EXERCISE 7 IN ALGEBRAIC NUMBER THEORY

(1) Let $F \subseteq K \subseteq L$ be field extensions. Let $\mathfrak{p}_L \mid \mathfrak{p}_K$ be primes in L and K, respectively, over $\mathfrak{p} \in F$. Then,

$$\begin{aligned} e(\mathfrak{p}_L/\mathfrak{p}) &= e(\mathfrak{p}_L/\mathfrak{p}_K) \cdot e(\mathfrak{p}_K/\mathfrak{p}), \text{ and} \\ f(\mathfrak{p}_L/\mathfrak{p}) &= f(\mathfrak{p}_L/\mathfrak{p}_K) \cdot f(\mathfrak{p}_K/\mathfrak{p}), \end{aligned}$$

where $e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p})$ denotes the ramification index and the inertia degree of $\mathfrak{P}/\mathfrak{p}$, respectively.

(2) (P) If a prime ideal $\mathfrak{p}$ of K is totally split in two separable extensions L/K and L'/K, then it is also totally split in the composite extension.

(3) (P) If L/K is a Galois extension of algebraic number fields with noncyclic Galois groups, then there are at most finitely many nonsplit prime ideals of K. Hint: Galois extensions over finite fields are cyclic extensions.

(4) (P) If L/K is a Galois extension of algebraic number fields, and $\mathfrak{P}$ a prime ideal that is unramified over K (i.e., $\mathfrak{p} = \mathfrak{P} \cap K$ is unramified in L), then there is one and only one automorphism $\phi_{\mathfrak{P}} \in G(L/K)$ such that

$$\phi_{\mathfrak{P}} a = a^q \mod \mathfrak{P} \quad \text{for all } \mathfrak{a} \in \mathcal{O},$$

where $q = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})]$. It is called the **Frobenius automorphism**. The decomposition $G_{\mathfrak{P}}$ is cyclic and $\phi_{\mathfrak{P}}$ is a generator of $G_{\mathfrak{P}}$.