

## Entiers algébriques

Dans toute la feuille, on appelle corps de nombres une extension finie de  $\mathbf{Q}$ . On note  $\mathcal{O}_{\mathbf{C}}$  l'ensemble des nombres complexes entiers sur  $\mathbf{Z}$  et, si  $K$  est un corps de nombres, on note  $\mathcal{O}_K = \mathcal{O}_{\mathbf{C}} \cap K$ . On appellera cet anneau l'anneau des entiers du corps de nombres  $K$ .

Tous les corps considérés seront des sous-corps de  $\mathbf{C}$ . Si on parle du polynôme minimal d'un élément, il sera entendu qu'il s'agit du représentant unitaire.

### Exercice 1. Préliminaires

1. Montrer que tout élément  $\alpha \in \mathcal{O}_{\mathbf{C}}$  est algébrique sur  $\mathbf{Q}$  et que réciproquement, un élément  $\alpha \in \overline{\mathbf{Q}}$  appartient à  $\mathcal{O}_{\mathbf{C}}$  si et seulement si son polynôme minimal  $P \in \mathbf{Q}[X]$  est à coefficients dans  $\mathbf{Z}$ .
2. Soit  $K$  un corps de nombres et  $\alpha \in \overline{\mathbf{Q}}$ . Montrer que  $\alpha \in \mathcal{O}_K$  si et seulement si le polynôme minimal de  $\alpha$  sur  $K$  est à coefficients dans  $\mathcal{O}_K$ .
3. Rappeler ce qu'est  $\mathcal{O}_K$ , quand  $K/\mathbf{Q}$  est une extension quadratique.

### Exercice 2. Trace et norme

Soit  $L/K$  une extension de corps de nombres et  $\alpha \in L$ . Soit

$$\begin{aligned} T_{\alpha}^L : L &\rightarrow L \\ x &\mapsto \alpha x. \end{aligned}$$

(On pourra omettre l'exposant  $L$  s'il est clair dans le contexte).

1. Montrer que  $T_{\alpha}^L$  est une application  $K$ -linéaire. On note respectivement  $\text{Tr}_{L/K}(\alpha)$  et  $\text{Nm}_{L/K}(\alpha)$  (et on appelle respectivement *trace* et *norme* de l'élément  $\alpha$ ) la trace et le déterminant de cette application  $K$ -linéaire.
2. Que valent  $\text{Tr}_{L/K}(\alpha)$  et  $\text{Nm}_{L/K}(\alpha)$  quand  $\alpha \in K$  ?
3. Montrer que

$$\begin{aligned} \forall \alpha, \beta \in L, \forall \lambda \in K, \quad \text{Tr}_{L/K}(\alpha + \lambda\beta) &= \text{Tr}_{L/K}(\alpha) + \lambda \text{Tr}_{L/K}(\beta) \\ \forall \alpha, \beta \in L, \quad \text{Nm}_{L/K}(\alpha\beta) &= \text{Nm}_{L/K}(\alpha) \text{Nm}_{L/K}(\beta). \end{aligned}$$

4. Soit  $M/L/K$  une tour de corps de nombres et  $\alpha \in L$ . Montrer que

$$\text{Tr}_{M/K}(\alpha) = [M : L] \text{Tr}_{L/K}(\alpha) \text{ et } \text{Nm}_{M/K}(\alpha) = \text{Nm}_{L/K}(\alpha)^{[M:L]}.$$

5. Soit  $K$  un corps de nombres et  $\alpha \in \overline{\mathbf{Q}}$ . Montrer que le polynôme caractéristique de l'application  $K$ -linéaire  $T_{\alpha}^{K(\alpha)}$  est le polynôme minimal de  $\alpha$  sur  $K$ .
6. Soit  $L/K$  une extension de corps de nombres et  $\alpha \in L$ . Montrer que

$$\text{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \text{Hom}_{\mathbf{K}}(L, \mathbf{C})} \sigma(\alpha) \text{ et } \text{Nm}_{L/K}(\alpha) = \prod_{\sigma \in \text{Hom}_{\mathbf{K}}(L, \mathbf{C})} \sigma(\alpha),$$

où  $\text{Hom}_{\mathbf{K}}(L, \mathbf{C})$  est l'ensemble des plongements  $K$ -linéaires de  $L$  dans  $\mathbf{C}$ .

7. Montrer que si  $\alpha \in \mathcal{O}_L$ ,  $\text{Tr}_{L/\mathbf{Q}}(\alpha)$  et  $\text{Nm}_{L/\mathbf{Q}}(\alpha)$  sont des entiers.

