Humboldt-Universität zu Berlin
Institut für Mathematik
Dr. D. Agostini, M. Sc. L. Lerer
L. Mädje

Zahlentheorie
SoSe 2019

Exercise Sheet 8

If you want your solutions to be corrected, you should hand them in by Monday, June 17.
Please write your name and immatriculation number on top of every exercise

---

Exercise 8.1 (2+2+2 points)

a) Find the prime factorization of $(2), (5), (11)$ in $\mathbb{Q}(i)$.

b) Find the prime factorization of (2) in $\mathbb{Q}(\sqrt{-23})$.

c) Fact: $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$. Use this to compute the factorization of $(7), (29), (31)$ in $\mathbb{Q}(\sqrt[3]{2})$.

Exercise 8.2 (2+1+4+4+4 points) Let K be a number field and $\mathcal{O}_K$ its field of integers.

a) Suppose $K = \mathbb{Q}(\alpha)$ and that $[K : \mathbb{Q}] = n$. Assume that $K/\mathbb{Q}$ is a Galois extension. Let $\operatorname{disc}(\alpha) := \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Prove that $\sqrt{\operatorname{disc}(\alpha)} \in K$.

The rest is Marcus, Exercise 3.18. We are going to prove that $\mathcal{O}_{\mathbb{Q}(\zeta_{23})} = \mathbb{Z}[\zeta_{23}]$ is not an UFD. Consider the number fields $K = \mathbb{Q}(\sqrt{-23})$ and $L = \mathbb{Q}(\zeta_{23})$. Let also $\alpha = \frac{1+\sqrt{-23}}{2}$ and consider the prime ideal $P = (2, \alpha) \subseteq \mathcal{O}_K$.

b) Prove that $K \subseteq L$.

c) Let Q be a prime ideal in $\mathcal{O}_L$ lying over P. Prove that $f_Q(P) = 11$ and conclude that $P \cdot \mathcal{O}_L = Q$ in $\mathcal{O}_L$. *Hint:* use Exercises 7.1 and 7.3.

d) Prove that $P^3 = (\alpha - 2)$. Then, using the ideal norm, show that P is not principal.

e) Using the ideal norm, prove that Q is not principal.

For the next exercise, recall the following fact. Let K be a number field, $\mathcal{O}_K$ its ring of integers and $p \in \mathbb{Z}$ a prime. We have a factorization $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$ with the corresponding inertia degrees $f_i = f_{\mathfrak{p}_i}(p)$. Then we have proved in the lectures that

$$\dim_{\mathbb{F}_p} (\mathcal{O}_K/\mathfrak{p}_i^{e_i}) = e_i f_i.$$

Exercise 8.3 (2+3+1 points) Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal.

a) Prove that the quotient ring $\mathcal{O}_K/I$ is finite.

Then, it makes sense to define the *absolute norm* of I as the number of elements in this quotient $\|I\| := |\mathcal{O}_K/I|$.

b) Now let $\mathcal{N}_{K/\mathbb{Q}}$ be the ideal norm: prove that $\mathcal{N}_{K/\mathbb{Q}}(I) = (\|I\|)$ as ideals in $\mathbb{Z}$.

c) Prove that if $J \subseteq \mathcal{O}_K$ is another nonzero ideal, then $\|I \cdot J\| = \|I\| \cdot \|J\|$.

Exercise 8.4 (3 points) Let K be a number field and $n > 0$ a positive integer. Show that there are only finitely many ideals $I \subset \mathcal{O}_K$ such that $\|I\| < n$.

Exercise 8.5 (2+3 points) Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, $\alpha \in \mathcal{O}_K$ an integral primitive element, $f \in \mathbb{Z}[X]$ the minimal polynomial of α, p a prime number and $\bar{f} \in \mathbb{F}_p[X]$ the reduction of f modulo p.

a) Show that $\mathfrak{c} := \{x \in \mathcal{O}_K : x\mathcal{O}_K \subset \mathbb{Z}[\alpha]\}$ is a nonzero ideal of $\mathcal{O}_K$.

b) Assume that $(p) + \mathfrak{c} = \mathcal{O}_K$. Construct a ring isomorphism

$$\mathcal{O}_K/(p) \xrightarrow{\sim} \mathbb{F}_p[X]/(\bar{f}).$$

Exercise 8.6 (2+5 points) Let K be a number field, $I \subset \mathcal{O}_K$ an ideal.

a) Prove that if $a \in I$ then $\|I\|$ divides $N_{K/\mathbb{Q}}(a)$.

b) Prove that $(\|I\|) \subset \mathbb{Z}$ is the ideal generated by the set $\{N_{K/\mathbb{Q}}(a) : a \in I\}$. (*Hint*: You can assume, or also prove, the following, "weak approximation" theorem: let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct nonzero prime ideals of $\mathcal{O}_K$ and $a_1, \ldots, a_n$ be nonnegative integers. Then there exists $x \in \mathcal{O}_K$ such that $v_{\mathfrak{p}_i}(x) = a_i$ where $v_{\mathfrak{p}_i}$ is the valuation associated to $\mathfrak{p}_i$. Feel free to assume $K/\mathbb{Q}$ Galois, if it makes life easier.)

Exercise 8.7 (4+4 points) Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{-5}$, $I = (120, 11\alpha - 19) \subset \mathcal{O}_K$.

a) Find all primes p such that $I \cap \mathbb{Z} \subset (p)$.

b) Find the prime factorization of I.