HW #9

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Reading Homework. Try Exercises 4.6, 4.7, 4.8, 4.9 in the textbook. Read its solutions in the back.

Question 1.

(1) Find all integers $a \in \mathbb{Z}$ such that $5X^2 = a$ has a solution in $\mathbb{Z}_5 = \mathcal{O}_{\mathbb{Q}_5}$.

(2) Show that $f(X) = X^4 - 2X^3 - X^2 + 6$ is irreducible in $\mathbb{Q}[X]$.

Hint. Use the 2-adic Newton polygon (Theorem 4.43) and Gauss's lemma to deduce that, if $f(X)$ is not irreducible, $f(X) = g(X)h(X)$ for $g(X), h(X) \in \mathbb{Z}[X]$ with $\deg g = \deg h = 2$. Deduce a contradiction by combining information you can obtain by applying Hensel's lemma mod 2 and mod 3.

Question 2. This generalizes HW#7, Question 2.

Let $n > 1$ be an integer, and let K be a number field that contains $\mathbb{Q}(\zeta_n)$. Let $\alpha \in K^\times$. Suppose that α is not an ℓ-th power in K for any prime divisor ℓ of n (i.e., for each prime divisor ℓ of n, there is no $x \in K$ such that $\alpha = x^\ell$). Consider $L = K(\sqrt[n]{\alpha})$. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and let p be the rational prime that $\mathfrak{p}$ divides.

(1) Show that $X^n - \alpha$ is irreducible in $K[X]$, so that $[L : K] = n$.

Hint. For a monic polynomial $h(X)$ dividing $X^n - \alpha$, its roots are all of the form $\zeta_n^j \sqrt[n]{\alpha}$. Look at the constant term of $h(X)$.

(2) Show that L/K is Galois, with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$.

(3) If $v_\mathfrak{p}(\alpha)$ is not divisible by n, show that $\mathfrak{p}$ is ramified in L.

(4) Suppose that $(n, p) = 1$. If $v_\mathfrak{p}(\alpha)$ is divisible by n, show that $\mathfrak{p}$ is unramified in L.

Hint. Use the relative discriminant.

(5) More precisely, in (3), show that f, g can be described as follows. Take $\alpha = \pi^{nm}u$, where π is a uniformizer of $K_\mathfrak{p}$, $m \in \mathbb{Z}$, and $v_\mathfrak{p}(u) = 0$. Consider the prime factorization of $X^n - u$ in $k_{K_\mathfrak{p}}[X]$, where $k_{K_\mathfrak{p}}$ is the residue field of $K_\mathfrak{p}$, written as

$$X^n - u = \overline{h}_1(X) \cdots \overline{h}_m(X), \quad \overline{h}_1(X), \cdots, \overline{h}_m(X) \in k_{K_\mathfrak{p}}[X].$$

Then, $g = m$, and $f = \frac{n}{m} = \deg \overline{h}_1 = \cdots = \deg \overline{h}_m$.

Hint. Show that $\zeta_n^j \not\equiv 1 \pmod{\mathfrak{p}}$ for $j = 1, \cdots, n-1$. Use this and Hensel's lemma to show that the prime fatcorization of $X^n - u$ in $K_{\mathfrak{p}}[X]$ is given by $X^n - u = h_1(X) \cdots h_m(X)$, where $\deg h_i = \deg \overline{h}_i$, and h_i is a lift of $\overline{h}_i$. Use (1) and Theorem 4.53 to finish.

(6) Suppose that $p|n$, and let $k = v_p(n)$ (i.e., p^k divides n and p^{k+1} does not). Suppose that $v_{\mathfrak{p}}(\alpha)$ is divisible by n, so that $\alpha = \pi^{nm}u$ for a uniformizer π of $K_{\mathfrak{p}}$, $m \in \mathbb{Z}$, and $v_{\mathfrak{p}}(u) = 0$. Finally, let

$$\epsilon = \begin{cases} 0 & \text{if } p \text{ is odd} \\ 1 & \text{if } p \text{ is even} \end{cases}$$

Show that $\mathfrak{p}$ is unramified in L if $u \in \mathcal{O}_{K_{\mathfrak{p}}}$ is a p^k-th power modulo $\pi^{ke_{K_{\mathfrak{p}}/\mathbb{Q}_p}+\epsilon}\mathcal{O}_{K_{\mathfrak{p}}}$.

Hint. Let $n = p^k n'$, $(p, n') = 1$. Use Exercise 4.4 to show that any element of $1 + \pi^{ke_{K_{\mathfrak{p}}/\mathbb{Q}_p}+\epsilon}\mathcal{O}_{K_{\mathfrak{p}}}$ is a p^k-th power. Use Theorem 4.53 to show that $\mathfrak{p}$ is unramified in $K(\sqrt[p^k]{\alpha})$ if α is a p^k-th power in $K_{\mathfrak{p}}$. Use (5) to show that $\mathfrak{p}$ is unramified in $K(\sqrt[n']{\alpha})$.

Question 3. Let K be a number field, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. For any positive integers $N, M > 0$, show that there exists a number field L over K which has a prime ideal $\mathfrak{q}$ that divides $\mathfrak{p}$ such that $e(\mathfrak{q}|\mathfrak{p}) \geq N$, $f(\mathfrak{q}|\mathfrak{p}) \geq M$.

Hint. Use Krasner's lemma, HW#8, Question 2(2).