Übungen zur Algebraischen Zahlentheorie (WS 2023)

PD Dr. Jürgen Müller, **Ausgabe:** 14.12.2023

(10.1) Exercise: Units in cyclotomic fields.
Let $\zeta := \zeta_5 \in \mathbb{C}$, let $K := \mathbb{Q}(\zeta)$, and let $\mathcal{O} := \mathcal{O}_K = \mathbb{Z}[\zeta]$.
a) For any $\alpha \in \mathcal{O}$ show that $N(\alpha) = \frac{1}{4} \cdot (a^2 - 5b^2)$ for suitable $a, b \in \mathbb{Z}$. Conclude that the group of units of $\mathcal{O}$ is infinite.
b) Show that $N(a + b\zeta) = \sum_{i=0}^{4} (-1)^i a^i b^{4-i}$, for $a, b \in \mathbb{Z}$. Use this to calculate $N(\zeta + k)$ for $k \in \{-3, -2, 2, 3, 4\}$, and write the latter as products of irreducible elements of $\mathcal{O}$. Similarly, provide factorisations of 11, 31, and 61 in $\mathcal{O}$.

Hint for a). Use Gaussian sums.

(10.2) Exercise: Real subfields of cyclotomic fields.
Let $\zeta := \zeta_m \in \mathbb{C}$ be a primitive m-th root of unity, where $m \geq 3$, let $\omega := \zeta + \zeta^{-1}$, let $K := \mathbb{Q}(\omega)$ and let $\mathcal{O} := \mathcal{O}_K$.
a) Show that $K = \mathbb{Q}(\zeta) \cap \mathbb{R}$ and that $\mathcal{O} = \mathbb{Z}[\omega]$.
b) Let $m := p$ be an odd prime. Show that $\operatorname{disc}(\mathcal{O}) = p^{\frac{p-3}{2}}$.

Hint. Show that both the sets $\{\zeta^{-(k-1)}, \ldots, \zeta^{-1}, 1, \zeta, \ldots, \zeta^{k-1}\} \subseteq \mathbb{Q}(\zeta)$ and $\{1, \omega, \zeta, \zeta\omega, \ldots, \zeta^{k-1}, \zeta^{k-1}\omega\} \subseteq \mathbb{Q}(\zeta)$ are integral bases, where $k := \frac{\varphi(m)}{2}$.

(10.3) Exercise: Primes in arithmetic progressions.
We consider another (easy) special case of **Dirichlet's Theorem [1837]** on primes in coprime residue classes:
a) Show that there are infinitely many $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv -1 \pmod 3$.
b) Show that there are infinitely many $p \in \mathcal{P}_{\mathbb{Z}}$ such that $p \equiv 1 \pmod 3$.

(10.4) Exercise: Legendre symbols.
Let $0 \neq a \in \mathbb{Z}$. Show that
a) there are infinitely many odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = 1$;
b) there are infinitely many odd primes $p \in \mathcal{P}$ such that $p \nmid a$ and $\left(\frac{a}{p}\right) = -1$.