is sharp. For example if $V = \mathbb{R}^n$ and $\Gamma = \mathbb{Z}^n$ and $X =]-1,1[^n$, then we have $\mathrm{vol}(X) = 2^{\dim(V)} \cdot \mathrm{vol}(V/\Gamma)$ and $X \cap \Gamma = \{0\}$.

Application 2.3.4: An n-dimensional ball B_r of radius r has volume

$$\mathrm{vol}(B_r) \ = \ \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} \cdot r^n.$$

Therefore the smallest non-zero vector in Γ has length

$$\leqslant \ \frac{2}{\sqrt{\pi}} \cdot \sqrt[n]{\mathrm{vol}(V/\Gamma) \cdot \Gamma(\tfrac{n}{2}+1)}.$$

More generally, for every k one can bound the combined lengths of k linearly independent vectors in Γ using *successive minima*.

3 Algebraic integers

3.1 Number fields

Definition 3.1.1: (a) A finite field extension $K/\mathbb{Q}$ is called an *(algebraic) number field.*

(b) A number field of degree $2, 3, 4, 5$,... is called *quadratic, cubic, quartic, quintic,...*

(c) The integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called the ring of *algebraic integers in* K.

In the rest of this chapter we fix such K and $\mathcal{O}_K$ and abbreviate $n := [L/K]$.

Proposition 3.1.2: (a) The ring $\mathcal{O}_K$ is Dedekind.

(c) $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

(b) Any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

3.2 Absolute discriminant

Proposition 3.2.1: (a) For any $\mathbb{Z}$-submodule $\Gamma \subset K$ of rank n with an ordered $\mathbb{Z}$-basis $(x_1, \ldots, x_n)$ the following value depends only on Γ:

$$\operatorname{disc}(\Gamma) := \operatorname{disc}(x_1, \ldots, x_n) \in \mathbb{Z} \smallsetminus \{0\}.$$

(b) For any two $\mathbb{Z}$-submodules $\Gamma \subset \Gamma' \subset K$ of rank n the index $[\Gamma' : \Gamma]$ is finite and we have

$$\operatorname{disc}(\Gamma) = [\Gamma' : \Gamma]^2 \cdot \operatorname{disc}(\Gamma').$$

Definition 3.2.2: The number

$$d_K \ := \ \operatorname{disc}(\mathcal{O}_K) \ \in \ \mathbb{Z} \smallsetminus \{0\}$$

is called the *discriminant of $\mathcal{O}_K$ or of K.*

Corollary 3.2.3: If there exist $a_1, \ldots, a_n \in \mathcal{O}_K$ such that $\operatorname{disc}(a_1, \ldots, a_n)$ is squarefree, then

$$\mathcal{O}_K = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_n.$$

3.3 Absolute norm

Definition 3.3.1: The *absolute norm* of a non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ is the index

$$\operatorname{Nm}(\mathfrak{a}) := [\mathcal{O}_K \colon \mathfrak{a}] \in \mathbb{Z}^{\geqslant 1}.$$

Proposition 3.3.2: For any $a \in A \smallsetminus \{0\}$ we have $\operatorname{Nm}((a)) = |\operatorname{Nm}_{K/\mathbb{Q}}(a)|$.

Proposition 3.3.3: For any integer $N \geqslant 1$ there exist only finitely many non-zero ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathrm{Nm}(\mathfrak{a}) \leqslant N$.

Proposition 3.3.4: For any two non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ we have

$$\mathrm{Nm}(\mathfrak{a}\mathfrak{b}) = \mathrm{Nm}(\mathfrak{a}) \cdot \mathrm{Nm}(\mathfrak{b}).$$

Let J_K denote the group of fractional ideals of $\mathcal{O}_K$.

Corollary 3.3.5: The absolute norm extends to a unique homomorphism

$$\mathrm{Nm}\colon J_K \longrightarrow (\mathbb{Q}^{>0}, \cdot).$$

3.4 Real and complex embeddings

Throughout the following we abbreviate $\Sigma := \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and set

$$\begin{aligned} r &:= \text{ the number of } \sigma \in \Sigma \text{ with } \sigma(K) \subset \mathbb{R}, \\ s &:= \text{ the number of } \sigma \in \Sigma \text{ with } \sigma(K) \not\subset \mathbb{R}, \text{ up to complex conjugation.} \end{aligned}$$

Proposition 3.4.1: We have $r + 2s = n$.

