Discriminants and integral bases

Exercise 1. [The ring of integers of a biquadratic field]

Let $m, n \neq 1$ be coprime square-free integers congruent to 1 modulo 4, and let $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$.

1. Prove that $\alpha \in K$ is an algebraic integer if and only if $\mathrm{Tr}_{K/\mathbb{Q}(\sqrt{m})}(\alpha), N_{K/\mathbb{Q}(\sqrt{m})}(\alpha) \in \mathcal{O}_{Q(\sqrt{m})}$.
2. By looking at traces, show that for every $\alpha \in \mathcal{O}_K$, there exist $a, b, c, d \in \mathbb{Z}$ such that
$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn}}{4}$$
and
$$a \equiv b \equiv c \equiv d \bmod 2.$$
3. Show that there exists $a', b', c', k \in \mathbb{Z}$ such that
$$\alpha - k\frac{1+\sqrt{m}}{2} \cdot \frac{1+\sqrt{n}}{2} = \frac{a' + b'\sqrt{m} + c'\sqrt{n}}{2}.$$
4. Deduce that $\left(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}}{2} \cdot \frac{1+\sqrt{n}}{2}\right)$ is an integral basis of $\mathcal{O}_K$.
5. Compute D_K.

   Remark. When m and n are both congruent to 2 or 3 modulo 4, one has to consider the cases $mn \equiv 1 \bmod 4$ and $mn \equiv 2, 3 \bmod 4$ separately (why can't $mn \equiv 0 \bmod 4$ happen ?).
6. Let $K = \mathbb{Q}(\sqrt{2}, i)$. We admit the fact that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}][\zeta]$, where $\zeta = \sqrt{2}\frac{1+i}{2}$. Let $\alpha = \alpha_1 + \alpha_2\zeta \in K$, with $\alpha_1, \alpha_2 \in \mathbb{Q}(\sqrt{2})$.
   (a) Find $\beta_1, \beta_2 \in \mathbb{Z}[\sqrt{2}]$ such that $|\alpha_i - \beta_i| \leq \frac{1}{2}$.
   (b) Show that $N_{K/\mathbb{Q}(\sqrt{2})}(\alpha - \beta) < 1$ with $\beta = \beta_1 + \beta_2\zeta$, and deduce that $\mathcal{O}_K$ is euclidean with respect to $N_{K/\mathbb{Q}(\sqrt{2})}$.

Exercise 2. [Eisenstein polynomials]

Let $P \in \mathbb{Z}[X]$ be Eisenstein at the prime p, *i.e.* writing $P = \sum_{i=0}^{n} a_i X^i$, we have $p \mid a_i$ for $0 \leq i < n, p \nmid a_n$ and $p^2 \nmid a_0$.

1. Prove that P is irreducible in $\mathbb{Q}[X]$.
2. We now assume $a_n = 1$. Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathbb{C}$ a root of P. We will show that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Assume for a contradiction that $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.
   (a) Prove that there exists $x \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$ such that $x = \frac{1}{p}(u_0 + u_1\alpha + \cdots + u_{n-1}\alpha^{n-1})$ for some $u_0, \ldots, u_{n-1} \in \mathbb{Z}$.
   (b) Let i_0 be the smallest i such that $p \nmid u_i$. Prove that $\frac{u_{i_0}\alpha^{n-1}}{p} \in \mathcal{O}_K$.
   (c) Prove that $p \mid u_{i_0}$ and deduce a contradiction.
3. Prove that $v_p(D_K) = v_p(\Delta(1, \alpha, \ldots, \alpha^{n-1}))$.

Exercise 3. [An application]

1. Let $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[4]{2}$. Compute $\Delta(1, \alpha, \alpha^2, \alpha^3)$ and D_K. Deduce that $(1, \alpha, \alpha^2, \alpha^3)$ is an integral basis of $\mathcal{O}_K$.
2. Let $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[3]{2}$.
   (a) Compute $v_2(D_K)$.
   (b) Compute $v_3(D_K)$. *(Hint : Compute the minimal polynomial of $\beta = \alpha + 1$)*
   (c) Prove that $(1, \alpha, \alpha^2)$ is an integral basis of $\mathcal{O}_K$.

Exercise 4. [A basis for the ring of integers]

Let K be a number field and $\alpha \in \mathcal{O}_K$ both of degree n. We write $d = \Delta(1, \alpha, \dots, \alpha^{n-1})$.

For all $k \in \{0, \dots, n-1\}$, let F_k be the $\mathbb{Z}$-module generated by $\left(\frac{1}{d}, \frac{\alpha}{d}, \dots, \frac{\alpha^k}{d}\right)$ and $R_k = F_k \cap \mathcal{O}_K$. We are going to define monic polynomials $f_1, \dots, f_{n-1} \in \mathbb{Z}[X]$ with f_i of degree i, and integers $d_1 \mid \cdots \mid d_{n-1}$ such that for $0 \leq k \leq n-1$, $\left(\frac{1}{d}, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_k(\alpha)}{d_k}\right)$ is an integral basis of R_k.

1. Explain why $R_{n-1} = \mathcal{O}_K$, and prove the result for $k = 0$.
2. By induction, assume the f_i have been constructed for each $i \leq k < n-1$ (with $f_0 = 1$). Let π be the projection from F_{k+1} to $\mathbb{Z}\frac{\alpha^{k+1}}{d}$. Prove that there exists a $\beta \in R_{k+1}$ such that $\pi(R_{k+1}) = \mathbb{Z}\pi(\beta)$. Prove that $\left(1, \dots, \frac{f_k(\alpha)}{d_k}, \beta\right)$ is an integral basis of R_{k+1}.
3. Prove that $\frac{\alpha^{k+1}}{d_k} = \pi\left(\alpha \frac{f_k(\alpha)}{d_k}\right)$ and deduce that $\frac{\alpha^{k+1}}{d_k} \in R_{k+1}$. Find an integer d_{k+1} and a monic polynomial $f_{k+1} \in \mathbb{Q}[X]$ of degree $k+1$ such that $d_k \mid d_{k+1}$ and $\beta = \frac{f_{k+1}(\alpha)}{d_{k+1}}$.
4. Prove that $\frac{f_{k+1}(\alpha) - \alpha f_k(\alpha)}{d_k} \in R_k$, and that it can be written $\frac{g(\alpha)}{d_k}$ for some $g \in \mathbb{Z}[X]$ of degree $< k$.
5. Show that $f_{k+1} - X f_k = g$ and conclude.