Übungen zur Algebraischen Zahlentheorie (WS 2023)

PD Dr. Jürgen Müller, **Ausgabe:** 26.10.2023

(3.1) Exercise: Discriminants.
a) Let $K \subseteq L$ be a separable finite field extension of degree $n := [L\colon K]$, and let $\mathcal{S} := [z_1, \ldots, z_n]$ be an n-tuple of elements of L. Show that $\mathrm{disc}(\mathcal{S}) \neq 0$ if and only if $\mathcal{S}$ is K-linearly independent.
b) Now let $L = K(z)$, and let $\mathcal{B}_z := \{1, z, \ldots, z^{n-1}\} \subseteq L$. Show that $\mathrm{disc}(z) := \mathrm{disc}(\mathcal{B}_z) = (-1)^{\binom{n}{2}} \cdot N_{L/K}((\partial\mu_z)(z))$, where $\mu_z \in K[X]$ is the minimum polynomial of z over K, and $\partial = \partial_X$ is the derivative.
c) Assume further that there is $f \in R[X]$ monic (not necessarily irreducible) such that $f(z) = 0$, where $R \subseteq K$ is integrally closed such that $K = \mathrm{Q}(R)$. (Thus z is integral over R.) Show that $\mathrm{disc}(z) \mid N_{L/K}((\partial f)(z)) \in R$.

(3.2) Exercise: Cyclotomic fields.
a) For $m \in \mathbb{N}$ let $\zeta_m := \exp(\frac{2\pi i}{m}) \in \mathbb{C}$ be a primitive m-th root of unity, let $\Phi_m \in \mathbb{Q}[X]$ be its minimum polynomial over $\mathbb{Q}$, being called the m-th **cyclotomic polynomial**, let $K_m := \mathbb{Q}(\zeta_m) \subseteq \mathbb{C}$ be the associated **cyclotomic field**, and let $\mathcal{O}_m \subseteq K_m$ be its ring of integers.

Show that $\mathbb{Q} \subseteq K_m$ is a Galois extension of degree $\varphi(m)$, where φ denotes Euler's totient function, and determine the Galois group $\mathrm{Aut}_{\mathbb{Q}}(K_m)$. Moreover, show that $\mathbb{Z}[\zeta_m] \subseteq \mathcal{O}_m$ (where actually we have equality, but we are not able to prove this here), and show that $\mathrm{disc}(\zeta_m) = \mathrm{disc}(\mathbb{Z}[\zeta_m]) \mid m^{\varphi(m)}$.

b) Let $2 \neq p \in \mathcal{P}$. Determine $\Phi_p \in \mathbb{Q}[X]$, and for $k \in \mathbb{Z}$ compute $N_{K_p/\mathbb{Q}}(\zeta_p^k) \in \mathbb{Z}$ and $T_{K_p/\mathbb{Q}}(\zeta_p^k) \in \mathbb{Z}$, as well as $N_{K_p/\mathbb{Q}}(1 - \zeta_p^k) \in \mathbb{Z}$. Moreover, show that $\mathrm{disc}(\zeta_p) = \mathrm{disc}(\mathbb{Z}[\zeta_p]) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$. In particular, conclude that $\mathcal{O}_3 = \mathbb{Z}[\zeta_3]$, and compare with Exercise (2.2).

Hint for b). Use Exercise (3.1).

(3.3) Exercise: Rings of integers.
Let $\alpha := \sqrt[3]{5} \in \mathbb{R}$ and $K := \mathbb{Q}(\alpha)$. Determine the embeddings of K into $\mathbb{C}$, an integral basis of K, the ring of integers $\mathcal{O} \subseteq K$, and its discriminant.

(3.4) Exercise: Rings of integers.
a) Let $\alpha := \sqrt[3]{175} \in \mathbb{R}$ and $K := \mathbb{Q}(\alpha)$. Determine the embeddings of K into $\mathbb{C}$, an integral basis of K, the ring of integers $\mathcal{O} \subseteq K$, and its discriminant.
b) Show that K does not have an integral basis $\mathcal{B}_\omega = \{1, \omega, \omega^2\}$ for any $\omega \in \mathcal{O}$.

Hint for a). Consider $\beta := \sqrt[3]{245} \in \mathbb{R}$ as well.