6. Discriminant et corps de nombres.

On fixe pour toute la suite un corps de nombre K de degré n sur $\mathbb{Q}$ (c.à.d. une extension de degré n sur $\mathbb{Q}$) et on note O_K l'anneau des entiers algébriques de K. On désigne par $\sigma_1, ..., \sigma_n$ les homomorphismes de K dans $\mathbb{C}$. Pour toute la suite on note simplement Tr et N pour la trace $\mathrm{Tr}_{K/\mathbb{Q}}$ et la norme $\mathrm{N}_{K/\mathbb{Q}}$.

Exercice 6.1 1. Montrer qu'il existe $u \in O_K$ tel que $K = \mathbb{Q}(u)$.

2. Montrer que si $x \in O_K$, alors $\mathrm{Tr}(x)$ et $\mathrm{N}(x)$ sont dans $\mathbb{Z}$.

Rappel de cours sur le discriminant : Soit $x_1, ..., x_n \in K$. Rappelons la définition du discriminant $\mathrm{Disc}(x_1, ..., x_n) := \det[\mathrm{Tr}(x_i x_j)]$. On a les propriétés suivantes :

1. $\mathrm{Disc}(x_1, ..., x_n) = (\det[\sigma_i(x_j)])^2$
2. $\mathrm{Disc}(x_1, ..., x_n) \neq 0$ si et seulement si $(x_1, ..., x_n)$ est une base de K sur $\mathbb{Q}$.
3. Soient $(e_1, ..., e_n)$ et $(e'_1, ..., e'_n)$ deux bases de K sur $\mathbb{Q}$. Notons A la matrice de passage de la première base vers la seconde. Alors
$$\mathrm{Disc}(e'_1, ..., e'_n) = (\det A)^2 \, \mathrm{Disc}(e_1, ..., e_n).$$
4. Si x est une élément primitif de K sur $\mathbb{Q}$ de polynôme minimal f alors
$$\mathrm{Disc}(1, x, ..., x^{n-1}) = \mathrm{Disc}(f) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2 = (-1)^{n(n-1)/2} \mathrm{N}(f'(x)).$$

Exercice 6.2 (Bases intégrales) 1. Montrer que si $x_1, .., x_n \in O_K$ alors $\mathrm{Disc}(x_1, ..., x_n) \in \mathbb{Z}$.

2. Soit $e_1, .., e_n \in O_K$ tel que $(e_1, ..., e_n)$ soit une base de K sur $\mathbb{Q}$ avec $|\mathrm{Disc}(e_1, ..., e_n)|$ minimal parmi de telles bases formées d'entiers algébriques. Montrer que $O_K = \mathbb{Z}e_1 \oplus .... \oplus \mathbb{Z}e_n$. (Indication : supposer qu'il existe $x = \sum a_i e_i \in O_K$ tel que $a_1 \notin \mathbb{Z}$ et utiliser la base $(x - b_1 e_1, e_2, ..., e_n)$ où b_1 est la partie entière de a_1.)
3. En déduire que O_K est un $\mathbb{Z}$-module libre de rang n.
4. Vérifier que toute base du $\mathbb{Z}$-module O_K est aussi une base de K sur $\mathbb{Q}$. On appelera une telle base, **base intégrale** de K.
5. Montrer que toutes les bases intégrales ont même discriminant. On appelera ce discriminant le **discriminant** de K que l'on notera $\mathrm{Disc}(K)$.

Pour l'exercice suivant, on utilisera le **"théorème de la base adaptée"** : *si M est un module libre de rang n sur un anneau principal A,et si N est un sous-module de M alors :*

1. *N est un module libre de rang $q \leq n$;*
2. *il existe une base $(e_1, ..., e_n)$ de M et des éléments non nuls $a_1, ..., a_q$ de A tels que $(a_1 e_1, .., a_q e_q)$ soit une base de N (et tels que $a_i \mid a_{i+1}$ pour $1 \leq i \leq q-1$.*

Exercice 6.3 Soit $(u_1, ..., u_n)$ une base de K formée d'entiers algébriques.

1. Montrer que le module quotient $O_K/(\mathbb{Z}u_1 \oplus ... \oplus \mathbb{Z}u_n)$ est fini. On appele **indice** du sous-module $\mathbb{Z}u_1 \oplus ... \oplus \mathbb{Z}u_n$ dans O_K le cardinal cardinal $O_K/\mathbb{Z}[u_1, ..., u_n]$.
2. Montrer que $\mathrm{Disc}(u_1, ..., u_n) = m^2 \mathrm{Disc}(K)$ où m est l'indice de $\mathbb{Z}u_1 \oplus ... \oplus \mathbb{Z}u_n$ dans O_K .

Exercice 6.4 Soit $u \in O_K$ un élément primitif de K sur $\mathbb{Q}$ tel que le polynôme minimal de u est d'Eisenstein en p. Le but de cet exercice est de montrer que $p \nmid [O_K : \mathbb{Z}[u]]$.

