Number Theory I und II

Prof. Richard Pink

Summary
Fall Semester 2023
Spring Semester 2024
ETH Zürich

Preliminary Version

January 21, 2024

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

Content

Part I

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 $S \subset A \smallsetminus \{0\}$ 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

$$S^{-1}A \;:=\; \left\{ \tfrac{a}{s} \;\middle|\; a \in A,\ s \in S \right\}$$

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 $A \smallsetminus \mathfrak{p}$ is multiplicative. The ring $A_{\mathfrak{p}} := (A \smallsetminus \mathfrak{p})^{-1}A$ 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 $(A \smallsetminus \{0\})^{-1}B = L$.

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 $\operatorname{disc}(b_1, \ldots, b_n) \in A \smallsetminus \{0\}$ 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

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

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

(c) $\mathfrak{ab} = \mathfrak{ba}$ and $(\mathfrak{ab})\mathfrak{c} = \mathfrak{a}(\mathfrak{bc})$ 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 $a, b \in A \smallsetminus \{0\}$ 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

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

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 $v_1, \dots, v_n$ 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 $v_1, \dots, v_m$.

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 $v_1, \dots, v_n$ 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 $v_1, \dots, v_n$ of V, a fundamental domain is:

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

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 $(e_1, \dots, e_n)$ of V we have

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

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

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

and

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

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 $n := [K/\mathbb{Q}]$.

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 $(x_1, \dots, x_n)$ the following value depends only on Γ:

$$\operatorname{disc}(\Gamma) := \operatorname{disc}(x_1, \dots, x_n) \in \mathbb{Q}^\times.$$

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

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

(c) For any $\mathbb{Z}$-submodule $\Gamma \subset \mathcal{O}_K$ of rank n we have $\operatorname{disc}(\Gamma) \in \mathbb{Z} \smallsetminus \{0\}$.

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 $a_1, \dots, a_n \in \mathcal{O}_K$ such that $\operatorname{disc}(a_1, \dots, a_n)$ is square-free, then

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

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 $a \in \mathcal{O}_K \smallsetminus \{0\}$ we have $\mathrm{Nm}((a)) = |\mathrm{Nm}_{K/\mathbb{Q}}(a)|$.

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

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

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 $\sigma_1, \dots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \dots, \sigma_n$ the non-real embeddings such that $\bar\sigma_{r+j} = \sigma_{r+j+s}$ for all $1 \leqslant j \leqslant s$.

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

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

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 $d \in \mathbb{Z} \smallsetminus \{0, 1\}$.

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) If $n \geqslant 2$, then for any such a we have $\frac{1-\zeta^a}{1-\zeta} \in \mathcal{O}_K^\times$. *(Cyclotomic units)*

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 primitive n-th roots of unity as simple roots.

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 $e\colon \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$ with the property

$$\forall \gamma \in \mathrm{Gal}(K/\mathbb{Q})\colon\ \gamma(\zeta) = \zeta^{e(\gamma)}.$$

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

(a) We have $\Phi_{\ell^\nu}(X) = \sum_{i=0}^{\ell-1} X^{i\ell^{\nu-1}}$.

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

(c) The ideal $(1-\zeta)$ is the unique prime ideal of $\mathcal{O}_K$ above $(\ell) \subset \mathbb{Z}$ and has the residue field $\mathcal{O}_K/(1-\zeta) \cong \mathbb{F}_\ell$.

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

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

Theorem 3.6.8: For arbitrary n we have:

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

(b) The discriminant $\mathrm{disc}(\mathcal{O}_K) \in \mathbb{Z}$ 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 $\zeta := e^{\frac{2\pi i}{\ell}}$.

Definition 3.7.1: The *Legendre symbol* of an integer a with respect to ℓ is

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

In the first two cases a is called a *quadratic residue*, otherwise a *quadratic non-residue modulo* (ℓ).

Proposition 3.7.2: 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 3.7.3: The *Gauss sum* associated to the prime ℓ is $g_\ell := \sum_{a=1}^{\ell-1} (\frac{a}{\ell}) \cdot \zeta^a$.

Proposition 3.7.4: The Gauss sum satisfies $g_\ell^2 = \ell^* := (-1)^{\frac{\ell-1}{2}} \ell$.

Proposition 3.7.5: The unique subfield of K of degree 2 over $\mathbb{Q}$ is $K' := \mathbb{Q}(\sqrt{\ell^*})$.

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 $(\frac{-1}{\ell}) = (-1)^{\frac{\ell-1}{2}}$. *(First supplement)*

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

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 3.4.4 this scalar product on $K_{\mathbb{R}}$ corresponds to the following scalar product on $\mathbb{R}^n$:

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

4.2 Lattice bounds

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

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

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 $c_{\bar\sigma} = c_\sigma$ and

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

Then there exists an element $a \in \mathfrak{a} \smallsetminus \{0\}$ 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 $a \in \mathfrak{a} \smallsetminus \{0\}$ with

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

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

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

Set $\Gamma := \ell(\mathcal{O}_K^\times)$ and 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

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

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

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

Lemma 5.2.2: We have a commutative diagram

$$\begin{array}{ccccccc} \mathcal{O}_K^\times & \hookrightarrow & K^\times & \xhookrightarrow{\ j\ } & (K_{\mathbb{C}})^\times & \xrightarrow{\ \ell\ } & \mathbb{R}^\Sigma \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \{\pm 1\} & \hookrightarrow & \mathbb{Q}^\times & \hookrightarrow & \mathbb{C}^\times & \xrightarrow{\ \log|\ |\ } & \mathbb{R} \end{array}$$

Consider the $\mathbb{R}$-subspaces

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

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 $(a,b) \in \mathbb{Z}^2$. But if it has a solution, it has infinitely many.

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

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

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.

6 Extensions of Dedekind rings

6.1 Modules over Dedekind rings

Let A be a Dedekind ring with quotient field K.

Definition 6.1.1: Consider an A-module M.

(a) An element $m \in M$ is called *torsion* if there exists $a \in A \smallsetminus \{0\}$ such that $am = 0$.

(b) The module M is called *torsion* if every element of M is torsion.

(c) The module M is called *torsion-free* if no non-zero element of M is torsion.

Theorem 6.1.2: Any finitely generated A-module is isomorphic to the direct sum of a torsion module and a torsion-free module.

Theorem 6.1.3: Any non-zero finitely generated torsion-free A-module is isomorphic to $\mathfrak{a} \oplus A^{r-1}$ for a non-zero ideal $\mathfrak{a} \subset A$ and an integer $r \geqslant 1$.

Theorem 6.1.4: Any finitely generated torsion A-module is isomorphic to

(a) $\bigoplus_{i=1}^{r} A/\mathfrak{p}_i^{e_i}$ for $r \geqslant 0$ and maximal ideals $\mathfrak{p}_i \subset A$ and integral exponents $e_i \geqslant 1$.

(b) $\bigoplus_{i=1}^{s} A/\mathfrak{a}_i$ for $s \geqslant 0$ and non-zero ideals $\mathfrak{a}_s \subset \ldots \subset \mathfrak{a}_1 \subsetneqq A$.

Proposition 6.1.5: Consider a K-vector space V of finite dimension n and a finitely generated A-submodule $M \subset V$ that generates V over K. Then M is isomorphic to a direct sum of n fractional ideals of A.

Proposition 6.1.6: For any fractional ideals $\mathfrak{a}, \mathfrak{b}$ of A there is a natural isomorphism

$$\mathfrak{b}\mathfrak{a}^{-1} \xrightarrow{\sim} \mathrm{Hom}_A(\mathfrak{a}, \mathfrak{b}), \quad c \mapsto (\varphi_c \colon a \mapsto ca).$$

6.2 Decomposition of prime ideals

For the rest of this chapter we take a finite separable field extension L/K of degree n. Then the integral closure B of A in L is a finitely generated A-module that generates L as a K-vector space and is a Dedekind ring. We abbreviate the residue field at any maximal ideal $\mathfrak{p} \subset A$ by $k(\mathfrak{p}) := A/\mathfrak{p}$, and likewise for any maximal ideal of B. Where applicable we let C be the integral closure of B in a finite separable extension M/L.

Consider a maximal ideal $\mathfrak{p} \subset A$. Throughout the following we impose the

Assumption 6.2.1: The residue field $k(\mathfrak{p})$ is perfect.

Note that $\mathfrak{p}B$ is a non-zero ideal of B and therefore has a unique prime factorization

$$\mathfrak{p}B \;=\; \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

with distinct maximal ideals $\mathfrak{q}_i \subset B$ and integral exponents $e_i \geqslant 1$.

Proposition 6.2.2: (a) The ideals $\mathfrak{q}_i$ are precisely the prime ideals of B above $\mathfrak{p}$.

(b) For each i the residue field $k(\mathfrak{q}_i)$ is a finite extension of the residue field $k(\mathfrak{p})$.

(c) Letting f_i denote the degree of this residue field extension, we have

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

Definition 6.2.3:

(a) The number $e_{\mathfrak{q}_i|\mathfrak{p}} := e_i$ is called the *ramification degree of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$.

(b) The number $f_{\mathfrak{q}_i|\mathfrak{p}} := f_i$ is called the *inertia degree of* $\mathfrak{q}_i$ *over* $\mathfrak{p}$.

(c) We call $\mathfrak{q}_i$ *unramified over* $\mathfrak{p}$ if $e_i = 1$.

(d) We call $\mathfrak{q}_i$ *ramified over* $\mathfrak{p}$ if $e_i > 1$.

Definition 6.2.4:

(a) We call $\mathfrak{p}$ *unramified in* B if all $e_i = 1$, that is, if $\mathfrak{p}B = \mathfrak{q}_1 \cdots \mathfrak{q}_r$.

(b) We call $\mathfrak{p}$ *ramified in* B if some $e_i > 1$.

(c) We call $\mathfrak{p}$ *totally split in* B if all $e_i = f_i = 1$, that is, if $r = n$ and $\mathfrak{p}B = \mathfrak{q}_1 \cdots \mathfrak{q}_n$.

(d) We call $\mathfrak{p}$ *totally inert in* B if $r = e_1 = 1$, that is, if $\mathfrak{p}B$ is prime.

(e) We call $\mathfrak{p}$ *totally ramified in* B if $r = f_1 = 1$, that is, if $\mathfrak{p}B = \mathfrak{q}^n$ for a prime $\mathfrak{q} \subset B$.

Proposition 6.2.5: Suppose that $B = A[\beta]$ and let $f \in A[X]$ be the minimal polynomial of β above K. Set $\bar{f} := f \bmod \mathfrak{p}$ and write $\bar{f} = \prod_{i=1}^{r} \bar{f}_i^{e_i}$ with inequivalent irreducible factors $\bar{f}_i \in k(\mathfrak{p})[X]$ and integral exponents $e_i \geqslant 1$. Choose $f_i \in A[X]$ with $\bar{f}_i = f_i \bmod \mathfrak{p}$. Then $\mathfrak{p}B = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ with distinct prime ideals $\mathfrak{q}_i := \mathfrak{p}B + f_i(\beta)B$.

Example 6.2.6: Take $L = \mathbb{Q}(\sqrt{d}\,)$ with $d \in \mathbb{Z} \smallsetminus \{1\}$ squarefree. Then an odd prime p of $\mathbb{Z}$ with

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{is (totally) ramified in } \mathcal{O}_L, \\ 1 & \text{is (totally) decomposed in } \mathcal{O}_L, \\ -1 & \text{is (totally) inert in } \mathcal{O}_L. \end{cases}$$

Proposition 6.2.7: For any a prime $\mathfrak{r} \subset C$ above $\mathfrak{q} \subset B$ above $\mathfrak{p} \subset A$ we have

$$e_{\mathfrak{r}|\mathfrak{p}} = e_{\mathfrak{r}|\mathfrak{q}} \cdot e_{\mathfrak{q}|\mathfrak{p}} \qquad \text{and} \qquad f_{\mathfrak{r}|\mathfrak{p}} = f_{\mathfrak{r}|\mathfrak{q}} \cdot f_{\mathfrak{q}|\mathfrak{p}}.$$

6.3 Decomposition group

From now until §6.5 we assume in addition that L/K is galois with Galois group Γ.

