HW #2

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Warning. You are not allowed to use any fact that appears in the later part of the text (i.e., §2∼).

Reading Homework. Try Exercises 1.3, 1.6, 1.7 in the textbook. Read their solutions in the back.

Question 1. Let $f(X) = X^3 - 15X - 20$.

(1) Show that $f(X)$ is irreducible in $\mathbb{Q}[X]$.

(2) Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(X)$. Use the techniques of Exercise 1.7 to show that

$$[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1 \text{ or } 2.$$

Hint. To exclude 3, you need to consider $f(X + a)$ instead for an appropriate a, just like Exercise 1.7(4).

(3) Show that there is no subring $\mathbb{Z}[\alpha] \subset R \subset K$ such that $[R : \mathbb{Z}[\alpha]] = 2$. Deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. [1]

Hint. Such an R must be a $\mathbb{Z}[\alpha]$-submodule of $\frac{1}{2}\mathbb{Z}[\alpha]$. When can it be a **ring**?

Question 2. Let K, L be number fields over $\mathbb{Q}$ (**not necessarily Galois**) such that $K \cap L = \mathbb{Q}$.

(1) If $(\mathrm{disc}(K), \mathrm{disc}(L)) = 1$, show that $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$ and $\mathrm{disc}(KL) = \mathrm{disc}(K)^{[L:\mathbb{Q}]}\,\mathrm{disc}(L)^{[K:\mathbb{Q}]}$.

Hint. Modify the proof of Proposition 1.35; use Proposition 1.16(6).

(2) In general, show that

$$\mathrm{lcm}(\mathrm{disc}(K), \mathrm{disc}(L)) \mid \mathrm{disc}(KL) \mid \mathrm{disc}(K)^{[L:\mathbb{Q}]}\,\mathrm{disc}(L)^{[K:\mathbb{Q}]}.$$

Question 3. Let p be an odd prime. In this Question, we will identify the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ using another method (related to the **Gauss sums** that will come later in the course).

(1) Let K be the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. Show that

$$K = \mathbb{Q}(\alpha), \quad \alpha := \sum_{1 \le a \le p-1,\ a \text{ is a quadratic residue mod } p} \zeta_p^a$$

(2) Show that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -1$.

Hint. Let $\sigma : K \to K$ be the unique nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. What is $\sigma(\alpha)$? What is $\alpha + \sigma(\alpha)$?

[1] This can be done more systematically using Dedekind's index criterion, which we will learn later.

(3) Recall the **Legendre symbol** from Introduction,

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is not a quadratic residue mod } p. \end{cases}$$

Show that, for $a, b \not\equiv 0 \pmod{p}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(4) Show that

$$(\alpha - \sigma(\alpha))^2 = \begin{cases} p & \text{if } -1 \text{ is a quadratic residue mod } p, \\ -p & \text{if } -1 \text{ is not a quadratic residue mod } p. \end{cases}$$

Hint. Write $(\alpha - \sigma(\alpha))^2$ as a double sum using the Legendre symbols, and massage it.

(5) Deduce that

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } -1 \text{ is a quadratic residue mod } p, \\ \mathbb{Q}(-\sqrt{p}) & \text{if } -1 \text{ is not a quadratic residue mod } p. \end{cases}$$

(6) Deduce that -1 is a quadratic residue mod p if and only if $p \equiv 1 \pmod{4}$.