Homework 10

Songyu Ye

November 8, 2025

Problem 1 Let

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

be real linear forms such that $\det(a_{ij}) \neq 0$, and let $c_1, \dots, c_n$ be positive real numbers such that

$$c_1 \cdots c_n > |\det(a_{ij})|.$$

Show that there exist integers $m_1, \dots, m_n \in \mathbb{Z}$ such that

$$|L_i(m_1, \dots, m_n)| < c_i, \qquad i = 1, \dots, n.$$

$$c_1 \cdots c_n > |\det(a_{ij})|.$$

Show that there exist integers $m_1, \dots, m_n \in \mathbb{Z}$ (not all zero) such that

$$|L_i(m_1, \dots, m_n)| < c_i, \qquad i = 1, \dots, n.$$

Hint. Use Minkowski's lattice point theorem.

Solution: Let $A = (a_{ij})$ and define the linear map

$$T : \mathbb{R}^n \to \mathbb{R}^n, \qquad T(x_1, \dots, x_n) = (L_1(x), \dots, L_n(x)).$$

Then T is invertible since $\det(A) \neq 0$. The image

$$\Gamma := T(\mathbb{Z}^n)$$

is a lattice in $\mathbb{R}^n$ with

$$\det(\Gamma) = |\det(A)| = |\det(a_{ij})|.$$

Let

$$D := \{y = (y_1, \dots, y_n) \in \mathbb{R}^n : |y_i| < c_i \text{ for all } i\}.$$

Then D is convex, symmetric about the origin, and

$$\mathrm{vol}(D) = \prod_{i=1}^{n} (2c_i) = 2^n c_1 \cdots c_n > 2^n |\det(a_{ij})| = 2^n \det(\Gamma).$$

By Minkowski's lattice point theorem, D contains a nonzero lattice point

$$y = (y_1, \dots, y_n) \in \Gamma \cap D, \quad y \neq 0.$$

Since $y \in \Gamma = T(\mathbb{Z}^n)$, there exists $m = (m_1, \ldots, m_n) \in \mathbb{Z}^n$, $m \neq 0$, such that

$$y = T(m) = (L_1(m), \ldots, L_n(m)).$$

Because $y \in D$, we have

$$|L_i(m_1, \ldots, m_n)| = |y_i| < c_i \quad \text{for } i = 1, \ldots, n.$$

This gives the desired integers $m_1, \ldots, m_n$.

Problem 2 Give a proof of the following theorem (attributed to Dirichlet) by using Minkowski's theorem.

Theorem 1. *Let $\alpha \in \mathbb{R}$ be a positive irrational number. Then there exist infinitely many pairs of $m, n \in \mathbb{Z}_{>0}$, which are coprime to each other, such that*

$$\left|\frac{n}{m} - \alpha\right| < \frac{1}{m^2}.$$

Hint. Try $\Gamma = \mathbb{Z}^2$,

$$D = \{(x, y) \in \mathbb{R}^2 : x \in (-M, M),\ y - \alpha x \in (-\varepsilon, \varepsilon)\}$$

for infinitely many values of $\varepsilon \to 0^+$ and suitably chosen $M > 0$ (depending on ε).

Solution: Fix $M > 1$ and consider the lattice $\Gamma = \mathbb{Z}^2$. For $\varepsilon > 0$ define the symmetric convex set

$$D_{M,\varepsilon} = \{(x, y) \in \mathbb{R}^2 : |x| \leq M,\ |y - \alpha x| \leq 1/M + \varepsilon\}.$$

Then

$$\mathrm{vol}(D_{M,\varepsilon}) = (2M) \cdot 2\Big(\frac{1}{M} + \varepsilon\Big) = 4(1 + M\varepsilon) > 2^2 \det(\Gamma) = 4.$$

By Minkowski's theorem, there exists a nonzero lattice point $(m, n) \in \Gamma \cap D_{M,\varepsilon}$. So for each $\varepsilon > 0$ there is $(m, n) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ with

$$|m| \leq M, \qquad |n - \alpha m| \leq \frac{1}{M} + \varepsilon. \tag{$*$}$$

Now restrict to the finite set

$$S_M = \{(m, n) \in \mathbb{Z}^2 : 0 < |m| \leq M\}.$$

For $(m, n) \in S_M$ set

$$f(m, n) = |n - \alpha m| - \frac{1}{M}.$$

Suppose, for contradiction, that no lattice point lies in the strip $|x| \leq M,\ |y - \alpha x| \leq 1/M$, i.e. $f(m, n) > 0$ for all $(m, n) \in S_M$. Since S_M is finite, we can define