Lemma 6.3.1: For any prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and any ideal $\mathfrak{a}$ of a ring we have

$$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i \quad \Longleftrightarrow \quad \exists\, i \colon \mathfrak{a} \subset \mathfrak{p}_i.$$

Theorem 6.3.2: (a) The group Γ acts on B and on the set of prime ideals of B.

(b) The group Γ acts transitively on the set of prime ideals $\mathfrak{q} \subset B$ above $\mathfrak{p}$.

Definition 6.3.3: The stabilizer of $\mathfrak{q}$ is called the *decomposition group of* $\mathfrak{q}$:

$$\Gamma_{\mathfrak{q}} := \big\{\gamma \in \Gamma \;\big|\; \forall x \in \mathfrak{q}\colon {}^{\gamma}x \in \mathfrak{q}\big\}.$$

Proposition 6.3.4:

(a) The numbers $e := e_{\mathfrak{q}|\mathfrak{p}}$ and $f := f_{\mathfrak{q}|\mathfrak{p}}$ depend only on $\mathfrak{p}$.

(b) We have $\mathfrak{p}B = \prod_{[\gamma]\in\Gamma/\Gamma_{\mathfrak{q}}} {}^{\gamma}\mathfrak{q}^{e}$.

(c) We have $n = r \cdot e \cdot f$.

(d) For any $\gamma \in \Gamma$ we have $\Gamma_{{}^{\gamma}\mathfrak{q}} = {}^{\gamma}\Gamma_{\mathfrak{q}}$.

Proposition 6.3.5:

(a) We have $\Gamma_{\mathfrak{q}} = 1$ if and only if $\mathfrak{p}$ is totally split in B.

(b) We have $\Gamma_{\mathfrak{q}} = \Gamma$ if and only if there is a unique prime $\mathfrak{q} \subset B$ above $\mathfrak{p}$.

Proposition 6.3.6: Set $L' := L^{\Gamma_{\mathfrak{q}}}$ and $B' := B \cap L'$ and $\mathfrak{q}' := \mathfrak{q} \cap B'$.

(a) Then $\mathfrak{q}$ is the unique prime of B above $\mathfrak{q}'$ and $\mathfrak{q}'B = \mathfrak{q}^{e}$.

(b) We have $e_{\mathfrak{q}|\mathfrak{q}'} = e$ and $f_{\mathfrak{q}|\mathfrak{q}'} = f$ and $e_{\mathfrak{q}'|\mathfrak{p}} = f_{\mathfrak{q}'|\mathfrak{p}} = 1$.

6.4 Inertia group

Next $\Gamma_{\mathfrak{q}}$ acts on the residue field $k(\mathfrak{q}) := B/\mathfrak{q}$ by a natural homomorphism

$$\Gamma_{\mathfrak{q}} \longrightarrow \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p})).$$

Definition 6.4.1: Its kernel is called the *inertia group of* $\mathfrak{q}$:

$$I_{\mathfrak{q}} := \big\{\gamma \in \Gamma \;\big|\; \forall x \in B\colon {}^{\gamma}x \equiv x \bmod \mathfrak{q}\big\}.$$

Proposition 6.4.2: The extension $k(\mathfrak{q})/k(\mathfrak{p})$ is finite galois and the above homomorphism induces an isomorphism $\Gamma_{\mathfrak{q}}/I_{\mathfrak{q}} \cong \mathrm{Aut}(k(\mathfrak{q})/k(\mathfrak{p}))$.

Proposition 6.4.3: Set $L'' := L^{I_{\mathfrak{q}}}$ and $B'' := B \cap L''$ and $\mathfrak{q}'' := \mathfrak{q} \cap B''$.

(a) Then $\mathfrak{q}'B'' = \mathfrak{q}''$ and $\mathfrak{q}''B = \mathfrak{q}^{e}$.

(b) We have $|I_{\mathfrak{q}}| = e$ and $[\Gamma_{\mathfrak{q}}\colon I_{\mathfrak{q}}] = f$ and $[\Gamma : \Gamma_{\mathfrak{q}}] = r$.

(c) We have $e_{\mathfrak{q}|\mathfrak{q}''} = e$ and $f_{\mathfrak{q}|\mathfrak{q}''} = e_{\mathfrak{q}''|\mathfrak{q}'} = 1$ and $f_{\mathfrak{q}''|\mathfrak{q}'} = f$.

6.5 Frobenius

Keeping L/K galois with group Γ, we now assume that $k(\mathfrak{p})$ is finite. Then $k(\mathfrak{q})/k(\mathfrak{p})$ is finite galois, and its Galois group is generated by the Frobenius automorphism $x \mapsto x^{|k(\mathfrak{p})|}$.

Proposition 6.5.1: (a) There exists $\gamma \in \Gamma_\mathfrak{q}$ that acts on $k(\mathfrak{q})$ through $x \mapsto x^{|k(\mathfrak{p})|}$.

(b) The coset $\gamma I_\mathfrak{q}$ is uniquely determined by $\mathfrak{q}$.

Definition 6.5.2: Any such γ is called a *Frobenius substitution at* $\mathfrak{q}$ and denoted by $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$.

Proposition 6.5.3: If $\mathfrak{q}$ is unramified over $\mathfrak{p}$, then in addition:

(a) The element $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ is uniquely determined by $\mathfrak{q}$.

(c) The conjugacy class of $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ in Γ is uniquely determined by $\mathfrak{p}$.

(d) If Γ is abelian, then $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}}$ is uniquely determined by $\mathfrak{p}$.

Caution 6.5.4: Do not confuse the Frobenius substitution $\mathrm{Frob}_{\mathfrak{q}|\mathfrak{p}} \in \Gamma_\mathfrak{q}$ with the Frobenius automorphism $x \mapsto x^{|k(\mathfrak{p})|}$ of $k(\mathfrak{q})$.

Example 6.5.5: Consider the cyclotomic field $L := \mathbb{Q}(\mu_n)$ for $n \not\equiv 2 \bmod (4)$.

(a) A rational prime p is ramified in $\mathcal{O}_L$ if and only if $p|n$.

(b) For any $p \nmid n$ the Frobenius substitution at p corresponds to the residue class of p under the isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

(c) A rational prime p is totally split in $\mathcal{O}_L$ if and only if $p \equiv 1 \bmod (n)$.

(d) If $n = p^\nu$ for a prime p, then p is totally ramified in $\mathcal{O}_L$.

6.6 Relative norm

Now we return to the situation that L/K is finite separable of degree n.

Definition 6.6.1: The *relative norm* of a fractional ideal $\mathfrak{b}$ of B is the A-submodule

$$\mathrm{Nm}_{L/K}(\mathfrak{b}) \;:=\; \big(\{\mathrm{Nm}_{L/K}(y) \mid y \in \mathfrak{b}\}\big) \;\subset\; K.$$

Proposition 6.6.2:

(a) This is a fractional ideal of A.

(b) If $\mathfrak{b} \subset B$ then $\mathrm{Nm}_{L/K}(\mathfrak{b}) \subset \mathfrak{b} \cap A$.

(c) For any $y \in L^\times$ we have $\mathrm{Nm}_{L/K}((y)) = (\mathrm{Nm}_{L/K}(y))$.

Proposition 6.6.3: For any two fractional ideals $\mathfrak{b}, \mathfrak{b}'$ of B we have

$$\mathrm{Nm}_{L/K}(\mathfrak{b}\mathfrak{b}') \;=\; \mathrm{Nm}_{L/K}(\mathfrak{b}) \cdot \mathrm{Nm}_{L/K}(\mathfrak{b}').$$

Proposition 6.6.4: For any fractional ideal $\mathfrak{c}$ of C we have

$$\mathrm{Nm}_{L/K}(\mathrm{Nm}_{M/L}(\mathfrak{c})) \;=\; \mathrm{Nm}_{M/K}(\mathfrak{c}).$$

Proposition 6.6.5: For any fractional ideal $\mathfrak{a}$ of A we have $\mathrm{Nm}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^n$.

Proposition 6.6.6: For any prime $\mathfrak{q} \subset B$ above $\mathfrak{p} \subset A$ we have $\mathrm{Nm}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}|\mathfrak{p}}}$.

6.7 Different

Recall from Proposition 1.7.1 that we have the non-degenerate symmetric K-bilinear form

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

Proposition 6.7.1: The subset

$$\mathfrak{d} \;:=\; \big\{ x \in L \;\big|\; \forall y \in B\colon\ \mathrm{Tr}_{L/K}(xy) \in A \big\}$$

is a fractional ideal of B which contains B.

Definition 6.7.2: The ideal $\mathrm{diff}_{B/A} := \mathfrak{d}^{-1} \subset B$ is called the *different of B over A*.

Proposition 6.7.3: Suppose that $B = A[\beta]$ and let $f \in A[X]$ be the minimal polynomial of β above K. Then $\mathrm{diff}_{B/A} = \big(\frac{df}{dX}(\beta)\big)$.

Proposition 6.7.4: In general $\mathrm{diff}_{B/A}$ is the ideal that is generated by $\frac{df}{dX}(\beta)$ for all $\beta \in B$ with $L = K(\beta)$ and minimal polynomial f over K.

Proposition 6.7.5: We have $\mathrm{diff}_{C/A} = \mathrm{diff}_{C/B} \cdot \mathrm{diff}_{B/A}$.

Theorem 6.7.6: For any prime $\mathfrak{q}$ of B above a prime $\mathfrak{p}$ of A we have $\mathfrak{q} \nmid \mathrm{diff}_{B/A}$ if and only if $\mathfrak{q}$ is unramified over $\mathfrak{p}$.

6.8 Relative discriminant

Definition 6.8.1 The *relative discriminant of B/A* is the ideal of A that is generated by the discriminants

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

for all tuples $(b_1, \ldots, b_n)$ in B.

Proposition 6.8.2: We have $\mathrm{disc}_{B/A} = \mathrm{Nm}_{L/K}(\mathrm{diff}_{B/A})$.

Proposition 6.8.3: We have $\mathrm{disc}_{C/A} = \mathrm{Nm}_{L/K}(\mathrm{disc}_{C/B}) \cdot \mathrm{disc}_{B/A}^{[M/L]}$.

Theorem 6.8.4: (a) A prime $\mathfrak{p} \subset A$ is ramified in B if and only if $\mathfrak{p} | \operatorname{disc}_{B/A}$.

(b) At most finitely many primes of A are ramified in B.

Theorem 6.8.5: For any number field $K \neq \mathbb{Q}$ there exists a rational prime which is ramified in $\mathcal{O}_K$.

Example 6.8.6: Consider distinct primes $p_1 \equiv \ldots \equiv p_r \equiv 1 \bmod (4)$ with $r \geqslant 1$. Then the extension $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})/\mathbb{Q}(\sqrt{p_1 \cdots p_r})$ is everywhere unramified.

7 Zeta functions

7.1 Riemann zeta function

Definition 7.1.1: The *Riemann zeta function* is defined by the series

$$\zeta(s) \;:=\; \sum_{n=1}^{\infty} n^{-s}.$$

Proposition 7.1.2: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Lemma 7.1.3: For all $\mathrm{Re}(s) > 1$ we have

$$\zeta(s) \;=\; \frac{s}{s-1} - s \cdot \int_1^{\infty} (x - \lfloor x \rfloor) x^{-s-1}\, dx.$$

Proposition 7.1.4: The function $\zeta(s) - \frac{1}{s-1}$ extends uniquely to a holomorphic function on the region $\mathrm{Re}(s) > 0$.

