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)

TAs: Chris Birkbeck (c.d.birkbeck@warwick.ac.uk),
George Turcas (g.c.turcas@warwick.ac.uk)

Version: March 1, 2017

Answers must be submitted by Wednesday March 15, 14:00

Exercise 1 (30 points)**.** Let $K = \mathbb{Q}(\sqrt{-155})$.

1. (3 points) Write down without proof the ring of integers, the discriminant and the signature of K.
2. (10 points) Describe a set of prime ideals of $\mathbb{Z}_K$ whose classes generate the class group of K. For each of these prime ideals, give the residue degree and ramification index.
3. (8 points) Factor the ideal $(\frac{5+\sqrt{-155}}{2})$ into primes.
4. (10 points) Prove that $\operatorname{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$.

Exercise 2 (35 points)**.** Let $d \neq 0, 1$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{d})$.

1. (15 points) Let $n \in \mathbb{Z}$. Prove that if neither n nor $-n$ are squares modulo d, then no integral ideal in K of norm n is principal. *Hint: consider the cases* $\operatorname{disc} K = d$ *and* $\operatorname{disc} K = 4d$ *separately.*
2. (3 points) From now on $d = 105$. Write down without proof the ring of integers, the discriminant and the signature of K.
3. (10 points) Find an element of norm -6 and an element of norm -5 in $\mathbb{Z}_K$. *Hint: write down the norm of a generic element of* $\mathbb{Z}_K$*, the norm of a generic element of* $\mathbb{Z}[\sqrt{105}]$*, and try small values of the variables.*
4. (7 points) Prove that $\operatorname{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Exercise 3 (35 points)**.** We consider the equation

$$y^2 = x^3 - 6, \quad x, y \in \mathbb{Z}. \tag{1}$$

1. (3 points) Write down without proof the ring of integers, signature and discriminant of $K = \mathbb{Q}(\sqrt{-6})$.
2. (10 points) Determine the class group of K.
3. (10 points) Let $(x, y) \in \mathbb{Z}^2$ be a solution of (1). Prove that $(y + \sqrt{-6})$ and $(y - \sqrt{-6})$ are coprime.
4. (4 points) Prove that there exists an ideal $\mathfrak{a}$ such that $(y + \sqrt{-6}) = \mathfrak{a}^3$.
5. (3 points) Prove that $\mathfrak{a}$ is principal.
6. (2 points) Using without proof the fact that $\mathbb{Z}_K^\times = \{\pm 1\}$, prove that $y + \sqrt{-6}$ is a cube in $\mathbb{Z}_K$.
7. (3 points) Prove that (1) 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 $K = \mathbb{Q}(\sqrt{-231})$.

1. Write down without proof the ring of integers, the discriminant and the signature of K.
2. Compute the decompositions of $2, 3, 5$ and 7 in K.
3. Prove that for every element $z \in \mathbb{Z}_K$ such that $|N_{\mathbb{Q}}^K(z)| \leq 57$, we have $z \in \mathbb{Z}$.
4. Let $\mathfrak{p}_2$ be a prime of $\mathbb{Z}_K$ above 2. Prove that the class of $\mathfrak{p}_2$ in $\mathrm{Cl}(K)$ has order 6.
5. Let $\mathfrak{p}_7$ be a prime of $\mathbb{Z}_K$ above 7. Prove that the class of $\mathfrak{p}_7$ in $\mathrm{Cl}(K)$ has order 2.
6. Prove that $[\mathfrak{p}_7]$ does not belong to the subgroup of $\mathrm{Cl}(K)$ generated by $[\mathfrak{p}_2]$. *Hint: prove that if it did, then $\mathfrak{p}_7\mathfrak{p}_2^3$ would be principal.*
7. Compute the prime factorisations of the ideals $(\frac{3+\sqrt{-231}}{2})$ and $(\frac{7+\sqrt{-231}}{2})$.
8. Prove that $\mathrm{Cl}(K) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 5. Let $d > 0$ be a squarefree integer, let $K = \mathbb{Q}(\sqrt{-d})$ and let disc_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. Prove that for all integers $i \geq 1$ such that $p^i < |\operatorname{disc} K|/4$, the ideal $\mathfrak{p}^i$ is not principal. *Hint: consider the cases* $\operatorname{disc} K = -d$ *and* $\operatorname{disc} K = -4d$ *separately.*

2. What does this tell you about the class number of K?

3. Using without proof the fact that there exists infinitely many squarefree positive numbers of the form $8k + 7$ for $k \in \mathbb{Z}_{>0}$, prove that for every $X > 0$ there exists a number field K such that $h_K > X$.

Exercise 6.

1. Log in to a university computer that has the computer algebra software `gp` installed (Linux computers should have it).

2. Type `gp` in a terminal to start the software.

3. Pick $d > 0$ squarefree.

4. Type `bnfinit(x^2+d).clgp[2]` and hit `Enter`. This will compute the class group of $K = \mathbb{Q}(\sqrt{-d})$ and display its structure in the form of a list $[a_1, \ldots, a_n]$ representing the group $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$.

5. Compute the class group $\mathrm{Cl}(K)$ by hand.