Algebraic Number Theory

Lecture Notes

January 17, 2025

Contents

1 Integral elements

Definition 1.1

$\varphi : A \longrightarrow B$, $b \in B$ is integral over A iff $\exists f \in A[t]$ monic with $f(b) = 0$. The ring B is integral over A if all $b \in B$ are integral over A.

Example 1.1. $\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ is integral over $\mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$.

Proposition 1.1

$\varphi : A \longrightarrow B$ then the following are equivalent:

(i) b is integral over A

(ii) $A[b]$ is finitely generated as an A-module.

(iii) $A[b] \subset C \subset B$, C is finitely generated as an A-module.

(iv) There exists a faithful $A[b]$-module M finite as an A-module.

Definition 1.2

$A \subset B$, $\overline{A} = \{b \in B \mid b \text{ integral over } A\}$ is called the integral closure of A in B.

Corollary 1.1

$\overline{A}$ is a ring.

Proposition 1.2

$A \subset B$, $B \subset C$ are integral $\Rightarrow A \subset C$ is integral.

Corollary 1.2

$A \subset B$ then $\overline{\overline{A}} = A$.

Our objects of study: $\mathcal{O}_K$. It is clearly integrally closed.

$$\begin{tikzcd} \mathbb{Q} \arrow[r] & K \\ \mathbb{Z} \arrow[u] \arrow[r] & \overline{\mathbb{Z}} =: \mathcal{O}_K \arrow[u] \end{tikzcd}$$

Figure 1: $\mathcal{O}_K$

Remark: A is UFD then $A = \overline{A} \subset \mathrm{Frac}(A)$

Proof. Same as for $\mathbb{Z} \subset \mathbb{Q}$. □

Proposition 1.3

$A = \overline{A} \subset K = \mathrm{Frac}(A)$. $L|K$ separable field extension. Then $l \in L$ integral over $A \Leftrightarrow f_l \in A[t]$.

Example 1.2. $K = \mathbb{Q}[\sqrt{5}]$ $\mathcal{O}_K = ?$. Let $x = a + b\sqrt{5} \in \mathcal{O}_K \subset K$. Then $f_x = (X - x)(X - \overline{x}) = X^2 - 2aX + a^2 - 5b^2$. Thus $2a, a^2 - 5b^2 \in \mathbb{Z}$. From this one can calculate that $\mathcal{O}_K = \mathbb{Q}[\frac{1+\sqrt{5}}{2}] \neq \mathbb{Q}[\sqrt{5}]$.

2 Free A-modules

Theorem 2.1: Structure theorem for finitely generated Abelian groups

Any finitely generated $\mathbb{Z}$-module M is isomorphic to $M = \mathbb{Z}^r \oplus \mathbb{Z}/(d_1) \oplus \cdots \oplus$, $d_i \mid d_{i+1}$. In other terms $M = \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/(p_i^{e_i})$

Construction: B is an A-algebra free as an A-module. Let $b \in B$. $\mathrm{tr}(b) := \mathrm{tr}(M_b)$, $\mathrm{Nm}(b) := \det(M_b)$ where M_b is the matrix of the multiplication map $\cdot b$. Then $\mathrm{tr} : B \longrightarrow A$ is additive and A-linear and $\mathrm{Nm} : B \longrightarrow A$ is multiplicative.

Proposition 2.1

$L|K$ finite extension, $[L : K] = n$. Let $l \in L$ with minimal polynomial $f_l(x) = x^m - a_1x^{m-1} + \cdots \pm a_m$. Let $s = \frac{n}{m}$. Then $\mathrm{tr}(l) = sa_1$, $\mathrm{Nm}(l) = a_m^s$.

3 Bilinear forms

Let M be free as an A-module and let $\Psi : M \times M \longrightarrow A$ be a bilinear form with Gram-matrix $G = (g_{ij})$, i.e. $g_{ij} = \Psi(e_i, e_j)$. The discriminat of Ψ with respect to the standard basis is $\operatorname{disc}\Psi = \det(G)$. Let B be a change-of-basis matrix. Then the Gram-matrix with respect to the new basis is given by $G' = B^tGB$ meaning that $\det(G) = \det(B)^2\det(G)$. This means that usually for rings the determinant of the Gram-matrix is not independent of the chosen basis. However if $A = \mathbb{Z}$, then the discriminant is independent of bases!

For a field extension $L|K$ we define $\operatorname{disc}_{L|K} := \operatorname{disc}\mathrm{Tr}$, where Tr is the trace form $\mathrm{Tr} : L \times L \to K$, $(l, l') \mapsto \mathrm{tr}(l \cdot l')$.

Example 3.1. $L = \mathbb{Q}[\sqrt{d}]$, $\mathcal{B} = (1, \sqrt{d})$, $\mathrm{Tr} = \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\sqrt{d}) \\ \mathrm{tr}(\sqrt{d}) & \mathrm{tr}(\sqrt{d}) \end{pmatrix}$. Then $\operatorname{disc}_{L|K}(\mathcal{B}) = 4d$.

