UNIVERSITÉ GRENOBLE-ALPES 2021-2022

Enseignant : Rémi Molinier Prépa Agreg
remi.molinier@univ-grenoble-alpes.fr

Devoir Maison

Exercice 1 – Pgcd dans les anneaux de polynômes
Soit A un anneau commutatif intègre.

1. Montrer que si A est un corps, alors $A[X]$ est euclidien.
2. Soit $a \in A$ non nul et non inversible, montrer que a et X ont un pgcd dans $A[X]$ et le déterminer.
3. En déduire que si A n'est pas un corps, alors $A[X]$ n'est pas principal. (On pourra chercher une relation de Bézout entre X et un élément non inversible de A)
4. En déduire que $A[X]$ est euclidien si et seulement si A est un corps.

Soient K un corps et L une extension de K.

5. Montrer que le morphisme d'extension $i\colon K \to L$ induit un morphisme d'anneau injectif $j\colon K[X] \to L[X]$.
6. Pour $P, Q \in K[X]$, comparer $j(\text{pgcd}(P,Q))$ et $\text{pgcd}(j(P), j(Q))$.

Soient $P = X^3 - 1 \in \mathbb{Q}[X]$ et $Q = X^{10} + X^9 + X^8 \in \mathbb{Q}[X]$.

7. Calculer $\text{pgcd}(P,Q)$ de deux façons différentes.

Exercice 2 – Racines dans $\mathbb{Q}$ d'un polynôme à coefficients entiers
Soient $n \in \mathbb{N}^*$ et $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$. Soit $r = p/q \in \mathbb{Q}$ une racine de P avec p et q premier entre eux.

1. Montrer que $p | a_0$ et $q | a_n$.
2. en déduire que $X^3 + X + 1$ est irréductible sur $\mathbb{Q}$.

Exercice 3 – Corps finis
Soit K un corps fini de cardinal $n \geq 2$.

1. Montrer que K est de caractéristique non nul p et que p est premier.

Soit $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

1. Montrer qu'il existe un unique morphisme de corps $c\colon \mathbb{F}_p \to K$ et que c induit une structure de $\mathbb{F}_p$-espace vectoriel sur K.
2. Montrer que K est de dimension fini sur $\mathbb{F}_p$.
3. En déduire qu'il existe $d \in \mathbb{N}$ tel quel que $n = p^d$.
4. Comparer $(X - 1_K)^p$ et $X^p - 1_K$ dans $K[X]$.

Exercice 4 – Multiplicativité des degrés
Soient k un corps, K une extension de k de degré fini m et L un extension de K de degré fini n.

1. Montrer que L est une extension de k de degré fini dont on explicitera le degré en fonction de m et n.

Soient K un corps et L une extension de degré fini n sur K.

2. Montrer que si n est premier, il existe $a \in L$ tel que $L = K[a]$ où $K[a]$ est l'image du morphisme d'anneau $\varphi_a\colon K[X] \to L$ qui envoie X sur a.

Deuxième composition
Mines Ponts 1975

Les deux parties du problème sont indépendantes l'une de l'autre.

PARTIE I

On considère l'équation du second degré

$$z^2 - bz + c = 0 \tag{1}$$

dont les coefficients b et c sont dans $\mathbf{Z}$ et vérifient $b^2 - 4c < 0$; α étant l'une des racines de cette équation, on désigne par $\mathbf{Z}_\alpha$ l'ensemble des nombres complexes $z = p + q\alpha$ où p et q appartiennent à $\mathbf{Z}$. On désigne également par $\mathbf{Q}_\alpha$ l'ensemble des nombres complexes $w = u + v\alpha$ où u et v appartiennent à $\mathbf{Q}$.

I.1) Montrer que $\mathbf{Z}_\alpha$ est un sous-anneau de $\mathbf{C}$. Que peut-on dire de la seconde racine de l'équation (1) ?

