Mathématiques spéciales

Feuille d'exercices n°7

1. Anneaux $\mathbb{Z}/n\mathbb{Z}$

Exercice 1.

1. Est-ce que $\overline{18}$ est inversible dans $\mathbb{Z}/49\mathbb{Z}$? Si oui, quel est son inverse ?
2. Est-ce que $\overline{42}$ est inversible dans $\mathbb{Z}/135\mathbb{Z}$? Si oui, quel est son inverse ?

Exercice 2.

Résoudre, dans $\mathbb{Z}/37\mathbb{Z}$, les équations ou systèmes d'équations suivants :

1. $\bar{7}y = \bar{2}$.
2. $\begin{cases} \bar{3}x + \bar{7}y &= \bar{3} \\ \bar{6}x - \bar{7}y &= \bar{0} \end{cases}$

Exercice 3.

Déterminer les inversibles de $\mathbb{Z}/8\mathbb{Z}$. Le groupe des inversibles $(\mathbb{Z}/8\mathbb{Z})^*$ est-il cyclique ?

Exercice 4.

Résoudre

1. $x^2 + x + \overline{7} = \overline{0}$ dans $\mathbb{Z}/13\mathbb{Z}$.
2. $x^2 - \overline{4}x + \overline{3} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 5.

Les groupes $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ et $(\mathbb{Z}/2\mathbb{Z})^3$ sont-ils isomorphes ?

Exercice 6.

1. Soient n, m, a trois entiers tels que $n \wedge m = 1$. Montrer que l'équation $nx \equiv a\ [m]$ admet une unique solution modulo m.
2. Soient n, m, a, b quatre entiers avec $n \wedge m = 1$. Montrer que le système

$$\begin{cases} x &\equiv a\ [n] \\ x &\equiv b\ [m]. \end{cases}$$

admet une unique solution modulo nm.

3. Un phare émet un signal jaune toutes les 15 secondes et un signal rouge toutes les 28 secondes. On aperçoit le signal jaune 2 secondes après minuit et le rouge 8 secondes après minuit. A quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?
4. Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors trois pièces. Mais les pirates se querellent et six d'entre eux sont tués. Le cuisinier recevrait alors quatre pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés et le partage laisserait cinq pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Exercice 7.

1. Donner la liste des éléments de $\mathbb{Z}/7\mathbb{Z}$ qui sont des carrés. Combien y en a-t-il ?
2. Soit a un élément $\mathbb{Z}/7\mathbb{Z}$. Quel est le cardinal de l'ensemble $\{-x^2 + a : x \in \mathbb{Z}/7\mathbb{Z}\}$?
3. En déduire que, pour un a donné dans $\mathbb{Z}/7\mathbb{Z}$, l'équation $x^2+y^2 = a$ a toujours une solution, où x, y sont dans $\mathbb{Z}/7\mathbb{Z}$.
4. Donner une solution explicite de l'équation $u^2 + v^2 \equiv -1 \pmod 7$, avec $u, v \in \mathbb{Z}$.

Exercice 8.

Soit $n \geq 3$ un entier.

1. Soit a un entier impair. Montrer que $a^{2^{n-2}} \equiv 1\ [2^n]$.
2. Le groupe $\left(\mathbb{Z}/(2^n\mathbb{Z})\right)^*$ est-il cyclique ?

Exercice 9.

Le but de cet exercice est de montrer qu'il n'existe pas d'entier $n \geq 2$ tel que n divise $2^n - 1$. On raisonne par l'absurde et on supposons qu'un tel entier n existe. On note p le plus petit diviseur premier de n.

1. Montrer que $p > 2$.
2. On note m l'ordre de la classe de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$.
   (a) Montrer que $m|p - 1$.
   (b) Montrer que $m|n$.
   (c) Conclure.

2. Arithmétique des polynômes

a. Exercices basiques

Exercice 10.

Résoudre les équations suivantes, où l'inconnue est un polynôme P de $\mathbb{R}[X]$:

1. $P(X^2) = (X^2+1)P(X)$ **2**. $P'^2 = 4P$
3. $P \circ P = P$.

Exercice 11.

Calculer le quotient et le reste de la division euclidienne de

1. $X^4 + 5X^3 + 12X^2 + 19X - 7$ par $X^2 + 3X - 1$;
2. $X^4 - 4X^3 - 9X^2 + 27X + 38$ par $X^2 - X - 7$;
3. $X^5 - X^2 + 2$ par $X^2 + 1$.

Exercice 12.

