Übungen zur Algebraischen Zahlentheorie (WS 2023)

PD Dr. Jürgen Müller, **Ausgabe:** 04.01.2024

(12.1) Exercise: Galois ramification.
Let $K \subseteq L$ be a Galois extension of algebraic number fields, let $G := \mathrm{Aut}_K(L)$, and let $\mathfrak{p} \in \mathcal{P}_K$. Show the following:
a) If $\mathfrak{p}$ is inert in L, then G is cyclic.
b) If $\mathfrak{p}$ is completely ramified in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G is cyclic of prime order. Likewise, if in all intermediate fields $K \subseteq M \subset L$ there is only a single prime lying over $\mathfrak{p}$, but not so in L, then G is cyclic of prime order.
c) If $\mathfrak{p}$ is unramified in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G has a unique smallest non-trivial subgroup H. Likewise, if $\mathfrak{p}$ splits completely in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G has a unique smallest non-trivial subgroup H.
d) If $\mathfrak{p}$ is inert in all intermediate fields $K \subseteq M \subset L$, but not so in L, then G has prime power order.

Hint for d). If a finite group G has a unique smallest non-trivial subgroup H, then G has prime power order, and H is a central subgroup of prime order.

(12.2) Exercise: Biquadratic fields.
Let $K \neq L$ be quadratic algebraic number fields, and let $p \in \mathcal{P}_\mathbb{Z}$.
a) Show that p might be completely ramified in K and L, but not so in KL. Likewise, show that in both K and L there might be only a single prime lying over p, but not so in KL.
b) Show that p might be unramified in K and L, but not so in KL. Likewise, show that p might split completely in K and L, but not so in KL.
c) Show that p might be inert in K and L, but not so in KL. Likewise, show that p might be pure in K and L, but not so in KL.
d) Still, if p is inert in *all* quadratic subfields of KL, what happens in KL?
e) Letting $\mathfrak{p} \in \mathcal{P}_{KL}(p)$, provide examples for $[e(\mathfrak{p}), f(\mathfrak{p})] \in \{[1,2],[2,1],[2,2]\}$.

(12.3) Exercise: Cyclotomic fields (partly GAP).
a) Let $r, e, f \in \mathbb{N}$. Show that there are rational primes $p, l \in \mathcal{P}_\mathbb{Z}$ such that $p \equiv 1 \pmod{e}$, and p splits into r distinct prime ideals in $\mathbb{Q}(\zeta_l)$, and such that $\mathbb{Q}(\zeta_l)$ has a subfield of degree rf. How does p split in this subfield?
b) Assuming the above setting, show that $\mathbb{Q}(\zeta_{pl})$ has a subfield in which p splits into r prime ideals, each having ramification index e and inertial degree f.
c) Write a GAP program which for $r, e, f \in \mathbb{N}$ computes rational primes p, l and a subfield of $\mathbb{Q}(\zeta_{pl})$ as above. Apply this in particular for $e := 2$, $f := 3$, $r := 5$.

(12.4) Exercise: Non-factorial cyclotomic number rings (GAP).
Show that the ring of integers of $\mathbb{Q}(\zeta_{31})$ is not factorial.

Hint. Use an element of small norm, and a suitable quadratic field.