

## FEUILLE D'EXERCICES 6 : CORPS

---

**Exercice 1.** Soit  $A$  un anneau intègre. On suppose que  $A \supseteq K$ , où  $K$  est un corps et un sous-anneau de  $A$ . Montrer que  $A$  est un  $K$ -espace vectoriel. On suppose de plus qu'il est de dimension finie. Montrer que  $A$  est un corps.

**Exercice 2.** Y a-t-il une structure de corps sur  $\mathbb{Z}/4\mathbb{Z}$  dont le groupe additif sous-jacent est le groupe  $(\mathbb{Z}/4\mathbb{Z}, +)$  ?

**Exercice 3.** Soit  $K$  un corps de caractéristique  $p$ .

- (1) Montrer que l'application  $\sigma : K \rightarrow K$  définie par  $\sigma(x) = x^p$  est un morphisme de corps.
- (2) Que vaut  $\sigma$  pour  $K = \mathbb{F}_p$  ?
- (3) On suppose que  $K$  est fini, montrer qu'alors  $\sigma$  est un isomorphisme.
- (4) Montrer que ce n'est pas nécessairement vrai si  $K$  est infini.

**Exercice 4.** On considère le groupe additif  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . On le munit d'une loi qui en fait un anneau. On nomme ses éléments  $0, 1, a, b$  ( $0$  et  $1$  sont respectivement les éléments neutres pour  $+$  et  $\cdot$ ).

- (1) Montrer que  $a + b = 1$ .
- (2) On suppose qu'un des éléments, disons  $a$ , est de carré nul. Montrer qu'alors  $ab = a$  et  $b^2 = 1$ .
- (3) On suppose que  $a^2 \neq 0 \neq b^2$  mais que  $ab = 0$ . Montrer qu'alors  $a^2 = a$  et  $b^2 = b$ . Montrer que l'anneau obtenu est isomorphe à l'anneau produit  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- (4) On suppose maintenant que  $a^2, b^2$  et  $ab$  sont non nuls. Montrer qu'alors  $a^2 = b, b^2 = a$  et  $ab = 1$ . Montrer que l'anneau obtenu est un corps.
- (5) Montrer qu'il existe un unique (à isomorphisme près) corps à quatre éléments.

**Exercice 5.** Soit  $\mathbb{F}_2$  le corps à deux éléments. Soit  $L = \mathbb{F}_2[X]/(X^2 + X + 1)$ .

- (1) Montrer que  $L$  est un corps à quatre éléments, et écrire ses tables d'addition et de multiplication.
- (2) Vérifier que  $L$  est isomorphe au corps construit dans l'exercice précédent.
- (3) Que se passe-t-il si on remplace  $X^2 + X + 1$  par  $X^2 + 1$  ?

**Exercice 6.** Posons  $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$ .

- (1) Montrer que  $\mathbb{Q}(i)$  est un corps.
- (2) Trouver un polynôme  $P \in \mathbb{Q}[X]$  tel que  $\mathbb{Q}(i) \simeq \mathbb{Q}[X]/(P)$ .

**Exercice 7.** A quel corps le quotient  $\mathbb{R}[X]/(X^2 + X + 1)$  est-il isomorphe ?

**Exercice 8.** Déterminer les degrés des extensions de corps suivantes :  $\mathbb{R} \subseteq \mathbb{C}$ ,  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$  et  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, i)$ .

**Exercice 9.** Montrer que  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ ,  $\mathbb{Q}(2^{1/6}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$  et que  $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$ . (Indication : pour la dernière égalité, donner une base du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ ).

**Exercice 10.** Soit  $F = X^3 + 3X - 2$  dans  $\mathbb{Q}[X]$ .

- (1) Montrer que  $\mathbb{Q}[X]/(F)$  est un corps.
- (2) Notons  $u$  la classe de  $X$  dans  $\mathbb{Q}[X]/(F)$ . Montrer que  $(1, u, u^2)$  est une  $\mathbb{Q}$ -base de  $\mathbb{Q}[X]/(F)$ .
- (3) Exprimer  $(2u^2 + u - 3)(3u^2 - 4u + 1)$  et  $(u^2 - u + 4)^{-1}$  dans cette base.
- (4) Combien  $F$  a-t-il de racines dans  $\mathbb{Q}[X]/(F)$  ?
- (5) Est-il isomorphe à un sous-corps de  $\mathbb{R}$  ?
- (6) Est-il isomorphe à un sous-corps de  $\mathbb{C}$  non contenu dans  $\mathbb{R}$  ?

