Übungen zur Algebraischen Zahlentheorie (WS 2023)

PD Dr. Jürgen Müller, **Ausgabe:** 11.01.2024

(13.1) Exercise: Primes as sums of two squares..
Let $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod 4$. Show (again), by using Minkowski's lattice point theorem, that p is a sum of two squares in $\mathbb{Z}$.

Hint. Consider the lattice $\{[a, b] \in \mathbb{Z}^2; b \equiv ua \pmod p\}$, where $u \in \mathbb{Z}$ such that $u^2 \equiv -1 \pmod p$.

(13.2) Exercise: Full lattices.
a) Let $n \in \mathbb{N}$, let $\Lambda \subseteq \mathbb{Z}^n \subseteq \mathbb{R}^n$ be a full sublattice, and let $\mathcal{F} \subseteq \mathbb{R}^n$ be a fundamental domain for Λ. Show that $\mathrm{vol}(\Lambda) = |\mathcal{F} \cap \mathbb{Z}^n|$.

b) Let $V \neq \{0\}$ be an Euclidean $\mathbb{R}$-vector space, and let $\Lambda \subseteq V$ be a lattice. Show the equivalence of the following assertions:
i) Λ is a full lattice.
ii) There is a bounded subset $M \subseteq V$ such that $V = \bigcup_{v \in \Lambda}(v + M)$.
iii) The quotient group V/Λ, equipped with the quotient topology, is compact.

(13.3) Exercise: Minkowski's Lattice Point Theorem.
Let V be an Euclidean $\mathbb{R}$-vector space such that $n := \dim_{\mathbb{R}}(V) \in \mathbb{N}$, and let $\Lambda \subseteq V$ be a full lattice. Show that the volume bound in Minkowski's theorem cannot be improved in general, by exhibiting a convex and centrally symmetric subset $X \subseteq V$ such that $\mathrm{vol}(X) = 2^n \cdot \mathrm{vol}(\Lambda)$, but $\Lambda \cap X = \{0\}$.

(13.4) Exercise: Minkowski's Linear Form Theorem.
Let $A = [a_{ij}] \in \mathrm{GL}_n(\mathbb{R})$, where $n \in \mathbb{N}$, and for $j \in \{1, \ldots, n\}$ let $L_j \colon \mathbb{R}^n \to \mathbb{R} \colon [x_1, \ldots, x_n] \mapsto \sum_{i=1}^n x_i a_{ij}$, that is the $\mathbb{R}$-linear form given by the j-th column of A. Moreover, let $c_1, \ldots, c_n \in \mathbb{R}$ such that $c_j > 0$ and $\prod_{j=1}^n c_j > |\det(A)$.

Show **Minkowski's Linear Form Theorem**, saying that there are $a_1, \ldots, a_n \in \mathbb{Z}$ such that $|L_j(a_1, \ldots, a_n)| < c_j$, for all $j \in \{1, \ldots, n\}$.