Proposition 3.1

$L|K$ finite separable extension of degree $n = [L : K]$. Let $\sigma_i : L \to \overline{L}$ be the embeddings of L in an algebraically closed field (or even the normal closure of L). Then for any $l \in L$, $tr(l) = \sum_{i=1}^n \sigma_i l$ and $\mathrm{Nm}(l) = \prod_{i=1}^n \sigma_i(l)$.

In particular, if $L|K$ is Galois, then $\mathrm{tr}(l) = \sum_{\sigma \in \mathrm{Gal}(L|K)} \sigma(l)$.

$\Psi : M \times M \to A$, $\mathrm{disc}(\Psi) = 0 \Leftrightarrow: \Psi$ is degenerate $\Leftrightarrow \Psi(m, \cdot) \equiv 0$ for some $m \neq 0 \Leftrightarrow \Psi(\cdot, m) \equiv 0$ for some $m \neq 0$. We need the trace form to be non-degenerate for separable $L|K$.

Theorem 3.1: Dedekind's theorem on the independence of characters

Let K be a field, G a group and $\chi_i : G \to K*$ pairwise different. Then $\{\chi_i\}_{i \in I}$ is linearly independent over K.

Proposition 3.2

Let $A = \overline{A} \subset K$ and B be the integral closure of A in L for a finite field extension $L|K$. Then for any $b \in B$, $\mathrm{tr}_{L|K}(b), \mathrm{Nm}_{L|K}(b) \in A$.

Proof. Since $b \in B$, $\mathrm{minpol}(b) \in A[X]$. □

Proposition 3.3

Let $L|K$ be a finite separable field extension, $n = [L : K]$. Let σ_i be the embeddings of L in its Galois closure. For a basis $\mathcal{B} = (l_1, \ldots, l_n)$ of L as a K-vector space we have $\mathrm{disc}_{L|K}^{\mathcal{B}} = \det^2((\sigma_i l_j)_{ij}) \neq 0$.

Proof. $\det(\mathrm{Tr}_{L|K}) = \det((\mathrm{tr}(l_i l_j)_{ij})) \det((\sum_k \sigma_k(l_i l_j))_{ij}) = \det((\sum_k \sigma_k (l_i)\sigma_k(l_j))) = \det^2(\sigma_k(l_i))$. Let $M = (\sigma_k l_j)_{kj}$ Suppose $\det M = 0$. Then the rows are linearly dependent, meaning $\sum \lambda_i \sigma_i(l_j) = 0 \forall j$. Thus $\sum \lambda_i \sigma_i \equiv 0$, contradicting Dedekind's theorem on the independence of characters. □

Theorem 3.2

Let $A \subset K$ be integrally closed, $L|K$ finite and separable of degree n. Then the integral closure B of A in L is a finitely generated A-module of rank n. The rank of a module B is defined as $\dim_K(K \otimes_A B)$. Furthermore

- if A is Noetherian, so is B.
- if A is a PID then $B \cong A^{\oplus n}$

Corollary 3.1

If $A = \mathbb{Z}$, $K|\mathbb{Q}$ a finite field extension, then $\mathcal{O}_\mathrm{K} = \mathbb{Z}^n$ where $n = [K : \mathbb{Q}]$.

Definition 3.1

A basis of $\mathcal{O}_\mathrm{K}$ as a $\mathbb{Z}$-module is called an integral basis of $\mathcal{O}_\mathrm{K}$.

Example 3.2.

- Let $K = \mathbb{Q}[\sqrt{d}]$ and $\mathcal{B} = (1, \sqrt{d})$ which is a basis of K consisting of integral elements. Then $\mathrm{disc}^{\mathcal{B}}_{K|\mathbb{Q}} = \det \begin{pmatrix} \mathrm{tr}(1) & \mathrm{tr}(\sqrt{d}) \\ \mathrm{tr}(\sqrt{d}) & \mathrm{tr}(d)) \end{pmatrix} = 4d$. Let $\mathcal{B}' = (e_1, e_2)$ be an integral basis of $\mathcal{O}_\mathrm{K}$. Then the elements of $\mathcal{B}$ can be written as a linear combinations over $\mathbb{Z}$ of the elements of $\mathcal{B}'$ meaning $\mathcal{B} = M\mathcal{B}'$ for some matrix M. Thus $4d = \mathrm{disc}^{\mathcal{B}} = \det^2(M)\,\mathrm{disc}^{\mathcal{B}'}$. Thus $\det(M) \mid 2$. If $|\det(M)| = 2$, $\mathbb{Z}(\mathcal{B}) \hookrightarrow \mathbb{Z}(\mathcal{B}')$ is of index 2. Thus the candidates to be checked for an integral basis of $\mathcal{O}_\mathrm{K}$ are $\frac{1}{2}, \frac{\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}$. Since the first two can be easily discarded, we get $(1, \frac{1+\sqrt{d}}{2})$ as an integral basis.

  not necessarily an integral basis!

- Let $\mathcal{B} = (e_1, \dots, e_n)$ be a basis of $K|\mathbb{Q}$ consisting of integral elements. $\mathrm{disc}^{\mathcal{B}}_{L|K} = \pm \prod_{i=1}^n p_i e_i$. If $e_i < 2$, then $\mathcal{B}$ is automatically an integral basis. Else if there is only one prime $p := p_i$ with $e_i = 2$ and the rest $e_j < 2$, we only have to check elements of the form $\sum_{i=1}^n \frac{n_i l_i}{p}$ to find an integral basis.