I.2) Soit f l'application de $\mathbf{Z}_\alpha$ dans $\mathbf{Z}$ définie par

$$f(p + q\alpha) = p^2 + bpq + cq^2 \ .$$

Montrer

$$f(x) = 0 \Longleftrightarrow x = 0$$
$$f(xy) = f(x)f(y) \ .$$

I.3) Soit G_α l'ensemble des éléments de $\mathbf{Z}_\alpha$ qui sont inversibles dans $\mathbf{Z}_\alpha$. Montrer que G_α est un groupe pour la multiplication. Quelle est l'image de G_α par f ? En déduire que si $x = p + q\alpha$ est un élément de G_α, on a l'inégalité :

$$q^2(4c - b^2) \leq 4 \ .$$

En discutant suivant les valeurs attribuées à b et à c, déterminer tous les éléments de G_α.

I.4) a) Montrer que $\mathbf{Q}_\alpha$ est un sous-corps de $\mathbf{C}$.

b) Montrer que l'ensemble des matrices à coefficients dans $\mathbf{Q}$ définies par

$$M_{u,v} = \begin{pmatrix} u & v \\ -vc & u + bv \end{pmatrix}$$

(où u et v sont des rationnels quelconques) est un corps pour l'addition et la multiplication matricielles. Démontrer que ce corps est isomorphe au corps $\mathbf{Q}_\alpha$.

I.5) a) Montrer que $\mathbf{Q}_\alpha$ est un sous-espace vectoriel de $\mathbf{C}$ considéré comme espace vectoriel sur $\mathbf{Q}$. Quelle est la dimension de ce sous-espace vectoriel ?

b) Montrer que la fonction définie sur $\mathbf{Q}_\alpha$ à valeurs dans $\mathbf{R}$

$$x \mapsto \sqrt{f(x)} = \sqrt{f(u + v\alpha)} = \sqrt{u^2 + buv + cv^2}$$

est une norme euclidienne sur l'espace vectoriel $\mathbf{Q}_\alpha$. Déterminer le produit scalaire dont dérive cette norme. Que peut-on dire de la restriction à $\mathbf{Q}_\alpha$ de la fonction module sur $\mathbf{C}$?

I.6) a) Étant donné un élément Y de $\mathbf{Q}_\alpha$, $Y \neq 0$, montrer que $\{Y, \alpha Y\}$ constitue une base de $\mathbf{Q}_\alpha$.

b) On considère deux éléments X et Y dans $\mathbf{Z}_\alpha$ avec $Y \neq 0$. Montrer qu'il existe un élément Q dans $\mathbf{Z}_\alpha$ et deux rationnels λ et μ appartenant à l'intervalle $[0; 1[$ tels que

$$X = YQ + R \text{ où } R = Y(\lambda + \mu\alpha) .$$

I.7) On suppose dans cette septième question qu'on a $c = 1$ et $b = -1$;

a) Montrer que, pour tout X dans $\mathbf{Z}_\alpha$ et pour tout Y dans $\mathbf{Z}_\alpha$, $Y \neq 0$, il existe un couple (Q, R) d'éléments de $\mathbf{Z}_\alpha$ tel que

$$X = YQ + R \text{ et } f(R) < f(Y) .$$

b) On donne $X = 5+7\alpha$ et $Y = 3+\alpha$. Déterminer une solution (Q, R) du problème précédent et montrer que cette solution n'est pas unique.

c) Soit I un idéal arbitraire de l'anneau $\mathbf{Z}_\alpha$. Montrer que cet idéal est principal.
Si le même idéal non nul est engendré par deux éléments distincts Z et Z' de $\mathbf{Z}_\alpha$, quelle est la relation qui existe entre Z et Z' ?

d) Montrer que l'ensemble des éléments $X = (5+7\alpha)A+(3+\alpha)B$ où A et B sont des éléments quelconques de $\mathbf{Z}_\alpha$ est un idéal. Déterminer tous les générateurs de cet idéal.