Remark 7.1.5: It is known that $\zeta(s)$ extends uniquely to a meromorphic function on $\mathbb{C}$ with a single pole at $s = 1$. This extension is again denoted by $\zeta(s)$.

Throughout the following we use the branch of the logarithm with $\log 1 = 0$.

Proposition 7.1.6: An infinite product of non-zero complex numbers $\prod_{k \geqslant 1} z_k$ converges to a non-zero value if and only if $\lim\limits_{k \to \infty} z_k = 1$ and $\sum\limits_{k \geqslant 1} \log z_k$ converges.

Proposition 7.1.7: For all $\mathrm{Re}(s) > 1$ we have the *Euler product*

$$\zeta(s) \;=\; \prod_{p \text{ prime}} (1 - p^{-s})^{-1} \;\neq\; 0.$$

Proposition 7.1.8: We have

$$\sum_{p \text{ prime}} p^{-s} \;=\; \log \tfrac{1}{s-1} + O(1) \quad \text{for real } s \to 1+.$$

Definition 7.1.9: For $x \in \mathbb{R}$ we denote the number of primes $\leqslant x$ by $\pi(x)$.

Corollary 7.1.10: There is no $\varepsilon > 0$ such that for $x \to \infty$ we have

$$\pi(x) \;=\; O\Big(\frac{x}{(\log x)^{1+\varepsilon}}\Big).$$

In particular there exist infinitely many primes.

7.2 Dedekind zeta function

Fix a number field K of degree n over $\mathbb{Q}$.

Definition 7.2.1: The *Dedekind zeta function of K* is defined by the series

$$\zeta_K(s) \;:=\; \sum_{\mathfrak{a}} \mathrm{Nm}(\mathfrak{a})^{-s},$$

where the sum extends over all non-zero ideals $\mathfrak{a} \subset \mathcal{O}_K$.

Proposition 7.2.2: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there, and we have the *Euler product*

$$\zeta_K(s) \;=\; \prod_{\mathfrak{p}} \big(1 - \mathrm{Nm}(\mathfrak{p})^{-s}\big)^{-1} \;\neq\; 0,$$

extended over all maximal ideals $\mathfrak{p} \subset \mathcal{O}_K$.

Proposition 7.2.3: We have

$$\log \zeta_K(s) \;=\; \sum_{\mathfrak{p}} \mathrm{Nm}(\mathfrak{p})^{-s} + \big(\text{holomorphic for } \mathrm{Re}(s) > \tfrac{1}{2}\big).$$

Theorem 7.2.4: The function $\zeta_K(s)$ extends uniquely to a meromorphic function on the region $\mathrm{Re}(s) > 1 - \frac{1}{n}$ which is holomorphic except for a pole of order 1 at $s = 1$.

Proposition 7.2.5: We have

$$\sum_{\mathfrak{p}} \mathrm{Nm}(\mathfrak{p})^{-s} \;=\; \log \tfrac{1}{s-1} + O(1) \;\text{ for real } s \to 1+.$$

Corollary 7.2.6: There exist infinitely many rational primes that split totally in $\mathcal{O}_K$.

7.3 Analytic class number formula

As before we set $\Sigma := \mathrm{Hom}(K, \mathbb{C})$ and let r be the number of embeddings $K \hookrightarrow \mathbb{R}$ and s the number of pairs of complex conjugate non-real embeddings $K \hookrightarrow \mathbb{C}$. With $K_{\mathbb{C}} := \mathbb{C}^{\Sigma}$ and

$$K_{\mathbb{R}} \;:=\; \{(z_\sigma)_\sigma \in K_{\mathbb{C}} \;\big|\; \forall \sigma \in \Sigma\colon z_{\bar\sigma} = \bar z_\sigma\}$$

as in §3.4 we then have

$$K_{\mathbb{R}} \cap \mathbb{R}^{\Sigma} \;=\; \{(t_\sigma)_\sigma \in \mathbb{R}^{\Sigma} \;\big|\; \forall \sigma \in \Sigma\colon t_{\bar\sigma} = t_\sigma\}.$$

The $\mathbb{R}$-subspace

$$H \;:=\; \ker\big(\mathrm{Tr}\colon K_{\mathbb{R}} \cap \mathbb{R}^{\Sigma} \to \mathbb{R}\big)$$

from §5.2 therefore becomes a euclidean vector space by its embedding $H \subset K_{\mathbb{R}} \subset K_{\mathbb{C}}$ and the scalar product from §4.1. By §2.2 it is thus endowed with a canonical translation invariant measure $d\,\mathrm{vol}$. Recall from Theorem 5.3.1 that $\Gamma := \ell(j(\mathcal{O}_K^\times))$ is a complete lattice in H.

Definition 7.3.1: The *regulator of K* is the real number

$$R \;:=\; \frac{\mathrm{vol}(H/\Gamma)}{\sqrt{r+s}} \;>\; 0.$$

Let $w := |\mu(K)|$ denote the number of roots of unity in K and let $h := |\operatorname{Cl}(\mathcal{O}_K)|$ the class number.

Theorem 7.3.2: *Analytic class number formula:* The residue of $\zeta_K(s)$ at $s = 1$ is

$$\mathrm{Res}_{s=1}\,\zeta_K(s) \;=\; \frac{2^r(2\pi)^s Rh}{w\sqrt{|d_K|}} \;>\; 0.$$

7.4 Dirichlet density

Consider a number field K and a subset A of the set P of maximal ideals of $\mathcal{O}_K$.

Definition 7.4.1: (a) The value

$$\overline{\mu}(A) \;:=\; \limsup_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A}\mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})^{-s}}$$

is called the *upper Dirichlet density of A.*

(b) The value

$$\underline{\mu}(A) \;:=\; \liminf_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A}\mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})^{-s}}$$

is called the *lower Dirichlet density of A.*

(c) If these coincide, their common value

$$\mu(A) \;:=\; \lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A}\mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P}\mathrm{Nm}(\mathfrak{p})^{-s}}$$

is called the *Dirichlet density of A.*

Proposition 7.4.2: (a) We have $0 \leqslant \underline{\mu}(A) \leqslant \overline{\mu}(A) \leqslant 1$.

(b) For any subset $B \subset A$ we have $\overline{\mu}(B) \leqslant \overline{\mu}(A)$ and $\underline{\mu}(B) \leqslant \underline{\mu}(A)$, and also $\mu(B) \leqslant \mu(A)$ if these exist.

(c) We have $\mu(A) = 0$ if A is finite.

(d) We have $\mu(A) = 1$ if $P \smallsetminus A$ is finite.

(e) For any disjoint subsets $A, B \subset P$, if two of $\mu(A)$, $\mu(B)$, $\mu(A \cup B)$ exist, then so does the third and we have $\mu(A) + \mu(B) = \mu(A \cup B)$.

Proposition-Definition 7.4.3: If the *natural density of* A

$$\gamma(A) := \lim_{x\to\infty} \frac{\big|\{\mathfrak{p} \in A \mid \mathrm{Nm}(\mathfrak{p}) \leqslant x\}\big|}{\big|\{\mathfrak{p} \in P \mid \mathrm{Nm}(\mathfrak{p}) \leqslant x\}\big|}$$

exists, so does the Dirichlet density $\mu(A)$ and they are equal.

7.5 Primes of absolute degree 1

Definition 7.5.1: The *absolute degree* of a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is the degree of $k(\mathfrak{p})$ over its prime field.

Proposition 7.5.2: The set of primes of absolute degree 1 has Dirichlet density 1.

Proposition 7.5.3: A subset $A \subset P$ has a Dirichlet density if and only if the set of all $\mathfrak{p} \in A$ of absolute degree 1 has a Dirichlet density, and then they are equal.

For any finite galois extension of number fields L/K we let $\mathrm{Split}_{L/K}$ denote the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ that are totally split in $\mathcal{O}_L$.

Proposition 7.5.4: $\mathrm{Split}_{L/K}$ has Dirichlet density $\frac{1}{[L/K]}$. In particular it is infinite.

Now consider two finite galois extensions of number fields $L, L'/K$.

Proposition 7.5.5: Then $\mathrm{Split}_{LL'/K} = \mathrm{Split}_{L/K} \cap \mathrm{Split}_{L'/K}$.

Proposition 7.5.6: The following are equivalent:

(a) $L \subset L'$.

(b) $\mathrm{Split}_{L'/K} \subset \mathrm{Split}_{L/K}$.

(c) $\mu(\mathrm{Split}_{L'/K} \smallsetminus \mathrm{Split}_{L/K}) < \frac{1}{2[L'/K]}$.

Proposition 7.5.7: The following are equivalent:

(a) $L = L'$.

(b) $\mathrm{Split}_{L'/K}$ and $\mathrm{Split}_{L/K}$ differ only by a set of Dirichlet density 0.

In particular, a number field K that is galois over $\mathbb{Q}$ is uniquely determined by the set of rational primes p that split totally in K.

7.6 Dirichlet L-series

Definition 7.6.1: (a) A homomorphism $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is called a *Dirichlet character of modulus* $N \geqslant 1$.

(b) The *conductor* of such χ is the smallest divisor $N'|N$ such that χ factors through a homomorphism $(\mathbb{Z}/N'\mathbb{Z})^\times \to \mathbb{C}^\times$.

(c) Such χ is called *primitive* if $N' = N$.

(d) Such χ is called *principal* if $N' = 1$, that is, if χ is the trivial homomorphism.

Convention 7.6.2: Often one identifies a Dirichlet character χ of modulus N with a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ by setting

$$\chi(a) \;:=\; \begin{cases} \chi(a \bmod (N)) & \text{if } \gcd(a,N) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Caution 7.6.3: When the conductor N' is smaller than the modulus N, one has to be somewhat careful with the divisors of N/N'.

Definition 7.6.4: The *Dirichlet L-function* associated to any Dirichlet character χ is

$$L(\chi, s) \;:=\; \sum_{n \geqslant 1} \chi(n) n^{-s}.$$

Proposition 7.6.5: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Proposition 7.6.6: For all $\mathrm{Re}(s) > 1$ we have the *Euler product*

$$L(\chi, s) \;=\; \prod_{p \nmid N} (1 - \chi(p) p^{-s})^{-1}.$$

Proposition 7.6.7: If a Dirichlet character χ of modulus N corresponds to a primitive Dirichlet character χ' of modulus N', then

$$L(\chi', s) \;=\; L(\chi, s) \cdot \prod_{p \mid N,\, p \nmid N'} (1 - \chi'(p) p^{-s})^{-1}.$$

Proposition 7.6.8: (a) For the principal Dirichlet character χ of modulus 1 we have $L(\chi, s) = \zeta(s)$.

(b) For every non-principal Dirichlet character χ the function $L(\chi, s)$ extends uniquely to a holomorphic function on the region $\mathrm{Re}(s) > 0$.

Theorem 7.6.9: The zeta function $\zeta_K(s)$ of the field $K := \mathbb{Q}(\mu_N)$ is the product of the L-functions $L(\chi, s)$ for all primitive Dirichlet characters χ of conductor dividing N.

Theorem 7.6.10: For any non-principal Dirichlet character χ we have $L(\chi, 1) \neq 0$.

Proposition 7.6.11: For any non-principal Dirichlet character χ we have

$$\sum_{p \text{ prime}} \chi(p) p^{-s} \;=\; O(1) \quad \text{for real } s \to 1+.$$

7.7 Primes in arithmetic progressions

Theorem 7.7.1: For any coprime integers a and $N \geqslant 1$ the set of rational primes $p \equiv a \bmod (N)$ has Dirichlet density $\frac{1}{\varphi(N)}$. In particular it is infinite.

7.8 Bonus Material: Abelian Artin L-functions

Consider an abelian extension of number fields L/K with Galois group Γ. Then for any prime $\mathfrak{q}$ of $\mathcal{O}_L$, the decomposition group $\Gamma_\mathfrak{q}$, the inertia group $I_\mathfrak{q}$, and the Frobenius substitution $\mathrm{Frob}_\mathfrak{q}$ depend only on the underlying prime $\mathfrak{p}$ of $\mathcal{O}_K$. We therefore denote them also by $\Gamma_\mathfrak{p}$, $I_\mathfrak{p}$, $\mathrm{Frob}_\mathfrak{p}$ respectively.

