Solutions 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.

Solution: Let

$$X:=\{\underline{x}\in\mathbb{R}^n\mid\forall i\in\{1,\ldots,n\}:|L_i(\underline{x})|<c_i\}.$$

Then X is convex and centrally symmetric, because the L_i are linear. We want to show that $\mathrm{vol}(X)>2^n$. Consider the matrix $A:=(a_{ij})$. Then

$$\begin{aligned}AX&=\{\underline{x}\in\mathbb{R}^n\mid\forall i\in\{1,\ldots,n\}:|L_i(A^{-1}\underline{x})|<c_i\}\\&=\{\underline{x}\in\mathbb{R}^n\mid\forall i\in\{1,\ldots,n\}:|x_i|<c_i\}\end{aligned}$$

and thus $\mathrm{vol}(AX)=2^nc_1\cdots c_n$. Also $\mathrm{vol}(AX)=|\det(A)|\cdot\mathrm{vol}(X)$ and therefore

$$\mathrm{vol}(X)=2^nc_1\cdots c_n\cdot|\det(A)|^{-1},$$

which by assumption is $>2^n$, as desired. Since $2^n=2^n\,\mathrm{vol}(\mathbb{R}^n/\mathbb{Z}^n)$, the conclusion follows using Minkowski's lattice point theorem with the lattice $\mathbb{Z}^n$.

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 $d(P,\ell)<\varepsilon$.

Solution: Consider the linear form $L_1(x_1,x_2):=\frac{1}{\sqrt{1+\alpha^2}}\cdot(x_2-\alpha x_1)$. Then for any point $P\in\mathbb{R}^2$ we have $|L_1(P)|=d(P,\ell)$. Consider the second linear form $L_2(x_1,x_2):=x_2$. Then L_1 and L_2 are linearly independent, so we can apply Minkowski's theorem on linear forms. For any $c_1>0$ choose $c_2\gg 0$ such that the inequality in Exercise 6 is satisfied. Thus there exists a lattice point $P=$

$(x_1, x_2) \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ with $|L_1(P)| < c_1$. Since $\alpha \notin \mathbb{Q}$, we then have $x_1 + \alpha x_2 \neq 0$ and hence $L_1(P) \neq 0$. Therefore $0 < d(P, \ell) < c_1$. Repeating the calculation with $d(P, \ell)$ in place of c_1 yields a second lattice point $P' \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ which satisfies $0 < d(P', \ell) < d(P, \ell)$. Iterating this we can thus produce lattice points $P, P', P'', \ldots \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ with $c_1 > d(P, \ell) > d(P', \ell) > d(P'', \ell) > \ldots > 0$. The strict inequalities imply that these points are all distinct. Thus there exist infinitely many points $P \in \mathbb{Z}^2 \smallsetminus \{(0,0)\}$ with $d(P, \ell) < c_1$.

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.

   Solution:

   (a) The polynomial is monic of degree 3, and its reduction modulo (2) has no zero in $\mathbb{F}_2$ and is therefore irreducible. Thus f is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$.

   (b) The element θ has the minimal polynomial f over $\mathbb{Q}$; hence it is integral over $\mathbb{Z}$. Thus we have $\mathbb{Z}[\theta] \subset \mathcal{O}_K$. This ring has the basis $1, \theta, \theta^2$ over $\mathbb{Z}$, whose discriminant is the discriminant of f by Proposition 1.7.4. Direct computation shows that this discriminant is -31. As this number is squarefree, by Corollary 3.2.3 it follows that that $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $\mathrm{disc}(\mathcal{O}_K) = -31$.

   (c) As the polynomial f has odd degree, it has at least one real root. But its derivative $f' = 3X^2 + 1$ is strictly positive on $\mathbb{R}$. Thus the graph of $f \colon \mathbb{R} \to \mathbb{R}$ is strictly monotone increasing, so the real root is unique and the other two complex roots of f are non-real. It follows that there exists precisely one embedding $K \hookrightarrow \mathbb{R}$ and two complex conjugate embeddings $K \hookrightarrow \mathbb{C}$ which do not land inside $\mathbb{R}$. In other words we have $r = s = 1$.

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.

   Solution:

   (a) Since $\mathrm{char}(K) \neq 2$, we have $L = K(\sqrt{f}\,)$ for some element $f \in K^\times$. After multiplying by the square of its denominator we can assume that $f \in A \smallsetminus \{0\}$. After dividing by any square factors we can then make f squarefree.

(b) The element $s := \sqrt{f} \in L$ satisfies the monic equation $s^2 = f$ with coefficients in A. Thus s lies in B. The subring $B' := A[s]$ then has the basis $1, s$ as an A-module. By Proposition 1.7.4 the discriminant of this basis is the discriminant of the polynomial $X^2 - f$ and thus equal to $4f$.

On the other hand B is a free A-module of rank 2 by Proposition 1.7.6. For any basis b, b' we have $\binom{1}{s} = M \cdot \binom{b}{b'}$ for a matrix $M \in \mathrm{Mat}_{2\times 2}(A)$. From the definition of the discriminant it follows, as in the proof of Proposition 3.2.1 (b), that

$$4f \;=\; \mathrm{disc}(1, s) = \det(M)^2 \cdot \mathrm{disc}(b, b').$$

As $4f$ is squarefree, this proves that $\det(M)$ is a non-zero constant in $\mathbb{F}_q$. Thus M is invertible over A and therefore $B = A[s]$.

*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.

Solution: See Theorem 6.3.3 in
`https://www.math.leidenuniv.nl/~evertse/Minkowski.pdf`.

*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.

Solution: See
`https://concretenonsense.wordpress.com/2009/02/10/lagranges-four-square-theorem/`.