Algebraic Number Theory 2018 — Set 2

Tutor: Vivien Vogelmann, vivienvogelmann@web.de
Deadline: 12.00 on Thursday, the 3rd of May, 2018

Each exercise is worth 4 points. The bonus exercise is also worth 4 points. If you get more then 16 points, you can transfer the excess points to other exercise sets.

Exercise 1. Let $K/\mathbb{Q}$ be a quadratic extension. For $x \in K$ we denote with $\mathrm{Mipol}_{\mathbb{Q}}(x) \in \mathbb{Q}[t]$ the minimum polynomial of x over $\mathbb{Q}$. Define $\mathcal{O}_K$ as $\{x \in K \mid \mathrm{Mipol}_{\mathbb{Q}}(x) \in \mathbb{Z}[t]\}$. (Later in the lectures we will see that $\mathcal{O}_K$ is in fact the ring of integers!)

Show that there is a square-free integer $d \in \mathbb{Z}$ such that $K \cong \mathbb{Q}(\sqrt{d})$.

Show that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$ and $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{d})/2]$ if $d \equiv 1 \pmod 4$.

Exercise 2. Consider the field $K = \mathbb{Q}(\sqrt{13}) \subset \mathbb{R}$. Let $\mathcal{O}_K$ be the ring of integers of K. (You may use exercise 1 to determine the ring of integers.) The unit group $\mathcal{O}_K^*$ is isomorphic to $\{\pm 1\} \times \mathbb{Z}$.

Find an $x \in \mathcal{O}_K^*$ such that -1 and x generate $\mathcal{O}_K^*$.

Exercise 3. Let a, b, and c be coprime integers satisfying $a^2 + b^2 = c^2$. Show that there exist integers m and n such that we have, possibly after swapping a and b,

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = \pm(m^2 + n^2).$$

Hint: Determine the rational solutions to $x^2 + y^2 = 1$; intersect the unit circle with the line $y = t(x-1)$.

Exercise 4. Determine explicitly all the units and prime elements of $\mathbb{Z}[\sqrt{2}]$. Hint: first show that this ring is Euclidean.

Exercise 5 (Bonus)**.** Important: this exercise continues on the next page.

In this exercise we will explore how to do computations in algebraic number theory with the computer algebra program Sage. Sage is an extension of the programming language Python. (If you don't know Python: it is a programming language that is comparatively easy to read and write; and this property transfers to Sage.)

Go to `https://cocalc.com` and create an account. Once you have logged in, create a project. Please call it "AlgZT 2018, [your name]". Add `vivienvogelmann@web.de` as collaborator to your project. In the homework that you hand in, write a note that you wrote the answer to exercise 5 online.

Open the project, and create a Sage worksheet. Call it "Set 2".

You can now write Sage (and Python) code, and click the "Run" button to execute the code.

(a) Choose your favourite integer n, such that $10^3 < n < 10^6$. Write `n = [your choice]` in the code.

(b) To make sure that you did not choose an integer with an integer with a large square factor, let d be the smallest prime $> n$. You can define d with `d = next_prime(n)` in the code.

Now you will have to start exploring some documentation.

The documentation is available at: `https://doc.sagemath.org`. There you should click "Reference". Then choose "Number Fields and Function Fields" in the Table of Contents and click on "Number Fields"

afterwards. The first entry is again called "Number Fields" and it explains how to define a number field in Sage. For the rest of this exercise, you will have to search the documentation (or other parts of the internet).

(c) Define the number field $K = (\sqrt{d})$.
(d) Define its ring of integers $\mathcal{O}_K$.
(e) Compute a basis of $\mathcal{O}_K$.
(f) Compute the structure of the group of units of $\mathcal{O}_K$.
(g) (confusingly you need `K.unit_group()` for this).
(h) Compute an element of norm -1.