HW #3

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, February 6 by 11:59pm on Gradescope.

Question 1. Let p be an odd prime. In HW2, we proved that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$. As this Galois group is a cyclic group of even order, there is a unique nontrivial group homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$. By Galois theory, there is a corresponding subfield $K \subset \mathbb{Q}(\zeta_p)$, which is the unique quadratic subfield. Show that

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \pmod 4 \\ \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Hint. Use $\mathrm{disc}(K) | \mathrm{disc}(\mathbb{Q}(\zeta_p))$.

Question 2. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n with $\alpha \in \mathcal{O}_K$, such that the minimal polynomial $p_\alpha(X)$ of α over $\mathbb{Q}$ satisfies the Eisenstein's irreducibility criterion with a prime number p (we say that $p_\alpha(X)$ is **Eisenstein at** p in short).

(1) If $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ are integers such that
$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in p\mathcal{O}_K,$$
then show that $a_0, a_1, \cdots, a_{n-1} \in p\mathbb{Z}$.
Hint. First, multiply the expression by α^{n-1} to show that $a_0 \in p\mathbb{Z}$. Then, inductively show that $a_1 \in p\mathbb{Z}$, $a_2 \in p\mathbb{Z}$, $\cdots$.

(2) If $x \in \mathcal{O}_K$ has an expression
$$x = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \quad b_0, \cdots, b_{n-1} \in \mathbb{Q},$$
show that each $b_i \in \mathbb{Q}$ has no p in its denominator.

(3) Prove that $(p, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$ by showing that there is no element of order p in the finite abelian group $\mathcal{O}_K/\mathbb{Z}[\alpha]$.

(4) Show that $\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} = \mathbb{Z}[\sqrt[5]{2}]$ as follows.
- Note that $[\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} : \mathbb{Z}[\sqrt[5]{2}]]$ divides $\mathrm{disc}(1, \sqrt[5]{2}, \cdots, \sqrt[5]{2^4})$, which has only 2 and 5 as prime factors (compute it).
- 2 does not divide $[\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} : \mathbb{Z}[\sqrt[5]{2}]]$ as the minimal polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}$, $X^5 - 2$, is Eisenstein at 2.
- 5 does not divide $[\mathcal{O}_{\mathbb{Q}(\sqrt[5]{2})} : \mathbb{Z}[\sqrt[5]{2}]]$ as the minimal polynomial of $\sqrt[5]{2} - 2$ over $\mathbb{Q}$, $(X+2)^5 - 2$, is Eisenstein at 5.

Question 3. In this exercise, we will prove the following

Theorem. For a Noetherian ring A, any finitely generated A-module is Noetherian.

(1) Let B be any commutative ring with 1 and M be a B-module. Let $N \subset M$ be a B-submodule, and let $M_1, M_2 \subset M$ be two B-submodules of M. Show that $M_1 = M_2$ if and only if $M_1 \cap N = M_2 \cap N$ and $\frac{M_1}{M_1 \cap N} = \frac{M_2}{M_2 \cap N}$ as B-submodules of $\frac{M}{M_1 \cap N}$.
(2) For any commutative ring B with 1, show that a B-module generated by a single element is of the form B/I for an ideal $I \subset B$.
(3) Prove the Theorem by induction on the number of generators of the module.

Question 4. In this exercise, we will prove the following

Theorem. Let F be a field, and A be a commutative F-algebra which is finitely generated as an F-module. Then, A is an integral domain if and only if A is a field.

As fields are integral domains, we only need to prove one direction. Suppose that A is an integral domain.

(1) Choose $a \in A$ nonzero. Show that the multiplication-by-a map $m_a : A \to A$ (i.e. $m_a(x) = ax$) is an **injective** F-linear map.
(2) Show that A as an F-vector space is of finite dimension. Deduce that m_a is surjective.
(3) Deduce that A is a field.