METU, Fall 2011, Math 523.

Homework 7

1. Let $K \subset L$ be number fields. A prime $\mathfrak{p} \subset \mathcal{O}_K$ is *ramified* in L if and only if $e(\mathfrak{P}|\mathfrak{p}) > 1$ for some prime $\mathfrak{P} \subset \mathcal{O}_L$ lying over $\mathfrak{p}$. Prove that only finitely many primes of $\mathcal{O}_K$ are ramified in L.

2. Set $\alpha = \sqrt[3]{19} \in \mathbf{R}$. Recall that $\{1, \alpha, (1+\alpha+\alpha^2)/3\}$ is an integral basis for $L = \mathbf{Q}(\alpha)$.

   - Show that $d_L = -3 \cdot 19^2$ and $[\mathcal{O}_L : \mathbf{Z}[\alpha]] = 3$. What is $\mathrm{disc}(1, \alpha, \alpha^2)$?
   - If $\beta = (1+\alpha+\alpha^2)/3$, then show that $\mathrm{disc}(1, \beta, \beta^2) = 4d_L$. Verify that the minimal polynomial of β over $\mathbb{Q}$ is $f(x) = x^3 - x^2 - 6x - 12$.
   - Find the ideal prime decomposition of $(p) \subset \mathcal{O}_L$ for $p \in \{2, 3, 5, 7\}$.

3. Let L be a number field. Prove that infinitely many primes $p \in \mathbf{Z}$ split completely (split into $[L : \mathbf{Q}]$ distinct factors) in L. Can you apply your argument to $L = \mathbf{Q}(\sqrt[3]{5})$ and construct an infinite family of totally split primes?

4. Let $\mathfrak{P} \subset L$ be a prime lying over $\mathfrak{p} \subset K$. Suppose that L/K is a normal extension with Galois group $G = \mathrm{Gal}(L/K)$. Show that

   - the decomposition group $D(\mathfrak{P}|\mathfrak{p})$ is a subgroup of G.
   - the inertia group $I(\mathfrak{P}|\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{P}|\mathfrak{p})$.

5. Let $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. You are given that $\mathcal{O}_L = \mathbf{Z}[\alpha]$ where $\alpha = (\sqrt{2} + \sqrt{6})/2$.

   - Show that $L/\mathbf{Q}$ is normal and $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
   - Prove that the fields $K_1 = \mathbf{Q}(\sqrt{2}), K_2 = \mathbf{Q}(\sqrt{3})$ and $K_3 = \mathbf{Q}(\sqrt{6})$ are all proper subfields of L.
   - Find a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ lying over p (by giving generators) for each prime $p \in \{2, 3, 5\}$. What is the inertia index $e(\mathfrak{P}|p\mathbf{Z})$ and residual degree $f(\mathfrak{P}|p\mathbf{Z})$?
   - Determine $\mathfrak{p}_i = \mathfrak{P} \cap K_i$ for each $i \in \{1, 2, 3\}$. (There are 9 cases in total.)
   - Let β be an element in $\mathcal{O}_L$ such that $L = \mathbf{Q}(\beta)$. Suppose that $f(x) = \min(\beta, \mathbf{Q})$. Does there exist a prime p such that the reduction of $f(x)$ modulo p is irreducible in $(\mathbf{Z}/p\mathbf{Z})[x]$?