Algebraic Number Theory 2018 — Set 8

Tutor: Vivien Vogelmann, `vivienvogelmann[at]web.de`
Deadline: 12.00 on Thursday, the 21st of June, 2018

Exercise 1. Compute the class number of $\mathbb{Q}(\sqrt{-p})$ for $p = 5$, 11, and 13.

Exercise 2. Let $K \subset \mathbb{R}$ be a finite extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. Prove that $\mathcal{O}_K^* \subset \mathbb{R}$ is dense if and only if $[K : \mathbb{Q}] \geq 4$ or K is totally real cubic. (A field is *totally real* if all its complex embeddings have image $\subset \mathbb{R}$.)

Theorem (Strong Minkowski bound). Let R be the ring of integers in a number field K of degree n with s pairs of complex embeddings. Then every ideal class of $\mathrm{Cl}(R)$ contains an integral ideal with norm not exceeding

$$M_R = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |D|^{1/2}.$$

You may use this theorem without proof.

Exercise 3.

(a) Let d be a positive integer. Show that there is an integer n such that for all number fields K with $D < d$ one has $[K : \mathbb{Q}] < n$.

(b) Let $K \neq \mathbb{Q}$ be a number field. Show that $D \neq \pm 1$.

Exercise 4 *(Lagrange's four squares theorem)***.** Let p be a prime number.

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

(ii) For $u, v \in \mathbb{Z}$ with $u^2 + v^2 + 1 \equiv 0 \pmod p$ show that the lattice

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

has volume p^2 in $\mathbb{R}^4$.

(iii) Show that every positive integer is the sum of four squares.

Hints for (iii): For a prime number p, observe that the open ball of radius $\sqrt{2p}$ contains a lattice point of $L_{u,v}$. Then use the multiplicativity of the norm $N\colon \mathbb{R}[i, j, k] \to \mathbb{R}$ of the quaternion algebra.

Exercise 5 (Sage)**.** In this exercise we will gather numerical evidence for a theorem of Hirzebruch. Let N be a big number, say $N = 10^4$.

(1) Generate a list P containing all the primes $3 < p < N$ such that $p \equiv 3 \pmod 4$.

(2) Write a function `ascf` (alternating sum continued fraction) that takes as input a prime number p, and outputs an integer. It does the following: let $[b_0; (b_1, \ldots, b_r)*]$ be the continued fraction expansion of $\sqrt{p}$. Then the output is $\sum_{i=1}^r (-1)^i b_i$. (Hint: Define `sqrtp` by `K.<sqrtp> = QuadraticField(p)`. Use `cf = continued_fraction(sqrtp)` to compute the continued fraction of $\sqrt{p}$. You can access the period of `cf` with `cf.period()`.)

(3) For all $p \in P$, verify Hirzebruch's theorem, which is the following statement: if the class number of $\mathbb{Q}(\sqrt{p})$ is 1, then the class number of $\mathbb{Q}(\sqrt{-p})$ is `ascf`$(p)/3$.