Proposition 3.4.2: We have ring isomorphisms

$$\begin{array}{ccl} K \otimes_{\mathbb{Q}} \mathbb{C} & \xrightarrow{\ \sim\ } & K_{\mathbb{C}} := \prod_{\sigma \in \Sigma} \mathbb{C}, \\ \cup & & \cup \\ K \otimes_{\mathbb{Q}} \mathbb{R} & \xrightarrow{\ \sim\ } & K_{\mathbb{R}} := \big\{ (z_\sigma)_\sigma \in K_{\mathbb{C}} \ \big|\ \forall \sigma \in \Sigma\colon z_{\bar\sigma} = \bar z_\sigma \big\}. \\ & & \\ x \otimes z & \longmapsto & (\sigma(x)z)_\sigma. \end{array}$$

The map $x \mapsto x \otimes 1$ induces an embdding $j\colon K \hookrightarrow K_{\mathbb{R}}$.

Proposition 3.4.3: For every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the image $j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$.

To describe this with more explicit coordinates we let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \ldots, \sigma_n$ the non-real embeddings such that $\bar\sigma_{r+j} = \bar\sigma_{r+j+s}$ for all $1 \leqslant j \leqslant s$.

Proposition 3.4.4: We have an isomorphism of $\mathbb{R}$-vector spaces

$$K_{\mathbb{R}} \xrightarrow{\ \sim\ } \mathbb{R}^n,\ (z_\sigma)_\sigma \longmapsto \big(z_{\sigma_1}, \ldots, z_{\sigma_r}, \mathrm{Re}\, z_{\sigma_{r+1}}, \ldots, \mathrm{Re}\, z_{\sigma_{r+s}}, \mathrm{Im}\, z_{\sigma_{r+1}}, \ldots, \mathrm{Im}\, z_{\sigma_{r+s}}\big).$$

3.5 Quadratic number fields

Proposition 3.5.1: The quadratic number fields are precisely the splitting fields of the poiynomials $X^2 - d$ for all squarefree integers $d \in \mathbb{Z} \setminus \{0, 1\}$.

Convention 3.5.2: For any positive integer d we let $\sqrt{d}$ be the positive real square root of d. For any negative integer d we uncanonically *choose* a square root $\sqrt{d}$ in $i\mathbb{R}$.

Proposition 3.5.2: For d as above and $K = \mathbb{Q}(\sqrt{d})$ we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod (4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod (4) \end{cases}$$

and

$$d_K = \begin{cases} 4d & \text{if } d \equiv 2, 3 \bmod (4), \\ d & \text{if } d \equiv 1 \bmod (4) \end{cases}$$

Corollary 3.5.4: The integer d is uniquely determined by K, namely as the squarefree part of d_K.

Remark 3.5.5: The possible discriminants of quadratic number fields are sometimes called *fundamental discriminants*. As the discriminant is somewhat more canonically associated to K than the number d, some authors prefer to write $K = \mathbb{Q}(\sqrt{d_K})$.

Definition 3.5.6: We have the following cases:

(a) If $d > 0$, there exist precisely two distinct embeddings $\sigma_1, \sigma_2 \colon K \hookrightarrow \mathbb{R}$ and we call K *real quadratic*. In this case we obtain a natural embedding

$$(\sigma_1, \sigma_2) \colon K \hookrightarrow \mathbb{R}^2.$$

(b) If $d < 0$, there exist precisely two distinct embeddings $\sigma, \bar{\sigma} \colon K \hookrightarrow \mathbb{C}$ that are conjugate under complex conjugation, and we call K *imaginary quadratic*. In this case we obtain a natural embedding

$$\sigma \colon K \hookrightarrow \mathbb{C}.$$

3.6 Cyclotomic fields

Fix an integer $n \geqslant 1$.

Definition 3.6.1: (a) An element $\zeta \in \mathbb{C}$ with $\zeta^n = 1$ is called an *n-th root of unity.*

(b) An element $\zeta \in \mathbb{C}^\times$ of precise order n is called a *primitive n-th root of unity.*

Proposition 3.6.2: The n-th roots of unity form a cyclic subgroup $\mu_n \subset \mathbb{C}^\times$, which is generated by any primitive n-th root of unity, for instance by $e^{\frac{2\pi i}{n}}$.

For the following we fix a primitive n-th root of unity ζ and set $K := \mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta)$.

Proposition 3.6.3: (a) An integral power ζ^a has order n if and only if $\gcd(a,n)=1$.

(b) For any such a we have $\frac{1-\zeta^a}{1-\zeta}\in\mathcal{O}_K^\times$.

Definition 3.6.4: The *n-th cyclotomic polynomial* Φ_n is the monic polynomial of degree $\varphi(n):=|(\mathbb{Z}/n\mathbb{Z})^\times|$ with the simple roots μ_n.

