# Exercise sheet 10
## Frobenius and reciprocity law

**Exercise 1.** [Basic results]

Let $L/K$ be a Galois extension of number fields with Galois group $G$. We fix $\mathfrak{p}$ a maximal ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$.

($a$) Recall the definition of the decomposition and inertia groups $D_\mathfrak{q}$ and $I_\mathfrak{q}$, and give their orders. If $\mathfrak{q}$ is unramified, what is the Frobenius $(\mathfrak{q}, L/K)$ ? Describe these groups when $\mathfrak{p}$ is totally ramified, totally split, or inert.

($b$) Consider the tower of extensions $K \subset L^{D_\mathfrak{q}} \subset L^{I_\mathfrak{q}} \subset L$ and how the primes $\mathfrak{p}$, $\mathfrak{q} \cap L^{D_\mathfrak{q}}$ and $\mathfrak{q} \cap L^{I_\mathfrak{q}}$ split in it.

($c$) Let $K'$ be a subextension of $L/K$. Prove that $\mathfrak{q}' = \mathfrak{q} \cap K'$ is unramified above $\mathfrak{p}$ if and only if $K' \subset L^{I_\mathfrak{q}}$ and $\mathfrak{p}$ is totally split in $K'$ if and only if $K' \subset L^{D_\mathfrak{q}}$.

($d$) Prove that for every $g \in G$, $gD_\mathfrak{q}g^{-1} = D_{g(\mathfrak{q})}$ and $gI_\mathfrak{q}g^{-1} = I_{g(\mathfrak{q})}$. Deduce that $g(\mathfrak{q}, L/K)g^{-1} = (g(\mathfrak{q}), L/K)$.

**Exercise 2.** [Applications of the theory]

($a$) Let $K/\mathbb{Q}$ be a Galois extension with Galois group isomorphic to $\mathfrak{A}_n$, $n \geq 5$. Prove that for every unramified prime $p$, the number of primes of $K$ above $p$ is at least $n$.

($b$) For any extension $L/K$ of number fields and $\mathfrak{p}$ a maximal ideal of $\mathcal{O}_K$, prove that there are subextensions $K_D$ and $K_I$ of $L/K$ such that for a subextension $K'$ of $L/K$, $\mathfrak{p}$ is unramified (resp. totally split) in $K'$ if and only if $K' \subset K_I$ (resp. $K' \subset K_D$).

($c$) Deduce that if $L$ and $M$ are finite extensions of a number field $K$ (in a common algebraic closure $\overline{K}$), then for every maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathfrak{p}$ is unramified in $L$ and $M$ if and only if it is unramified in $LM$. Prove the same equivalence for $\mathfrak{p}$ totally split.

($d$) With the same notations as in Exercise 1, assume that $\mathfrak{p}$ is totally ramified in every strict subextension $K'$ of $L/K$. Prove that it is totally ramified in $L$ unless $G$ is cyclic of prime order.

($e$) With the same notations again, assume that $\mathfrak{p}$ is unramified in every strict subextension $K'$ of $L/K$. Prove that $\mathfrak{p}$ is unramified in $L$ unless $G$ admits a nontrivial minimal subgroup for inclusion. In this case, prove that such a subgroup is cyclic of prime order $p$ and that $G$ is a $p$-group.

**Exercise 3.** [Application of the reciprocity law for cyclotomic fields]

Let $n \geq 3$ and $p \equiv 1 \mod n$ a prime, such that 2 is a $n$-th power modulo $p$. We fix $K = \mathbb{Q}(\zeta_p)$.

($a$) Prove that there is a unique subfield $F \subset K$ such that $[F : \mathbb{Q}] = n$.

($b$) As usual, we identify $\mathrm{Gal}(K/\mathbb{Q})$ to $(\mathbb{Z}/p\mathbb{Z})^*$ via the cyclotomic character. How can we see the groups $\mathrm{Gal}(K/F)$ and $\mathrm{Gal}(F/\mathbb{Q})$ through this identification ?

($c$) Using the relationship between the Frobenius $(2, F/\mathbb{Q})$ and $(2, K/\mathbb{Q})$, prove that the prime 2 is totally split in $F$.

($d$) Assume there exists $y \in \mathcal{O}_F$ such that $F = \mathbb{Z}[y]$. How does the minimal polynomial of $y$ split modulo 2 ? Derive a contradiction.

($e$) Apply this result for $p = 31$.