Algebraic number theory
Exercise sheet for chapter 4

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk)
Aurel Page (a.r.page@warwick.ac.uk)
TA: Pedro Lemos (lemos.pj@gmail.com)

Version: March 2, 2017

Answers must be submitted by Friday March 11, 14:00

Exercise 1 (20 points)**.** Let $d > 0$ be a squarefree integer, let $K = \mathbb{Q}(\sqrt{-d})$ and let Δ_K be the discriminant of K. Let p be a prime that splits in K and let $\mathfrak{p}$ be a prime ideal above p.

1. (15 points) Prove that for all integers $i \geq 1$ such that $p^i < |\Delta_K|/4$, the ideal $\mathfrak{p}^i$ is not principal. *Hint: consider the cases* $\Delta_K = -d$ *and* $\Delta_K = -4d$ *separately.*

2. (5 points) What does this tell you about the class number of K?

Exercise 2 (40 points)**.** Let $K = \mathbb{Q}(\sqrt{-87})$.

1. (5 points) Write down without proof the ring of integers, the discriminant and the signature of K.

2. (10 points) Describe all the integral ideals of K of norm up to 5 (give generators for some prime ideals, and express the integral ideals as products of these prime ideals). What does this tell you about the class number of K?

3. (10 points) Factor the ideal $(\frac{3+\sqrt{-87}}{2})$ into primes.

4. (15 points) Prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$.

Exercise 3 (40 points)**.** In this exercise we consider the equation

$$y^2 = x^5 - 2, \quad x, y \in \mathbb{Z}.$$

1. (5 points) Let $K = \mathbb{Q}(\sqrt{-2})$. Write down without proof the signature, the discriminant, the ring of integers of K, and then compute the class number of K.

2. (10 points) Let (x, y) be a solution of the equation. Prove that the ideals $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime. *Hint: reduce the equation modulo* 4 *to prove that* y *must be odd.*

3. (10 points) You may assume without proof that $\mathbb{Z}_K^\times = \{\pm 1\}$. Prove that $y + \sqrt{-2}$ is a 5-th power in $\mathbb{Z}_K$.

4. (15 points) Prove that the equation has no solution.

UNASSESSED QUESTIONS

The next questions are not worth any points. I still recommend you to try to solve them, for practice. Corrections will be available online, just like for the marked questions.

Exercise 4. Let $K = \mathbb{Q}(\sqrt{-29})$.

1. Determine the ring of integers and discriminant of K.

2. Determine the decomposition of 2, 3 and 5 in K.

3. Factor the ideals $(1 + \sqrt{-29})$ and $(3 + 2\sqrt{-29})$ into primes.

4. Determine the order in the class group of K of the images of the primes above 2 and of the primes above 5.

5. Prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z}$.

Exercise 5 (Difficult)**.** Let K be a number field, and let $m \geq 1$ be an integer. In this exercise we write $\mathrm{Cl}(K)[m] = \{c \in \mathrm{Cl}(K) \mid c^m = 1\}$.

1. Prove that if h_K is coprime to m, then $\mathrm{Cl}(K)[m] = \{1\}$.

2. Let $G_m(K) = \{x^m \colon x \in K^\times\}$, and let $L_m(K)$ be the set of elements $x \in K^\times$ such that in the prime ideal factorisation of (x), all the exponents are multiples of m.

   (a) Prove that $G_m(K)$ is a subgroup of $L_m(K)$.
   We define $S_m(K) = L_m(K)/G_m(K)$.

   (b) Let $x \in L_m(K)$. Prove that there exists a unique fractional ideal $\mathfrak{a}_x$ such that $(x) = \mathfrak{a}_x^m$.

   (c) Prove that the map $f \colon S_m(K) \to \mathrm{Cl}(K)[m]$, defined by $f(x) = [\mathfrak{a}_x]$, is well-defined, and is a group homomorphism.

   (d) Prove that f is surjective.

   (e) What is the kernel of f?

   From now on, K is an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ squarefree. We write $\bar{\cdot}$ for the complex conjugation in K.

3. Let $x = a + b\sqrt{-d} \in K$ be an element such that $N_{\mathbb{Q}}^{K}(x) = 1$. Let $\phi : K \to K$ be defined by $\phi(y) = \bar{y} - xy$.

   (a) Prove that ϕ is $\mathbb{Q}$-linear.

   (b) Compute the matrix of ϕ on the basis $(1, \sqrt{-d})$.

   (c) Compute the determinant of ϕ. Is ϕ injective?

   (d) Prove that there exists $y \in K^{\times}$ such that $x = \bar{y}/y$.

4. Let $[\mathfrak{a}] \in \mathrm{Cl}(K)[2]$ and let $a = N(\mathfrak{a})$.

   (a) Prove that there exists $x \in K^{\times}$ such that $\mathfrak{a}^2 = (x)$.

   (b) Prove that there exists $y \in K^{\times}$ such that $x = a\bar{y}/y$.

   (c) Let $\mathfrak{b} = y\mathfrak{a}$. Prove that there exists $b \in \mathbb{Q}^{\times}$ such that $\mathfrak{b}^2 = (b)$.

   (d) Prove that $\mathfrak{a}$ is in the same ideal class as a product of the ramified prime ideals of $\mathbb{Z}_K$.

   Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the ramified prime ideals of K.

5. *Prove that if the product $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_t^{e_t}$ with $0 \leq e_i \leq 1$ is principal then $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_t^{e_t} = (\sqrt{-d})$ or all the e_i are zero. Hint: consider the norm of such an ideal, and look at elements of $\mathbb{Z}_K$ of that norm.*

6. Prove that $\mathrm{Cl}(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}$.