Algebraic number theory — Exercise sheet 4

https://www.maths.tcd.ie/~mascotn/teaching/2022/MAU34109/index.html

Version: November 11, 2022

Email your answers to mascotn@tcd.ie by Wednesday November 23 noon.

Exercise 4.1: A Mordell-Weil equation (100 pts)

The goal of this exercise is to solve the Diophantine equation

$$y^2 = x^3 - 148 \qquad (x, y \in \mathbb{Z}) \tag{1}$$

We let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-37}$, and note that (1) can be rewritten as

$$(y + 2\alpha)(y - 2\alpha) = x^3.$$

You may use without proof the following facts:

- $148 = 4 \cdot 37$, and 37 is prime,
- $\mathbb{Z}_K^\times = \{\pm 1\}$.

1. (5 pts) Prove that the equation has no solution such that $37 \mid y$.
2. (30 pts) Determine $\mathbb{Z}_K$ and $\mathrm{Cl}(K)$, as well as the decomposition of 37 in K.
3. (15 pts) Let (x, y) be a hypothetical solution of (1). Prove that there is at most one prime $\mathfrak{p}$ of K that divides both $(y+2\alpha)$ and $(y-2\alpha)$. Which prime is that?
4. (35 pts) Deduce that at least one of $y + 2\alpha$ or $y - 2\alpha$ is a cube or twice a cube in $\mathbb{Z}_K$.

   Hint: Prove that $(y+2\alpha) = \mathfrak{b}^3\mathfrak{p}^r$ *and* $(y-2\alpha) = \mathfrak{b}'^3\mathfrak{p}^{r'}$ *for some ideals* $\mathfrak{b}, \mathfrak{b}' \lhd \mathbb{Z}_K$ *and integers* $r, r' \geqslant 0$. *How small can you make* r *and* r'*?*
5. (15 pts) Find all the solutions of (1).

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice (they may even give you inspiration to help you solve Exercise 1), and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 4.2: Class group computations

Determine the class group of the following number fields:

1. $\mathbb{Q}(\sqrt{-29})$,
2. $\mathbb{Q}(\sqrt{-33})$.

Exercise 4.3: A norm equation

Let $n \geqslant 0$ be an integer. The goal of this exercise is to determine the number of solutions to the Diophantine equation

$$x^2 + 10y^2 = 7^n \qquad (x, y \in \mathbb{Z}) \tag{2}$$

in terms of n.

We let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-10}$, and note that (2) can be rewritten as

$$N_{\mathbb{Q}}^{K}(x + \alpha y) = 7^n.$$

You may freely use the fact that $\mathbb{Z}_K^\times = \{\pm 1\}$.

1. Determine $\mathbb{Z}_K$ and $\mathrm{Cl}(K)$.
2. Determine the decomposition of 7 in $\mathbb{Z}_K$, and the image in $\mathrm{Cl}(K)$ of the primes appearing in this factorisation.
3. Let $\mathfrak{a}$ be an of $\mathbb{Z}_K$ of norm 7^n. What does the factorisation into primes of $\mathfrak{a}$ look like? What does this tell you about the image of $\mathfrak{a}$ in $\mathrm{Cl}(K)$?
4. Express the number of solutions to (2) in terms of n.

Exercise 4.4: Arbitrarily large class numbers

Let $d > 0$ be a squarefree integer, and let $K = \mathbb{Q}(\sqrt{-d})$. Suppose that $p \in \mathbb{N}$ is a prime which 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 $d \not\equiv 1 \pmod 4$ *and* $d \equiv 1 \pmod 4$ *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 $k \in \mathbb{N}$, prove that for every $X > 0$ there exists a number field K such that $h_K > X$.

Exercise 4.5: A non-Euclidean PID

Recall that a domain R is Euclidean *if there exists a size function $s : R \setminus \{0\} \longrightarrow \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $s(r) < s(b)$ (example: $R = K[x]$ where K is a field, $s = \deg$).*

One proves in commutative algebra that every Euclidean domain is automatically a PID, and one usually mentions that the converse does not hold, but counter-examples are not easy to exhibit.

The purpose of this exercise is to provide an example of a PID which is not Euclidean. As such, unlike other exercises, this exercise is more about commutative algebra than algebraic number theory, and will therefore not really help you to prepare for the exam; but I thought some of you might like to see this example since it is a nice application of algebraic number theory.

Let $K = \mathbb{Q}(\sqrt{-19})$.

1. Determine $\mathbb{Z}_K$.

2. Prove that $\mathbb{Z}_K$ is a PID.

3. Prove that $\mathbb{Z}_K^\times = \{\pm 1\}$.

4. Prove that $\mathbb{Z}_K$ has no ideal of norm 2 nor 3.

5. Let R be a Euclidean domain with size function s which is not a field, let $R^\times$ be the group of units of R, and let $U = R^\times \cup \{0\}$. Prove that there exists an $m \in R \setminus U$ such that every element of the quotient ring $R/(m)$ can be represented by an element of U (in other words, such that the restriction to U of the projection morphism $R \longrightarrow R/(m)$ remains surjective).

   Hint: Consider an element of $R \setminus U$ of minimal size.

6. Prove that there does not exist any size function for which $\mathbb{Z}_K$ is Euclidean.