1. Montrer que $p^{-1}u^n \in O_K$ et $p^2 \nmid \mathrm{N}(u)$.
2. Supposons que $p \mid [O_K : \mathbb{Z}[u]]$. Montrer qu'il existe $x \in O_K \setminus \mathbb{Z}[u]$ tel que $px \in \mathbb{Z}[u]$.

3. En déduire qu'il existe des entiers $b_0, ..., b_{n-1}$ non tous divisibles par p tel que $x = p^{-1}(b_0 + b_1 u + ... + b_{n-1}u^{n-1})$.
4. Soit $y = p^{-1}(b_r u^r + ... + b_{n-1}u^{n-1})$ avec r le plus petit entier tel que b_r non divisible par p. Montrer que y est un entier algébrique.
5. Soit $z = p^{-1}b_r u^{n-1}$. Montrer que z est aussi un entier algébrique.
6. Montrer que $p^n \mathrm{N}(z) = b_r^n \mathrm{N}(u)^{n-1}$.
7. En déduire une contradiction.

Pour la suite, on considère un **"corps cubique pur"** K, c.à.d. tel que $K = \mathbb{Q}(\sqrt[3]{d})$ avec d entier strcitement supérieur à 1 sans facteur cubique. Le but du problème suivant est de déterminer l'anneau des entiers $O_{\mathbb{Q}(\sqrt[3]{d})}$.

Problème 6.1 On note $\theta_1 = \sqrt[3]{d}$.

1. (a) Quel est le polynôme minimal de θ_1 et quels sont ses conjugués.
   (b) Calculer $\mathrm{Disc}(1, \theta_1, \theta_1^2)$.
   (c) Démontrer qu'il existe deux entiers positifs a et b uniques tels que ab soit sans facteur carré et $d = ab^2$. On pose $\theta_2 = \sqrt[3]{a^2 b}$. Démontrer que θ_2 est un élément primitif de K sur $\mathbb{Q}$ et que $\mathrm{Disc}(1, \theta_2, \theta_2^2) = -27a^4b^2$.
   (d) Démontrer que $(1, \theta_1, \theta_2)$ est une base de K sur $\mathbb{Q}$ et que $\mathrm{Disc}(1, \theta_1, \theta_2) = -27a^2b^2$.
2. Soeint u, v, w les indices respectifs des sous-modules $\mathbb{Z}[\theta_1]$, $\mathbb{Z}[\theta_2]$ et $\mathbb{Z}[1, \theta_1, \theta_2]$ dans O_K.
   (a) Montrer que $(a, u) = 1$ (on utilisera l'exercice 6.4). En déduire que :
      i. si $3 \mid a$ alors $\mathrm{Disc}(K)$ est divisible par $27a^2$;
      ii. sinon $\mathrm{Disc}(K)$ est divisible par a^2.
   (b) Montrer que $(b, v) = 1$. En déduire que :
      i. si $3 \mid b$, alors $\mathrm{Disc}(K)$ est divisible par $27b^2$;
      ii. sinon $\mathrm{Disc}(K)$ est divisible par b^2.
   (c) Démontrer que $\mathrm{Disc}(K)$ est divisible par a^2b^2, est négatif et divise $27a^2b^2$.
3. Démontrer que si $d \equiv 0 \mod 3$ alors $\mathrm{Disc}(K) = -27a^2b^2$ et $(1, \theta_1, \theta_2)$ est une base intégrale de K.
4. Plus généralement démontrer le résultat précédent pour $d \not\equiv \pm 1 \mod 9$: on pourra vérifier que $\theta_1 - d$ a un polynôme minimal d'Einsenstein en 3.
5. On suppose que $d \equiv 1 \mod 9$. On considère $\alpha = (1 + \theta_1 + \theta_1^2)/3$.
   (a) Montrer que α est un entier algébrique. (On calculera son polynôme minimal.)
   (b) En déduire que $3 \mid w$ et donc que $\mathrm{Disc}(K) = -3a^2b^2$.
   (c) Montrer que $(\alpha, \theta_1, \theta_2)$ est une base intégrale de K.
6. Si $d \equiv -1 \mod 9$ montrer que $((1 - \theta_1 + \theta_1^2)/3, \theta_1, \theta_2)$ est une base intégrale de K.
7. Conclusion (théorème dû à Dedekind en 1900) :
   (a) Si $d \not\equiv \pm 1 \mod 9$ alors $\mathrm{Disc}(K) = -27a^2b^2$ et $(1, \theta_1, \theta_2)$ est une base intégrale de K.
   (b) Si $d \equiv \pm 1 \mod 9$ alors $\mathrm{Disc}(K) = -3a^2b^2$ et
      i. $((1 + \theta_1 + b\theta_2)/3, \theta_1, \theta_2)$ est une base intégrale de K si $d \equiv 1 \mod 9$,
      ii. $((1 - \theta_1 + b\theta_2)/3, \theta_1, \theta_2)$ est une base intégrale de K si $d \equiv -1 \mod 9$