HW #5

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Reading Homework. Try Exercises 2.3, 2.4, 2.5 in the textbook. Read its solutions in the back.

Question 1. Let $K=\mathbb{Q}(\sqrt[3]{3})$. The splitting of rational primes for K was done in Example 2.15.

(1) Show that the Galois closure of K over $\mathbb{Q}$ is $L:=\mathbb{Q}(\sqrt[6]{-3})$. Namely, show that L is the smallest number field Galois over $\mathbb{Q}$ that contains K as a subfield. What is $\mathrm{Gal}(L/\mathbb{Q})$?

Hint. Use $\sqrt{3}e^{\pi i/6}=2+e^{2\pi i/3}$.

(2) Let $\alpha:=\sqrt[6]{-3}$. Namely, let α be a root of the polynomial X^6+3. Compute

$$D(1,\alpha,\cdots,\alpha^5).$$

(3) Show that $[\mathcal{O}_L:\mathbb{Z}[\alpha]]$ is a power of 2.[1]

Hint. Use Exercise 1.7.

(4) Show that $\mathrm{disc}(L)$ is a power of 3.

Hint. Use that $L=\mathbb{Q}(\zeta_3,\sqrt[3]{3})$ and HW #2, Question 2.

(5) Let's say we take it for granted[2] that 2 is unramified in L. Let

$$(2)=\mathfrak{p}_1\cdots\mathfrak{p}_g$$

be the prime ideal factorization of (2) in $\mathcal{O}_L$. Find g and the residue degrees of $\mathfrak{p}_1,\cdots,\mathfrak{p}_g$.

Hint. Use the computations in Example 2.15, and Exercise 2.4.

Question 2. For a rational prime $p\equiv 5 \pmod 8$, this Question will find a unit[3] in $\mathbb{Q}(\sqrt{p})$ that is not itself a root of unity.

(1) Let

$$\alpha:=\prod_{1\le a\le p-1,\ a\text{ is a quadratic residue mod }p}(1+\zeta_p^a).$$

Show that $\alpha\in\mathbb{Q}(\sqrt{p})$.

(2) Show that α is a unit in $\mathbb{Q}(\sqrt{p})$. Namely, show that $\alpha\in\mathcal{O}_{\mathbb{Q}(\sqrt{p})}^\times$.

Hint. Use Exercise 1.5.

(3) Show that the only roots of unity in $\mathbb{Q}(\sqrt{p})$ are ±1. Thus, our goal is to show that $\alpha\neq\pm1$.

[1] In fact, the Dedekind's criterion implies that $[\mathcal{O}_L:\mathbb{Z}[\alpha]]\neq 1$; can you see why?

[2] We will learn that this follows from the fact that $\mathrm{disc}(L)$ is not divisible by 2.

[3] We will learn later that there are infinitely many such units, and a more systematic way to find them.

(4) Choose any embedding of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$. Show that α is sent to a positive real number. Deduce that $\alpha \neq -1$.

Hint. Use that $\left(\frac{-1}{p}\right) = 1$ so that one can divide quadratic residues mod p into pairs $\bigcup_{1 \leq a \leq \frac{p-1}{4},\, a \text{ is a quadratic residue mod } p} \{a, -a\}$.

(5) Using that $\left(\frac{2}{p}\right) = -1$, show that

$$\left(\prod_{1 \leq a \leq p-1,\, a \text{ is a quadratic residue mod } p} (1 + X^a) \right) - 1$$

is not divisible by $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$ (as an element in $\mathbb{Z}[X]$). Deduce that $\alpha \neq 1$.

Hint. Note that $\left(\frac{2}{p}\right) = -1$ implies that $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.