Soit $P \in \mathbb{K}[X]$, soit $a \in \mathbb{K}$ et soit R le reste de la division euclidienne de P par $(X-a)^2$. Exprimer R en fonction de $P(a)$ et de $P'(a)$.

Exercice 13.

Soit $P \in \mathbb{R}[X]$, $a, b \in \mathbb{R}$, $a \neq b$. Sachant que le reste de la division euclidienne de P par $(X-a)$ vaut 1 et que le reste de la division euclidienne de P par $X-b$ vaut -1, que vaut le reste de la division euclidienne de P par $(X-a)(X-b)$?

Exercice 14.

Donner une condition nécessaire et suffisante sur $(\lambda, \mu) \in \mathbb{C}^2$ pour que X^2+2 divise $X^4 + X^3 + \lambda X^2 + \mu X + 2$.

Exercice 15.

Déterminer les pgcd suivants :

1. $P(X) = X^4 - 3X^3 + X^2 + 4$ et $Q(X) = X^3 - 3X^2 + 3X - 2$;
2. $P(X) = X^5 - X^4 + 2X^3 - 2X^2 + 2X - 1$ et $Q(X) = X^5 - X^4 + 2X^2 - 2X + 1$;
3. $P(X) = X^n - 1$ et $Q(X) = (X-1)^n$, $n \geq 1$.

Exercice 16.

Trouver deux polynômes U et V de $\mathbb{R}[X]$ tels que $AU + BV = 1$, où $A(X) = X^7 - X - 1$ et $B(X) = X^5 - 1$.

Exercice 17.

Soient P et Q des polynômes de $\mathbb{C}[X]$ non constants. Montrer que P et Q ont un facteur commun si, et seulement si, il existe $A, B \in \mathbb{C}[X]$, $A \neq 0$, $B \neq 0$, tels que $AP = BQ$ et $\deg(A) < \deg(Q)$, $\deg(B) < \deg(P)$.

Exercice 18.

Décomposer le polynôme suivant en produit d'irréductibles de $\mathbb{R}[X]$:

$$P(X) = 2X^4 + X^2 - 3.$$

Exercice 19.

Soit P le polynôme $X^4 - 6X^3 + 9X^2 + 9$.

1. Décomposer $X^4 - 6X^3 + 9X^2$ en produit de facteurs irréductibles dans $\mathbb{R}[X]$.
2. En déduire une décomposition de P en produit de facteurs irréductibles dans $\mathbb{C}[X]$, puis dans $\mathbb{R}[X]$.

Exercice 20.

Démontrer que

1. $X^{n+1}\cos\big((n-1)\theta\big) - X^n\cos(n\theta) - X\cos\theta + 1$ est divisible par $X^2 - 2X\cos\theta + 1$;
2. $nX^{n+1} - (n+1)X^n + 1$ est divisible par $(X-1)^2$.

Exercice 21.

Soient $A, B, P \in \mathbb{K}[X]$ avec P non-constant. On suppose que $A \circ P | B \circ P$. Démontrer que $A|B$.

Exercice 22.

Le but de cet exercice est de déterminer

$$E = \{P \in \mathbb{R}[X];\ P(X^2) = (X^3+1)P(X)\}.$$

1. Démontrer que le polynôme nul ainsi que le polynôme $X^3 - 1$ sont solutions du problème.
2. Analyse du problème. Soit $P \in E$ non nul.
   (a) Montrer que P est de degré 3.
   (b) Démontrer que $P(1) = 0$, puis que $P'(0) = P''(0) = 0$ (on pourra penser à dériver la relation $P(X^2) = (X^3+1)P(X)$).
   (c) En effectuant la division euclidienne de P par $X^3 - 1$, démontrer qu'il existe $\lambda \in \mathbb{R}$ tel que $P(X) = \lambda(X^3 - 1)$.
3. Synthèse du problème : en déduire l'ensemble E.

Exercice 23.

Déterminer tous les polynômes $P \in \mathbb{R}[X]$ vérifiant $P(0) = 0$ et $P(X^2+1) = \big(P(X)\big)^2 + 1$

Exercice 24.

1. Rappeler la décomposition en produits d'irréductibles de $X^n - 1$.
2. En déduire la décomposition en produits d'irréductibles de $1 + X + \cdots + X^{n-1}$.
3. Calculer $\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right)$.
4. Pour $\theta \in \mathbb{R}$, calculer $\prod_{k=0}^{n-1} \sin\left(\frac{k\pi}{n} + \theta\right)$.

Exercice 25.