Let $f \in K[X]$ with $f = \prod(X\alpha_i)$ in $\overline{K}$. $\Delta(f) := \prod_{i<j}(\alpha_i - \alpha_j))$ which is a polynomial in the coefficients of f. If $\deg f = 2$ and $f \in \mathbb{R}[X]$. Then if $x_1 = z \in \mathbb{C} \setminus \mathbb{R}$. then $x_2 = \overline{z}$, meaning $z - \overline{z} \in i\mathbb{R} \Rightarrow (z - \overline{z})^2 \in \mathbb{R}_{\leq 0}$. If $\deg f = 3$ and α_1 is real and α_2 is not real, then $\alpha_3 = \overline{\alpha_1}$. Thus $\Delta(f) \in i\mathbb{R}$.

Proposition 3.4

$\mathcal{O}_K$ is the maximal subring of K finitely generated as a $\mathbb{Z}$-module.

Proof. Let $B \subset K$ be a finitely generated $\mathbb{Z}$-module. Then by a previous theorem since $\mathbb{Z}$ is a PID we have $B = \mathbb{Z}^n$. Let $b \in B$. Thus $\mathbb{Z}[b]$ is free and finite as a $\mathbb{Z}$-module meaning that b is integral over $\mathbb{Z}$. Thus $b \in \mathcal{O}_K$. □

Proposition 3.5

Let $L|K$ be a field extension. Let $L = K[x]$ and f_x be the minimal polynomial of x over K. With $\deg f = n$ and $\mathcal{B} = (1, x, \ldots, x^{n-1})$ basis of L let $x_i = \sigma_i(x)$ be the different images of x under embeddings of L in its algebraic closure. Then

$$\operatorname{disc}^{\mathcal{B}}_{L|K} = \prod_{i<j} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \operatorname{Nm}(f'(x))$$

Example 3.3. Let $f = X^n - a$ and $L = K[x]|K$ with $x^n = a$, $n \neq= 0 \in L$. Then $g = f' = nx^{n-1} = n\frac{x^n}{x} = \frac{na}{x}$. Clearly then $y \in K[x]$. Since $x = \frac{na}{y} \in K[y]$ we have $K[x] = K[y]$. We need now only the minimal polynomial of y. $0 = f(x) = f(\frac{na}{y}) = (\frac{na}{y})^n - a = 0 \implies y^n - n^n a^{n-1} = 0$. Thus $\operatorname{Nm}(y) = \pm n^n \cdot a^{n-1}$ and $\operatorname{disc}^{\mathcal{B}} = \pm n^n a^{n-1}$.

Corollary 3.2

If $f = X^n + aX + b$ then $\operatorname{disc}(f) = \_\, a^n + \_\, b^{n-1}$.

By a simple calculation

meaning calculation to be inserted

$$\boxed{\operatorname{disc}(f) = (-1)^{\binom{n}{2}}(1-n)^{n-1}a^n + (-1)^{\binom{n}{2}} n^n b^{n-1}}$$

We thus get

$$\begin{aligned}
\operatorname{disc}(X^2 + aX + b) &= a^2 - 4b \\
\operatorname{disc}(X^3 + aX + b) &= -27b^2 - 4a^3 \\
\operatorname{disc}(X^5 + aX + b) &= 5^5 b^4 - 4^4 a^5
\end{aligned}$$

Example 3.4. $\operatorname{disc}(X^5 - X - 1) = 19 \cdot 5 \cdot 3$ meaning that $\mathcal{B} = (1, \cdot, x^4)$ is an integral basis of $\mathcal{O}_K$.

Proposition 3.6

Let $K|\mathbb{Q}$ be a finite field extension and $\mathscr{B}$ a $\mathbb{Q}$-basis of K. Then $\operatorname{sgn}(\operatorname{disc}^{\mathscr{B}}) = (-1)^s$ where s is the number of non-real embedding of K in $\mathbb{C}$.

Theorem 3.3: Stickelberger's theorem

Let $K|\mathbb{Q}$ be a finite extension of degree n and $\mathscr{B}$ be a basis of integral elements. Then $\operatorname{disc}^{\mathscr{B}} \equiv 0, 1 \pmod 4$.

4 Dedekind rings

Example 4.1. Let $K|\mathbb{Q}$ be a finite extension of degree n. Then

- $\mathcal{O}_K = \mathbb{Z}^n$
- is Noetherian
- is integrally closed
- $\operatorname{Frac}(\mathcal{O}_K) = K$.

Let $\mathfrak{a} \subset \mathcal{O}_K$ be a non-zero ideal. Pick a non-zero element $a \in \mathfrak{a}$. Then $\mathbb{Z}^n = (a) \subset \mathfrak{a} \subset \mathcal{O}_K = \mathbb{Z}^n$ thus $\mathfrak{a} = \mathbb{Z}^n$ is a free $\mathbb{Z}$-module. This implies that $\mathcal{O}_K/\mathfrak{a}$ is finite. In fact if we take a prime ideal $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ then $\mathfrak{p}$ is maximal since every finite domain is a field.