### Degré d'une extension, règle et compas

**Exercice 11.** Soit  $K/k$  une extension de corps de degré 5, engendrée par un élément  $\alpha$ . Montrer que  $\alpha^2$  engendre la même extension.

**Exercice 12.** Soit  $K$  un corps engendré sur  $k$  par deux éléments  $\alpha$  et  $\beta$  de degrés respectifs  $m$  et  $n$ . On suppose que  $m$  et  $n$  sont premiers entre eux. Montrer que  $[K : k] = mn$ .

**Exercice 13.** Soient  $\alpha, \beta \in \mathbb{C}$ . On suppose que  $\alpha + \beta$  et  $\alpha\beta$  sont algébriques. Montrer que  $\alpha$  et  $\beta$  le sont aussi.

**Exercice 14.** Peut-on construire à la règle et au compas un carré dont l'aire est égale à celle d'un triangle donné ?

**Exercice 15.** Soit  $\alpha$  une racine réelle de  $X^3 + 3X + 1$ . Peut-on construire  $\alpha$  à la règle et au compas ?

**Exercice 16.** On cherche à trissecter à la règle et au compas l'angle  $\pi/3$ . Montrer que ceci revient à construire le nombre  $\alpha = \cos(\pi/9)$ . Montrer que  $\alpha$  est racine du polynôme  $8X^3 - 6X - 1$  et conclure.

**Exercice 17.** Pour chacun des sous-corps suivants de  $\mathbb{C}$ , dire s'il contient  $i$  :

$$(a) \mathbb{Q}(\sqrt{-2}) \quad (b) \mathbb{Q}(\sqrt[4]{-2}) \quad (c) \mathbb{Q}(\alpha) \text{ où } \alpha^3 + \alpha + 1 = 0.$$

**Exercice 18.** Soit  $\alpha = \sqrt[3]{2}$ . Quel est le polynôme irréductible qui annule  $1 + \alpha^2$  sur  $\mathbb{Q}$  ?

**Exercice 19.** Quel est le polynôme irréductible qui annule  $\sqrt{3} + \sqrt{5}$  sur

$$(a) \mathbb{Q} \quad (b) \mathbb{Q}(\sqrt{5}) \quad (c) \mathbb{Q}(\sqrt{10}) \quad (d) \mathbb{Q}(\sqrt{15}) ?$$

**Exercice 20. Polynômes irréductibles.**

- (1) Montrer que les polynômes  $X^7 + X + 1$  et  $X^6 + X^3 + 1$  sont irréductibles dans  $\mathbb{F}_2[X]$ .

- (2) Montrer que les polynômes  $X^3 + 2X + 1$ ,  $X^3 + X^2 + 2$  et  $X^4 + X^2 + 2$  sont irréductibles dans  $\mathbb{F}_3[X]$ .

**Exercice 21. Calculs dans  $\mathbb{F}_{16}$ .**

- (1) Vérifier que  $X^4 + X + 1$  est irréductible dans  $\mathbb{F}_2[X]$ .
- (2) Justifier que  $K = \mathbb{F}_2[X]/(X^4 + X + 1)$  est un corps de cardinal 16.
- (3) Soit  $x$  la classe de  $X$  dans  $K$ . Montrer que  $x$  engendre le groupe  $K^*$ .

**Exercice 22. Algèbre linéaire et Sylow.**

Soit  $\mathbb{F}_q$  un corps avec  $q = p^r$  et  $n \geq 1$ .

- (1) Déterminer le cardinal de  $\text{GL}_n(\mathbb{F}_q)$ .
- (2) Montrer que l'ensemble des matrices triangulaires dont la diagonale est constituée de 1 est un  $p$ -sous-groupe de Sylow de  $\text{GL}_n(\mathbb{F}_q)$ .
- (3) Soit  $G$  un groupe fini et  $S$  un  $p$ -Sylow de  $G$ . Soit  $H$  un sous-groupe de  $G$ . Montrer qu'il existe  $g \in G$  tel que  $gSg^{-1} \cap H$  est un  $p$ -Sylow de  $H$ . *Indication : utiliser l'action de  $H$  sur  $G/S$ .*
- (4) Dédurre des questions précédentes l'existence d'un  $p$ -Sylow pour tout groupe.