Homework 4 - Number Theory

Exercise 1. Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_F$ for a number field F. The norm $N(\mathfrak{a})$ of $\mathfrak{a}$ is the number of elements in $\mathcal{O}_F/\mathfrak{a}$.

a) If $\alpha \in \mathcal{O}_F$ show the equality $N((\alpha)\mathcal{O}_F) = |N_{F/\mathbb{Q}}(\alpha)|$.

b) If $\mathfrak{p} \cap \mathbb{Z} = (p)$, then $N(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$ where $f(\mathfrak{p}/p)$ is the residue class degree.

c) If $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_F)$, then $N(\mathfrak{p}^m) = N(\mathfrak{p})^m$ for all $m \geq 1$.

d) Prove the ideal norm is multiplicative; that is, $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ for all non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_F$.

Exercise 2. Let F be a number field of degree n over the rationals.

a) Show that $n = r + 2c$ where r is the number of real embeddings of F and c is the number of pairs of complex embeddings of F.

In what follows, F is the splitting field of $f(X) \in \mathbb{Q}[X]$ with zeros $\alpha_1, \ldots, \alpha_m$ in $\mathbb{C}$.

b) Suppose $\sigma\colon F \hookrightarrow \mathbb{C}$ is an embedding of F into $\mathbb{C}$. Show that $\sigma(\alpha_i)$ is a zero of $f(X)$ for all $1 \leq i \leq m$. Deduce that σ permutes the zeros of $f(X)$, i.e. $\sigma(\alpha_i) = \alpha_{\pi(i)}$ for some $\pi \in \Sigma_m$ and all i, and $\sigma(F) = F$.

c) If $\alpha_i \in \mathbb{R}$ for $1 \leq i \leq m$, show that $r = n$ and $c = 0$.

d) If $\alpha_i \in \mathbb{C} \setminus \mathbb{R}$ for some $1 \leq i \leq m$, show that $r = 0$ and $2c = n$.

Exercise 3. Show that the degree 2 extension $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ of $\mathbb{Q}(\sqrt{-5})$ is unramified.

(In conjunction with class field theory, the above implies $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$ is the only abelian unramified extension of $\mathbb{Q}(\sqrt{-5})$ since the ideal class group of $\mathbb{Z}[\sqrt{-5}]$ has order 2.)

Exercise 4. Read §**10**. **Cyclotomic Fields** in the textbook and solve the following exercises.

a) If $n|m$ then $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$. If n is odd then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$.

In the following, let $n \geq 3$ and $\mathbb{Q}(\zeta_n)^+$ be the subfield $\mathbb{Q}(\zeta_n) \cap \mathbb{R}$ of $\mathbb{Q}(\zeta_n)$.

b) Show that $\theta_n = \zeta_n + \zeta_n^{-1} = 2\cos(\frac{2\pi}{n})$ and deduce $\mathbb{Q}(\theta_n) \subseteq \mathbb{Q}(\zeta_n)^+$.

c) Show that ζ_n is a zero of a quadratic polynomial with coefficients in $\mathbb{Q}(\theta_n)$. Deduce that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\theta_n)] = 2$ and $\mathbb{Q}(\theta_n) = \mathbb{Q}(\zeta_n)^+$.

d) For which values of n is $\mathbb{Q}(\zeta_n)^+$ a quadratic number field? Write each of these fields on the form $\mathbb{Q}(\sqrt{d})$ for $d \neq 0, 1$ square-free.

Exercise 5. **a**) Suppose $f(X) \in \mathbb{Z}[X]$ is non-constant. Prove that there exist infinitely many rational primes p for which $f(X)$ has a zero modulo p.

b) Suppose F is a number field with rings of integers $\mathcal{O}_F = \mathbb{Z}[\alpha]$ for some α. Prove that there exist infinitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ such that $f(\mathfrak{p}/p) = 1$, where $\mathfrak{p} \cap \mathbb{Z} = (p)$.

c) There exist infinitely many rational primes congruent to 1 modulo n for every natural number n.