I.8) Soit A_α l'ensemble des automorphismes φ de l'espace vectoriel $\mathbf{Q}_\alpha$ tels que

$$\varphi(xy) = \varphi(x)\varphi(y)$$

pour tous éléments x et y dans $\mathbf{Q}_\alpha$. Déterminer tous les éléments de A_α.

PARTIE II

On considère l'équation du troisième degré

$$x^3 - x^2 - 2x + 1 = 0 . \tag{2}$$

II.1) Montrer que toutes les racines de (2) sont réelles et appartiennent à l'intervalle $]-2; 2[$. Soit θ l'une de ces racines, montrer que θ n'est pas rationnel et que $2 - \theta^2$ est une autre racine de l'équation (2).

Dans la suite, on désigne par $\mathbf{Q}_\theta$ l'ensemble des réels $x = u + v\theta + w\theta^2$ où u, v, w sont trois rationnels arbitraires.

Montrer que $\mathbf{Q}_\theta$ est un sous-espace vectoriel de $\mathbf{R}$ considéré comme espace vectoriel sur le corps $\mathbf{Q}$ des rationnels. Quelle est la dimension de cet espace vectoriel ? Que peut-on dire de l'ensemble des trois racines de l'équation (2) ?

On admet que $\mathbf{Q}_\theta$ est un sous-corps du corps des réels.

II.2) On désigne par A_θ l'ensemble des automorphismes φ du corps $\mathbf{Q}_\theta$. Montrer que A_θ est un sous-groupe du groupe des automorphismes de l'espace vectoriel $\mathbf{Q}_\theta$.

Montrer que A_θ est un ensemble de trois éléments que l'on désignera par φ_0, φ_1, φ_2 et que l'on définira explicitement. Trouver les espaces propres de φ_1, φ_2.

(On pourra supposer que φ_0 désigne l'automorphisme identité de $\mathbf{Q}_\theta$ autrement dit l'élément unité de A_θ) .

II.3) On considère les trois applications de $\mathbf{Q}_\theta$ dans lui-même T_1, T_2, T_3 définies par

$$\begin{aligned} T_1(x) &= \varphi_0(x) + \varphi_1(x) + \varphi_2(x) \\ T_2(x) &= \varphi_0(x)\varphi_1(x) + \varphi_0(x)\varphi_2(x) + \varphi_1(x)\varphi_2(x) \\ T_3(x) &= \varphi_0(x)\varphi_1(x)\varphi_2(x)\ . \end{aligned}$$

a) Montrer que les images de ces trois applications T_1, T_2, T_3 sont incluses dans $\mathbf{Q}$.

De façon plus générale, soit un polynôme P, élément de $\mathbf{Q}[X_1, X_2, X_3]$, symétrique et homogène [a].

Montrer que l'application de $\mathbf{Q}_\theta$ dans $\mathbf{Q}_\theta$ définie par :

$$x \mapsto P\left(\varphi_0(x), \varphi_1(x), \varphi_2(x)\right)$$

est à valeurs dans $\mathbf{Q}$.

b) Montrer que l'application B définie par :

$$\forall (x, y) \in \mathbf{Q}_\theta \times \mathbf{Q}_\theta\ ,\ B(x, y) = T_1(xy)$$

est un produit scalaire.

Montrer que l'application T_2 est une forme quadratique sur l'espace $\mathbf{Q}_\theta$.

Cette forme quadratique est-elle non dégénérée positive ?

Question subsidiaire : démontrer que Q_θ est effectivement un corps.

a. i.e. $P(X_1, X_2, X_3) = P(X_{\sigma(1)}, X_{\sigma(2)}, X_{\sigma(3)})$ pour tout σ dans $\mathscr{S}_3$ et $\exists k \in \mathbf{N}$, $\forall \lambda \in \mathbf{Q}$, $P(\lambda X_1, \lambda X_2, \lambda X_3) = \lambda^k P(X_1, X_2, X_3)$.