Definition 7.8.1: The *Artin L-function* associated to a homomorphism $\chi\colon \Gamma \to \mathbb{C}^\times$ is

$$L_K(\chi, s) \;:=\; \prod_{\substack{\mathfrak{p} \\ \chi|I_\mathfrak{p}=1}} \big(1 - \chi(\mathrm{Frob}_\mathfrak{p})\,\mathrm{Nm}(\mathfrak{p})^{-s}\big)^{-1}.$$

Example 7.8.2: In the case $K = \mathbb{Q}$ and $L = \mathbb{Q}(\mu_N)$ and the usual identification $\Gamma \cong (\mathbb{Z}/N\mathbb{Z})^\times$ the Artin L-function $L_K(\chi, s)$ is the Dirichlet L-function $L(\chi, s)$ for the primitive Dirichlet character associated to χ.

Proposition 7.8.3: This product converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Proposition 7.8.4: For the trivial homomorphism χ we have $L_K(\chi, s) = \zeta_K(s)$.

Proposition 7.8.5: The zeta function $\zeta_L(s)$ is the product of the L-functions $L_K(\chi, s)$ for all χ.

Theorem 7.8.6: For every non-trivial χ the function $L_K(\chi, s)$ extends uniquely to a holomorphic function on the region $\mathrm{Re}(s) > 1 - \frac{1}{[K/\mathbb{Q}]}$.

(Proof only in the case $L = K(\mu_m)$.)

Theorem 7.8.7: For every non-trivial χ we have $L_K(\chi, 1) \neq 0$.

7.9 Bonus Material: Cebotarev density theorem

Consider an arbitrary Galois extension of number fields L/K with Galois group Γ. For any $\gamma \in \Gamma$ we denote the conjugacy class by $O_\Gamma(\gamma) := \{{}^\delta\gamma \mid \delta \in \Gamma\}$ and let P_γ denote the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ that are unramified in $\mathcal{O}_L$ and whose Frobenius substitution for some (and equivalently every) $\mathfrak{q}|\mathfrak{p}$ lies in $O_\Gamma(\gamma)$.

Theorem 7.9.1: The set P_γ has the Dirichlet density $\frac{|O_\Gamma(\gamma)|}{|\Gamma|}$.

8 Theory of valuations

8.1 p-adic Numbers

Fix an integer $b \geqslant 2$.

Fact 8.1.1: Any integer $n \geqslant 0$ can be written uniquely to base b as a finite sum

$$n \;=\; \sum_{i\geqslant 0}{}' a_i b^i \qquad \text{with} \quad a_i \in \{0,1,\dots,b-1\}.$$

Here the last k digits determine n mod (b^k), and the last k digits of the sum or product of two integers $m, n \geqslant 0$ depend only on the last k digits of m and n.

Proposition 8.1.2: There is a natural injective ring homomorphism

$$\mathbb{Z} \hookrightarrow \bigtimes_{k\geqslant 0} (\mathbb{Z}/b^k\mathbb{Z}), \quad n \longmapsto (n + b^k\mathbb{Z})_k.$$

Proposition 8.1.3: The image of this map is contained in the subring

$$\mathbb{Z}_b \;:=\; \underbrace{\Big\{(x_k + b^k\mathbb{Z})_k \in \bigtimes_{k\geqslant 0} (\mathbb{Z}/b^k\mathbb{Z}) \;\Big|\; \forall k \geqslant 0\colon x_k \equiv x_{k+1} \bmod (b^k)\Big\}}_{=:\,\varprojlim_k \mathbb{Z}/b^k\mathbb{Z}}.$$

Proposition 8.1.4: The following map is bijective:

$$\bigtimes_{k\geqslant 0} \{0,1,\dots,b-1\} \;\longrightarrow \mathbb{Z}_b, \quad (a_i)_i \longmapsto \Big(\sum_{i=0}^{k-1} a_i b^i + b^k\mathbb{Z}\Big)_k.$$

Observation 8.1.5: One computes with these systems (a_i) by hand in the same way as with non-negative integers to base b, except that the sequence of digits $\dots a_2 a_1 a_0$ extends infinitely to the left. This is similar to the decimal expansion of a real number, but in this case the sequence of digits is unique.

Convention 8.1.6: One writes an element in the image of the above map as a formal power series

$$\sum_{i\geqslant 0} a_i b^i.$$

One computes with such expressions in the same way as with formal power series, except that one has to deal with the carry.

Proposition 8.1.7: (a) For any coprime integers $b, b' \geqslant 2$ there is a natural ring isomorphism

$$\mathbb{Z}_{bb'} \;\cong\; \mathbb{Z}_b \times \mathbb{Z}_{b'}.$$

(b) For any integer $r \geqslant 0$ there is a natural ring isomorphism

$$\mathbb{Z}_{b^r} \;\cong\; \mathbb{Z}_b.$$

Throughout the following we assume that $b = p$ is a prime number.

Definition 8.1.8: The elements of $\mathbb{Z}_p$ are called *p-adic integers*.

Proposition 8.1.9: A system of polynomials $f_1, \dots, f_r \in \mathbb{Z}_p[X_1, \dots, X_m]$ has a common solution in $(\mathbb{Z}_p)^m$ if and only if their residue classes modulo (p^k) have a common solution in $(\mathbb{Z}/p^k\mathbb{Z})^m$ for all $k \geqslant 0$.

Proposition 8.1.10: (a) The set of units of $\mathbb{Z}_p$ is $\mathbb{Z}_p^\times = \mathbb{Z}_p \smallsetminus p\mathbb{Z}_p$.

(b) The ideal (p) of $\mathbb{Z}_p$ is the unique maximal ideal.

(c) Every non-zero ideal of $\mathbb{Z}_p$ is generated by p^r for a unique integer $r \geqslant 0$.

(d) The ring $\mathbb{Z}_p$ is a principal ideal domain.

Definition 8.1.11: The ring of formal Laurent series with finite principal part

$$\mathbb{Q}_p := \left\{ \sum_{i \in \mathbb{Z}} a_i p^i \;\middle|\; \begin{array}{l} \text{all } a_i \in \{0, 1, \dots, p-1\} \\ \text{and } a_i = 0 \text{ for all } i \ll 0 \end{array} \right\}$$

with the addition and multiplication defined as above. The elements of $\mathbb{Q}_p$ are called *(rational) p-adic numbers*.

Proposition 8.1.12: We have $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}] = \mathrm{Quot}(\mathbb{Z}_p)$.

Remark 8.1.13: Again the digits of a rational p-adic number are uniquely determined, and one computes with them by hand in the same way as with real numbers by writing them with a decimal point as $\dots a_2 a_1 a_0 . a_{-1} \dots a_k$ for some $k \ll 0$.

Remark 8.1.14: We have $\mathrm{card}(\mathbb{Q}_p) = \mathrm{card}(\mathbb{Z}_p) = \mathrm{card}(\mathbb{R})$.

Proposition 8.1.15: We have

(a) $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times$.

(b) $\mu(\mathbb{Q}_p) = \begin{cases} \mu_{p-1} & \text{if } p > 2, \\ \mu_2 & \text{if } p = 2. \end{cases}$

(c) $\mathbb{Z}_p^\times = \begin{cases} \mu_{p-1} \times (1 + p\mathbb{Z}_p) & \text{if } p > 2, \\ \mu_2 \times (1 + 4\mathbb{Z}_2) & \text{if } p = 2. \end{cases}$

(d) The second factor in (c) is isomorphic to $\mathbb{Z}_p$.

8.2 Valuations

Definition 8.2.1: A *(non-trivial rank 1) valuation* on a field K is a map

$$K \to \mathbb{R} \cup \{\infty\}, \quad x \mapsto v(x)$$

with the properties

(a) For any $x \in K$ we have $v(x) = 0$ if and only if $x = 0$.

(b) For any $x, y \in K$ we have $v(xy) = v(x) + v(y)$.

(c) For any $x, y \in K$ we have $v(x + y) \geqslant \min\{v(x), v(y)\}$.

(d) There exists $x \in K$ with $v(x) \notin \{0, \infty\}$.

Remark 8.2.2: The map with $v(0) = 0$ and $v(x) = 0$ for all $x \neq 0$ is called the *trivial valuation*. Some of the results below also hold for it, and sometimes one allows it as well, but we exclude it without further mention.

Definition 8.2.3: (a) A valuation v is called *discrete* if $v(K^\times)$ is discrete in $\mathbb{R}$.

(b) A discrete valuation v is called *normalized* if $v(K^\times) = \mathbb{Z}$.

(c) Two valuations v and v' are called *equivalent* if $v' = c \cdot v$ for some constant $c > 0$.

Proposition 8.2.4: Every discrete valuation is equivalent to a unique normalized valuation.

Proposition 8.2.5: Let A be a Dedekind ring with quotient field K, and let $\mathfrak{p}$ be a maximal ideal of A. For any $x \in K^\times$ let $\mathrm{ord}_\mathfrak{p}(x)$ denote the exponent of $\mathfrak{p}$ in the prime factorization of the fractional ideal (x), and set $\mathrm{ord}_\mathfrak{p}(0) := \infty$. Then $\mathrm{ord}_\mathfrak{p}$ is a normalized discrete valuation on K.

Examples 8.2.6: Consider a field k and a prime p.

(a) The polynomial ring $A = k[t]$ with $K = k(t)$ and $\mathfrak{p} = (t - a)$ for some $a \in A$.

(b) The field $K = k(t)$ with $v(f/g) := \deg(g) - \deg(f)$ for any $f, g \in k[t] \smallsetminus \{0\}$.

(c) The power series ring $A = k[[t]]$ with $K = k((t))$ and $\mathfrak{p} = (t)$.

(d) The ring $A = \mathbb{Z}$ with $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$.

(e) The ring $A = \mathbb{Z}_p$ with $K = \mathbb{Q}_p$ and $\mathfrak{p} = (p)$.

Basic Properties 8.2.7: For any valuation v on K we have:

(a) For any $x \in K^\times$ and $n \in \mathbb{Z}$ we have $v(x^n) = n \cdot v(n)$.

(b) For any root of unity $\zeta \in K$ we have $v(\zeta) = 0$.

(c) For any $x \in K$ and $n \in \mathbb{Z}$ we have $v(nx) \leqslant v(x)$.

(d) For any $x, y \in K$ we have $v(x + y) = \max\{v(x), v(y)\}$ if $v(x) \neq v(y)$.

Proposition-Definition 8.2.8: For any valuation v on K we have:

(a) The subset $\mathcal{O}_v := \{x \in K : v(x) \geqslant 0\}$ is a subring, called the *valuation ring* associated to v.

(b) We have $\mathrm{Quot}(\mathcal{O}_v) = K$.

(c) We have $\mathcal{O}_v^\times := \{x \in K : v(x) = 1\}$.

(d) The subset $\mathfrak{m}_v := \{x \in K : v(x) > 0\}$ is the unique maximal ideal of $\mathcal{O}_v$.

(e) If the valuation is discrete, then $\mathcal{O}_v$ is a principal ideal domain.

8.3 Complete valuations

Definition 8.3.1: The *completion* of a ring A with respect to an ideal $\mathfrak{a}$ is the subring

$$A_\mathfrak{a} := \varprojlim_k (A/\mathfrak{a}^k) := \left\{(x_k + \mathfrak{a}^k)_k \in \bigtimes_{k\geqslant 0}(A/\mathfrak{a}^k) \;\middle|\; \forall k \geqslant 0\colon x_k \equiv x_{k+1} \bmod \mathfrak{a}^k\right\}.$$

It is equipped with a natural ring homomorphism

$$i\colon A \longrightarrow A_\mathfrak{a},\ x \mapsto (x + \mathfrak{a}^k)_k.$$

Example 8.3.2: For any ring R the completion of $R[t]$ with respect to the ideal (t) is naturally isomorphic to $R[[t]]$.

