Université Lyon I
Département de Mathématiques

Année universitaire 2024-2025
L3 MGA
Anneaux et Corps

FEUILLE D'EXERCICES 2 : 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 $\sigma : K \to K$ définie par $\sigma(x) = x^p$ est un morphisme de corps.

(2) Que vaut σ pour $K = \mathbb{F}_p$?

(3) On suppose que K est fini, montrer qu'alors σ 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 polyôme $P \in \mathbb{Q}[X]$ 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 :

(1) $\mathbb{R} \subseteq \mathbb{C}$,
(2) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$,
(3) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ et
(4) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, i)$.

Exercice 9

(1) Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$,
(2) Montrer que $\mathbb{Q}(2^{1/6}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ et que $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

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 $\mathbb{R}$?

Exercice 11

Soit K/k une extension de corps de degré 5, engendrée par un élément α. Montrer que α^2 engendre la même extension.

Exercice 12

Soit K un corps engendré sur k par deux éléments α et β 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 sur $\mathbb{Q}$. Montrer que α et β le sont aussi.

Exercice 14

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

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

Exercice 15

Soit $\alpha = \sqrt[3]{2}$. Quel est le polynôme minimal de $1 + \alpha^2$ sur $\mathbb{Q}$?

Exercice 16

Quel est le polynôme minimal de $\sqrt{3} + \sqrt{5}$ sur

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

Exercice 17

(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 18

(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 α la classe de X dans K. Montrer que α engendre le groupe K^*.

Exercice 19

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

(1) Déterminer le cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$.
(2) Montrer que l'ensemble des matrices triangulaires dont la diagonale est constituée de 1 est un p-sous-groupe de Sylow de $\mathrm{GL}_n(\mathbb{F}_q)$.
(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) Déduire des questions précédentes l'existence d'un p-Sylow pour tout groupe fini non trivial.

Exercice 20

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

Exercice 21

Soit α une racine réelle de $X^3 + 3X + 1$. Peut-on construire α à la règle et au compas ?

Exercice 22

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 α est racine du polynôme $8X^3 - 6X - 1$ et conclure.

Exercice 23

Le but de cet exercice est de montrer que la réciproque du corollaire du théorème de Wantzel est fausse. Soit $P = X^4 + 2X - 2 \in \mathbb{Q}[X]$.

(1) Montrer que P a exactement deux racines réelles. On les note a_1, a_2.
(2) Montrer que P est irréductible sur $\mathbb{Q}$, et en déduire le degré de l'extension $\mathbb{Q}(a_i)/\mathbb{Q}$ pour $i = 1, 2$.
(3) Montrer qu'il existe $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ tels que $P = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$.
(4) Montrer que le nombre $b = \beta + \delta$ est algébrique sur $\mathbb{Q}$ et que $[\mathbb{Q}(b) : \mathbb{Q}] = 3$.
(5) Montrer que l'une des deux racines réelles a_1, a_2 n'est pas constructible.

Exercice 24

Soit k un corps. Soit P et Q deux polynômes non constants dans $k[X]$. On veut un critère numérique pour décider si P et Q sont premiers entre eux.

(1) Soit p et q les degrés de P et Q respectivement. Montrer que P et Q ne sont pas premiers entre eux si et seulement si il existe deux polynômes non nuls A et B tels que
   (a) $PA = QB$;
   (b) $\deg(A) < \deg(Q)$;

(c) $\deg(B) < \deg(P)$.

(2) En déduire que P et Q sont premiers entre eux si et seulement si l'application

$$\begin{array}{rccc} \mathcal{R} : & k_{q-1}[X] \times k_{p-1}[X] & \longrightarrow & k_{p+q-1}[X] \\ & (A, B) & \longmapsto & AP + BQ \end{array}$$

est bijective.

(3) Déterminer la matrice M de $\mathcal{R}$ dans les bases canoniques. Le *résultant* $R(P, Q)$ est par définition le déterminant de M.

Soient α et β deux nombres complexes algébriques sur $\mathbb{Q}$. Notons P_α et P_β leurs polynômes minimaux.

(4) Vérifier que les deux polynômes de $\mathbb{C}[X]$, $P = P_\alpha(X)$ et $Q = P_\beta(\alpha + \beta - X)$ ont une racine commune.

(5) Soit $\tilde{Q} = P_\beta(T - X) \in (\mathbb{Q}(T))[X]$ et $\tilde{P} = P_\alpha$ pensé comme un polynôme de $(\mathbb{Q}(T))[X]$. Montrer que $R(\tilde{P}, \tilde{Q})$ appartient à $\mathbb{Q}[T]$ et s'annule en $\alpha + \beta$.

(6) Déterminer le polynôme minimal de $\sqrt{2} + \sqrt{3}$ sur $\mathbb{Q}$.

(7) Trouver un polynôme annulateur de $\alpha\beta$ en considérant $Q = X^q P_\beta(\frac{\alpha\beta}{X})$.