Theorem 3.6.5: The polynomial Φ_n is an irreducible element of $\mathbb{Z}[X]$.

Theorem 3.6.6: The extension $K/\mathbb{Q}$ is finite galois of degree $\varphi(n)$ and there is a natural isomorphism $e\colon \operatorname{Gal}(K/\mathbb{Q})\xrightarrow{\sim}(\mathbb{Z}/n\mathbb{Z})^\times$ with the property

$$\forall\gamma\in\operatorname{Gal}(K(\mu_n)/K)\colon\ \gamma(\zeta)=\zeta^{e(\gamma)}.$$

Theorem 3.6.7: If $n=\ell^\nu$ for a prime ℓ and an integer $\nu\geqslant 1$, then:

(a) The ideal $(1-\zeta)$ of $\mathcal{O}_K$ satisfies $(1-\zeta)^{\ell^{\nu-1}(\ell-1)}=(\ell)$.

(b) $\mathcal{O}_K=\mathbb{Z}[\zeta]\cong\mathbb{Z}[X]/(\Phi_{\ell^\nu})$.

(c) $\operatorname{disc}(\mathcal{O}_K)=\pm\ell^{\ell^{\nu-1}(\nu\ell-\nu-1)}$.

Theorem 3.6.8: For arbitrary n we have:

(a) $\mathcal{O}_K=\mathbb{Z}[\zeta]$.

(b) The discriminant $\operatorname{disc}(\mathcal{O}_K)\in\mathbb{Z}$ is divisible precisely by the primes dividing n.

3.7 Quadratic Reciprocity

Fix an odd prime ℓ and set $K:=\mathbb{Q}(\mu_\ell)$ and $\zeta:=e^{\frac{2\pi i}{n}}$.

Proposition 3.7.1: The unique subfield of K of degree 2 over $\mathbb{Q}$ is $K':=\mathbb{Q}(\sqrt{\ell^*}\,)$ for $\ell^*:=(-1)^{\frac{\ell-1}{2}}\ell$.

Definition 3.7.2: The *Legendre symbol* of an integer a with respect to ℓ is

$$\left(\frac{a}{\ell}\right) := \begin{cases} 0 & \text{if } a\equiv 0 \bmod (\ell),\\ +1 & \text{if } a\equiv b^2 \bmod (\ell) \text{ for some } b\in\mathbb{Z}\smallsetminus\ell\mathbb{Z},\\ -1 & \text{otherwise.}\end{cases}$$

Proposition 3.7.3: For any integers a,b we have:

(a) $(\frac{a}{\ell})=(\frac{b}{\ell})$ whenever $a\equiv b \bmod (\ell)$.

(b) $(\frac{a}{\ell})\equiv a^{\frac{\ell-1}{2}} \bmod (\ell)$.

(c) $(\frac{ab}{\ell})=(\frac{a}{\ell})(\frac{b}{\ell})$.

(d) $(\frac{-1}{\ell})=(-1)^{\frac{\ell-1}{2}}$.

Definition 3.7.4: The *Gauss sum* associated to the prime ℓ is $g_\ell := \sum_{a=1}^{\ell-1} (\frac{a}{\ell}) \cdot \zeta^a$.

Proposition 3.7.5: The Gauss sum satisfies $g_\ell^2 = \ell^*$.

Proposition 3.7.6: For any distinct odd primes ℓ, p we have $(\frac{\ell^*}{p}) = (\frac{p}{\ell})$.

Theorem 3.7.7: *(Gauss Quadratic Reciprocity Law)*

(a) For any distinct odd primes ℓ, p we have $(\frac{\ell}{p})(\frac{p}{\ell}) = (-1)^{\frac{(p-1)(\ell-1)}{4}}$.

(b) For any odd prime ℓ we have $(\frac{-1}{\ell}) = (-1)^{\frac{\ell-1}{2}}$.

(c) For any odd prime ℓ we have $(\frac{2}{\ell}) = (-1)^{\frac{\ell^2-1}{8}}$.

4 Additive Minkowski theory

4.1 Euclidean embedding

We endow $K_{\mathbb{C}} := \mathbb{C}^\Sigma$ with the standard hermitian scalar product

$$\big\langle (z_\sigma)_\sigma, (w_\sigma)_\sigma \big\rangle \ := \ \sum_{\sigma\in\Sigma} \bar{z}_\sigma w_\sigma.$$

Proposition 4.1.1: Its restriction to $K_{\mathbb{R}} \times K_{\mathbb{R}}$ has values in $\mathbb{R}$ and turns $K_{\mathbb{R}}$ into a euclidean vector space.