Example 8.3.3: The ring $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the ideal (p).

Now consider a Dedekind ring A with quotient field K and a maximal ideal $\mathfrak{p}$. Pick an element $\pi \in \mathfrak{p} \smallsetminus \mathfrak{p}^2$.

Proposition 8.3.4: (a) The set of units of $A_\mathfrak{p}$ is $A_\mathfrak{p}^\times = A_\mathfrak{p} \smallsetminus \pi A_\mathfrak{p}$.

(b) The ideal $\mathfrak{m}_\mathfrak{p} := (\pi)$ of $A_\mathfrak{p}$ is the unique maximal ideal.

(c) Every nonzero ideal of $A_\mathfrak{p}$ is equal to $\mathfrak{m}_\mathfrak{p}^r$ for a unique integer $r \geqslant 0$.

(d) The ring $A_\mathfrak{p}$ is a principal ideal domain.

(e) It is the valuation ring for the discrete valuation $\mathrm{ord}_{\mathfrak{m}_\mathfrak{p}}$ on the field $K_\mathfrak{p} := A_\mathfrak{p}[\pi^{-1}]$.

(f) The natural homomorphism $i\colon A \to A_\mathfrak{p}$ is injective.

(g) It therefore induces an injective homomorphism $i\colon K \hookrightarrow K_\mathfrak{p}$.

(h) For any $x \in K$ we have $\mathrm{ord}_\mathfrak{p}(x) = \mathrm{ord}_{\mathfrak{m}_\mathfrak{p}}(i(x))$.

Definition 8.3.5: A normalized discrete valuation v on a field K is called *complete* if the natural homomorphism $i\colon K \hookrightarrow K_{\mathfrak{m}_v}$ is an isomorphism.

Example 8.3.6: The valuations on $k((t))$ and on $\mathbb{Q}_p$ are complete.

Proposition 8.3.7: The valuation $\mathrm{ord}_{\mathfrak{m}_\mathfrak{p}}$ on the completion $K_\mathfrak{p}$ is complete.

8.4 Absolute Values

Definition 8.4.1: A *(non-trivial) absolute value* on a field K is a map

$$K \to \mathbb{R}^{\geqslant 0}, \quad x \mapsto |x|$$

with the properties

(a) For any $x \in K$ we have $|x| = 0$ if and only if $x = 0$.

(b) For any $x, y \in K$ we have $|xy| = |x| \cdot |y|$.

(c) For any $x, y \in K$ we have $|x + y| \leqslant |x| + |y|$.

(d) There exists $x \in K$ with $|x| \notin \{0, 1\}$.

Remark 8.4.2: The map with $|0| = 0$ and $|x| = 1$ for all $x \neq 0$ is called the *trivial absolute value*. Some of the results below also hold for it, and sometimes one allows it as well, but we exclude it without further mention.

Caution 8.4.3: Don't confuse an absolute value with a valuation, as many do. ☹

Example 8.4.4: The usual absolute value on $\mathbb{R}$ or $\mathbb{C}$ or any subfield thereof.

Proposition 8.4.5: For any absolute value $|\ |$ and any real number $0 < s \leqslant 1$ the map $|\ |^s$ is also an absolute value.

Proposition 8.4.6: Any absolute value $|\ |$ on a field K turns K into a metric space with the metric $d(x, y) := |x - y|$.

Proposition-Definition 8.4.7: For any two absolute values $|\ |$ and $|\ |'$ on K the following are equivalent:

(a) They define the same topology on K.

(b) For any $x \in K$ we have $|x|' < 1$ if and only if $|x| < 1$.

(c) There exists a real number $s > 0$ such that for all $x \in K$ we have $|x|' = |x|^s$.

Two such absolute values are called *equivalent*.

Definition 8.4.8: An absolute value $|\ |$ is called *ultrametric* if it satisfies the stronger property

(c) For any $x, y \in K$ we have $|x + y| \leqslant \max\{|x|, |y|\}$.

Proposition 8.4.9: (a) For any valuation v on K and any constant $0 < c < 1$ the map $|x| := c^{v(x)}$ is an ultrametric absolute value on K.

(b) Any ultrametric absolute value arises in this fashion from a valuation.

(c) Two valuations are equivalent if and only if the associated absolute values are equivalent.

Basic Properties 8.4.10: For any absolute value $|\ |$ on K we have:

(a) For any $x \in K^\times$ and $n \in \mathbb{Z}$ we have $|x^n| = |x|^n$.

(b) For any root of unity $\zeta \in K$ we have $|\zeta| = 1$. In particular $|-1| = |1| = 1$.

(c) For any $x \in K$ and $n \in \mathbb{Z}$ we have $|nx| \leqslant |n| \cdot |x|$.

(d) For any $x, y \in K$ we have $|x - y| \geqslant ||x| - |y||$.

(e) For any $x, y \in K$ we have $|x+y| = \max\{|x|, |y|\}$ if $|x| \neq |y|$ and $|\ |$ is ultrametric.

Definition 8.4.11: An absolute value $|\ |$ is called *archimedean* if for every $x \in K$ there exists $n \in \mathbb{Z}$ with $|x| < n$. Otherwise it is called *nonarchimedean*.

Theorem 8.4.12: An absolute value $|\ |$ is ultrametric if and only if it is nonarchimedean.

Definition 8.4.13: On the field $\mathbb{Q}$ we have the usual absolute value

$$|x|_\infty := \begin{cases} x & \text{if } x \geqslant 0, \\ -x & \text{if } x < 0, \end{cases}$$

and for every prime number p the *p-adic absolute value*

$$|x|_p := \begin{cases} p^{-\operatorname{ord}_p(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0, \end{cases}$$

where $\operatorname{ord}_p(x)$ is the exponent of p in the prime factorization of x.

Theorem 8.4.14: Every absolute value on $\mathbb{Q}$ is equivalent to exactly one of the above.

The normalization in Definition 8.4.13 is specially chosen to achieve:

Theorem 8.4.15: For every $x \in \mathbb{Q}^\times$ we have

$$\prod_{p \leqslant \infty} |x|_p = 1.$$

8.5 Completion of a metric space

Consider a metric space (X, d).

Definition 8.5.1: A sequence (x_n) in X is ...

(a) ... said to *converge to* $x \in X$ and we write $x = \lim_{n\to\infty} x_n$, if

$$\forall\, \varepsilon > 0\ \exists\, n_0\ \forall\, n > n_0 \colon d(x_n, x) < \varepsilon.$$

(b) ... called a *Cauchy sequence* if

$$\forall\, \varepsilon > 0\ \exists\, n_0\ \forall\, n, m > n_0 \colon d(x_n, x_m) < \varepsilon.$$

Proposition 8.5.2: Any convergent sequence is a Cauchy sequence and has a unique limit.

Proposition 8.5.3: The metric space (X, d) is called *complete* if every Cauchy sequence has a limit.

Definition 8.5.4: A *completion of* (X, d) is a complete metric space $(\hat{X}, \hat{d})$ together with a map $i \colon X \to \hat{X}$ such that

(a) for all $x, y \in X$ we have $\hat{d}(i(x), i(y)) = d(x, y)$, and

(b) for every continuous map $f \colon X \to Y$ to a complete metric space (Y, e) there exists a unique continuous map $\hat{f} \colon \hat{X} \to Y$ such that $\hat{f} \circ i = f$.

Proposition 8.5.5: A completion exists and is unique up to unique isometry.

8.6 Complete absolute values

Definition 8.6.1: An absolute value on a field is complete if and only if the associated metric space is complete.

Proposition 8.6.2: The completion of a field K with an absolute value $|\ |$ is a complete field $\hat{K}$ with the operations

$$\begin{aligned} \big(\lim_{n\to\infty} x_n\big) + \big(\lim_{n\to\infty} y_n\big) &= \lim_{n\to\infty} \big(x_n + y_n\big) \\ \big(\lim_{n\to\infty} x_n\big) \cdot \big(\lim_{n\to\infty} y_n\big) &= \lim_{n\to\infty} \big(x_n \cdot y_n\big) \end{aligned}$$

and with

$$\big|\lim_{n\to\infty} x_n\big| = \lim_{n\to\infty} |x_n|$$

Example 8.6.3: The field $\mathbb{R}$ is the completion of $\mathbb{Q}$ for the absolute value $|\ |_\infty$.

Theorem 8.6.4: *(Ostrowski)* Any field that is complete with respect to an archimedean absolute value is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ and the absolute value is equivalent to the usual absolute value.

Proposition 8.6.5: A nonarchimedean absolute value $|\ |$ on a field K is complete if and only if the associated valuation v is complete.

8.7 Power series

Fix a complete nonarchimedean absolute value $|\ |$ associated to the valuation v on K.

Proposition 8.7.1: (a) A series $\sum_{n\geqslant 0} x_n$ in K converges if and only if $\lim_{n\to\infty} x_n = 0$.

(b) Convergent series in K can be arbitrarily rearranged and subdivided without changing convergence or the limit.

Proposition 8.7.2: If v is normalized discrete, fix an element $\pi \in K$ with $v(\pi) = 1$ and a set of representatives $\mathcal{R}$ of $\mathcal{O}_v/\mathfrak{m}_v$ with $0 \in \mathcal{R}$. Then:

(a) Every element $x \in K$ can be written uniquely as a convergent Laurent series

$$x \;=\; \sum_{i\in\mathbb{Z}} a_i \pi^i$$

with $a_i \in \mathcal{R}$ and $a_i = 0$ for all $i \ll 0$.

(b) Such an element lies in $\mathcal{O}_v$ if and only if $a_i = 0$ for all $i < 0$.

Now we assume that $\mathbb{Q} \subset K$ and that the restriction of $|\ |$ to $\mathbb{Q}$ is $|\ |_p$.

Proposition 8.7.3: For any $x \in K$ with $|x-1| < 1$ the series

$$\log(x) \;:=\; \sum_{n\geqslant 1} (-1)^{n-1} \cdot \frac{(x-1)^n}{n}$$

converges and satisfies

$$\log(xy) \;=\; \log(x) + \log(y).$$

Lemma 8.7.4: For every $n \geqslant 0$ we have $\mathrm{ord}_p(n!) = \sum_{i\geqslant 1} \left\lfloor \frac{n}{p^i} \right\rfloor < \frac{n}{p-1}$.

Proposition 8.7.5: For every $x \in K$ with $|x| < p^{-\frac{1}{p-1}}$ the series

$$\exp(x) \;:=\; \sum_{n\geqslant 0} \frac{x^n}{n!}$$

converges and satisfies

$$\exp(x+y) \;=\; \exp(x) \cdot \exp(y).$$

Proposition 8.7.6: Exp and log induce mutually inverse group isomorphisms

$$(K,+) \;>\; \left\{x \in K : |x| < p^{-\frac{1}{p-1}}\right\} \;\cong\; \left\{x \in K^\times : |x-1| < p^{-\frac{1}{p-1}}\right\} \;<\; (K^\times, \cdot).$$

Example 8.7.7: Exp and log induce mutually inverse group isomorphisms

$$\begin{aligned} (p\mathbb{Z}_p, +) &\;\cong\; (1 + p\mathbb{Z}_p, \cdot) \quad \text{if } p > 2, \\ (4\mathbb{Z}_p, +) &\;\cong\; (1 + 4\mathbb{Z}_2, \cdot) \quad \text{if } p = 2. \end{aligned}$$

9 Extensions of valuations

Throughout we fix a field K with an absolute value $|\ |$.

9.1 Normed vector spaces

Definition 9.1.1: A *norm* on a K-vector space V is a map $\|\ \|: V \to \mathbb{R}^{\geqslant 0}$ such that

(a) For any $v \in V$ we have $\|v\| = 0$ if and only if $v = 0$.

