JProf. Abhishek Oswal
Dr. Andreas Demleitner

Exercises “Algebraic Number Theory”

Sheet 8

Problem 1: (2+3 points)
Let $(V, \langle\cdot,\cdot\rangle)$ be a Euclidean vector space of dimension n.

(1) Let Λ, Λ' be complete lattices in V. Furthermore, we let $(v_1, \ldots, v_n)$ and $(v'_1, \ldots, v'_n)$ be $\mathbb{Z}$-bases of Λ and Λ', respectively. Denote by $A = (a_{ij})_{i,j} \in \mathrm{GL}(n, \mathbb{R})$ the matrix whose entries are given by

$$v'_j = \sum_{i=1}^{n} a_{ij} v_i.$$

Show that $\mathrm{vol}(\Lambda') = |\det(A)|\,\mathrm{vol}(\Lambda)$.

(2) Let $\Lambda \subseteq V$ be a complete lattice and let $\Lambda' \subseteq \Lambda$ be a sublattice of finite index, i.e., $(\Lambda : \Lambda') = |\Lambda/\Lambda'| < \infty$. Show that Λ' is complete and that

$$\mathrm{vol}(\Lambda') = (\Lambda : \Lambda') \cdot \mathrm{vol}(\Lambda).$$

Hint: You may use the structure theorem for finitely generated modules over a PID without proving it. Over $\mathbb{Z}$, it asserts that

Theorem. *Let M be a finitely generated $\mathbb{Z}$-module. Then there exist $r \geq 0$ and positive integers $d_1, \ldots, d_s$ such that*

$$M \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z}$$

and $d_i \mid d_{i+1}$ for all i.

Problem 2: (3+3+3+2 points)
Let p be a prime.

(1) Show that there exist integers u, v such that $u^2 + v^2 + 1 \equiv 0 \pmod{p}$.

Hint: The statement is clear for $p = 2$. For odd p, investigate the sets

$$S = \{u^2 \pmod{p} \mid u \in \mathbb{Z}\} \qquad \text{and} \qquad S' = \{-1 - v^2 \pmod{p} \mid v \in \mathbb{Z}\}.$$

(2) For $u, v \in \mathbb{Z}$ such that $u^2 + v^2 + 1 \equiv 0 \pmod{p}$, define the subgroup

$$\Lambda_{u,v} := \{(a,b,c,d) \in \mathbb{Z}^4 \mid c \equiv ua + vb \pmod{p} \quad \text{and} \quad d \equiv ub - va \pmod{p}\}.$$

of $\mathbb{Z}^4$. Show that $\Lambda_{u,v}$ has index $\leq p^2$ in $\mathbb{Z}^4$. Conclude that $\Lambda_{u,v}$ is a complete lattice in $\mathbb{R}^4$, whose volume is $\leq p^2$.

(3) Show that p is a sum of four perfect squares.

Hint: The volume of an (open) ball of radius R in $\mathbb{R}^4$ is given by $\frac{\pi^2}{2} \cdot R^4$. What happens for $R = \sqrt{2p}$?

(4) Show that every positive integer $n \in \mathbb{Z}_{>0}$ is the sum of four perfect squares.

Hint: Use that the Euclidean norm on $\mathbb{R}^4$ coincides with the multiplicative (!) norm of quaternions, that is, for $(a, b, c, d) \in \mathbb{R}^4$, one has

$$||(a, b, c, d)||^2 = |a + bi + cj + dk|^2.$$

Explanation: The space of quaternions $\mathbb{H}$ is a 4-dimensional $\mathbb{R}$-vector space spanned by $\{1, i, j, k\}$. The rules

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji, \quad ij = k, \quad i, j, k \text{ commute with real numbers}$$

turn $\mathbb{H}$ into an $\mathbb{R}$-algebra. One can show that $\mathbb{H}$ is a skew-field (but not a field, since the multiplication is not commutative).

(Feel free to use the above-mentioned facts about quaternions without providing proofs.)

Problem 3: (4 points)
Let L_i $(1 \leq i \leq n)$ be real linear forms given by

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

Write $A := (a_{ij})_{i,j}$ and assume that $\det(A) \neq 0$. Let $c_1, \ldots, c_n$ be positive real numbers such that

$$|\det(A)| < c_1 \cdot \ldots \cdot c_n.$$

Show that there is $(m_1, \ldots, m_n) \in \mathbb{Z}^n \setminus \{0\}$ such that

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

for all i.

Abgabedetails:

Wann? Bis spätestens Donnerstag, 12. Dezember 2024, 12:00.

Wo? Sie haben zwei Optionen:

- Ins Postfach von Demleitner im 3. Stock des mathematischen Instituts
- Geben Sie unserem Tutor Jannek Link das Blatt in der Vorlesung

Wie? Abgabe in Gruppen bis zu zwei Personen erlaubt, sogar erwünscht. Alle Namen und Matrikelnummern auf das Blatt schreiben. Abgabe in deutscher Sprache ist in Ordnung.