Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Exercise Sheet 8

Exercise 8.1. Use the Minkowski bound $M_K = \frac{n!}{n^n}(4/\pi)^{r_2}|\Delta_K|^{1/2}$ to compute class numbers h_K of the following fields.

(a) $K = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$.

(b) $K = \mathbb{Q}(\sqrt{-D})$ for $D = 11$ and $D = 19$.

Exercise 8.2. Let p be a prime congruent to 1 modulo 4. Recall that -1 is a quadratic residue, so that there exists $r \in \mathbb{Z}$ such that $p|r^2 + 1$. Consider the lattice $\Lambda \subset \mathbb{Z}^2$ generated by $(0, p)$ and $(1, r)$.

(a) Show that Λ contains a vector of length less than $\sqrt{2p}$;

(b) Use (a) to prove that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Exercise 8.3. In this exercise we prove Lagrange's four-square theorem. Recall that the volume of a ball of radius R in $\mathbb{R}^{2k}$ is $\frac{\pi^k R^{2k}}{k!}$.

(a) Verify Euler's identity

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax-by-cz-dt)^2 + (ay+bx+ct-dz)^2 + (az-bt+cx+dy)^2 + (at+bz-cy+dx)^2 .$$

(b) Show that for any prime p there exist integers r, s such that $p|r^2 + s^2 + 1$.

(c) Consider the lattice $\Lambda = \{(a, b, c, d) \in \mathbb{Z}^4 \mid a \equiv rc+sd \pmod p, b \equiv rd-sc \pmod p\}$, where r and s are as in part (b). Show that the covolume of Λ is $|\Lambda| = p^2$ and that there exists a nonzero vector $(a, b, c, d) \in \Lambda$ such that $a^2 + b^2 + c^2 + d^2 < 2p$;

(d) Using (a) and (c) show that any non-negative integer can be written as a sum of four prefect squares.

Exercise 8.4*. Show that for any d there exist only finitely many number fields $K \subset \mathbb{C}$ of discriminant $\Delta_K = d$.

(*Hint: construct a convex body $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of volume $2^{n-r_2}|d|^{1/2}$ such that all but one of coordinates are bounded in absolute value by $1/2$ on B. Show that for any non-zero $x \in \mathcal{O}_K$ that maps to B its minimal polynomial is of degree n with bounded coefficients.*)