(b) For any $v \in V$ and $x \in K$ we have $\|xv\| = |x| \cdot \|v\|$.

(c) For any $v, w \in V$ we have $\|v + w\| \leqslant \|x\| + \|y\|$.

Definition 9.1.2: Two norms $\|\ \|$ and $\|\ \|'$ on V are called *equivalent* if there exist constants $c, c' > 0$ such that

$$\forall\, v \in V:\ \ c \cdot \|v\| \leqslant \|v\|' \leqslant c' \cdot \|v\|.$$

Theorem 9.1.3: If K is complete and $\dim_K(V) < \infty$, any norms on V are equivalent.

9.2 Extensions of complete absolute values

Assume that $|\ |$ is complete.

Proposition 9.2.1: If $|\ |$ is archimedean, it possesses a unique extension to any algebraic extension of K. It is given by the formula $|y| = |\mathrm{Nm}_{L/K}(y)|^{1/[L/K]}$, and is again archimedean and complete.

For the rest of this section we assume that $|\ |$ is complete and nonarchimedean. Let $\mathcal{O}_\mathfrak{p}$ be its valuation ring with the maximal ideal $\mathfrak{p}$ and the residue field $k := \mathcal{O}_\mathfrak{p}/\mathfrak{p}$.

Definition 9.2.2: For $f(X) = \sum_{i=0}^n a_i X^i \in K[X]$ we set

$$|f|\ :=\ \max\{|a_i| : 0 \leqslant i \leqslant n\}.$$

We call f *primitive* if $|f| = 1$.

Proposition 9.2.3: *(Hensel's Lemma)* Consider a primitive $f \in \mathcal{O}_\mathfrak{p}[X]$ and a decomposition $(f \bmod \mathfrak{p}) = \bar{g} \cdot \bar{h}$ with coprime polynomials $\bar{g}$, $\bar{h} \in k[X]$. Then there exist $g, h \in \mathcal{O}_\mathfrak{p}[X]$ with $(g \bmod \mathfrak{p}) = \bar{g}$ and $(h \bmod \mathfrak{p}) = \bar{h}$ and $\deg(g) = \deg(\bar{g})$ and $f = g \cdot h$.

Corollary 9.2.4: (a) For any irreducible $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ with $a_n \neq 0$ we have $|f| = \max\{|a_0|, |a_n|\}$.

(b) If $|f| = 1$, then all irreducible factors of f mod $\mathfrak{p}$ are equivalent.

Theorem 9.2.6: Consider any finite field extension L/K of degree n.

(a) There exists a unique absolute value on L which extends $|\ |$.

(b) This is given by the formula $|y| = |\operatorname{Nm}_{L/K}(y)|^{1/n}$.

(c) This extension is again nonarchimedean and complete.

Corollary 9.2.7: For any algebraic extension L/K there exists a unique absolute value on L that extends $|\ |$.

9.3 Newton Polygons

Assume that $|\ |$ is complete and nonarchimedean and associated to a valuation v.

Proposition 9.3.1: For any irreducible monic polynomial $f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in K[X]$ and any zero α in an algebraic closure of K we have $|\alpha| = |a_0|^{1/n}$.

Definition 9.3.2: (a) A *convex polygon* $P \subset \mathbb{R}^2$ is the graph of a piecewise linear convex function $I \to \mathbb{R}$ for some closed interval I.

(b) If such P contains a straight line segment of slope ξ over the maximal interval $[a, b] \subset I$ with a, b, then ξ is called a *slope of P of multiplicity* $b - a$.

(c) A point on P where the slope changes is called a *break point of P*.

Fix a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ with $a_0, a_n \neq 0$ and consider the finite set

$$S \ := \ \big\{(i, v(a_i)) \ \big|\ 0 \leqslant i \leqslant n \text{ with } a_i \neq 0\big\}.$$

Definition 9.3.3: The *Newton polygon* of f is the unique convex polygon over the interval $[0, n]$ with all end points and break points in S, such that each point of S lies vertically above a point in P.

Proposition 9.3.4: Write $f(X) = a_n \cdot \prod_{i=1}^{n} (X - \alpha_i)$ with $\alpha_i \in \bar{K}$. Then for every real number ξ, the multiplicity of ξ as a slope of the Newton polygon of f is the number of i with $v(\alpha_i) = -\xi$.

Proposition 9.3.5: The decomposition of the Newton polygon into straight line segments corresponds to a factorization of f over K. In other words, for every real number ξ we have

$$f_\xi(X) \ := \ \prod_{\substack{1 \leqslant i \leqslant n \\ v(\alpha_i) = -\xi}} (X - \alpha_i) \ \in \ K[X].$$

Now assume in addition that the valuation v is normalized.

Proposition 9.3.6: Then all end points and break points of the Newton polygon lie in $\mathbb{Z}^2$.

Proposition 9.3.7: If the Newton polygon of f has a single slope of the form $\frac{m}{n}$ for an integer m coprime to $n = \deg(f)$, then f is irreducible.

Note 9.3.8: In the case $m = -1$ this is the Eisenstein criterion.

9.4 Lifting prime ideals

As before we assume that $|\ |$ is complete and associated to a valuation v with valuation ring $\mathcal{O}_\mathfrak{p}$ and maximal ideal $\mathfrak{p}$ and residue field $k(\mathfrak{p}) := \mathcal{O}_\mathfrak{p}/\mathfrak{p}$. Consider a separable finite extension L/K and let v also denote the unique valuation on L that extends v.

Proposition 9.4.1: (a) The integral closure of $\mathcal{O}_\mathfrak{p}$ in L is the ring

$$\mathcal{O}_\mathfrak{q} \ := \ \{y \in L : v(y) \geqslant 0\}.$$

(b) There is a unique prime $\mathfrak{q}$ of $\mathcal{O}_\mathfrak{q}$ above $\mathfrak{p}$, given by

$$\mathfrak{q} \ := \ \{y \in L : v(y) > 0\}.$$

From Section 6.2 we obtain:

Proposition 9.4.2: Assume that $k(\mathfrak{p})$ is perfect. Then:

(a) The ramification degree of $\mathfrak{q}$ over $\mathfrak{p}$ is $e_{\mathfrak{q}|\mathfrak{p}} = [v(L^\times) : v(K^\times)]$.

(b) The inertia degree of $\mathfrak{q}$ over $\mathfrak{p}$ is $f_{\mathfrak{q}|\mathfrak{p}} = [k(\mathfrak{q})/k(\mathfrak{p})]$.

(c) We have $[L/K] = e_{\mathfrak{q}|\mathfrak{p}} \cdot f_{\mathfrak{q}|\mathfrak{p}}$.

9.5 Extensions of absolute values

Proposition 9.5.1: *(Simultaneous approximation)* Consider pairwise inequivalent norms $|\ |_1, \dots, |\ |_n$ on a field K and elements $a_1, \dots, a_n \in K$. Then for every $\varepsilon > 0$ there exists an $x \in K$ such that $|x - a_i| < \varepsilon$ for all i.

Proposition 9.5.2: For any finite separable field extension L/K and any field extension $\hat{K}/K$ we have

$$L \otimes_K \hat{K} \ \cong \ \bigtimes_{i=1}^{r} \hat{L}_i$$

for finite separable field extensions $\hat{L}_i/\hat{K}$ with $[L/K] = \sum_{i=1}^r [\hat{L}_i/\hat{K}]$.

Now we fix an absolute value $|\ |$ on K that is not necessarily complete, and a finite separable extension L/K. We apply the above to the completion $\hat{K}$ of K with respect to $|\ |$ with the extended absolute value $|\ |\hat{}$. For each i let $|\ |_i\hat{}$ denote the unique absolute value on $\hat{L}_i$ that extends $|\ |$ on $\hat{K}$.

Lemma 9.5.3: Two absolute values on L that extend $|\ |$ are equivalent if and only if they are equal.

Proposition 9.5.4: The different extensions of $|\ |$ to L are precisely the restrictions $|\ |_i$ of the $|\ |_i\hat{}$ to L, and for each of them the completion of L is $\hat{L}_i$.

Proposition 9.5.5: Assume that $|\ |$ is archimedean. Then either

(a) $\hat{K} \cong \mathbb{C}$ and all $\hat{L}_i \cong \mathbb{C}$ and $[L/K] = r$.

(b) $\hat{K} \cong \mathbb{R}$ and all $\hat{L}_i \cong \mathbb{R}$ or $\mathbb{C}$ and $[L/K] = r_1 + r_2$, where r_1 is the number of i with $\hat{L}_i \cong \mathbb{R}$ and r_2 the number of i with $\hat{L}_i \cong \mathbb{C}$.

For the rest of this section we assume that $|\ |$ is nonarchimedean and corresponds to the discrete valuation $\mathrm{ord}_{\mathfrak{p}}$ for a maximal ideal $\mathfrak{p}$ of a Dedekind ring A with $\mathrm{Quot}(A) = K$. Let $\mathcal{O} \subset \hat{K}$ denote the respective completions and $\mathfrak{m} \subset \mathcal{O}$ the maximal ideal. By Proposition 9.4.1 the integral closure $\mathcal{O}_i \subset \hat{L}_i$ of $\mathcal{O}$ is the valuation ring for $|\ |_i^{\wedge}$. Let $\mathfrak{n}_i$ denote its unique maximal ideal. Let B denote the integral closure of A in L.

Proposition 9.5.6: The isomorphism in Proposition 9.5.2 induces an isomorphism

$$B \otimes_A \mathcal{O} \;\cong\; \bigtimes_{i=1}^{r} \mathcal{O}_i$$

Proposition 9.5.7: (a) The prime ideals of B above $\mathfrak{p}$ are precisely the r different ideals $\mathfrak{q}_i := \mathfrak{n}_i \cap B$.

(b) For each of them we have $e_{\mathfrak{q}_i|\mathfrak{p}} = e_{\mathfrak{n}_i|\mathfrak{m}}$ and $f_{\mathfrak{q}_i|\mathfrak{p}} = f_{\mathfrak{n}_i|\mathfrak{m}}$.

Note 9.5.8: This explains the formula $[L/K] = \sum_{i=1}^{r} e_{\mathfrak{q}_i|\mathfrak{p}} \cdot f_{\mathfrak{q}_i|\mathfrak{p}}$ in terms of extensions of valuations.

Proposition 9.5.9: (a) The isomorphism in Prop. 9.5.6 induces an isomorphism

$$\mathrm{diff}_{B/A} \otimes_A \mathcal{O} \;\cong\; \bigtimes_{i=1}^{r} \mathrm{diff}_{\mathcal{O}_i/\mathcal{O}}\,.$$

(b) The embedding $A \subset \mathcal{O}$ induces an equality

$$\mathrm{disc}_{B/A} \cdot \mathcal{O} \;=\; \prod_{i=1}^{r} \mathrm{disc}_{\mathcal{O}_i/\mathcal{O}}\,.$$

Proposition 9.5.10: If L/K is galois with Galois group Γ, then each $\hat{L}_i/\hat{K}$ is galois with Galois group $\Gamma_{\mathfrak{q}_i}$, and the respective inertia groups are equal: $I_{\mathfrak{q}_i} = I_{\mathfrak{n}_i}$.

Note 9.5.11: Passing to the completion is therefore similar to passing to the decomposition group.

9.6 Local and global fields

Recall that a Hausdorff topological space is called *locally compact* if every neighborhood of every point contains a compact neighborhood. For example $\mathbb{R}^n$ is locally compact, but an infinite dimensional Hilbert or Banach space is not. On locally compact spaces one can do analysis in much the same way as on $\mathbb{R}^n$.

Theorem 9.6.1: For an field K with an absolute value $|\ |$ the following are equivalent:

(a) K is locally compact.

(b) $|\ |$ is complete and, if it is nonarchimedean, the associated valuation is discrete and has finite residue field.

