Homework 5 - Number Theory

Exercise 1. Let L/K be a Galois extension of number fields with Galois group G and suppose $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_L)$ lies above $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$. If K' is an intermediate field between K and L, define $\mathfrak{p}' = \mathfrak{q} \cap \mathcal{O}_{K'} \in \mathrm{Spec}(\mathcal{O}_{K'})$. Denote the corresponding decomposition groups by $G_{\mathfrak{q}/\mathfrak{p}}$ and $G_{\mathfrak{q}/\mathfrak{p}'}$ and likewise for the inertia groups.

a) Let H be a subgroup of G and set $K' = L^H$. Show that $G_{\mathfrak{q}/\mathfrak{p}'} = G_{\mathfrak{q}/\mathfrak{p}} \cap H$ and $I_{\mathfrak{q}/\mathfrak{p}'} = I_{\mathfrak{q}/\mathfrak{p}} \cap H$.

b) The decomposition field $Z_{\mathfrak{q}}$ is the largest intermediate field K' for which $e(\mathfrak{p}'/\mathfrak{p}) = f(\mathfrak{p}'/\mathfrak{p}) = 1$.

c) The inertia field $T_{\mathfrak{q}}$ is the largest intermediate field K' for which $e(\mathfrak{p}'/\mathfrak{p}) = 1$.

d) Suppose L_1 and L_2 are finite extensions of K. Then $\mathfrak{p}$ is unramified (resp. totally split) in both L_1 and L_2 if and only if $\mathfrak{p}$ is unramified (resp. totally split) in L_1L_2.

e) The Galois group G is generated by the Frobenius elements $\mathfrak{Fr}_{\mathfrak{q}}$ of all unramified prime ideals $\mathfrak{q}$ of $\mathrm{Spec}(\mathcal{O}_L)$. (**Hint**: Use Corollary 13.7 in the textbook: If almost every prime ideal in a finite field extension K'/K is totally split, then $K = K'$.)

Exercise 2. Suppose $F/\mathbb{Q}$ is a Galois extension with Galois group Σ_3. Let K be the unique quadratic number field contained in F and L a cubic extension of the rationals contained in F. Denote by $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_F)$ an unramified prime lying above the rational prime p with corresponding Frobenius element $\mathfrak{Fr}_{\mathfrak{q}} \in \Sigma_3$. Determine the factorization of p in F, L and K if

a) $\mathfrak{Fr}_{\mathfrak{q}} = 1$,

b) $\mathfrak{Fr}_{\mathfrak{q}}$ has order 2,

c) $\mathfrak{Fr}_{\mathfrak{q}}$ has order 3.

Give an example of a number field F as above.

Exercise 3. Let p be an odd prime number and assume $p \nmid ab$ for $a, b \in \mathbb{Z}$.

a) Show the formulas

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$$

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$$

for the Legendre symbol mod p.

b) Is 59 a quadratic residue modulo 97?

c) Show the supplementary quadratic reciprocity law

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8 \end{cases}$$

by computing in $\mathbb{Q}(\zeta_8)$ and its subfield $\mathbb{Q}(\sqrt{2})$.

d) For $p > 3$,

$$(\frac{6}{p}) = \begin{cases} 1 & p \equiv \pm 1, \pm 5 \bmod 24 \\ -1 & p \equiv \pm 7, \pm 11 \bmod 24. \end{cases}$$

Exercise 4. Suppose F is a number field. Define the codifferent of F by

$$\mathfrak{c}_F = \{\beta \in F \mid \mathrm{Tr}_{F/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z} \text{ for all } \alpha \in \mathcal{O}_F\}.$$

a) Show that $\mathcal{O}_F \subseteq \mathfrak{c}_F$.
b) Let $\alpha_1, \dots \alpha_n$ be an integral $\mathbb{Q}$-basis of F with dual basis elements $\beta_1, \dots, \beta_n$ for the non-degenerate symmetric bilinear form $\langle\,,\rangle_{F/\mathbb{Q}}$ defined by $\mathrm{Tr}_{F/\mathbb{Q}}$. Show that $\mathfrak{c}_F$ is a fractional ideal of F contained in the fractional ideal generated by β_i for $1 \leq i \leq n$.
c) The different $\mathfrak{d}_F = \mathfrak{c}_F^{-1}$ of F is an integral ideal.
d) Write $\beta_i = \Sigma_j c_{i,j}\alpha_j$ where $c_{i,j} \in \mathbb{Q}$. Then $\mathfrak{c}_F = \mathbb{Z}\{\beta_1\} + \cdots + \mathbb{Z}\{\beta_n\}$ and $N(\mathfrak{c}_F) = |\det(c_{i,j})|$. Use duality of the basis elements to deduce that $N(\mathfrak{d}_F) = |\Delta_F|$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ lying above the rational prime p. Write $(p)\mathcal{O}_F = \mathfrak{p}^{e(\mathfrak{p}/p)-1}\mathfrak{a}$ for an integral ideal $\mathfrak{a}$ of F.
e) Verify the inclusion $\mathrm{Tr}_{F/\mathbb{Q}}(\mathfrak{a}) \subseteq (p)$.
f) Verify that $p^{-1}\mathcal{O}_F = ((p)\mathcal{O}_F)^{-1}$, $((p)\mathcal{O}_F)^{-1}\mathfrak{a} \subseteq \mathfrak{c}_F$ and $\mathfrak{p}^{e(\mathfrak{p}/p)-1} | \mathfrak{d}_F$.
g) Conclude that p ramifies in F if and only if p divides Δ_F.