Remark 4.1. This means that $\mathcal{O}_K$ is of (Krull-)dimension 1.

Definition 4.1

A ring A is a Dedekind ring if A is an integrally closed, Noetherian ring of dimension one.

Example 4.2. $\mathcal{O}_K, K[x]$ are Dedekind.

Lemma 4.1

Let $A \subset B$ be a ring extension such that B is a finite A-module. Then A is a field $\Leftrightarrow$ B is a field.

Proposition 4.1

Let $A \subset K := \mathrm{Frac}(A)$ be a Dedekind ring and $L|K$ be a finite separable field extension. Then the integral closue $B = \overline{A} \subset L$ is also a Dedekind ring.

Section on local properties missing

5 Valuations and DVR's

Definition 5.1

A valuation v on a field K is a group homomorphism $v : K^* \longrightarrow G$ where G is a totally ordered Abelian group satisfying $v(\lambda + \mu) \geq \min(v(\lambda), v(\mu))$. A valuation is discrete is $G = \mathbb{Z}$.

Remark 5.1. We sometimes assume that $v : K^* \longrightarrow \mathbb{Z}$ is surjective.

Definition 5.2

A domain A is a discrete valuation ring (DVR) if $A = v^{-1}(\mathbb{N}_{\geq 0})$ for some discrete valuation on $\mathrm{Frac}(A)$.

Example 5.1. Let $K = \mathbb{Q}$ and fix a prime number p. Then for $\frac{a}{b} = p^m \frac{\overline{a}}{\overline{b}}$ with $(\overline{a}, \overline{b}) = (\overline{a}, p) = (\overline{b}, p) = 1$ we assign $v_p(\frac{a}{b}) = m$. This is a discrete valuation. Its DVR is $v_p^{-1}(\mathbb{N}) = \{\frac{a}{b} \mid p \nmid b\} = \mathbb{Z}_{(p)}$.

Proposition 5.1

Let $v : K^* \longrightarrow \mathbb{Z}$ be a valuation and $A = v^{-1}(\mathbb{N})$. Let $t \in v^{-1}(1)$.

(i) A is noetherian

(ii) $m = t$ is the only maximal ideal

(iii) $\mathfrak{a} \in A$ ideal then $\mathfrak{a} = (t^n)$.

(iv) A is integrally closed

Theorem 5.1

Let $(A, \mathfrak{m})$ be a local Dedekind domain. Then A is a DVR.

Remark 5.2. Let A be a Dedekind ring and $\mathfrak{m} \subset A$ maximal. Then $A_{\mathfrak{m}}$

is a local Dedekind ring $\implies A_{\mathfrak{m}}$ is a DVR.

Theorem 5.2

Let $A \subset K$ be a Dedekind ring, and $\mathfrak{a} \subset A$ be an ideal. Then $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{m}_i^{e_i}$. This product is unique upto refactoring.

Lemma 5.1

Let A be a Dedekind ring, then any ideal $\mathfrak{a} \subset A$ contains a product of maximal ideals.

Lemma 5.2

Let A be a ring $\mathfrak{m} \subset A$ maximal. Let $\mathfrak{m}_{\mathfrak{m}}$ be the maximal ideal of the local ring $A_{\mathfrak{m}} = (A \setminus \mathfrak{m})^{-1}A$. Then for any $n \in \mathbb{N}$ $A/\mathfrak{m}^n \cong A_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}^n$.

6 Projective modules over Dedekind rings

Definition 6.1

$M \in \mathrm{Mod}(A)$ is *projective* if for every modules N and N^* with a surjection $\pi : N \twoheadrightarrow N^*$ and homomorphism $\alpha : M \longrightarrow N^*$ there exists a so called *lift* $\widetilde{\alpha} : M \longrightarrow N$ such that $\alpha = \pi \circ \widetilde{\alpha}$.

Example 6.1.

- $M = A^n$ is projective.
- M is projective $\implies M \oplus M'$ is free for some M'.

Corollary 6.1

$0 \neq \mathfrak{a} \subset A$ ideal is a Dedekind ring. Then $\mathfrak{a}$ is projective as an A-module.

Corollary 6.2: Existence of inverse

For any $\mathfrak{a} \neq 0$ there exists an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = (c)$ for some $c \in A$.

7 Ideal class group

Definition 7.1

A fractional ideal is finitely generated A-module in $K = \operatorname{Frac} A$.

Remark 7.1. $M = \langle \frac{a_i}{s_i} \rangle$. Let $s = \prod_{i=1}^{N} a_i$. Then $sM = \langle a_i \rangle = \mathfrak{a}$ is an ideal. Thus all fractional ideals are of the from $\frac{1}{s}\mathfrak{a}$ for some ideal $\mathfrak{a}$.

Remark 7.2. Let $\lambda, \mu \in K^*$. Define $(\lambda) = A\lambda$. Then $(\lambda) = (\mu) \Leftrightarrow \mu \in (\lambda) \wedge \lambda \in (\mu) \Leftrightarrow \lambda = u\mu$ for some unit u.