Proposition 4.1.2: Under the isomorphism of Proposition 3.4.2 this scalar product on $K_{\mathbb{R}}$ corresponds to the following scalar product on $\mathbb{R}^n$:

$$\big\langle (x_j)_j, (y_j)_j \big\rangle \ := \ \sum_{i=1}^{r} x_j y_j + \sum_{i=r+1}^{n} 2x_j y_j.$$

4.2 Lattice bounds

Proposition 4.2.1: For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ we have

$$\mathrm{vol}(K_{\mathbb{R}}/j(\mathfrak{a})) \ = \ \sqrt{\mathrm{disc}(\mathfrak{a})} \ = \ \mathrm{Nm}(\mathfrak{a}) \cdot \sqrt{|d_K|}.$$

Theorem 4.2.2: Consider a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ and positive real numbers c_σ for all $\sigma \in \Sigma$ such that

$$\prod_{\sigma\in\Sigma} c_\sigma \ > \ (\tfrac{2}{\pi})^s \cdot \sqrt{|d_K|} \cdot \mathrm{Nm}(\mathfrak{a}).$$

Then there exists an element $a \in \mathfrak{a} \setminus \{0\}$ with the property

$$\forall \sigma \in \Sigma\colon\ |\sigma(a)| < c_\sigma.$$

4.3 Finiteness of the class group

Theorem 4.3.1: For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ there exists an element $a \in \mathfrak{a} \setminus \{0\}$ with

$$|\,\mathrm{Nm}_{K/\mathbb{Q}}(a)| \ \leqslant \ (\tfrac{2}{\pi})^s \cdot \sqrt{|d_K|} \cdot \mathrm{Nm}(\mathfrak{a}).$$

Proposition 4.3.2: Every ideal class in $\mathrm{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subset \mathcal{O}_K$ with

$$\mathrm{Nm}(\mathfrak{a}) \ \leqslant \ (\tfrac{2}{\pi})^s \cdot \sqrt{|d_K|}.$$

Theorem 4.3.3: The class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite.

4.4 Discriminant bounds

Theorem 4.4.1: For any n and c there exist at most finitely many number fields $K/\mathbb{Q}$ of degree n and with $|d_K| \leqslant c$.

Theorem 4.4.2: For any number field K of degree n over $\mathbb{Q}$ we have

$$\sqrt{|d_K|} \;\geqslant\; \frac{n^n}{n!} \cdot \Big(\frac{\pi}{4}\Big)^{n/2}.$$

Theorem 4.4.3: *(Hermite)* For any c there exist at most finitely many number fields $K/\mathbb{Q}$ with $|d_K| \leqslant c$.

Theorem 4.4.4: *(Minkowski)* For any number field $K \neq \mathbb{Q}$ we have $|d_K| > 1$.

5 Multiplicative Minkowski theory

5.1 Roots of unity

Lemma 5.1.1: We have a short exact sequence

$$\begin{array}{ccccccccc} 1 \longrightarrow (S^1)^\Sigma \longrightarrow K_\mathbb{C}^\times & = & (\mathbb{C}^\times)^\Sigma & \xrightarrow{\ \ell\ } & \mathbb{R}^\Sigma \longrightarrow 0, \\ & & (z_\sigma)_\sigma & \longmapsto & (\log|z_\sigma|)_\sigma. \end{array}$$

Let $\mu(K)$ denote the group of elements of finite order in $K^\times$.

Proposition 5.1.2: The group $\mu(K)$ is a finite subgroup of $\mathcal{O}_K^\times$ and we have a short exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \longrightarrow \Gamma := \ell(\mathcal{O}_K^\times) \longrightarrow 0.$$

Proposition 5.1.3: The group $\mu(K)$ is cyclic of even order.

Example 5.1.4: For any squarefree $d \in \mathbb{Z} \smallsetminus \{1\}$ we have

$$\mu(\mathbb{Q}(\sqrt{d})) \ = \ \begin{cases} \text{cyclic of order 6 if } d = -3, \\ \text{cyclic of order 4 if } d = -1, \\ \text{cyclic of order 2 otherwise.} \end{cases}$$

5.2 Units

Lemma 5.2.1: The group Γ is a lattice in $\mathbb{R}^\Sigma$.

