5. Anneaux de polynômes / Anneaux euclidiens

Exercice 1

1. Soient $P = 2X^3 + 4X^2 + 3X + 2$ et $G = 3X^4 + 2X + 4$ dans $(\mathbb{Z}/5\mathbb{Z})[X]$. Calculer $P + G$ et PG.
2. Trouver toutes les racines dans $\mathbb{Z}/5\mathbb{Z}$ du polynôme $X^5 + 3X^3 + X^2 + 2X$.

Exercice 2 Montrer que le polynôme $X^{163} + 24X^{57} - 6$ a au moins une racine sur $\mathbb{R}$. A-t-il des racines dans $\mathbb{Q}$? Même exercice avec le polynôme $X^7 + 3X^2 + 2$.

Exercice 3 Quelles sont les racines de $X^5 - X$ dans $\mathbb{Z}/5\mathbb{Z}$? de X^2 dans $\mathbb{Z}/4\mathbb{Z}$? de $X^2 - X$ dans $\mathbb{Z}/6\mathbb{Z}$?

Exercice 4 Soit K un corps commutatif de caractéristique différente de 2 (c.à.d. telle que $2 \neq 0$). Soit $P = aX^2 + bX + c \in K[X]$ de degré 2.

Écrire sous forme canonique P (c.à.d. sous la forme $a(X - \alpha)^2 + \beta$ pour $\alpha, \beta \in K$). À quelle condition, le polynôme P est-il scindé sur K.

Exercice 5 Soit K un corps commutatif.

1. On considère un polynôme unitaire P de $K[X]$ de degré 2 et scindé sur K. Exprimer les coefficients de P en fonction de ses racines.
2. Même question avec un polynôme unitaire de degré 3.
3. Même question avec un polynôme unitaire de degré $n \geq 4$.

Exercice 6 Soit P un polynôme de $\mathbb{C}[X]$ et $\alpha \in \mathbb{C}$. Montrer que α est racine de P de multiplicité $n \geq 1$ si et seulement si $P(\alpha) = P'(\alpha) = \ldots = P^{(n-1)}(\alpha) = 0$ et $P^{(n)}(\alpha) \neq 0$.

Ce résultat est-il vrai pour tout corps commutatif K à la place de $\mathbb{C}$?

Exercice 7

1. Soit A un anneau intègre. Quels sont les éléments inversibles de $A[X]$?
2. Quels sont les éléments inversibles de $\mathbb{Z}[X]$?
3. Quels sont les éléments inversibles de $(\mathbb{Z}/7\mathbb{Z})[X]$?

Exercice 8 Soient A et B des anneaux et $\varphi : A \to B$ une application. On dit que φ est un morphisme d'anneaux si $\forall a, a' \in A,\ \varphi(aa') = \varphi(a)\varphi(a')$ et $\varphi(a + a') = \varphi(a) + \varphi(a')$, et $f(1_A) = 1_B$.

1. Montrer que pour tout $b \in A$, l'application $\varphi_b : A[X] \to A$ définie par

$$\varphi_b(a_0 + a_1X + \ldots + a_nX^n) = a_0 + a_1b + \ldots + a_nb^n$$

est un morphisme d'anneaux. C'est le morphisme **évaluation en** b**.**

2. Si $A = \mathbb{Z}/7\mathbb{Z}$ calculer $\varphi_2(X^2 + 3)$, $\varphi_3((X^4 + 2X)(X^3 - 3X^2 + 3))$, $\varphi_0(2X^3 - X^2 + 3X + 2)$.
3. On pose $A = \mathbb{Z}/5\mathbb{Z}$. Utiliser le petit théorème de Fermat pour calculer $\varphi_3(X^{231} + 3X^{117} - 2X^{53} + 1)$.

Exercice 9

1. Calculer le reste et le quotient de la division euclidienne de $X^6 + 3X^5 + 4X^2 - 3X + 2$ par $X^2 + 2X - 5$ dans $\mathbb{Z}/7\mathbb{Z}$.
2. Factoriser $X^4 + 4$ dans $\mathbb{Z}/5\mathbb{Z}$ en facteurs linéaires.

Exercice 10

1. Trouver un PGCD de $X^{10} - 3X^9 + 3X^8 - 11X^7 + 11X^6 + 19X^4 - 13X^3 + 8X^2 - 9X + 3$ et $X^6 - 3X^5 + 3X^4 - 9X^3 + 5X^2 - 5X + 2$ dans $\mathbb{Q}[X]$.
2. Trouver une relation de Bézout pour ces deux polynômes.