Definition 7.2: Ideal class group

Define the *ideal class group* Cl_K through the following exact sequence $0 \longrightarrow A^* \longrightarrow K^* \longrightarrow \operatorname{Frac}\operatorname{Id}(A) \longrightarrow \mathrm{Cl}_K \longrightarrow 0$, where Frac Id is the set of all fractional ideals. Then Cl_K is a group.

Definition 7.3

Let $A \subset K = \operatorname{Frac} A$ be a Dedekind ring and $L|K$ be a finite field extension. Let B be the integral closure of A in L. Then B is Dedekind. Let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}^e = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$. The e_i are called the *ramification index* of $\mathfrak{p}_i$. $f_i = [B/\mathfrak{p}_i : A/\mathfrak{p}]$ is called the *inertial degree.*

Theorem 7.1

$n = \sum_{i=1}^{g} e_i f_i$. If $L|K$ is Galois then the Galois group G acts transitively on the prime ideals $\mathfrak{p}_i$. We then have $e_i = e$, $f_i = f$ for all i and thus $n = efg$.

Proposition 7.1

Let $A \subset K$ be Dedekind.

- $\mathfrak{a} \subset A$ is projective
- M is projective $\Rightarrow M \cong A^{n-1} \oplus \mathfrak{a}$.
- $A^{n-1} \oplus \mathfrak{a} \cong A^{n-1} \oplus \mathfrak{b} \Leftrightarrow \mathfrak{a} \sim \mathfrak{b}$.
- $\forall S \subset A$ $S^{-1}A \otimes_A M \cong S^{-1}M$.

Theorem 7.2: L

t $A \subset K$ be Dedekind, $L|K$ finite field extension and B the integral closure of A in L. Assume that $B \cong A^n$ and that $\forall \mathfrak{p} \subset A$ $A/\mathfrak{p}$ is perfect. Let $\mathscr{B}$ be a basis of B as an A-module. Then $(\Delta_{L|K}) = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$. Then $\mathfrak{p} \subset A$ is ramified $\Leftrightarrow$ $\mathfrak{p}$ is one of the $\mathfrak{p}_i$.

Corollary 7.1

Let $K|\mathbb{Q}$ be finite. Then there are only finitely many primes dividing $\Delta_{K|\mathbb{Q}}$, meaning that only finitely many primes ramify.

8 Norm of an ideal

Definition 8.1

Let $L|K$ a finite field extension and $\mathfrak{q} \subset \mathcal{O}_K$. Then $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}$ is also prime. Let $[\mathcal{O}_K/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = f$. Then the define the *norm* of $\mathfrak{q}$ by $\mathrm{Nm}(\mathfrak{q}) = \mathfrak{q}^f$. Define $\mathrm{Nm}(\prod_i \mathfrak{q}_i^{e_i}) = \prod_i \mathrm{Nm}(\mathfrak{q}_i)^{e_i}$.

Proposition 8.1

- $\mathfrak{a} \subset \mathcal{O}_K$ then $\mathrm{Nm}(\mathfrak{a}^e) = \mathfrak{a}^n$.
- $L|K$ Galois, then $\mathrm{Nm}(\mathfrak{a}) = \prod_{\sigma \in G} \sigma(\mathfrak{q})$.
- $\mathrm{Nm}_{M|K} = \mathrm{Nm}_{L|K} \circ \mathrm{Nm}_{M|L}$ for a tower $K \to L \to M$ of fields.
- $b \in \mathcal{O}_K$ then $\mathrm{Nm}((b)) = (\mathrm{Nm}(b))$.

9 Latices

Definition 9.1: Latice

Let $V \cong \mathbb{R}^n$ be a Euclidean vector space $(V, \langle\cdot\rangle)$. A subgroup $\Lambda \subset V$ is called a *latice* if

- $\Lambda \cong \mathbb{Z}^n$
- Λ is spanned by a basis of V

Example 9.1. $\mathbb{Z}^n \subset \mathbb{R}^n$. If $\mathscr{B}_lambda = (l_1, \ldots, l_n)$ is a latice basis, then for any other basis $\mathscr{B}'_\Lambda = A \cdot \mathscr{B}_\Lambda$ with $A \in \mathrm{GL}_n(\mathbb{Z})$

Definition 9.2

Let Λ ba lattice. The *covolume* of Λ for a basis $\mathscr{B}_\Lambda = (l_i)$ is the determinant $\det(G)$ where $G = (g_{ij})$ with $g_{ij} = \langle l_i, l_j \rangle$.

Remark 9.1.

- For a different basis $\mathscr{B}' = A\mathscr{B}$ we have $\deg(G') = \det(A^t G A) = \det(A)^2 \det(B)$.
- $\mathrm{covol}(\Lambda) = \mathrm{vol}(V/\Lambda) = \mathrm{vol}(F)$ where $F = \{\sum_{i=1}^n x_i l_i \mid x_i \in [0,1]\}$.

Definition 9.3

A subset $K \subset V$ is called

- *central* if $x \in K \Leftrightarrow -x \in K$.
- *convex* if $x, y \in K \Rightarrow tx + (1-t)y \in K \forall t \in [0,1]$.

Theorem 9.1: Minkowskis latice point theorem

Let $K \subset V$ be a compact, convex and central subset such that $\mu(K) \geq 2^n \mu(F_\Lambda)$. Then K contains a non-zero latice point of Λ.

