

Algebraic Number Theory

Problem sheet 3

- (3+2 points) Let \mathcal{O} be a Dedekind domain with field of fractions K , and \mathfrak{a} a nonzero fractional ideal of K , (i.e. finitely generated \mathcal{O} -submodule of K), let us recall the inverse of \mathfrak{a} is $\mathfrak{a}^{-1} := \{x \in K | x\mathfrak{a} \subseteq \mathcal{O}\}$.
 - Prove that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$. Deduce that the set of fractional ideals is a free abelian group generated by prime ideals of \mathcal{O} .
 - Show that $\mathfrak{a}^{-1} = \text{Hom}_{\mathcal{O}}(\mathfrak{a}, \mathcal{O})$.
- (3 points) Verify the Chinese Remainder Theorem for Dedekind domains: If $A \triangleleft \mathcal{O}$ is an ideal in the Dedekind domain \mathcal{O} with decomposition $A = P_1^{\nu_1} \dots P_t^{\nu_t}$ as a product of prime ideals then we have

$$\mathcal{O}/A \cong \bigoplus_{i=1}^t \mathcal{O}/P_i^{\nu_i}.$$

- (3 points) Show that a lattice $\Gamma \subset V$ is complete if and only if V/Γ is compact.
- (1 point) Show that Minkowski's lattice point theorem cannot be improved, by giving an example of a centrally symmetric convex set $X \subseteq V$ such that $\text{vol}(X) = 2^n \text{vol}(\Gamma)$ which does not contain any nonzero point of the lattice Γ .
- (2 points) (**Minkowski's Theorem on Linear Forms**) Let $L_i(x_1, \dots, x_n) = \sum_{j=1}^n a_{ij}x_j$ ($i = 1, \dots, n$) be real homogeneous linear polynomials such that $\det((a_{ij}))_{ij} \neq 0$ and let c_1, \dots, c_n be positive real numbers with $c_1 \dots c_n > |\det((a_{ij}))_{ij}|$. Verify that there exist not all zero integers $m_1, \dots, m_n \in \mathbb{Z}$ such that $|L_i(m_1, \dots, m_n)| < c_i$ ($i = 1, \dots, n$). (Hint: Use Minkowski's lattice point theorem)
- (2+2 points) Show that the map

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{Q}} K &\rightarrow K_{\mathbb{C}} \\ z \otimes \alpha &\mapsto z \cdot (j\alpha) \end{aligned}$$

is an isomorphism of rings. Moreover, prove that its restriction to $\mathbb{R} \otimes_{\mathbb{Q}} K$ also induces an isomorphism between $K \otimes_{\mathbb{Q}} \mathbb{R}$ and $K_{\mathbb{R}}$.

- (1 point for each) Let $K = \mathbb{Q}[\sqrt{d}]$ be an **imaginary** quadratic field, where $d < 0$ is squarefree. Show that \mathcal{O}_K is a PID if d is one of the following integers:

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Remark. Historically, Gauss proved the above result and conjectured that there was no other such d , which was finally proved by Baker, Heegner and Stark in the middle of the 20th century, after people has worked on it for more than 150 years.

- (1 point for each) Let $K = \mathbb{Q}[\sqrt{d}]$ be a **real** quadratic field, where $d > 0$ is squarefree. Show that \mathcal{O}_K is a PID if d is one of the following integers:

$$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, \\ 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97$$

Remark. It is conjectured that there are infinitely many real quadratic fields of class number 1, which is still an open problem.

9. (a) (4 points) Let $X_t := \{z \in K_{\mathbb{R}} \mid \sum_{\tau} |z_{\tau}| < t\}$ for any positive real number t . Verify $\text{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}$.
- (b) (4 points) Assume $|K/\mathbb{Q}| = n$. Show $|d_K|^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{n/2}$. (Hint: choose t so that $\text{vol}(X_t) > 2^n \text{vol}(\Gamma)$ where $\Gamma = j(\mathcal{O}_K) \subset K_{\mathbb{R}}$. Apply the inequality between geometric and arithmetic mean on the numbers $|\tau(\alpha)|$ where $0 \neq \alpha \in \mathcal{O}_K$ is the element with $j(\alpha) \in X_t$ guaranteed by Minkowski's lattice point theorem. Finally, note that $1 \leq |N_{K/\mathbb{Q}}(\alpha)|$.)
- (c) (1 point) Show that whenever the degree $|K : \mathbb{Q}|$ goes to infinity, so does the discriminant d_K . Moreover, we have $d_K > 1$ for all extensions $K \neq \mathbb{Q}$.

Remark. One can prove that for any integer d , there are only finitely many number fields with discriminant d . (We will prove this in next sheet)

10. (a) (3 points) Let $A \triangleleft \mathcal{O}_K$ be an ideal whose class has order m in the class group (ie. m is the smallest integer such that $A^m = (\alpha)$ is a principal ideal). Prove that $A\mathcal{O}_L = (\beta)$ where $L = K(\beta)$ and $\beta^m = \alpha$.
- (b) (1 point) Verify that for each number field K there is a finite extension L/K in which all ideals of \mathcal{O}_K become principal (ie. all ideals of \mathcal{O}_K capitulate in \mathcal{O}_L).
- (c) (2 points) Verify that the ring Ω of all algebraic integers (in \mathbb{C}) is a *Bézout domain*, ie. all finitely generated ideals are principal (but not noetherian, so not a PID).
11. (a) (3 points) Show that over a Bézout domain every finitely generated torsion-free module is free.
- (b) (2 points) Verify that $\bigcup_{n=1}^{\infty} \mathbb{C}[[x^{1/n}]]$ is a Bézout domain.
12. In this exercise we compute the rank of the unit group \mathcal{O}_K^{\times} as an abelian group using a multiplicative version of Minkowski's theory.
- (a) (3 points) Let $K_{\mathbb{C}}^{\times} = \prod_{\tau} \mathbb{C}^{\times}$ be the multiplicative group of invertible elements in the ring $K_{\mathbb{C}}$ and let $N: K_{\mathbb{C}}^{\times} \rightarrow \mathbb{C}^{\times}$ be the group homomorphism defined as the product of coordinates. Further define the homomorphism $l := \log |\cdot|: K_{\mathbb{C}}^{\times} \rightarrow \prod_{\tau} \mathbb{R}$ coordinatewise. Show that the kernel of $l \circ j: \mathcal{O}_K^{\times} \rightarrow \prod_{\tau} \mathbb{R}$ is the torsion subgroup in \mathcal{O}_K^{\times} , ie. the group $\mu(K)$ of roots of unity in K .
- (b) (2 points) Verify that for each $\alpha \in \mathcal{O}_K^{\times}$ the element $l \circ j(\alpha) \in \prod_{\tau} \mathbb{R}$ is fixed by the complex conjugation (permuting $\tau \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$). Further show that the sum of coordinates of $l \circ j(\alpha)$ equals 0.
- (c) (5 points) Show that $l \circ j(\mathcal{O}_K^{\times})$ is a full lattice in the subspace H where

$$H = \{x_{\tau} \in \prod_{\tau} \mathbb{R} \mid \sum_{\tau} x_{\tau} = 0 \text{ and } x_{\sigma_k} = x_{\overline{\sigma_k}} \ (k = 1, \dots, s)\}.$$

In particular, $\mathcal{O}_K^{\times} \cong \mu(K) \times \mathbb{Z}^{r+s-1}$ (as an abelian group).