Exercice 11 Soient $m \geq 1$ et $n \geq 1$ deux entiers ; on pose $d = \mathrm{PGCD}(m, n)$.

1. Montrer qu'il existe u, v entiers positifs tels que $|um - vn| = d$.
   Dans la suite de l'exercice, on notera $\alpha = \max(um, vn)$ et $\beta = \min(um, vn)$. On fixe K un corps commutatif.
2. (a) Établir l'identité dans $K[X]$:
   $$(X^\alpha - 1) - (X^\beta - 1) = X^\beta(X^d - 1)$$
   .
   (b) Soient k et $l \geq 1$ deux entiers. Montrer que, si k divise l, alors $X^k - 1$ divise $X^l - 1$.
   (c) Soit $P \in K[X]$ divisant à la fois $X^m - 1$ et $X^n - 1$. Démontrer que P divise $X^d - 1$.
   (d) En déduire que $X^d - 1$ est le PGCD de $X^m - 1$ et $X^n - 1$.
3. Soient A, B deux polynômes de $K[X]$ et soit D leur PGCD.
   (a) Montrer que, pour tout polynôme unitaire $C \in K[X]$, CD est le PGCD de AC et de BC.
   (b) Soient p et $q \geq 1$ deux entiers. Déterminer le PGCD de $X^p + X^{p-1} + \cdots + X + 1$ et de $X^q + X^{q-1} + \cdots + X + 1$.

Exercice 12 On appelle ensemble des **entiers de Gauss** l'ensemble $\mathbb{Z}[i]$ des nombres complexes de la forme
$$\{a + ib,\ a, b \in \mathbb{Z}\}.$$

1. Montrer que $\mathbb{Z}[i]$ est un anneau intègre.
2. Si $\alpha = a + ib \in \mathbb{Z}[i]$ on pose $N(\alpha) = a^2 + b^2$. Montrer que l'application N permet de définir une division euclidienne sur $\mathbb{Z}[i]$. [Idée : pour α et $\beta \neq 0$ dans $\mathbb{Z}[i]$, $\frac{\alpha}{\beta} = r + si$ où $r, s \in \mathbb{Q}$. Choisisez q_1 et q_2 les entiers les plus proches de r et s et posez $q = q_1 + iq_2$.]
3. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?
4. Quel est le reste de la division euclidienne de $7 + 2i$ par $3 - 4i$?
5. Calculer un PGCD de $8 + 6i$ et $5 - 15i$.

Exercice 13 On pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$.

1. Montrer que l'application $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ définie par $N(a+b\sqrt{2}) = |a^2 - 2b^2|$ permet de définir une division euclidienne sur $\mathbb{Z}[\sqrt{2}]$.

2. Quels sont les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$?

Exercice 14 Quels sont les polynômes irréductibles de $\mathbb{C}[X]$? Quels sont les polynômes irréductibles de $\mathbb{R}[X]$?

Exercice 15
1. Décomposer le polynôme réel $P = X^3 + X^2 + X + 1$ en produit de facteurs irréductibles dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.
2. Soit n un entier non nul. Quelles sont les racines du polynôme $1 + X + \cdots + X^n$ sur $\mathbb{C}$?
3. Décomposer $X^6 + 1$ en un produit de facteurs du premier degré dans $\mathbb{C}[X]$. Que peut-on faire dans $\mathbb{R}[X]$? dans $\mathbb{Q}[X]$?

Exercice 16 Dire si les éléménts donnés sont irréductibles dans l'anneau indiqué :

1. 5 dans $\mathbb{Z}$
2. -17 dans $\mathbb{Z}$
3. 14 dans $\mathbb{Z}$
4. 2X-3 dans $\mathbb{Z}[X]$
5. 2X-10 dans $\mathbb{Z}[X]$
6. 2X-3 dans $\mathbb{Q}[X]$
7. 2X-10 dans $\mathbb{Q}[X]$
8. 2X-10 dans $\mathbb{Z}/11\mathbb{Z}[X]$

Exercice 17 Factoriser $4X^2-4X+8$ en produit d'irréductibles en le considérant comme un élément de $\mathbb{Z}[X]$, $\mathbb{Q}[X]$ et $\mathbb{Z}/11\mathbb{Z}[X]$.