Let $K|\mathbb{Q}$ be a number field of degree n. Since the extension is separable there exists an $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ with $f = f_\alpha$ its minimal polynomial. We will construct $V_K \cong \mathbb{R}^n$. For any root α_i of f we get an embedding $K \to \mathbb{C}$. Let r be the number of purely real embeddings and s be the number of pairs of non-real complex embeddings. Then $n = r + 2s$. Let now

$$V_K = \bigoplus_{\sigma_i : K \to \mathbb{R}} \mathbb{R} \bigoplus_{\sigma_i : K \to \mathbb{C}} \mathbb{C}$$

Then $\dim_\mathbb{R} V_k = r + 2s = n$. Consider $v \in V_K$ with $v = (x_1, \ldots, x_r, z_1, \ldots, z_s)$. Define

$$\|v\|^2 = \sum_{i=1}^k x_i^2 + 2 \sum_{i=1}^s \|z_i\|^2$$

. Let $\nu : K \to V_K$ be given by $\nu(a)_i = \sigma_i(a)$.

Theorem 9.2

$\nu(O_K)$ is a lattice in V_K of covolume $2^{-s}\sqrt{|\Delta_K|}$.

Theorem 9.3

Let $K|\mathbb{Q}$ be finite. Then for any class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_\mathrm{K})$ there exists an ideal $\mathfrak{a} \in [\mathfrak{a}]$ such that

- $\mathfrak{a} \subset \mathcal{O}_\mathrm{K}$.
- $\mathrm{Nm}(\mathfrak{a}) \leq \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|\Delta_K|}$

Corollary 9.1

$\mathrm{Cl}(\mathcal{O}_\mathrm{K})$ is finite.

Corollary 9.2

Let $K|\mathbb{Q}$ be a number field of degree $n \geq 2$. Then $\Delta_K \neq 1$.

Proposition 9.1

- $\mathrm{covol}(\sigma(\mathrm{Nm}(\mathfrak{a})))\sqrt{|\Delta_K|}$.
- $x_i \in \mathbb{R}_{\geq 0}$

Proposition 9.2: AM-GM Inequality

For $x_i \in \mathbb{R}_{\geq 0}$ we have $\sqrt[n]{\prod_i x_i} \leq \frac{\sum_i x_i}{n}$

Proof. WLOG we may assume that $\sum_i x_i = 1$. Let $K := \{x \in \mathbb{R}_{\geq 0} \mid \sum_i x_i = 1\}$. The set is clearly compact. Consider now $f : K \to \mathbb{R}$ given by $(x_i) \mapsto \prod_i x_i$. Since the function is continuous, there must a maximum. Then $\nabla f = (\prod_i x_i)(\frac{1}{x_1}, \dots, \frac{1}{x_n})^t$. Let x be the maximum of f and $t \in \mathbb{R}^n$ arbitrary. $f(x + \varepsilon t) = f(x) + \varepsilon t \cdot \nabla F$ for $\varepsilon \to 0$. Thus $t \perp \nabla f(x)$. Choosing $t = (1, -1, 0, \dots, 0)^t$ we get $x_1 = x_2$. Similarly $x_1 = \dots = x_n = \frac{1}{n}$. Thus we get $\prod_i x_i \leq \frac{1}{n}$. □

$K = K(t) := \{x \in V_K \mid \sum_{i=1}^r |x_i| + 2\sum_{i=1}^s \|x_{r+1}\| \leq t\}$. Then K is closed. Furtehrmore $\mathrm{vol}(K(t)) = t^n \mathrm{vol}(K(1))$.

Proposition 9.3

$\mathrm{vol}\, K(1) = \frac{2^r(\frac{\pi}{2})^2}{n!}$.

Theorem 9.4

For anny class $\eta \in \mathrm{Cl}(\mathcal{O}_\mathrm{K})$ there exists a non-fractional ideal $\mathfrak{a} \in \eta$ with $\mathrm{Nm}(\mathfrak{a}) \leq \frac{n!}{n^n}(\frac{4}{\pi})^s\sqrt{|\Delta_K|}$.

Theorem 9.5

A subgroup $\Gamma \subset V$ is discrete $\Leftrightarrow$ Γ is a lattice.

10 Unit theorem

Main result to be proved:

Theorem 10.1: Unit theorem

Let $K|\mathbb{Q}$ be finite of degree $n = r + 2s$. Then $u_K = {\mathcal{O}_\mathrm{K}}^* = \mu(K) \oplus \mathbb{Z}^{r+s-1}$ where $\mu(K) = \{\lambda \in K \mid \exists n(\lambda) : \lambda^{n(\lambda)} = 1\}$.

Example 10.1. $\mu(\mathbb{Q}(i)) = \langle i \rangle$.