On dit qu'un polynôme $P \in \mathbb{C}[X]$ de degré n est réciproque s'il s'écrit $P = a_n X^n + \cdots + a_0$ avec $a_k = a_{n-k}$ pour tout k dans $\{0, \ldots, n\}$.

1. Soit $P \in \mathbb{C}[X]$ de degré n. Démontrer que P est réciproque si et seulement si $P(X) = X^n P\left(\frac{1}{X}\right)$.
2. Montrer qu'un produit de polynômes réciproques est réciproque.
3. On suppose que P et Q sont réciproques et que $Q|P$. Démontrer que $\frac{P}{Q}$ est réciproque.
4. Soit $P \in \mathbb{C}[X]$ un polynôme réciproque.
   (a) Démontrer que si α est une racine de P, alors $\alpha \neq 0$ et α^{-1} est une racine de P.
   (b) Démontrer que si 1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
   (c) Démontrer que si le degré de P est impair, alors -1 est racine de P.
   (d) Démontrer que si P est de degré pair et si -1 est une racine de P, alors sa multiplicité est supérieure ou égale à 2.
5. Démontrer que tout polynôme réciproque de $\mathbb{C}[X]$ de degré $2n$ se factorise en
$$P = a_{2n}(X^2 + b_1 X + 1)\ldots(X^2 + b_n X + 1).$$
Que peut-on dire si le degré de P est impair ?

b. Exercices d'approfondissement

Exercice 26.

Déterminer les polynômes P de degré supérieur ou égal à 1 et tels que $P'|P$.

Exercice 27.

Déterminer les couples (A, B) de polynômes non nuls de $\mathbb{R}[X]$ tels que le quotient et le reste dans la division euclidienne de A par B et dans la division euclidienne de B par A soient identiques.

Exercice 28.

Soient n, p deux entiers naturels non nuls et soit $P(X) = \sum_{k=0}^{n} a_k X^k$ un polynôme de $\mathbb{C}[X]$. Pour chaque $k \in \{0, \dots, n\}$, on note r_k le reste de la division euclidienne de k par p. Démontrer que le reste de la division euclidienne de P par $X^p - 1$ est le polynôme $R(X) = \sum_{k=0}^{n} a_k X^{r_k}$.

Exercice 29.

1. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{C}) \subset \mathbb{R}$.
2. Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $P(\mathbb{R}) \subset \mathbb{R}$.
3. Soit $P \in \mathbb{C}[X]$. Démontrer que $P(\mathbb{Q}) \subset \mathbb{Q}$ si et seulement si $P \in \mathbb{Q}[X]$.

Exercice 30.

On note

$$\mathcal{S} = \{P \in \mathbb{R}[X];\ \exists P_1, P_2 \in \mathbb{R}[X];\ P = P_1^2 + P_2^2\}.$$

1. Montrer que $\mathcal{S}$ est stable par produit. On pourra considérer l'application $\phi : \mathbb{C}[X] \to \mathbb{R}[X]$, $P \mapsto P\bar{P}$.
2. Soit $P \in \mathbb{R}[X]$ tel que $P(x) \geq 0$ pour tout $x \in \mathbb{R}$. Montrer qu'il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Exercice 31.

Si $P \in \mathbb{Z}[X]$, on appelle contenu de P, et on note $c(P)$, le pgcd des coefficients de P.

1. Soit $P, Q \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que p divise tous les coefficients de PQ. Montrer que p divise tous les coefficients de P ou tous les coefficients de Q.
2. Soit $P, Q \in \mathbb{Z}[X]$ et $R(X) = \frac{PQ}{c(P)c(Q)} \in \mathbb{Z}[X]$. Démontrer que $c(R) = 1$. En déduire que l'on a $c(PQ) = c(P)c(Q)$.
3. Soit Q un polynôme de $\mathbb{Z}[X]$. On suppose que Q n'est pas irréductible dans $\mathbb{Q}[X]$. Démontrer qu'il existe deux polynômes A et B de $\mathbb{Z}[X]$ tels que $Q = AB$, avec $\deg(A) < \deg(Q)$ et $\deg(B) < \deg(Q)$.
4. Soit $A(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. On suppose qu'il existe un nombre premier p tel que
$$p | a_k,\ \text{pour tout } 0 \leq k \leq n-1,\ p \not| a_n,\ p^2 \not| a_0.$$
Démontrer que A est irréductible dans $\mathbb{Q}[X]$.
5. Démontrer qu'il existe dans $\mathbb{Q}[X]$ des polynômes irréductibles de tout degré $n \geq 1$.