METU, Fall 2011, Math 523.

Homework 10

1. Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime ideal lying over $\mathfrak{p} \subset \mathcal{O}_K$ such that $e(\mathfrak{P}|\mathfrak{p}) = 1$.
   - If $\sigma \in G$, then show that $\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$.
   - Explain why the order of Artin symbol $\left(\frac{L/K}{\mathfrak{P}}\right)$ is $f(\mathfrak{P}|\mathfrak{p})$.
   - Prove that $\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{P}}\right) = 1_G$.

2. Let $K = \mathbf{Q}(\sqrt[3]{2}, \zeta_3)$. Recall that $K/\mathbf{Q}$ is normal and $\mathrm{Gal}(K/\mathbf{Q}) \cong S_3$.
   - Show that 2 and 3 are the only primes in $\mathbf{Z}$ which ramify in K.
   - Let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime ideal lying over 7. Find $N(\mathfrak{P})$.
   - Show that $(\frac{K/\mathbf{Q}}{\mathfrak{P}})(\zeta_3) = \zeta_3$.
   - Evaluate $N_{\mathbf{Q}}^{K}(5 + \zeta_3)$. If $5 + \zeta_3 \in \mathfrak{P}$, then find $(\frac{K/\mathbf{Q}}{\mathfrak{P}})(\sqrt[3]{2})$.

3. Let $K = \mathbf{Q}(i)$ and let p be an odd prime. Show that p splits in K if and only if

$$\left(\frac{d_K}{p}\right) = 1.$$

   Let $\mathfrak{p} = (\pi)$ be a prime ideal of $\mathcal{O}_K$ lying over p generated by $\pi \in \mathcal{O}_K$. What is $N_{\mathbf{Q}}^{K}(\pi)$? Prove that an odd prime $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.

4. Let n be a nonzero integer, and let p be an odd prime not dividing n. Then $p | x^2 + ny^2$ where $\gcd(x, y) = 1$ if and only if $(\frac{-n}{p}) = 1$.

5. Let $K = \mathbf{Q}(\sqrt{-5})$. Verify that $H = K(\sqrt{5})$ is the Hilbert class field of K, i.e. maximal unramified abelian extension of K (Hint: $\mathrm{Cl}(K) \cong \mathrm{Gal}(H/K)$). Show that

$$\left\{ \begin{array}{c} \left(\frac{-5}{p}\right) = 1 \text{ and } x^2 - 5 = 0 \text{ has} \\ \text{an integer solution modulo } p. \end{array} \right\} \Longleftrightarrow p \equiv 1, 9 \pmod{20}.$$