Lemma 10.1: Easy finiteness lemma

Let $M \in \mathbb{R}$ and $m \in \mathbb{N}$. Then

$$\#\left(\{z \in \mathbb{C} \mid \text{ integral over } \mathbb{Z}; \deg(z) \leq m; \|\sigma_i z\| \leq M \forall i\}\right) < \infty$$

Proposition 10.1

LEt $z \in K^*$. Then we have $z \in \mu(K) \Leftrightarrow \|\sigma(z)\| = 1 \forall \sigma : K \to \mathbb{C}$

Remark 10.1. $\mu(K) \subset U_K = {\mathcal{O}_\mathrm{K}}^* \subset \mathcal{O}_\mathrm{K}$

Theorem 10.2

$\operatorname{rank} U_K = r + s - 1$. In particular $U_K \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}$.

11 Regulator

Let $K|\mathbb{Q}$ be a number field. Then ${\mathcal{O}_\mathrm{K}}^* = \mathbb{Z}/(m) \oplus \mathbb{Z}^{r+s-1}$. We can embed $L : \mathcal{O}_\mathrm{K} \to \mathbb{R}^{r+s}$ by $L(x) = (\log(|\sigma_1(x)|), \ldots, \log(\|\sigma_{r+s}(x)\|^2))$ .The image $\operatorname{im} L$ is a lattice in $H = ((1, \ldots, 1)^t)^\perp$.

Definition 11.1: Regulator

The *regulator* R_K of K is

$$R_K = \frac{1}{\sqrt{r+s}} \cdot \operatorname{covol}((L(\mathcal{O}_K{}^*) \subset H))$$

Let $v = \frac{1}{\sqrt{r+s}}(1, \dots, 1)^t$, which is of norm 1. Then $R_K = \operatorname{covol}(\Lambda = (L(\varepsilon_1), \dots, L(\varepsilon_{r+s-1}), v))$

Proposition 11.1

$R_K = |\det(M_{ij})|$ with $(M_{ij}) = (L(\varepsilon_1), \dots, v)$

Corollary 11.1

$R_K = |\det((L(\varepsilon_1), \dots, L(\varepsilon_{r+s-1})))|$

Example 11.1. Let $K = \mathbb{Q}[\sqrt{d}]$ and $\varepsilon = a + b\sqrt{d}$ be a generator of U_K. $R_K = \log|z|$.

12 Dedekind zeta Function

Definition 12.1

Let $K|\mathbb{Q}$ be a number field of degree $n = r + 2s$. Let $\sigma_i, \dots, \sigma_{r+s}$ be the embeddings of K in $\mathbb{C}$, $h := \operatorname{Cl}(\mathcal{O}_K)$ and $\mathbb{R}_K$ the regulator of K. The *Dirichlet zeta function* is defined by

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subset \mathcal{O}_K} \frac{1}{\operatorname{Nm}(\mathfrak{a})^s}$$

Remark 12.1. For $K = \mathbb{Q}$ the function is well defined for $s > 1$ (even for $s \in \mathbb{C}, \Re(s) > 1$, not relevant here though). Note that the function $x \mapsto x^{-s}$ is strictly decreasing. Thus $\int_{n-1}^{n} x^{-s}\,\mathrm{d}x > \frac{1}{n^s} > \int_{n}^{n+1} x^{-s}\,\mathrm{d}x$. Hence $1 + \int_1^\infty x^{-s}\,\mathrm{d}x > \zeta_{\mathbb{Q}}(s) > \int_1^\infty x^{-s}\,\mathrm{d}x$. Therefore $s > (s-1)\zeta_{\mathbb{Q}}(s) > 1$. Thus

$$\lim_{s \to 1^+} \zeta_{\mathbb{Q}}(s)(s-1) = 1$$

.

Theorem 12.1: Dream

$\lim_{s\to 1^+}\zeta_K(s)(s-1) = h_K\cdot c_K$ for some easy function c_K depending on r, s, R_K.

1° trick:

Proposition 12.1

$$\zeta_K(s) = \sum_{c\in \mathrm{Cl}(\mathcal{O}_K)}\sum_{[\mathfrak{a}]=c}\frac{1}{\mathrm{Nm}(\mathfrak{a})^s} =: \sum_{c\in \mathrm{Cl}(\mathcal{O}_K)}\zeta_c(s)$$

.

Definition 12.2: Fundamental domain

Let $l^* = (1,\ldots,1,2,\ldots,2)$ (r and s times respectively). Then $l^*, L(\varepsilon_1),\ldots,L(\varepsilon_{r+s-1})$ is a basis of $\mathbb{R}^{r+s}$ for ε_i being a list of generators of U_K. Then the *fundamental doamin* $X\subset\mathbb{R}^n$ is defined by

$$\begin{aligned}X = \{x\in\mathbb{R}^n\ | 0 \le \arg(x_1) \le \frac{2\pi}{m};\\ &\mathrm{Nm}(x)\neq 0;\\ &L(x) = \lambda l^* + \sum_{i=1}^{r+s-1}\lambda_i L(\varepsilon_i)\forall\lambda\in\mathbb{R}_{\ge 0}, \lambda_i\in[0,1)\}\end{aligned}$$

Proposition 12.2

Let $c\in\mathrm{Cl}(\mathcal{O}_K)$ and $\mathfrak{a}'$ be a non-fractional ideal such that $c^{-1} = [\mathfrak{a}']$. Then

$$\zeta_C = \mathrm{N}(a')^s\sum_{(a)\subset\mathfrak{a}}\frac{1}{|\mathrm{N}(a)|^s} = \mathrm{N}(\mathfrak{a}')^s\sum_{a\in\mathfrak{a}';\sigma(a)\in X}\frac{1}{|\mathrm{N}(a)|^s}$$

Define $S := \{x\in X \mid \mathrm{N}(x) = 1\}$ and $T := \{x\in X\mid \mathrm{N}(x)\le 1\}$.