Consider the homomorphisms

$$\begin{array}{lrl} \mathrm{Nm}\colon & K_\mathbb{C}^\times = (\mathbb{C}^\times)^\Sigma \longrightarrow \mathbb{C}^\times, & (z_\sigma)_\sigma \longmapsto \prod_{\sigma\in\Sigma} z_\sigma \\ \mathrm{Tr}\colon & (\mathbb{R}^\times)^\Sigma \longrightarrow \mathbb{R}, & (t_\sigma)_\sigma \longmapsto \sum_{\sigma\in\Sigma} t_\sigma \end{array}$$

Lemma 5.2.2: We have a commutative diagram

$$\begin{array}{ccccccc} \mathcal{O}_K^\times & \hookrightarrow & K^\times & \overset{j}{\hookrightarrow} & (K_\mathbb{C})^\times & \overset{\ell}{\twoheadrightarrow} & \mathbb{R}^\Sigma \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \{\pm1\} & \hookrightarrow & \mathbb{Q}^\times & \hookrightarrow & \mathbb{C}^\times & \overset{\log|\ |}{\twoheadrightarrow} & \mathbb{R} \end{array}$$

Consider the $\mathbb{R}$-subspaces

$$\begin{array}{ccl} (\mathbb{R}^\Sigma)^+ & := & \big\{(t_\sigma)_\sigma \in \mathbb{R}^\Sigma \bigm| \forall\sigma\colon t_{\bar\sigma} = t_\sigma\big\}, \\ H & := & \ker\big(\mathrm{Tr}\colon (\mathbb{R}^\Sigma)^+ \to \mathbb{R}. \end{array}$$

Lemma 5.2.3: We have $\Gamma \subset H$ and $\dim_\mathbb{R}(H) = r + s - 1$.

5.3 Dirichlet's unit theorem

Theorem 5.3.1: The group Γ is a complete lattice in H.

Theorem 5.3.2: The group $\mathcal{O}_K^\times$ is isomorphic to $\mu(K) \times \mathbb{Z}^{r+s-1}$.

Caution 5.3.3: The isomorphism is uncanonical.

Corollary 5.3.4: The group $\mathcal{O}_K^\times$ is finite if and only if K is $\mathbb{Q}$ or imaginary quadratic.

Corollary 5.3.5: The group $\mathcal{O}_K^\times$ has $\mathbb{Z}$-rank 1 if and only if $(r,s) \in \big\{(2,0),(1,1),(0,2)\big\}$. In that case we have

$$\mathcal{O}_K^\times \;=\; \mu(K) \times \varepsilon^{\mathbb{Z}}$$

for some unit ε of infinite order.

Definition 5.3.6: Any choice of such ε is then called a *fundamental unit*.

5.4 The real quadratic case

Suppose that $K = \mathbb{Q}(\sqrt{d})$ for a squarefree $d > 1$ and choose an embedding $K \hookrightarrow \mathbb{R}$.

Fact 5.4.1: There is a unique choice of fundamental unit $\varepsilon > 1$.

Proposition 5.4.2: If $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, then

(a) $\mathcal{O}_K^\times = \big\{a + b\sqrt{d} \;\big|\; a,b \in \mathbb{Z},\ a^2 - b^2 d = \pm 1\big\}$.

(b) $\mathcal{O}_K^\times \cap \mathbb{R}^{>1} = \big\{a + b\sqrt{d} \;\big|\; a,b \in \mathbb{Z},\ a^2 - b^2 d = \pm 1,\ a,b > 0\big\}$.

(c) The fundamental unit $\varepsilon > 1$ is the element $a + b\sqrt{d} \in \mathcal{O}_K^\times \cap \mathbb{R}^{>1}$ as in (b) with the smallest value for a, or equivalently for b.

Theorem 5.4.3: For any squarefree integer $d > 1$ there are infinitely many solutions $(a,b) \in \mathbb{Z}^2$ of the diophantine equation $a^2 - b^2 d = 1$.

Remark 5.4.4: The equation $a^2 - b^2 d = -1$ may or may not have a solution $(a,b) \in \mathbb{Z}^2$.

Proposition 5.4.5: The fundamental unit $\varepsilon > 1$ of K with discriminant D satisfies

$$\varepsilon \;>\; \frac{\sqrt{D} + \sqrt{D-4}}{2} \;>\; 1.$$

Consequently, if some unit of infinite order $u > 1$ is known, we have $u = \varepsilon^k$ for some $1 \leqslant k \leqslant \log(u)/\log((\sqrt{D} + \sqrt{D-4})/2)$ and one can efficiently find ε.

Remark 5.4.6: One can effectively find ε using continued fractions.

References

- Atiyah, M. F., MacDonald, I. G.: *Introduction to Commutative Algebra*, Westview Press, 1969.
- Hungerford, T.W.: *Algebra.* Springer 1974
- Neukirch, Jürgen: *Algebraic Number Theory.* Springer 1999.

Change Log:

Version of 06.10.2023:

6. 10. 2023: Some typos in §2.1–2 corrected and Sections 3.6–7 added.