$$\delta := \min_{(m,n) \in S_M} f(m, n) > 0.$$

Choose ε with $0 < \varepsilon < \delta$. By Minkowski there exists $(m, n) \in S_M$ satisfying $(*)$, so

$$f(m, n) = |n - \alpha m| - \frac{1}{M} \leq \varepsilon < \delta,$$

contradicting the definition of δ. Hence our assumption was false, and there exists a nonzero $(m, n) \in \mathbb{Z}^2$ with

$$|m| \leq M, \qquad |n - \alpha m| \leq \frac{1}{M}.$$

For this pair we have

$$\left|\frac{n}{m} - \alpha\right| = \frac{|n - \alpha m|}{|m|} \leq \frac{1/M}{|m|} \leq \frac{1}{m^2}.$$

Since we can choose M arbitrarily large, this yields infinitely many such pairs (m, n) with $m > 0$. Finally, given such (m, n) with $\gcd(m, n) = d > 1$, write $m = dm'$, $n = dn'$. Then

$$\left|\frac{n'}{m'} - \alpha\right| = \left|\frac{n}{m} - \alpha\right| < \frac{1}{m^2} \leq \frac{1}{m'^2},$$

so (m', n') is coprime and also satisfies the inequality. Thus there are infinitely many coprime $m, n \in \mathbb{Z}_{>0}$ with $\left|\frac{n}{m} - \alpha\right| < \frac{1}{m^2}$.

Problem 3 The following subproblems are designed to let you apply Minkowski's theorem to prove Lagrange's theorem on four squares.

Theorem 2. *For each $n \in \mathbb{Z}_{\geq 0}$, there exist $w, x, y, z \in \mathbb{Z}$ such that*

$$n = w^2 + x^2 + y^2 + z^2.$$

(1) Reduce to the case where n is square-free and (say) $n \geq 3$.

(If you like, you can further reduce to the case where n is a prime: if two numbers are sums of four squares, then so is their product. This can be shown by considering quaternionic norms for $w + xi + yj + zk$, for example.)

(2) Show that there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 \equiv -1 \pmod{n}$.

(By CRT, it is enough to do this when n is a prime. Then you can prove this by elementary number theory.)

(3) Apply Minkowski's theorem to cleverly designed $\Gamma, D \subset \mathbb{R}^4$.

Hint. Try the following and notice that a nonzero element in the intersection gives a desired solution to the equation:

$$\Gamma = \{(w, x, y, z) \in \mathbb{Z}^4 : \ y \equiv ax + by \pmod{n}, \ z \equiv bx - ay \pmod{n}\},$$

$$D = \{\, w^2 + x^2 + y^2 + z^2 < 2n \,\}.$$

Solution: We prove that every $n \in \mathbb{Z}_{\geq 0}$ is a sum of four squares. If $n = 0$ or 1 the statement is clear. If $n = 2$ then $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Moreover, if n_1 and n_2 are sums of four squares, then so is $n_1 n_2$: this follows from the multiplicativity of the norm on Hamilton's quaternions. Thus it suffices to treat n prime with $n \geq 3$.

Fix an odd prime p. Among the residues mod p, there are $(p+1)/2$ quadratic residues (including 0). The set

$$S = \{-1 - t^2 : t \in \mathbb{F}_p\}$$

also has at most $(p+1)/2$ distinct values. Since $\mathbb{F}_p$ has p elements, the pigeonhole principle forces S to contain a square. Thus there exist a, b with $a^2 \equiv -1 - b^2 \pmod{p}$, i.e. $a^2 + b^2 \equiv -1 \pmod{p}$. For $p = 2$ one checks directly that $1^2 + 0^2 \equiv -1 \pmod{2}$. Using CRT, we obtain $a, b \in \mathbb{Z}$ with

$$a^2 + b^2 \equiv -1 \pmod{n}.$$

Fix such a, b. Define a lattice $\Gamma \subset \mathbb{Z}^4$ by

$$\Gamma = \left\{ (w,x,y,z) \in \mathbb{Z}^4 : \begin{array}{ll} y \equiv ax + bw & \pmod{n}, \\ z \equiv bx - aw & \pmod{n} \end{array} \right\}.$$

Equivalently, Γ is the kernel of the surjective homomorphism

$$\phi : \mathbb{Z}^4 \to (\mathbb{Z}/n\mathbb{Z})^2, \quad \phi(w,x,y,z) = (\, y - ax - bw,\ z - bx + aw \,).$$

