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

Zahlentheorie
SoSe 2019

Exercise Sheet 5

If you want your solutions to be corrected, you should hand them in by Monday, May 20.
Please write your name and immatriculation number on top of every exercise

---

For the first exercise, we will need the a fact, whose proof is in Marcus, Theorem 12. Let K, L be two number fields and suppose that the composite field KL has degree $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$. We denote by $\mathcal{O}_K, \mathcal{O}_L$ the respective rings of integers, and by $\mathcal{O}_L\mathcal{O}_L$ the composite ring.

$$\mathcal{O}_K\mathcal{O}_L = \{a_1b_1 + \cdots + a_rb_r \,|\, a_i \in \mathcal{O}_K, b_i \in \mathcal{O}_L\}$$

Consider also the two discriminants $\operatorname{disc}(K), \operatorname{disc}(L)$ and their greatest common divisor

$$d = \gcd(\operatorname{disc}(K), \operatorname{disc}(L)).$$

Fact: *In the above notations, we have that*

$$\mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L.$$

In particular, if $d = 1$, then $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$.

With this one can solve the first exercise:

Exercise 4.1 (2+2+2+2 points) In this exercise we will show that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$, for every $n \in \mathbb{N}$. In the exercise sessions, we proved this when n is a power of a prime.

a) Suppose that m, n are coprime. Show that $\mathbb{Q}(\zeta_{nm}) = \mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m)$. Show moreover that $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

b) Prove that $\operatorname{disc}(\zeta_m)$ divides a power of m. [*Hint:* Write $x^m - 1 = \Phi_m(x)g(x)$, where $\Phi_m(x)$ is the minimal polynomial of ζ_m. Then derive and apply the norm.]

c) Prove that $\mathcal{O}_{\mathbb{Q}(\zeta_{nm})} = \mathcal{O}_{\mathbb{Q}(\zeta_m)}\mathcal{O}_{\mathbb{Q}(\zeta_n)}$.

d) Prove that $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.

Exercise 4.2 (1+3+3 points)

a) Let A be a domain and let $x \in \operatorname{Frac} A$. Define the set

$$(A : x) := \{a \in A \,|\, ax \in A\}.$$

Prove that $(A : x)$ is an ideal in A, and that $x \in A$ if and only if $(A : x) = A$.

b) Let A be a domain. For every maximal ideal $\mathfrak{m} \subseteq A$, we can look at the localization $A_\mathfrak{m}$ as a subring of $\operatorname{Frac} A$. Prove that

$$A = \bigcap_{\mathfrak{m} \text{ maximal}} A_\mathfrak{m}.$$

c) Let A be a noetherian domain that has at least a nonzero prime and such that for every nonzero prime $\mathfrak{p}$, the localization $A_{\mathfrak{p}}$ is a DVR. Prove that A is a Dedekind domain.

Exercise 4.3 (2+3+2 points) (Chinese Remainder Theorem) Let A be a ring. Two ideals $I, J \subseteq A$ are called *coprime* if $I + J = A$. Now suppose that $I_1, \ldots, I_n \subseteq A$ are pairwise coprime ideals.

a) For every $j = 2, \ldots, n$ the ideals I_1, I_j are coprime, hence there are $x_j \in I_1, y_j \in I_j$ such that $x_j + y_j = 1$. Let $y = y_2 \cdot y_3 \ldots y_n$. Prove that $y \in I_2 \cdot I_3 \ldots I_n$ and that $x = 1 - y \in I_1$.

b) The previous point shows that for any $j = 1, \ldots, n$ there are x_j, y_j such that $x_j \in I_j$, y_j is in the product of all the ideals, apart from I_j, and $x_j + y_j = 1$. Use this to prove that

$$I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$$

c) Define a natural map

$$A/I_1 I_2 \ldots I_n \to A/I_1 \times A/I_2 \times \cdots \times A/I_n$$

and show that it is an isomorphism.