Examen Partiel

Mercredi 13 mars 2024 - Durée 1h30
Corrigé

Exercice 1.1. — Soit $E = \{P \in \mathbf{Q}[X] \mid P(\mathbf{Z}) \subset \mathbf{Z}\}$.

1. Soit $n \in \mathbf{Z}$. On note $E_n = \{P \in \mathbf{Q}[X] \mid P(n) \in \mathbf{Z}\}$.
   (a) Montrer que E_n est un sous-anneau de $\mathbf{Q}[X]$.
   (b) En déduire que E est un anneau contenant $\mathbf{Z}[X]$.
2. (a) Montrer que E est un anneau intègre.
   (b) Quels sont les éléments inversibles de E ?
3. Soit p un nombre premier. Montrer que $\dfrac{1}{p}(X^p - X) \in E$.

Solution 1.1. —

1. (a) Soit $\Phi_n : \mathbf{Q}[X] \to \mathbf{Q}$, définie par $\Phi_n(P) = P(n)$. Φ_n est un morphisme d'anneau (c'est le morphisme d'évaluation). Ainsi $E_n = \Phi_n^{-1}(\mathbf{Z})$ est l'image réciproque du sous-anneau $\mathbf{Z}$ de $\mathbf{Q}$. C'est un sous-anneau de $\mathbf{Q}[X]$.
   (b) $E = \bigcap_{n \in \mathbf{Z}} E_n$ est un sous-anneau de $\mathbf{Q}[X]$. Manifestement il contient $\mathbf{Z}[X]$.
2. (a) E est un sous-anneau de $\mathbf{Q}[X]$ intègre, donc est intègre.
   (b) Si P est inversible dans E alors P est inversible dans $\mathbf{Q}[X]$, donc $\deg P = 0$ et $P = \lambda \in \mathbf{Q}^*$. Mais $P(0) = \lambda$ doit appartenir à $\mathbf{Z}$. L'inverse de P dans E est également une constante $\mu \in \mathbf{Z}$ et on doit avoir $\lambda\mu = 1$. Donc $E^* = \{\pm 1\}$.
3. D'après le théorème de Fermat, on a pour tout entier $n \in \mathbf{Z}$, $n^p \equiv n \pmod p$, ainsi p divise $n^p - n$ et $\dfrac{1}{p}(n^p - n) \in \mathbf{Z}$. Ainsi $\dfrac{1}{p}(X^p - X) \in E_n$ pour tout $n \in \mathbf{Z}$.

Exercice 1.2. — Soit $n = 2024$.

1. (a) Rappeler pourquoi $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/23\mathbf{Z}$.
   (b) Quel est le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$?
2. On considère l'application S de $(\mathbf{Z}/n\mathbf{Z})^*$ vers $(\mathbf{Z}/n\mathbf{Z})^*$ définie par $S(x) = x^2$.
   (a) Montrer que S définit un morphisme de groupe.
   (b) Montrer que $|\ker S| = 16$.
3. (a) Montrer que $5^8 \equiv 2017 \pmod n$. *Indication : on pourra montrer que* $5^8 \equiv -7 \pmod n$.
   (b) En déduire une solution de l'équation $x^2 = \overline{2017}$ dans $\mathbf{Z}/n\mathbf{Z}$.
   (c) Quel est le nombre de solutions de l'équation $x^2 = \overline{2017}$ dans $\mathbf{Z}/n\mathbf{Z}$?