Lemma 12.1

S is bounded.

Lemma 12.2

T is bounded.

Lemma 12.3

Let $u \in U_K$ and $m_u : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ given by $(x_1, \ldots, z_{r+s})^t \mapsto (\sigma_1(u)x_1, \ldots, \sigma_{r+s}(u)z_{r+s})^t$. Then m_u is volume preserving.

Let $\mu(K) = \langle \eta \rangle$. Define $T_K := \eta^k T$ for $k = 0, \ldots, m-1$. Also define $T_{\text{all}} = \bigcup_{k=0}^{m-1} T_K$. Then clearly $\mu(T_{\text{all}}) = m\mu(T)$. Let $\overline{T} \subset T_{\text{all}}$ such that $x_i > 0$ for $i = 1, \ldots, r$. Then

$$\mu(\overline{T}) = 2^{-r}\mu(T_{\text{all}}) = \frac{m}{2^r}\mu(T)$$

Proposition 12.3

$\text{vol}(T) = \frac{R_K \cdot \pi^s \cdot 2^r}{m}$

13 Analytic class number formula

Theorem 13.1: Dirichlet Principle

Let $X \subset \mathbb{R}^n$ be a cone, and $\Lambda \subset \mathbb{R}^n$ a lattice of covolume μ. Let $F : X \longrightarrow \mathbb{R}_{>0}$ be a homogeneous function of degree n, i.e. $F(rx) = r^n F(x)$. Suppose T is bounded of volume V. Then is

$$\zeta(s) := \sum_{\lambda \in X \cap \Lambda} \frac{1}{F(\lambda)^s}$$

well-defined for $s > 1$ and $\lim_{s \to 1^+}(s-1)\zeta(s) = \frac{V}{\mu}$.

Applying the theorem above for ζ_K we get the analytic class number formula:

$$\lim_{s \to 1^+} \zeta_K(s)(s-1) = \frac{2^{r+2}\pi^s h_K R_K}{m\sqrt{|D|}}$$

Theorem 13.2: Euler's identity

$$\zeta_K(s) = \prod_{0 \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}}$$

13.1 Characters

Definition 13.1: Characters

A *character* is a group homomorphism $G \to \mathbb{C}^*$ for some group G.

Definition 13.2: Dual group

Let G be a group. Then $\widehat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$ is called the *dual group* to G.

Remark 13.1. Let G be a finite abelian group. Then $\#(G) = \#\left(\widehat{G}\right)$ and there is a natural isomorphism $G \cong \widehat{G}$.

Definition 13.3: Character modulo m

A *character modulo m* is a map $\chi : (\mathbb{Z}/(m))^* \to \mathbb{C}^*$.

Remark 13.2. A character modulo m χ can be extended to $\mathbb{Z} \to \mathbb{Z}/(m) \to \mathbb{C}^* \cup \{0\} = \mathbb{C}$ by

$$\widetilde{\chi}(a) = \begin{cases} \chi([a]) & (a, m) = 1 \\ 0 & \text{else} \end{cases}$$

Definition 13.4

- A character modulo m is *primitive* if for each divisor m' of m, if χ factorizes to a $\chi' : \mathbb{Z}/(m') \to \mathbb{C}$, then $m' = m$.
- A character is called *quadratic* if $\chi = \chi^{-1} \Leftrightarrow \chi^2 = 1 \Leftrightarrow (Z/(m))^* \to \{\pm 1\}$.

Example 13.1. Cosider the case where $m = 8$. We have $(\mathbb{Z}/8)^* = V_4 = \langle -1, 3 \rangle$. Then

$$\chi_8 = \begin{cases} -1 \mapsto 1 \\ 3 \mapsto -1 \end{cases}$$

is primitive.

$$\chi_4 = \begin{cases} -1 \mapsto -1 \\ 3 \mapsto -1 \end{cases}$$

is however not primitive. $\chi_8 \cdot \chi_4$ is primitive.

Theorem 13.3

Let $K = \mathbb{Q}[\sqrt{d}]$ be of discriminant D. Then there exists a primitive quadratic character $\chi_K = \chi : \mathbb{Z} \longrightarrow \{\pm 1, 0\}$ modulo $|D|$ such that for p a prime in $\mathbb{Z}$ we have:

- (p) is prime in $\mathcal{O}_{\mathrm{K}} \Leftrightarrow \chi(p) = -1$
- $(p) = \mathfrak{p}_1\mathfrak{p}_2, \mathfrak{p}_1 \neq \mathfrak{p}_2$ in $\mathcal{O}_{\mathrm{K}} \Leftrightarrow \chi(p) = 1$
- $(p) = \mathfrak{p}^2$ in $\mathcal{O}_{\mathrm{K}} \Leftrightarrow \chi(p) = 0$.