# TD 2 : Discriminants et anneaux de Dedekind

**Exercice 1.** [Discriminant]

($a$) Pour $d$ entier sans facteur carré différent de 0 et 1, et $K = \mathbb{Q}(\sqrt{d})$, calculer $\operatorname{disc}(1, \sqrt{d})$, puis $\operatorname{disc}(K)$.

($b$) Pour $X^3 + aX + b \in \mathbb{Q}[X]$ irréductible sur $\mathbb{Q}$ et $\alpha$ une racine de $P$, calculer $\operatorname{disc}(1, \alpha, \alpha^2)$.

Pour $K/\mathbb{Q}$ un corps de nombres de plongements $\sigma_1, \cdots, \sigma_n$ et $\alpha_1, \cdots, \alpha_n$ une $\mathbb{Z}$-base entière de $\mathcal{O}_K$, on note $M = (\sigma_i(\alpha_j))_{i,j}$ et $P$ et $N$ les contributions des permutations respectivement paires et impaires au calcul de $\det(M)$, de sorte que $\det(M) = P + N$.

($c$) Montrer que $\operatorname{disc}(K) = \det(M)^2$.

($d$) Montrer que $P$ et $N$ sont des entiers, et en déduire que $\operatorname{disc}(K) \equiv 0$ ou 1 mod 4 (théorème de Stickelberger).

**Exercice 2.** [Anneau d'entiers d'un corps cubique]

Soit $K = \mathbb{Q}(\alpha)$ avec $\alpha$ une racine de $P(X) = X^3 - X^2 - 2X - 8$.

($a$) Montrer que $P$ est irréductible dans $\mathbb{Q}[X]$ en raisonnant sur la valeur d'une racine possible.

($b$) Soit $\beta = (\alpha^2 + \alpha)/2$. Montrer que $\beta^3 - 3\beta^2 - 10\beta - 8 = 0$, en déduire que $\beta \in \mathcal{O}_K$.

($c$) Montrer que $\operatorname{disc}(1, \alpha, \alpha^2) = -4 \cdot 503$ puis que $\operatorname{disc}(1, \alpha, \beta) = -503$. En déduire que $(1, \alpha, \beta)$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$.

($d$) Montrer que pour tout $x \in \mathcal{O}_K$, $\operatorname{disc}(1, x, x^2)$ est pair. En déduire que $\mathcal{O}_K$ ne peut pas être de la forme $\mathbb{Z}[x]$.

**Exercice 3.** [Bases des anneaux d'entiers]

Soit $K/\mathbb{Q}$ un corps de nombres de degré $n$ et $\alpha \in \mathcal{O}_K$ de degré $n$ également. On pose $d = \operatorname{disc}(1, \alpha, \cdots, \alpha^{n-1})$.

($a$) Pour tout $k \leq n-1$, on pose $F_k$ le $\mathbb{Z}$-module engendré par $(1/d, \alpha/d, \cdots, \alpha^k/d)$ et $R_k = F_k \cap \mathcal{O}_K$. Rappeler pourquoi $R_{n-1} = \mathcal{O}_K$.

On va définir par récurrence des polynômes unitaires $(f_1, \cdots, f_{n-1})$ de $\mathbb{Z}[X]$ avec $f_i$ de degré $i$ et des diviseurs élémentaires positifs $d_1 | \cdots | d_{n-1}$ tels que pour tout $k \in \{0, \cdots, n-1\}$, la famille

$$\left(1, \frac{f_1(\alpha)}{d_1}, \cdots, \frac{f_k(\alpha)}{d_k}\right)$$

est une $\mathbb{Z}$-base de $R_k$. Pour $k = n$, on aura donc une $\mathbb{Z}$-base de $\mathcal{O}_K$ de cette forme.

($b$) Montrer le cas $k = 0$.

($c$) Supposons qu'on a défini la famille jusqu'à l'étape $k < n-1$. On pose $\pi$ la projection de $F_{k+1}$ dans $\mathbb{Z}\alpha^{k+1}/d$, et on fixe $\beta \in R_{k+1}$ tel que $\pi(R_{k+1}) = \mathbb{Z}\pi(\beta)$. Montrer que $(1, \cdots, \frac{f_k(\alpha)}{d_k}, \beta)$ est une $\mathbb{Z}$-base de $R_{k+1}$.

($d$) Montrer que $\alpha^{k+1}/d_k = \pi(\alpha f_k(\alpha)/d_k)$, et en déduire que cet élément appartient à $\pi(R_{k+1})$, d'où un $m \in \mathbb{Z}$ tel que $m\pi(\beta) = \pi(\alpha^{k+1}/d_k)$. En posant $d_{k+1} = |m|d_k$, montrer que

$$\pm\beta = \frac{f_{k+1}(\alpha)}{d_{k+1}}$$

pour un polynôme $f_{k+1} \in \mathbb{Q}[X]$ unitaire de degré $k+1$.

($e$) Montrer que $(f_{k+1}(\alpha) - \alpha f_k(\alpha))/d_k \in R_k$ par construction, et qu'on peut donc l'écrire sous la forme $g(\alpha)/d_k$ avec $g \in \mathbb{Z}[X]$ de degré au plus $k$.

($e$) Montrer l'égalité des polynômes $f_{k+1}(X) - Xf_k(X) = g(X)$ et conclure.

($f$) Montrer qu'étant donné une telle famille, $d_k$ est le plus petit entier $m \in \mathbb{N}_{\geq 1}$ tel que $mR_{k+1} = \mathbb{Z}[\alpha]$, en déduire l'unicité des diviseurs élémentaires.

($g$) Montrer que

$$\mathrm{disc}(\alpha) = (d_1 \cdots d_{n-1})^2 \,\mathrm{disc}(K).$$

($h$) Montrer que pour $i + j < n$, on a $d_i d_j | d_{i+j}$. En déduire que $d_1^{n(n-1)}$ divise $\mathrm{disc}(\alpha)$.