Algebraic Number Theory 2018 — Set 5

Tutor: Vivien Vogelmann, `vivienvogelmann[at]web.de`
Deadline: 12.00 on Friday, the 1st of June, 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 $f \in \mathbb{Q}[X]$ be the polynomial $X^3 - 2X - 2$. Let α be a root of f, and let K denote $\mathbb{Q}(\alpha)$. In this exercise you may use that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let p be a prime number (in $\mathbb{Z}$). The ideal (p) in $\mathcal{O}_K$ can decompose as product of prime ideals in one of the following ways:

1. $(p) = \mathfrak{p}^3$
2. $(p) = \mathfrak{p}_1^2\mathfrak{p}_2$
3. $(p) = \mathfrak{p}$
4. $(p) = \mathfrak{p}_1\mathfrak{p}_2$
5. $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$

Find an explicit prime number p for each of these five options. Prove that your answer is correct.

Hint: Compute the discriminant of $\mathcal{O}_K$, which tells you where to look for ramifying primes. This covers the first two cases. For the last three cases, factor f modulo small prime numbers p. You do not need more then the first 10 primes.

Exercise 2. Let $0 \to V_1 \to V_2 \to \ldots \to V_n \to 0$ be an exact sequence of vector spaces over some field. Prove: $\sum_{i=1}^{n}(-1)^i \dim(V_i) = 0$.

Exercise 3. Prove the remaining case of Satz 2.5.10 in the lecture notes: Let d be an integer congruent 1 (mod 4), and let $\mathcal{O}$ be the ring $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Prove the following:

— If $d = 5 \pmod 8$, then (2) is a prime ideal of $\mathcal{O}$.

— If $d = 1 \pmod 8$, then 2 unramified in $\mathcal{O}$, and we have $(2) = \left(2, \frac{1+\sqrt{d}}{2}\right) \cdot \left(2, \frac{1-\sqrt{d}}{2}\right)$.

Exercise 4. Let $R \subseteq \mathcal{O}_K$ be a subring of $\mathcal{O}_K$ with $K = \mathrm{Quot}(R)$. The *conductor* of R is

$$\mathfrak{f} = \{x \in \mathcal{O}_K \mid (x) \subseteq R\}.$$

(See also Satz 2.5.7.) Prove that (i) the set $\mathfrak{f}$ is an ideal; (ii) it is the biggest ideal of $\mathcal{O}_K$ that is contained in R; and (iii) show that $\mathfrak{f} \neq (0)$.

Exercise 5 (Bonus)**.** In this exercise we will use Sage to collect numerical data on the splitting behaviour of primes in number fields. The goal is to formulate a statement on the asymptotic behaviour.

(i) Let K be a number field of degree d. For computational purposes restrict to $d \leq 5$. Let N be a positive integer, say 1000. We denote with $\pi(n)$ the nth prime number. For $n \leq N$, compute how $p = \pi(n)$ splits in K. Count how many primes are inert, how many primes split completely; and more generally count how often each splitting type occurs.

(ii) Let L be the Galois closure of K, and let G be the Galois group of $L/\mathbb{Q}$. Then G acts on $\Sigma = \mathrm{Hom}(K, L)$. Note that $\#\Sigma = d$. For each $g \in G$, we get a partition of Σ into orbits under multiplication by g. The lengths of these orbits are a partition of d. Use `G.cycle_index()` to compute how often each partition occurs as g ranges over the elements of G.

Compare these two computations, and formulate a conjecture relating the two.