Solution 1.2. —

1. (a) On a $2024 = 2025 - 1 = 45^2 - 1 = 44 \cdot 46 = 8 \cdot 11 \cdot 23$. D'après le théorème chinois, l'anneau $\mathbf{Z}/n\mathbf{Z}$ est isomorphe à l'anneau $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/23\mathbf{Z}$.
   (b) On $|(\mathbf{Z}/n\mathbf{Z})^*| = \varphi(n) = \varphi(8)\varphi(11)\varphi(23) = 4 \times 10 \times 22 = 16 \times 5 \times 11 = 880$
2. (a) On a bien $S(1) = 1$ et $S(xy^{-1}) = S(x)S(y^{-1})$ car $(\mathbf{Z}/n\mathbf{Z})^*$ est un groupe commutatif.
   (b) $S(x) = 1$ si et seulement si $x^2 \equiv 1 \pmod{n}$, c'est-à-dire, $\begin{cases} x^2 \equiv 1 \pmod{8}, \\ x^2 \equiv 1 \pmod{11}, \\ x^2 \equiv 1 \pmod{23} \end{cases}$
   Tous les éléments de $(\mathbf{Z}/8\mathbf{Z})^*$ vérifient $x^2 = 1$. Il y en a 4. Les solutions de $x^2 = 1$ dans $\mathbf{Z}/p\mathbf{Z}$ sont ± 1.
   L'équation $x^2 = 1$ a donc $4 \times 2 \times 2 = 16$ solutions dans $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/23\mathbf{Z}$.
   Ainsi $|\ker S| = 16$.
3. (a) Calculons $5^8 \pmod 8$. On obtient $5^2 = 1$ donc $5^8 = 1$.
   Calculons $5^8 \pmod{11}$. On obtient $5^2 = 3$, $5^4 = 3^2 = -2$ et $5^8 = 4 \pmod{11}$.
   Calculons $5^8 \pmod{23}$. On obtient $5^2 = 2$, $5^4 = 2^2 = 4$ et $5^8 = 16 = -7 \pmod{23}$.
   Ainsi $5^8 + 7$ est divisible par 8, 11 et 23 donc par n.
   On obtient $5^8 \equiv -7 \equiv 2017 \pmod{n}$.
   (b) On déduit que $5^4 = 625$ est solution de $x^2 \equiv 2017 \pmod{n}$.
   (c) Il y a 16 solutions : ce sont les 625ε où $\varepsilon \in \ker S$.

Exercice 1.3. —
On note $\mathcal{P}$ l'ensemble des nombres premiers p congrus à 1 modulo 8. Le but de cet exercice est de montrer que $\mathcal{P}$ est infini (cas particulier du théorème de la progression arithmétique de Dirichlet).

1. Donner la liste des 3 plus petits éléments de $\mathcal{P}$.
2. Soit p un nombre premier impair et a un entier tel que p divise $a^4 + 1$. On note $\overline{a}$ la classe de a modulo p.
   (a) Montrer que $\overline{a} \in (\mathbf{Z}/p\mathbf{Z})^*$. Quel est l'inverse de $\overline{a}$?
   (b) Montrer que $\overline{a}$ est d'ordre 8.
   (c) En déduire que $p \in \mathcal{P}$.
3. On suppose que $\mathcal{P}$ est fini et on note $a = \prod_{p \in \mathcal{P}} p$. Soit p_0 un diviseur premier de $1 + 16a^4$.
   (a) Montrer que 8 divise $p_0 - 1$.
   (b) En déduire que p_0 divise a.
   (c) En déduire que p_0 divise 1.
4. En déduire que l'ensemble $\mathcal{P}$ est infini.

Solution 1.3. —

1. On trouve $p = 17, 41, 73$.
2. (a) On a $\overline{a} \cdot (-\overline{a})^3 = 1$, donc $\overline{a}$ est inversible d'inverse $(-\overline{a})^3$.
   (b) On a $(\overline{a})^4 = -1$ donc $(\overline{a})^8 = 1$. L'ordre de $\overline{a}$ divise 8 mais ne divise par 4.
   (c) L'ordre de a divise l'ordre de $(\mathbf{Z}/p\mathbf{Z})^*$ (th. de Lagrange). Donc 8 divise $p - 1$.
3. (a) D'après la question précédente, puisque p_0 divise $1 + (2a)^4$.
   (b) $p_0 \in \mathcal{P}$ donc p_0 divise a.
   (c) p_0 divise a^4 et $1 + 16a^4$ donc leur différence. p_0 divise 1.
4. Si $\mathcal{P}$ était fini alors a serait égal à 1 (pas de diviseur premier). Mais $a > 17 \cdot 41$. Donc $\mathcal{P}$ est infini.