Exercice 18 Notons

$$\mathbb{Q}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

1. Vérifier que $\mathbb{Q}[i]$ est un sous-corps de $\mathbb{C}$.
2. Montrer que $X^2 + (2 - i)X - i$ est irréductible dans $\mathbb{Q}[i]$.

Exercice 19 Pour un polynôme P non nul de $\mathbb{Z}[X]$, on appelle contenu de P, noté $c(P)$, le PGCD de ses coefficients. On dit que P est primitif si $c(P) = 1$.

1. Montrer que le produit de deux polynômes primitifs est primitif.
2. Soient P, Q deux polynômes de $\mathbb{Z}[X]$. Montrer que $c(PQ) = c(P)c(Q)$.
3. Soit P un polynôme primitif non constant de $\mathbb{Z}[X]$. Montrer que P est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il est irréductible dans $\mathbb{Q}[X]$.

Exercice 20
1. Déterminer les polynômes irréductibles de degré au plus 3 dans $\mathbb{Z}/2\mathbb{Z}[X]$.
2. Déterminer les polynômes irréductibles de degré 4 dans $\mathbb{Z}/2\mathbb{Z}[X]$.
3. Soit a, b, c, d des entiers. Montrer que le polynôme $X^4 + 2aX^3 + 2bX^2 + (2c + 1)X + (2d + 1)$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 21 Déterminer si les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$:

$$4X^3 - 3X - \frac{1}{2} \; ; \quad X^6 - 3X^3 + 12X - 3 \; ; \quad X^n - 2 \text{ avec } n \geq 1.$$

Exercice 22 Montrer que pour p un nombre premier, le polynôme

$$P = X^{p-1} + X^{p-2} + ... + X + 1$$

Indication : on considérera le polynôme $Q = (X+1)^{p-1} + (X+1)^{p-2} + ... + (X+1) + 1$.

Exercice 23 Soit $P = X^6 + 22X^5 + 6X^4 + 12X^3 + 52X^2 - 14X - 30$ dans $\mathbb{Z}[X]$. Pour tout nombre premier p, on notera P_p le réduit modulo p de P dans $\mathbb{Z}/p\mathbb{Z}[X]$.

1. Montrer que P est irréductible dans $\mathbb{Q}[X]$.
2. Décomposer en facteurs irréductibles P_2 dans $\mathbb{Z}/2\mathbb{Z}[X]$.
3. Décomposer en facteurs irréductibles P_3 dans $\mathbb{Z}/3\mathbb{Z}[X]$.
4. Décomposer en facteurs irréductibles P_5 dans $\mathbb{Z}/5\mathbb{Z}[X]$.

Exercice 24 On dit qu'un nombre complexe (ou réel) est *algébrique* s'il est racine d'un polynôme non nul à coefficients rationnels.

Soit $\alpha \in \mathbb{C}$ un nombre algébrique et soit $I := \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\}$.

1. Montrer I est un sous-groupe de $(\mathbb{Q}[X], +)$.
2. Montrer que pour tout $P \in I$ et tout $Q \in \mathbb{Q}[X]$, on a $QP \in I$.
   On dit qu'une partie d'un anneau vérifiant les propriétés (1) et (2) est un idéal.
3. Montrer qu'il existe un unique polynôme unitaire P_α qui engendre I
   (c.à.d. tel que $I = \{QP_\alpha \in \mathbb{Q}[X] \mid Q \in \mathbb{Q}[X]\}$).
4. Montrer que P_α est l'unique polynôme irréductible unitaire de $\mathbb{Q}[X]$ qui annule α.
5. Soit $d = \deg P_\alpha$. On considère $\mathbb{Q}[\alpha] = \{P(\alpha) \in \mathbb{C} \mid P \in \mathbb{Q}[X]\}$. Montrer que

$$\mathbb{Q}[\alpha] = \{\lambda_0 + \lambda_1\alpha + \ldots + \lambda_{d-1}\alpha^{d-1} \in \mathbb{C} \mid \lambda_0, \ldots, \lambda_{d-1} \in \mathbb{Q}\}.$$

6. Montrer que $\mathbb{Q}[\alpha]$ est un sous-corps de $\mathbb{C}$.
7. Montrer que $\mathbb{Q}[\alpha]$ est un espace vectoriel sur $\mathbb{Q}$ de dimension d.
8. Supposons que $d = 2$ et $\alpha \in \mathbb{R}$. Montrer qu'il existe alors un rationnel positif a tel que $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{a}]$.