HW #4

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Reading Homework. Try Exercise 2.1 in the textbook. Read its solutions in the back.

Question 1. Consider $K = \mathbb{Q}(\sqrt[3]{28})$. Let $\alpha = \sqrt[3]{28}$, so that the minimal polynomial of α over $\mathbb{Q}$ is $f(X) = X^3 - 28$.

(1) Compute $D(1, \alpha, \alpha^2)$. Deduce that if $p \neq 2, 3, 7$ is a rational prime, then $(p, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$.
(2) Use the Dedekind's criterion with α to compute the prime ideal factorization of (5) in $\mathcal{O}_K$.
(3) Let
$$\beta = \frac{-\alpha^2 + 2\alpha + 2}{6} \in K.$$
Show that $\beta \in \mathcal{O}_K$ by showing that the minimal polynomial of β over $\mathbb{Q}$ is $g(X) = X^3 - X^2 + 5X + 1$.
(4) Compute $D(1, \beta, \beta^2)$. Deduce that $(3, [\mathcal{O}_K : \mathbb{Z}[\beta]]) = 1$.
Hint. Use that $D(1, \beta, \beta^2) = [\mathcal{O}_K : \mathbb{Z}[\beta]]^2 \operatorname{disc}(K)$.
(5) Use the Dedekind's criterion **with** β to compute the prime ideal factorization of (3) in $\mathcal{O}_K$. What will happen if you mindlessly used the Dedekind's criterion with α to compute a factorization of (3)?

Question 2. Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$. Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Q}$. Suppose that p is a rational prime such that $f(X)$ mod p factors into a product
$$f(X) = f_1(X) \cdots f_r(X) \pmod{p},$$
such that $f_1(X), \cdots, f_r(X) \in \mathbb{F}_p[X]$ are mutually distinct monic irreducible polynomials in $\mathbb{F}_p[X]$.

Our goal is to show that, under these assumptions, $(p, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$.

(1) Suppose on the contrary that p divides $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then, it divides $D(1, \alpha, \cdots, \alpha^{n-1})$, where $n = \deg f$. Recall that
$$D(1, \alpha, \cdots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2,$$
where $\alpha_1, \cdots, \alpha_n$ are the roots of $f(X)$ in the Galois closure L of $K/\mathbb{Q}$. Deduce that, if p divides $D(1, \alpha, \cdots, \alpha^{n-1})$, then there are $i \neq j$ such that $\alpha_i - \alpha_j \in \mathfrak{p}$ for some prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ lying over p.
(2) Show that $f(X)$, as an element of $(\mathcal{O}_L/\mathfrak{p})[X]$, has repeated roots.

(3) Using that $\mathcal{O}_L/\mathfrak{p}$ is also a finite field, and that $(\mathcal{O}_L/\mathfrak{p})/\mathbb{F}_p$ is a separable extension, show that, if $f(X)$ has repeated roots in $\mathcal{O}_L/\mathfrak{p}$, then its factorization into monic irreducible polynomials in $\mathbb{F}_p[X]$ must have some multiplicities. This gives rise to a contradiction.
(4) Deduce that p is unramified in K.