HW #2

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, January 30 by 11:59pm on Gradescope.

Question 1. Let A be a commutative ring with 1, and let M, N be A-modules. Find the natural A-module structure on the set $\mathrm{Hom}_A(M, N)$, as claimed in the lecture notes.

Question 2. Let $f(X) = X^3 + aX + b$, $a, b \in \mathbb{Q}$, such that $f(X)$ is irreducible in $\mathbb{Q}[X]$ (i.e. $f(X)$ has no rational roots). Let α be a root of $f(X)$, and let $K = \mathbb{Q}(\alpha)$ be a degree 3 number field. Show that

$$D(1, \alpha, \alpha^2) = -27b^2 - 4a^3.$$

Question 3. Read the proof of the **Primitive Element Theorem**. Using the Primitive Element Theorem, we aim to prove that, for a number field K, $\mathrm{disc}(K) \neq 0$.

(1) Use the Primitive Element Theorem to show that one can find $\alpha \in \mathcal{O}_K$ satisfying $K = \mathbb{Q}(\alpha)$.
(2) Show that $D(1, \alpha, \cdots, \alpha^{n-1}) \neq 0$, where $n = [K : \mathbb{Q}]$. Deduce that $\mathrm{disc}(K) \neq 0$.

Question 4. Let $n > 1$ be an integer, and choose a primitive n-th root of unity $\zeta_n \in \mathbb{C}$. This is an algebraic integer, and the field $\mathbb{Q}(\zeta_n)$ is called the **n-th cyclotomic field**. We will focus on the case when $n = p^a$ is a prime power.

(1) Prove the **Eisenstein's irreducibility criterion**: given a polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X],$$

if there is a prime number p such that the following two Conditions are satisfied, then $f(X)$ is irreducible in $\mathbb{Z}[X]$ (and thus $\mathbb{Q}[X]$, by Gauss's Lemma).

Condition 1. p divides $a_{n-1}, a_{n-2}, \cdots, a_0$.
Condition 2. p^2 does not divide a_0.

(2) Using the Eisenstein's irreducibility criterion, show that the minimal polynomial of ζ_{p^a} over $\mathbb{Q}$ is

$$\Phi_{p^a}(X) = X^{p^{a-1}(p-1)} + X^{p^{a-1}(p-2)} + \cdots + X^{p^{a-1}} + 1.$$

This polynomial is called the **p^a-th cyclotomic polynomial.**

Hint. First, note that the minimal polynomial of ζ_{p^a} must divide

$$\frac{X^{p^a} - 1}{X^{p^{a-1}} - 1} = \Phi_{p^a}(X).$$

Then, use the Eisenstein's irreducibility criterion to $\Phi_{p^a}(X+1)$.

(3) Deduce that the conjugates of ζ_{p^a} are $\zeta_{p^a}^k$, $1 \leq k \leq p^a$, $(k, p) = 1$, and that $\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}$ is Galois with
$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times.$$
In particular, $\mathbb{Q}(\zeta_{p^a})$ does not depend on the choice of a primitive p^a-th root of unity.

Question 5. Let p be a prime number, and $a \geq 1$.

(1) Compute $D(1, \zeta_{p^a}, \cdots, \zeta_{p^a}^{p^{a-1}(p-1)-1})$.

(2) Show that $N_{\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}}(1 - \zeta_{p^a}) = p$. Deduce that, for any $k \in (\mathbb{Z}/p^a\mathbb{Z})^\times$,
$$\frac{1 - \zeta_{p^a}^k}{1 - \zeta_{p^a}} \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}^\times.$$
This kind of a unit is called a **cyclotomic unit**.

(3) Let $p \geq 5$. Show that
$$\frac{1 - \zeta_{p^a}^2}{1 - \zeta_{p^a}} = 1 + \zeta_{p^a} \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}^\times,$$
is of infinite order. This shows that the multiplicative group of units $\mathcal{O}_{\mathbb{Q}(\zeta_{p^a})}^\times$ as an abelian group is infinite.

Hint. We have a freedom to choose ζ_{p^a}. Choose $\zeta_{p^a} = e^{\frac{2\pi i}{p^a}}$, and show that $\left|1 + e^{\frac{2\pi i}{p^a}}\right| > 1$ (the absolute value as a complex number).