Hence $|\operatorname{coker} \phi| = n^2$ and

$$[\mathbb{Z}^4 : \Gamma] = n^2,$$

so the determinant of Γ is

$$\det(\Gamma) = n^2.$$

Let

$$D = \{(w,x,y,z) \in \mathbb{R}^4 : w^2 + x^2 + y^2 + z^2 < 2n\}.$$

Then D is convex, symmetric, and

$$\operatorname{vol}(D) = \frac{\pi^2}{2}(\sqrt{2n})^4 = 2\pi^2 n^2 > 16n^2 = 2^4 \det(\Gamma),$$

since $\pi^2 > 8$. By Minkowski's lattice point theorem, D contains a nonzero point

$$(w,x,y,z) \in \Gamma \cap D, \quad (w,x,y,z) \neq (0,0,0,0).$$

Because $(w,x,y,z) \in \Gamma$, we have

$$y \equiv ax + bw \pmod{n}, \qquad z \equiv bx - aw \pmod{n}.$$

Compute modulo n:

$$\begin{aligned} y^2 + z^2 &\equiv (ax + bw)^2 + (bx - aw)^2 \\ &= (a^2 + b^2)(x^2 + w^2) \equiv -(x^2 + w^2) \pmod{n}. \end{aligned}$$

Thus

$$w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{n}.$$

Set

$$Q := w^2 + x^2 + y^2 + z^2.$$

We have $0 < Q < 2n$ (since $(w, x, y, z) \neq 0$ and lies in D), and $n \mid Q$, so necessarily $Q = n$.

Hence

$$n = w^2 + x^2 + y^2 + z^2,$$

as desired.

Problem 4 Show that in every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}_K$ there exists an element $a \neq 0$ such that

$$|N_{K/\mathbb{Q}}(a)| \leq M\,(\mathcal{O}_K : \mathfrak{a}),$$

where

$$M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

(the so-called *Minkowski bound*).

Hint. Use exercise 2 to proceed as in (5.3), and make use of the inequality between arithmetic and geometric means,

$$\frac{1}{n}\sum_{\tau} |z_\tau| \;\geq\; \Big(\prod_{\tau} |z_\tau|\Big)^{1/n}.$$

Solution: Let K have degree $n = r+2s$ and discriminant d_K, and write $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$. Let

$$\Phi : K \to K_{\mathbb{R}}$$

be the Minkowski embedding.

For a nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$, the image $\Lambda = \Phi(\mathfrak{a})$ is a lattice with

$$\det(\Lambda) = 2^{-s}\sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}).$$

This is because in the standard identification $K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^n$, each complex embedding contributes a factor 2 in the Euclidean volume element. This gives

$$\mathrm{vol}(\mathbb{R}^n/\Phi(\mathcal{O}_K)) = |\det A| \cdot 2^{-s} = 2^{-s}\sqrt{|\operatorname{disc}(\mathcal{O}_K)|} = 2^{-s}\sqrt{|d_K|}.$$

and the fact that for lattices, determinant scales by index:

For $t > 0$ set
$$X_t = \Big\{ z = (z_\tau) \in K_{\mathbb{R}} : \sum_\tau |z_\tau| < t \Big\}.$$
This set is convex, centrally symmetric, and by Exercise 2 has volume
$$\mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!}.$$

Choose t so that
$$\left(\frac{t}{n}\right)^n = M\,(\mathcal{O}_K : \mathfrak{a}), \qquad M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$
Equivalently,
$$t^n = n!\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}).$$

Then
$$\mathrm{vol}(X_t) = 2^r \pi^s \frac{t^n}{n!} = 2^r \pi^s \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}) = 2^{r+2s}\sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}) = 2^n \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}).$$

Since
$$2^n \det(\Lambda) = 2^n \cdot 2^{-s}\sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}) = 2^{r+s}\sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}) \le 2^n \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a}),$$
we have $\mathrm{vol}(X_t) \ge 2^n \det(\Lambda)$, so (by Minkowski, enlarging t slightly if a strict inequality is required) there exists a nonzero $\alpha \in \mathfrak{a}$ with $\Phi(\alpha) \in X_t$. Hence
$$\sum_\tau |\tau(\alpha)| < t.$$

By the arithmetic–geometric mean inequality,
$$\Big(\prod_\tau |\tau(\alpha)|\Big)^{1/n} \le \frac{1}{n}\sum_\tau |\tau(\alpha)| < \frac{t}{n},$$
so
$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_\tau |\tau(\alpha)| \le \left(\frac{t}{n}\right)^n = M\,(\mathcal{O}_K : \mathfrak{a}).$$
Thus every nonzero ideal $\mathfrak{a}$ contains a nonzero α with $|N_{K/\mathbb{Q}}(\alpha)| \le M\,(\mathcal{O}_K : \mathfrak{a})$.