(c) K is isomorphic to a finite extension of $\mathbb{R}$ or $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ for a prime p, and $|\ |$ is equivalent to the unique extension of the usual absolute value on that field.

Definition 9.6.2: Such a field K is called a *local field*.

Remark 9.6.3: The characteristic of a nonarchimedean local field is either zero or equal to the characteristic of its residue field.

Definition 9.6.4: To exhibit the analogy we sometimes write $\mathbb{Q}_\infty := \mathbb{R}$ and denote the usual absolute value by $|\ |_\infty$.

Definition 9.6.5: A field that is isomorphic to a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$ for a prime p is called a *global field*.

Proposition 9.6.6: A field with an absolute value is a local field if and only if it is the completion of a global field at an absolute value.

Remark 9.6.7: There is a delicate interplay between properties of global field and properties of their associated associated local fields, which can go both ways.

10 Infinite Galois theory

10.1 Topological groups

Definition 10.1.1: A *topological group* is a group G endowed with a topology, such that the following maps are continuous:

$$\begin{aligned} G \times G \to G, &\quad (g,h) \mapsto gh, \\ G \to G, &\quad g \mapsto g^{-1}. \end{aligned}$$

Example 10.1.2: Every group with the discrete topology is a topological group.

Remark 10.1.3: Some authors require that the topology is also Hausdorff.

Example 10.1.4: Let K be a field with an absolute value $|\ |$ and endow $\mathrm{GL}_n(K)$ with the topology induced by the product topology on $\mathrm{Mat}_{n\times n}(\mathbb{R}) \cong \mathbb{R}^{n^2}$.

Proposition 10.1.5: Every subgroup of a topological group becomes a topological group with the induced topology.

Proposition 10.1.6: Every (finite or infinite) product of topological groups, endowed with the product topology, is a topological group.

Proposition 10.1.7: For every topological group G and any $g \in G$ the maps $G \to G$, $x \mapsto gx$ and $x \mapsto xg$ and $x \mapsto {}^g x$ are homeomorphisms.

Proposition 10.1.8: Every open subgroup of a topological group is closed.

Definition 10.1.9: A *topological isomorphism* between topological groups is a group isomorphism which is also a homeomorphism.

10.2 Profinite groups

Definition 10.2.1: A *profinite group* is a topological group that is topologically isomorphic to a closed subgroup of a (possibly infinite) product of discrete finite groups.

Proposition 10.2.2: For every profinite group G we have:

(a) G ist compact und Hausdorff.

(b) Every open subgroup has finite index.

(c) The open normal subgroups form a neighborhood base of the identity element.

Example 10.2.3: The topology induced by the p-adic metric on $\mathbb{Z}_p$ is the same as that induced by the product topology on $\bigtimes_{n\geqslant 0}\mathbb{Z}/p^n\mathbb{Z}$. Thus the additive group $(\mathbb{Z}_p,+)$ and the group of units $(\mathbb{Z}_p^\times,\cdot\,)$ are profinite groups.

Proposition 10.2.4: Every closed subgroup of a profinite group is a profinite group with the induced topology.

Proposition 10.2.5: Every factor group of a profinite group by a closed subgroup is a profinite group with the induced topology.

Definition 10.2.6: The *profinite completion* of a group G is the profinite group

$$\varprojlim_N G/N \;:=\; \Big\{(g_N N)_N \in \bigtimes_N G/N \;\Big|\; \forall\, N'\subset N\subset G\colon g_{N'}N = g_N N\Big\},$$

where the product extends over all normal subgroups $N \lhd G$ of finite index.

Example 10.2.7: The profinite completion $\hat{\mathbb{Z}}$ of the group $\mathbb{Z}$ is isomorphic to $\prod_p \mathbb{Z}_p$.

10.3 Infinite Galois theory

Consider a galois extension of fields L/K which may or may not be finite.

Proposition 10.3.1: There is a natural injective group homomorphism

$$\mathrm{Gal}(L/K) \to \bigtimes_{K'} \mathrm{Gal}(K'/K),\ \gamma \mapsto (\gamma|_{K'})_{K'},$$

where the product extends over all intermediate fields K' that are finite and galois over K. Its image is the closed subgroup

$$\varprojlim_{K'} \mathrm{Gal}(K'/K) \ := \ \big\{(\gamma_{K'})_{K'} \ \big|\ \forall\, K''/K'/K\colon \gamma_{K''}|_{K'} = \gamma_{K'}\big\}.$$

This turns $\Gamma := \mathrm{Gal}(L/K)$ into a profinite group.

Theorem 10.3.2: *(Main Theorem of Galois theory)* There are natural mutually inverse bijections

$$\begin{array}{ccc} \big\{\text{Intermediate fields of } L/K\big\} & \underset{\longleftarrow}{\overset{\sim}{\longrightarrow}} & \big\{\text{closed subgroups of } \Gamma\big\} \\ K' & \longmapsto & \mathrm{Gal}(L/K') \\ L^{\Gamma'} & \longleftarrow\!\shortmid & \Gamma' \end{array}$$

Example 10.3.3: For any finite field k with algebraic closure $\bar{k}$, there is a natural isomorphism $\hat{\mathbb{Z}} \cong \mathrm{Gal}(\bar{k}/k)$ that sends 1 to the Frobenius automorphism $x \mapsto x^{|k|}$.

Example 10.3.4: Consider a prime number p.

(a) The extension $L := \mathbb{Q}(\bigcup_{n\geqslant 0} \mu_{p^n})/\mathbb{Q}$ has galois group $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_p^\times$.

(b) It has a unique subfield L' with $\mathrm{Gal}(L'/\mathbb{Q}) \cong \mathbb{Z}_p$.

In Iwasawa theory one is interested in more general Galois extensions of a number field with galois group $\mathbb{Z}_p$, which are called $\mathbb{Z}_p$*-extensions*.

Remark 10.3.5: Many questions in number theory, among them highly interesting unproven conjectures, can be phrased as questions concerning the structure of the galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

11 Galois theory of local fields

Throughout this chapter we fix a nonarchimedean local field K with normalized valuation v and valuation ring $\mathcal{O}$ and finite residue field $k = \mathcal{O}/\mathfrak{m}$ of characteristic p.

11.1 Multiplicative group

Proposition 11.1.1: The reduction homomorphism $\mathcal{O}^\times \to k^\times$ is surjective and has a unique splitting, that is, a homomorphism $k^\times \to \mathcal{O}^\times$, $\alpha \mapsto \tilde{\alpha}$, such that $\tilde{\alpha} + \mathfrak{m} = \alpha$.

Definition 11.1.2: The element $\tilde{\alpha}$ is called the *Teichmüller representative* of α.

Definition 11.1.3: A generator of the ideal $\mathfrak{m}$ is called a *uniformizer of* K.

Proposition 11.1.4: In the case $\mathrm{char}(K) = p$ we have:

(a) The ring homomorphism $\mathcal{O} \twoheadrightarrow k$ has a unique splitting, that is, a ring homomorphism $k \to \mathcal{O}$, $\alpha \mapsto \tilde{\alpha}$, such that $\tilde{\alpha} + \mathfrak{m} = \alpha$.

(b) For any uniformizer u of K there is a natural isomorphism $k((u)) \cong K$.

Remark 11.1.5: One might think that this makes the theory of local fields of positive characteristic boring. But it does not tell us anything about the galois theory of such fields, which is as intricate as the galois theory of p-adic fields.

Proposition 11.1.6: (a) The group μ_K of roots of unity in $K^\times$ is finite.

(b) If K is an extension of degree n of $\mathbb{Q}_p$, there is an uncanonical group isomorphism

$$K^\times \;\cong\; \mathbb{Z} \times \mu_K \times \mathbb{Z}_p^n.$$

(c) If K has characteristic p, there is an uncanonical group isomorphism

$$K^\times \;\cong\; \mathbb{Z} \times k^\times \times \mathbb{Z}_p^{\mathbb{N}}.$$

11.2 Unramified extensions

Proposition 11.2.1: For any integer $n \geqslant 1$ there exists an unramified extension L/K of degree n. It is unique up to isomorphism over K and galois over K. Its residue field ℓ is an extension of degree n of k, and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$ is cyclic of order n.

Proposition 11.2.2: Consider a finite extension M/K with intermediate fields K', L.

(a) M/K is unramified if and only if M/L and L/K are unramified.

(b) If L/K is unramified, then so is LK'/K'.

(c) If L/K and K'/K is unramified, then so is LK'/K.

Definition 11.2.3: An algebraic extension L/K is called *unramified* if it is a union of unramified finite extensions of K.

Proposition 11.2.4: (a) There exists a maximal unramified extension K^{nr} and it is unique up to isomorphism over K, though the isomorphism is not unique.

(b) The extension K^{nr}/K is galois. The residue field $\bar{k}$ of $\mathcal{O}_{K^{\mathrm{nr}}}$ is an algebraic closure of k and there are canonical isomorphisms

$$\mathrm{Gal}(K^{\mathrm{nr}}/K) \;\cong\; \mathrm{Gal}(\bar{k}/k) \;\cong\; \hat{\mathbb{Z}}.$$

11.3 Tame extensions

Definition 11.3.1: A finite extension L/K is called *tame* if its ramification index is not divisible by p.

Proposition 11.3.2: (a) Any extension of the form $K(\sqrt[e]{a})/K$ for $p \nmid e \geqslant 1$ and $a \in K$ is tame.

(b) If in addition $v(a)$ is coprime to e, the extension is totally ramified of degree e.

Proposition 11.3.3: Any finite extension L/K that is tame and totally ramified of degree e has the form $L = K(\sqrt[e]{u})$ for a uniformizer $u \in K$.

Proposition 11.3.4: Consider a finite extension M/K with intermediate fields K', L.

(a) M/K is tame if and only if M/L and L/K are tame.

(b) If L/K is tame, then so is LK'/K'.

(c) If L/K and K'/K is tame, then so is LK'/K.

Definition 11.3.5: An algebraic extension L/K is called *tame* if it is a union of tame finite extensions of K.

Proposition 11.3.6: (a) There exists a maximal tame extension K^{tr} and it is unique up to isomorphism over K, though the isomorphism is not unique.

(b) The extension K^{tr}/K is galois and contains a maximal unramified extension K^{nr}.

Proposition 11.3.7: (a) The galois group of $K^{\mathrm{tr}}/K^{\mathrm{nr}}$ is naturally isomorphic to

$$\hat{\mathbb{Z}}^{(p)}(1) \;:=\; \varprojlim_n \mu_n(\bar{k}) \;:=\; \Big\{(\zeta_n)_n \in \bigtimes_n \mu_n(\bar{k}) \;\Big|\; \forall\, n|n' \colon \zeta_{n'}^{n'/n} = \zeta_n\Big\},$$

where the product extends over all integers $p \nmid n \geqslant 1$.

(d) The galois group of K^{tr}/K is isomorphic to the semidirect product

$$\hat{\mathbb{Z}} \ltimes \hat{\mathbb{Z}}^{(p)}(1),$$

where $1 \in \hat{\mathbb{Z}}$ acts on $\hat{\mathbb{Z}}^{(p)}(1)$ by the map $x \mapsto x^{|k|}$.

Remark 11.3.8: This inverse limit is uncanonically isomorphic to the prime-to-p part

$$\hat{\mathbb{Z}}^{(p)} \;:=\; \prod_{\ell \neq p} \mathbb{Z}_\ell$$

of the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$. The notation $\hat{\mathbb{Z}}^{(p)}(1)$ is chosen to indicate the nontrivial action of $\mathrm{Gal}(K^{\mathrm{nr}}/K)$.

11.4 The lower numbering filtration

Fix a finite galois extension L/K with galois group Γ and residue field $\ell = \mathcal{O}_L/\mathfrak{m}_L$. Let v_L denote the normalized valuation on L.

