D-MATH
Prof. Richard Pink

Algebraic Number Theory

FS 2018

Exercise Sheet 3

Lattices and Minkowski Theory

*1. 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

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

where B is the closed ball of radius 1.

2. 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: Use the reduced norm on the ring of quaternions $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$.

   (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

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

   (d) For any such α, β show that

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

   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.

3. (a) Show that the number fields $\mathbb{Q}(\sqrt{11})$ and $\mathbb{Q}(\sqrt{-11})$ have class number 1.

   (b) Show that the class group of $\mathbb{Q}(\sqrt{-14}))$ is cyclic of order 4.

   (c) Show that $f := X^3 + X + 1 \in \mathbb{Q}[X]$ is irreducible and that the cubic number field $\mathbb{Q}(\theta)$ with $f(\theta) = 0$ has class number 1.

4. (a) Let K be a number field. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ and $m \geqslant 1$ an integer such that $\mathfrak{a}^m = (\alpha)$. Let L/K be a finite extension containing an element $\sqrt[m]{\alpha}$ such that $\sqrt[m]{\alpha}^{\,m} = \alpha$. Show that $\mathfrak{a}\mathcal{O}_L = \sqrt[m]{\alpha}\,\mathcal{O}_L$.

   (b) Show that there is a finite field extension L/K such that for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the ideal $\mathfrak{a}\mathcal{O}_L$ is principal.

5. Let p be a prime with $p \equiv 3 \bmod 4$. It is known that the class number of $K := \mathbb{Q}(\sqrt{p})$ is odd. Use this fact to prove that there exist $a, b \in \mathbb{Z}$ such that

$$|a^2 - pb^2| = 2.$$

   Hint: Show that $(2, 1+\sqrt{p}) = (2, 1+\sqrt{p})^{|\operatorname{Cl}(\mathcal{O}_K)|} \cdot \mathfrak{a}$ for a principal ideal $\mathfrak{a}$.