8. Soit  $L$  un corps de nombres. Montrer qu'un élément  $\alpha \in \mathcal{O}_L$  est une unité de  $\mathcal{O}_L$  si et seulement si  $\text{Nm}_{L/\mathbf{Q}}(\alpha) = \pm 1$ .
9. Soit  $d$  un entier sans facteur carré et  $L = \mathbf{Q}(\sqrt{d})$ . Déterminer la trace et la norme d'un élément  $\alpha \in L$ . Montrer que  $\alpha \in \mathcal{O}_L$  si et seulement si  $\text{Tr}_{L/\mathbf{Q}}(\alpha)$  et  $\text{Nm}_{L/\mathbf{Q}}(\alpha)$  sont entiers.
10. Soit  $d < 0$  un entier sans facteur carré et  $L = \mathbf{Q}(\sqrt{d})$ . Montrer que si  $d \notin \{-1, -3\}$ , alors  $\mathcal{O}_L^\times = \{\pm 1\}$ . Que se passe-t-il si  $d = -1$  ou  $d = -3$ ?

**Exercice 3. (Entiers des  $\mathbf{Q}(\zeta_p)$ )**

Dans tout cet exercice,  $p$  est un nombre premier impair,  $\zeta_p = e^{2i\pi/p}$  et  $L = \mathbf{Q}(\zeta_p)$ . On note simplement  $\text{Tr} = \text{Tr}_{L/\mathbf{Q}}$  et  $\text{Nm} = \text{Nm}_{L/\mathbf{Q}}$ . Soit  $\pi = 1 - \zeta_p$ .

1. Calculer  $\text{Nm}(\pi)$  et  $\text{Tr}(\pi)$ . Calculer également  $\text{Tr}(\zeta_p^j)$  en fonction de  $j$ .
2. On suppose que  $a$  et  $b$  sont des entiers premiers avec  $p$ . Montrer que  $\frac{1 - \zeta_p^a}{1 - \zeta_p^b} \in \mathcal{O}_L^\times$ . En déduire que si  $j \in \{1, \dots, p-1\}$ ,  $\pi$  et  $1 - \zeta_p^j$  sont associés dans  $\mathcal{O}_L$  et que  $p\mathcal{O}_L = \pi^{p-1}\mathcal{O}_L$ .
3. Montrer que  $\pi\mathcal{O}_L \cap \mathbf{Z} = p\mathbf{Z}$ . (On pourra remarquer que  $\pi\mathcal{O}_L \cap \mathbf{Z}$  est un idéal de  $\mathbf{Z}$ .)
4. Soit  $x \in K$  un élément écrit sous la forme  $x = a_0 + a_1\zeta_p + \dots + a_{p-2}\zeta_p^{p-2}$ , où les  $a_i$  sont des coefficients rationnels.
  - (a) Montrer que  $\text{Tr}(\pi x) = a_0 p$ .
  - (b) En utilisant la question 3, montrer que si  $x \in \mathcal{O}_L$ , alors  $\text{Tr}(\pi x) \in p\mathbf{Z}$  et en déduire que  $a_0 \in \mathbf{Z}$ .
  - (c) En déduire que si  $x \in \mathcal{O}_L$ , les coefficients  $a_i$  sont entiers.
  - (d) Déduire de ce qui précède que  $\mathcal{O}_L = \mathbf{Z}[\zeta_p]$ .

**Exercice 4. (Théorème de Kronecker)**

Soit  $\alpha \in \mathcal{O}_{\mathbf{C}}$  de degré  $d \geq 2$ . On suppose que toutes les racines du polynôme minimal de  $\alpha$  sont de module  $\leq 1$ . On note  $T = T_\alpha^{\mathbf{Q}(\alpha)} \in \text{End}_{\mathbf{Q}}(\mathbf{Q}(\alpha))$ .

1. Démontrer que les coefficients du polynôme caractéristique  $P_n$  de  $T^n$  sont des nombres entiers de valeur absolue  $\leq 2^d$ .
2. En déduire que  $\alpha$  est une racine de l'unité (théorème de Kronecker).
3. En considérant le nombre  $\alpha = \frac{3}{5} + \frac{4}{5}i$ , montrer que le théorème de Kronecker est faux si l'on suppose simplement  $\alpha$  algébrique.

**Exercice 5. (Nombres de Pisot)**

On appelle *nombre de Pisot* tout nombre réel  $r > 1$  appartenant à  $\mathcal{O}_{\mathbf{C}}$  tel que les autres racines du polynôme minimal de  $r$  sur  $\mathbf{Q}$  soient toutes de module  $< 1$ . Montrer que la distance de  $r^n$  à  $\mathbf{Z}$  tend vers 0 quand  $n \rightarrow \infty$ .