Definition 11.4.1: For every real number $s \geqslant -1$ we define the *s-th ramification group of L/K in the lower numbering* as

$$\Gamma_s := \big\{\gamma \in \Gamma \;\big|\; \forall\, a \in \mathcal{O}_L \colon v_L({}^\gamma a - a) \geqslant s+1\big\}.$$

Proposition 11.4.2: (a) For every s we have $\Gamma_s = \Gamma_{\lceil s \rceil}$.

(b) For every s we have $\Gamma_s \lhd \Gamma$.

(c) We have $\Gamma_{-1} = \Gamma$.

(d) The subgroup Γ_0 is the inertia group.

(e) There exists s with $\Gamma_s = 1$.

Proposition 11.4.3: (a) There is a natural isomorphism $\Gamma/\Gamma_0 \cong \mathrm{Gal}(\ell/k)$.

(b) Any uniformizer u of L induces an injective homomorphism

$$\Gamma_0/\Gamma_1 \;\hookrightarrow\; \ell^\times, \quad [\gamma] \mapsto \Big[\frac{{}^\gamma u}{u}\Big].$$

(c) For any integer $s \geqslant 1$, any uniformizer u of L induces an injective homomorphism

$$\Gamma_s/\Gamma_{s+1} \;\hookrightarrow\; (\ell, +), \quad [\gamma] \mapsto \Big[\frac{{}^\gamma u - u}{u}\Big].$$

Proposition 11.4.4: (a) The factor group Γ/Γ_0 is cyclic.

(b) The factor group Γ_0/Γ_1 is cyclic of order prime to p.

(c) The subgroup Γ_1 is a p-group.

Corollary 11.4.5: The galois group Γ is solvable.

Proposition 11.4.6: The extension L/K is ...

(a) ... trivial if and only if $\Gamma_{-1} = 1$.

(b) ... unramified if and only if $\Gamma_0 = 1$.

(c) ... tame if and only if $\Gamma_1 = 1$.

Definition 11.4.5: (a) The group Γ_1 is called the *wild inertia group* of L/K.

(b) The factor group Γ_0/Γ_1 is called the *tame inertia group* of L/K.

Proposition 11.4.7: For any intermediate field K' of L/K and any $s \geqslant -1$, the s-th ramification group of $\Gamma' = \mathrm{Gal}(L/K')$ in its own right is equal to $\Gamma' \cap \Gamma_s$.

Remark 11.4.8: Thus the lower numbering filtration behaves well with respect to the passage of subgroups. But to extend it to infinite galois groups we must study its behavior under passage to factor groups.

11.5 The upper numbering filtration

We keep the situation of Section 11.4.

Lemma 11.5.1: There exists an element $b \in L$ such that $\mathcal{O}_L = \mathcal{O}[b]$.

Definition 11.5.2: For any $\gamma \in \Gamma$ we set $i_{L/K}(\gamma) := v_L(^\gamma b - b)$.

Lemma 11.5.3: For any $\gamma \in \Gamma$ and any s we have $\gamma \in \Gamma_s$ if and only if $i_{L/K}(\gamma) \geqslant s+1$.

Now consider an intermediate field L' of L/K which is galois over K. Let π denote the canonical projection $\Gamma \twoheadrightarrow \bar{\Gamma} := \mathrm{Gal}(L'/K)$ with kernel $\Gamma' := \mathrm{Gal}(L/L')$.

Proposition 11.5.4: For any $\bar{\gamma} \in \bar{\Gamma}$ we have

$$i_{L'/K}(\bar{\gamma}) \;=\; \frac{1}{e_{L/L'}} \cdot \sum_{\gamma \in \pi^{-1}(\bar{\gamma})} i_{L/K}(\gamma).$$

Construction 11.5.5: We are interested in the function

$$\eta_{L/K} \colon [-1, \infty[\longrightarrow [-1, \infty[, \quad s \mapsto \int_0^s \frac{dx}{[\Gamma_0 : \Gamma_x]}.$$

Here for $s < 0$ we interpret $\int_0^s$ as $-\int_{-s}^0$, and $[\Gamma_0 : \Gamma_x]$ as $[\Gamma_x : \Gamma_0]^{-1}$ for $x < 0$.

Proposition 11.5.6: The function $\eta_{L/K}$ is monotone increasing and bijective.

Proposition 11.5.7: For any $s \in [-1, \infty[$ we have

$$\eta_{L/K}(s) \;=\; \frac{1}{|\Gamma_0|} \cdot \sum_{\gamma \in \Gamma} \min\{i_{L/K}(\gamma), s+1\} - 1.$$

Theorem 11.5.8: *(Herbrand)* For any $s \in [-1, \infty[$ we have $\pi(\Gamma_s) = \bar{\Gamma}_{\eta_{L/L'}(s)}$.

Proposition 11.5.9: We have $\eta_{L/K} = \eta_{L'/K} \circ \eta_{L/L'}$.

Definition 11.5.10: For any real number $t \geqslant -1$ we define the *t-th ramification group of L/K in the upper numbering* as $\Gamma^t := \Gamma_{\eta_{L/K}^{-1}(t)}$.

Proposition 11.5.11: For any $t \in [-1, \infty[$ we have $\pi(\Gamma^t) = \bar{\Gamma}^t$.

Now consider an arbitrary galois extension L/K which is not necessarily finite.

Definition 11.5.12: For any real number $t \geqslant -1$ we define the *t-th ramification group of L/K* as

$$\mathrm{Gal}(L/K)^t \;:=\; \varprojlim_{L'} \mathrm{Gal}(L'/K)^t,$$

where the limit extends over all intermediate fields L' that are finite and galois over K.

Proposition 11.5.13: For any intermediate field L' of L/K that is galois over K and any real number $t \geqslant -1$ the restriction induces a surjection $\mathrm{Gal}(L/K)^t \twoheadrightarrow \mathrm{Gal}(L'/K)^t$.

11.6 Abelian extensions of $\mathbb{Q}_p$

Fix a prime number p.

Proposition 11.6.1: *(Kummer theory)* Consider a field K of chacteristic $\neq p$ which contains all p-th roots of unity μ_p. Let L/K be the maximal abelian extension whose galois group has exponent dividing p. Then L is generated by the p-th roots of all elements of $K^\times$ and there is a natural isomorphism

$$\mathrm{Gal}(L/K) \;\cong\; \mathrm{Hom}(K^\times/(K^\times)^p, \mu_p),\ \gamma \mapsto \big([x] \mapsto \tfrac{\gamma x}{x}\big).$$

Proposition 11.6.2: The maximal abelian extension of $\mathbb{Q}_p$ whose galois group has exponent p has degree p^3 if $p = 2$, respectively p^2 if $p > 2$.

Theorem 11.6.3: Every finite abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\mu_n)$ for some n.

Corollary 11.6.4: The maximal abelian extension of $\mathbb{Q}_p$ is

$$\mathbb{Q}_p^{\mathrm{ab}} \;=\; \mathbb{Q}_p\big(\textstyle\bigcup_n \mu_n\big).$$

Its galois group over $\mathbb{Q}_p$ possesses an isomorphism

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \;\cong\; \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times.$$

Remark 11.6.5: Since $\mathbb{Q}_p^\times \;\cong\; \mathbb{Z} \times \mathbb{Z}_p^\times$, this induces an uncanonical isomorphism between $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ and the profinite completion $(\mathbb{Q}_p^\times)\hat{}$. In local class field theory one actually makes this isomorphism canonical.

Remark 11.6.6: For $\mathbb{R} = \mathbb{Q}_\infty$ there is also a natural isomorphism

$$\mathrm{Gal}(\mathbb{Q}_\infty^{\mathrm{ab}}/\mathbb{Q}_\infty) \;\cong\; \{\pm 1\} \;\cong\; (\mathbb{Q}_\infty^\times)\hat{}.$$

11.7 The Kronecker-Weber theorem

Theorem 11.7.1: *(Kronecker-Weber)* Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.

Corollary 11.7.2: The maximal abelian extension of $\mathbb{Q}$ is

$$\mathbb{Q}^{\mathrm{ab}} \;=\; \mathbb{Q}\big(\textstyle\bigcup_n \mu_n\big).$$

Its galois group over $\mathbb{Q}$ possesses a natural isomorphism

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \;\cong\; \hat{\mathbb{Z}}^\times.$$

12 More material to be added

References

[AM] Atiyah, M. F., MacDonald, I. G.: *Introduction to Commutative Algebra*, Westview Press, 1969.

[G] Gouvêa: *p-adic Numbers.* Springer 1997

[H] Hungerford, T.W.: *Algebra.* Springer 1974

[IR] Ireland, K., Rosen, M.: *A Classical Introduction to Modern Number Theory.* Springer 1990

[L] Lang, S.: *Algebraic Number Theory.* Springer 1994

[M] Milne, J.S.: *Algebraic number theory.* Course Notes from 1996, last version from July 2020: `http://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[N] Neukirch, J.: *Algebraic Number Theory.* Springer 1999.

[R] Ribes, L., Zalesskii, P.: *Profinite groups.* Springer 2010.

[Se] Serre, J.-P.: *Local fields.* Springer 1979.

[Si] Siegel, C. L.: *Lectures on the Geometry of Numbers.* Springer 1989

[SL] Stevenhagen, P., Lenstra, H. W.: Chebotarëv and his density theorem. *Math. Intelligencer* **18** (1996), no.2, 26–37.

[Tsch] Tschebotareff, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Ann.* **95** (1926), no. 1, 191–228.

Some (rather incomplete) indications for individual chapters:

Chapter 1: [AM] Ch.5; [H] Ch.VIII; [N] Ch.I §2-3; [L] Ch.I

Chapter 2: [N] Ch.I §4; [L] Ch.V; [Si]

Chapter 3: [N] Ch.I §3, §5, §8, §10; [L] Ch.IV; [IR] Ch.5-6, Ch.13.

Chapter 4: [N] Ch.I §5-6, Ch.II §2; [L] Ch.VI

Chapter 5: [N] Ch.I §7; [L] Ch.V

Chapter 6: [AM] Ch.9; [N] Ch.I §9, Ch.II §2;

Chapter 7: [L] Ch.VI §3, Ch.VIII; [SSL], [Tsch]

Change Log:

Version of 21.01.2024:

Chapters 8–11 added.

Version of 22.11.2023:

22. 12. 2023: Bibliography expanded.

15. 12. 2023: Corrected the formula for the regulator in Definition 7.3.1.

13. 12. 2023: Corrected formulas in Propositions 7.5.6 (c) and 7.6.7.

Version of 12.11.2023:

12. 12. 2023: Section 7.8 added and Theorem 7.7.2 moved to Section 7.9.

28. 11. 2023: In Proposition 6.7.4 the condition "$L = K(\beta)$" added.

16. 11. 2023: Corrections in Def. 6.4.1 and Props. 6.4.3 and 6.6.6.

Version of 09.11.2023:

09. 11. 2023: Assumption 6.2.1 added and the rest of §6.2 renumbered. As a result of Assumption 6.2.1 substantial changes in §6.3–4 and reformulations in 6.7.6 and 6.8.4–7.

08. 11. 2023: Corrected Proposition 5.4.5: $\varepsilon \geqslant \frac{\sqrt{D}+\sqrt{D-4}}{2} > 1$.

07. 11. 2023: Chapter 7 added.

Version of 31.10.2023:

31. 10. 2023: Chapter 6 added.

25. 10. 2023: Corrected $\sqrt{|\operatorname{disc}(\mathfrak{a})|}$ in Proposition 4.2.1.

20. 10. 2023: Corrected Theorem 4.2.2.

18. 10. 2023: Corrected Definition 3.6.4 and two typos in Proposition 4.1.2.

13. 10. 2023: Proposition 3.2.1 and typos in §3.6 corrected.

12. 10. 2023: Theorem 3.6.7 expanded.

11. 10. 2023: Typos in §3.1-4 corrected and items 3.7.1-5 rearranged and renumbered.

Version of 06.10.2023:

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