D-MATH
Prof. Richard Pink

Number Theory I

HS 2023

Exercise sheet 4

Lattices, Minkowski Theory, Quadratic Extensions

1. *(Minkowski's theorem on linear forms)* Let

$$L_i(x_1,\ldots,x_n) = \sum_{j=1}^{n} a_{ij}x_j, \qquad i=1,\ldots,n,$$

be real linear forms such that $\det(a_{ij}) \neq 0$, and let $c_1,\ldots,c_n$ be positive real numbers such that $c_1\cdots c_n > |\det(a_{ij})|$. Show that there exist integers $m_1,\ldots,m_n \in \mathbb{Z}$, not all zero, such that for all $i \in \{1,\ldots,n\}$

$$|L_i(m_1,\ldots,m_n)| < c_i.$$

Hint: Use Minkowski's lattice point theorem.

2. Consider a line $\ell := \mathbb{R}\cdot(1,\alpha)$ in the plane $\mathbb{R}^2$ with an irrational slope $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$. Show that for any $\varepsilon > 0$, there are infinitely many lattice points $P \in \mathbb{Z}^2$ of distance $d(P,\ell) < \varepsilon$.

3. (a) Show that the polynomial $f := X^3 + X + 1$ is irreducible over $\mathbb{Q}$.

Consider the cubic number field $K := \mathbb{Q}(\theta)$ with $f(\theta) = 0$.

(b) Determine the ring of integers $\mathcal{O}_K$ and its discriminant.

(c) Determine the number of real resp. non-real complex embeddings of K.

4. Let $\mathbb{F}_q$ be a finite field with q elements and assume that q is odd. Consider the polynomial ring $A := \mathbb{F}_q[t]$ and its quotient field $K := \mathbb{F}_q(t)$.

(a) Show that every quadratic extension of K has the form $L = K(\sqrt{f}\,)$ for a squarefree polynomial $f \in A$.

(b) Determine the integral closure B of A in L.

*5. Show *Minkowski's second theorem about successive minima*: Let Γ be a complete lattice in a euclidean vector space $(V,\langle\ ,\ \rangle)$ of finite dimension n. The *successive minima* $\lambda_1,\ldots,\lambda_n$ *of* Γ are defined iteratively by choosing for any $1 \leqslant i \leqslant n$ an element $\gamma_i \in \Gamma \smallsetminus \bigoplus_{j=1}^{i-1}\mathbb{R}\gamma_j$ of minimal length $\lambda_i := \|\gamma\|$. Then

$$\frac{2^n}{n!}\,\mathrm{vol}(V/\Gamma) \;\leqslant\; \lambda_1\cdots\lambda_n\cdot\mathrm{vol}(B) \;\leqslant\; 2^n\,\mathrm{vol}(V/\Gamma),$$

where B is the closed ball of radius 1.

*6. Show *Lagrange's four square theorem*: Every nonnegative integer n can be written as the sum of four squares.

(a) Show that if m and n are sums of four squares, then so is mn.

Hint: Show that the reduced norm on the ring of quaternions $\mathbb{Z}\oplus\mathbb{Z}i\oplus\mathbb{Z}j\oplus\mathbb{Z}k$ that is given by $\|a+bi+cj+dk\| = \sqrt{a^2+b^2+c^2+d^2}$ is multiplicative.

(b) Reduce the theorem to the case that n is a prime number p.

(c) Find integers α, β such that $\alpha^2+\beta^2 \equiv -1 \bmod p$.

Hint: Consider the intersection of the sets

$$S := \left\{\alpha^2 \bmod p \;\middle|\; 0 \leqslant \alpha < \frac{p}{2}\right\} \quad \text{and} \quad S' := \left\{-1-\beta^2 \bmod p \;\middle|\; 0 \leqslant \beta < \frac{p}{2}\right\}.$$

(d) For any such α, β show that

$$\Gamma := \left\{a = (a_1,\ldots,a_4) \in \mathbb{Z}^4 \;\middle|\; a_1 \equiv \alpha a_3+\beta a_4 \bmod (p),\ a_2 \equiv \beta a_3-\alpha a_4 \bmod (p)\right\}$$

contains a nonzero point a in the open ball of radius $\sqrt{2p}$ in $\mathbb{R}^4$.

(e) Show that $\|a\|^2 = p$ and conclude.