**Université Paris 7 Denis Diderot**
**L3Math-Info (Algèbre et géométrie)**
**2009-2010**

# Feuille d'exercices IX

On appelle *corps de nombres* toute extension finie de $\mathbb{Q}$.

**Exercice 1** Soit $K$ un corps de nombres. On appelle *entier algébrique* dans $K$ tout élément de $K$ qui est une racine d'un polynôme unitaire à coefficient dans $\mathbb{Z}$ et on désigne par $\mathcal{O}_K$ l'ensemble des entiers algébriques dans $K$.

1) Vérifier que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.
2) Soit $\alpha$ un entier algébrique dans $K$. Montrer que le sous-groupe $M_\alpha$ de $(K, +)$ engendré par les $\alpha^n$ ($n \in \mathbb{N}$) est de type fini et que la multiplication par $\alpha$ induit un endomorphisme du groupe $M_\alpha$.
3) En déduire que $\mathcal{O}_K$ est un sous-anneau de $K$ contenant $\mathbb{Z}$.
4) Montrer que, pour tout $x \in K$, il existe un élément non-nul $a \in \mathbb{Z}$ tel que $ax \in \mathcal{O}_K$. En déduire que $K$ est le corps des fractions de $\mathcal{O}_K$ et qu'il existe une base $(e_1, \ldots, e_r)$ de $K$ sur $\mathbb{Q}$ qui est contenue dans $\mathcal{O}_K$.
5) Pour tout $a \in K$, on désigne par $f_a : K \to K$ qui envoie $x$ en $ax$. Montrer que cette application est $\mathbb{Q}$-linéaire, et est inversible si et seulement si $a \neq 0$.
6) Montrer que, si $a \in \mathcal{O}_K$, alors $\mathrm{Tr}(f_a) \in \mathbb{Z}$.
7) Montrer que l'application $F : K \times K \to \mathbb{Q}$ qui envoie $(x, y)$ en $\mathrm{Tr}(f_{xy})$ est une forme $\mathbb{Q}$-bilinéaire symétrique non-dégénérée sur $K$.
8) Soit $(e'_1, \ldots, e'_r)$ une base duale de $(e_1, \ldots, e_r)$ pour la forme biliéaire $F$. Autrement dit, on a
$$\mathrm{Tr}(f_{e'_i e_j}) = \delta_{ij}.$$
On prend $c \in \mathbb{Z}$ non-nul tel que $ce'_i \in \mathcal{O}_K$ pour tout $i$. Pour $z = b_1 e_1 + \cdots + b_r e_r \in K$ (où $b_1, \ldots, b_r \in \mathbb{Q}$), calculer $F(cz, e'_i)$.
9) En déduire que $\mathcal{O}_K$ est contenu dans le sous-groupe de $(K, +)$ engendré par les $c^{-1} e_i$ ($i = 1, \cdots, r$).
10) En déduire que $(\mathcal{O}_K, +)$ est un groupe abélien libre de rang $r$.
11) Si $\boldsymbol{w} = (w_1, \ldots, w_r)$ est une base de $K$ sur $\mathbb{Q}$. On désigne par $d(\boldsymbol{w})$ le déterminant de la matrice $(F(w_i, w_j))_{1 \leqslant i,j \leqslant r}$. Montrer que si $\boldsymbol{w}$ est une autre base de $K$ sur $\mathbb{Q}$ et si $A$ est la matrice de transition ($\boldsymbol{w}' = A\boldsymbol{w}$), alors $d(\boldsymbol{w}') = \text{dét}\,(A)^2 d(\boldsymbol{w})$.
12) En déduire que, si $\boldsymbol{w}$ et $\boldsymbol{w}'$ sont deux bases de $\mathcal{O}_K$ sur $\mathbb{Z}$, alors on a $d(\boldsymbol{w}) = d(\boldsymbol{w}')$ (cette valeur est appelé le *discriminant* de $K$, notée $d_K$).

**Exercice 2** Dans cette exercice, le symbole $K$ désigne le corps $\mathbb{Q}(i)$ des nombres de Gauss.

1) Soit $\alpha = c + id$ un élément dans $K$. Montrer que $\alpha$ est la racine du polynôme quadratique
$$P_\alpha(X) = X^2 + aX + b \in \mathbb{Q}[X]$$
avec $a = -2c$ et $b = c^2 + d^2$.
2) En déduire que $\mathbb{Z}[i] \subset \mathcal{O}_K$.

3) Montrer que, si $\alpha = c + id$ est un élément dans $\mathcal{O}_K$, alors $2c$ et $2d$ sont des entiers. En déduire que $c$ et $d$ sont en fait des entiers.
4) En déduire que $\mathcal{O}_K = \mathbb{Z}[i]$.
5) Calculer le discriminant de $\mathbb{Q}(i)$.

**Exercice 3** Soient $p$ un nombre premier, $\omega = e^{2i\pi/p}$ et $K = \mathbb{Q}(\omega)$.

1) Montrer que $1 + \omega + \cdots + \omega^{p-1} = 0$.
2) En déduire que $[K : \mathbb{Q}] \leqslant p - 1$.
3) Montrer que, pour tout $i \in \{1, \cdots, p-1\}$, $1 + \omega + \cdots + \omega^{i-1}$ est un élément dans $\mathcal{O}_K^\times$.
4) Soit $a = 1 - \omega$. Montrer que $\mathcal{O}_K p = (\mathcal{O}_K a)^{p-1}$.
5) Montrer que l'idéal de $\mathcal{O}_K$ engendré par $a$ est permier et que $\mathcal{O}_K/\mathcal{O}_K a$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
6) Montrer que $[K : \mathbb{Q}] = p - 1$ et que $1, \omega, \ldots, \omega^{p-1}$ est une base de $\mathcal{O}_K$ sur $\mathbb{Z}$.
7) Déterminer le discriminant de $K$.