MAT 5210 Homework 4

1. Suppose β is a root of an irreducible polynomial $f(X) = X^3 + pX + q \in \mathbf{Z}[X]$. Verify that $1, \beta, \beta^2, \beta^3$ have traces $3, 0, -2p, -3q$ respectively. Compute $\mathrm{tr}(\beta^4)$, and deduce that $\Delta(1, \beta, \beta^2)^2 = -4p^3 - 27q^2$.

2. Suppose α is a root of a monic irreducible polynomial $f(X) \in \mathbf{Z}[X]$. Prove that if $\deg(f) = n$ and $K = \mathbf{Q}(\alpha)$, then show that

$$\Delta(1, \alpha, \dots, \alpha^{n-1})^2 = (-1)^{\frac{n(n-1)}{2}} \mathrm{Norm}_{K/\mathbf{Q}}(f'(\alpha))$$

3. Let $K : \mathbf{Q}$ be a number field, and $\omega = \{\omega_1, \dots, \omega_n\}$ be a basis of K (as a $\mathbf{Q}$-vector space). Let $\theta = \{\theta_1, \dots, \theta_n\}$ be a subset of K such that

$$\theta_j = \sum_{k=1}^{n} c_{kj}\omega_k \qquad (c_{kj} \in \mathbf{Q})$$

for $1 \leq j \leq n$.

   (a) Prove that $\Delta(\theta) = \det(c_{ij})\Delta(\omega)$.

   (b) Hence show that θ is a basis of K if and only if $\Delta(\theta) \neq 0$ (Hint: take $\omega = \{1, \alpha, \dots, \alpha^{n-1}\}$ in Question 2).

4. Let K be a number field. Prove that the ring of integers $\mathcal{O}_K$ is a Euclidean domain with Euclidean function

$$\mathrm{Norm}_{K/\mathbf{Q}} : \mathcal{O}_K \setminus \{0\} \to \mathbf{N} \setminus \{0\}$$

if and only if for all $\alpha \in K$, there exists $\beta \in \mathcal{O}_K$ such that $\left|\mathrm{Norm}_{K/\mathbf{Q}}(\alpha - \beta)\right| < 1$. Hence show that if $K = \mathbf{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7$, then $\mathcal{O}_K$ is a Euclidean domain. (Hint: consider the nearest point on a lattice).

5. Suppose that $[K : \mathbf{Q}] = n$. We say an embedding $\sigma : K \hookrightarrow \mathbf{C}$ is real if $\sigma(K) \subset \mathbf{R}$, and complex if $\sigma(K) \subset \mathbf{C} \setminus \mathbf{R}$. Let there be a total of r real embeddings, and s pairs of conjugate complex embeddings $K \hookrightarrow \mathbf{C}$, with $n = r + 2s$. Show that if $\omega = \{\omega_1, \dots, \omega_n\}$ is an integral basis of the ring of integers $\mathcal{O}_K$, then the sign of $\Delta(\omega)^2 \in \mathbf{Z}$ is $(-1)^s$. Verify this for $K = \mathbf{Q}(\alpha)$, where $\alpha^3 = m$ is a non-cube integer.

6. (a) Show that $f(X) = X^3 - X + 2$ is an irreducible polynomial in $\mathbf{Z}[X]$.

(b) Let θ be a root of $f(X) = 0$. Calculate $\Delta(1, \theta, \theta^2)^2$.

(c) **Stickelberger's Theorem** (see optional question) says that for any integral basis ω of $\mathcal{O}_K$, the discriminant $\Delta(\omega)^2$ satisfies $\Delta(\omega)^2 \equiv 0, 1 (\text{mod } 4)$. Use it to show that $\{1, \theta, \theta^2\}$ is an integral basis of $\mathcal{O}_K$.

7. Suppose the monic polynomial $f \in \mathbf{Z}[X]$ satisfies Eisenstein's criterion at the prime p. Let α be a root of f and $K = \mathbf{Q}(\alpha)$. Show that $\mathbf{Z}[\alpha]$ is a subgroup of $\mathcal{O}_K$, and the index

$$[\mathcal{O}_K : \mathbf{Z}[\alpha]]$$

is <u>NOT</u> divisible by p.

Optional Question:

1. (Stickelberger's Theorem) Let K be a number field with $\sigma_i : K \hookrightarrow \mathbf{C}$ being the embeddings of $\mathbf{C}$.

Suppose $\omega = \{\omega_1, \ldots, \omega_n\}$ is an integral basis of $\mathcal{O}_K$, and $\Delta(\omega) := \det(\sigma_i(w_j))$. Let P be the sum of the positive terms of the expansion of the determinant $\Delta(\omega)$, and let N be the sum of the negative terms of the determinant of $\Delta(\omega)$, i.e.

$$\Delta(\omega) = \sum_{\tau \in A_n} \left(\prod_{i=1}^{n} \sigma_i(\omega_{\tau(i)}) \right) - \sum_{\tau \notin A_n} \left(\prod_{i=1}^{n} \sigma_i(\omega_{\tau(i)}) \right) = P - N.$$

(a) Let $(\mathbf{C} \supseteq) M \supseteq K \supseteq Q$ be the 'Galois closure' of $K : \mathbf{Q}$. Show that

$$P + N,\ PN \in \mathbf{Q}\ (= M^{\mathrm{Gal}(M/\mathbf{Q})})$$

(b) Consequently, show that

$$\Delta(\omega)^2 = (P - N)^2 \equiv 0 \text{ or } 1 \ (\text{mod } 4).$$