2023-2024
L2 Licence de mathématiques
Structures Algébriques

Examen - Session 1 - 16 mai 2024

Durée : 2h00. Aucun document ni calculatrice autorisé

Toute réponse non justifiée est considérée comme zéro

<u>Exercice 1 :</u> On note $P(X) = -X^3 + 1$ et $Q(X) = X^2 + X$.

a. Calculer le polynôme $P \circ Q(X)$. Quel est son degré ?

b. Montrer que 1 est une racine de P.
En déduire une factorisation de P comme un polynôme de $\mathbb{R}[X]$.

c. Montrer que P et Q sont premier entre eux.

Solution :

a. Utilisant la formule $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$ on obtient

$$\begin{aligned} P \circ Q(X) = P(Q(X)) = & \; -(X^2 + X)^3 + 1 \\ = & \; -((X^2)^3 + 3 \times (X^2)^2 \times X + 3 \times X^2 \times X + X^3) + 1 \\ = & \; -X^6 - 3X^5 - 3X^4 - X^3 + 1 \end{aligned}$$

Donc le degré de $P \circ Q$ est 6.

b. Si $P(1) = 0$ alors 1 est une racine de P. On calcule : $P(1) = -(1)^3 + 1 = -1 + 1 = 0$. Donc 1 est une racine de P. Cela implique que le polynôme $X - 1$ divise P. D'après une division euclidienne de P par $X - 1$ on a $\boxed{P(X) = (X-1)(-X^2 - X - 1)}$.

c. Le polynôme $-X^2 - X - 1$ est un polynôme de degré 2. Il est irréductible car son discriminant est $(-1)^2 - 4 \times (-1) \times (-1) = -3$ est négatif. . On peut alors dire que la factorisation

$P(X) = (X-1)(-X^2 - X - 1)$ est une décomposition de P comme produit des polynômes irréductibles de $\mathbb{R}[X]$.

De même $\boxed{Q(X) = X(X+1)}$ est une décomposition de Q comme produit des polynômes irréductibles.
Donc $\boxed{P \text{ et } Q \text{ n'ayant aucun facteur irréductible en commun sont premiers entre eux}}$.

<u>Exercice 2 :</u>

a. Soient a, b, c des entiers non nuls tels que $a \wedge b = 1$ et $a \wedge c = 1$. Montrer que $a \wedge bc = 1$.

D'après le théorème de Bézout

1) il existe $(u_1, v_1) \in \mathbb{Z}^2$ tel que $au_1 + bv_1 = 1$.

2) et il existe $(u_2, v_2) \in \mathbb{Z}^2$ tel que $au_2 + cv_2 = 1$.

Donc

$$\begin{aligned} (au_1 + bv_1) \times (au_2 + cv_2) \; &= 1 \times 1 \\ \text{on obtient alors} \quad a(au_1u_2 + cu_1v_2 + bv_1u_2) + bc(v_1v_2) \; &= 1 \end{aligned}$$

Utilisant le théorème de Bézout encore une fois on peut conclure que a et bc sont premiers entre eux.

b. (Ordre d'un entier modulo a) Soient $a, b \geq 2$ deux entiers. Montrer l'équivalence suivante :

$$\exists k > 0 \text{ tel que } b^k \equiv 1 \pmod{a} \iff a \wedge b = 1 \tag{1}$$

indication : pour $\Leftarrow$ penser à l'ordre de $\bar{b}$ dans un groupe bien choisi.

$\Rightarrow$ Supposons qu'il existe $k > 0$ tel que $b^k \equiv 1$ modulo a. Autrement dit a divise $b^k - 1$. C'est-à-dire il existe un entier $l \in \mathbb{Z}$ tel que $b^k - 1 = al$ ou $\boxed{b \times b^{k-1} - a \times l = 1}$. D'après le théorème de Bézout on peut conclure que a et b sont premiers entre eux.

$\Leftarrow$ On considère le groupe multiplicatif

$$(\mathbb{Z}/a\mathbb{Z})^* = \{\bar{m} \in \mathbb{Z}/a\mathbb{Z} \mid \ m \wedge a = 1\}.$$

Puisque $(\mathbb{Z}/a\mathbb{Z})^*$ est de cardinal fini, tout élément de ce groupe est d'ordre fini. Puisque $a \wedge b = 1$, on a $\bar{b} \in (\mathbb{Z}/a\mathbb{Z})^*$ Notons k l'ordre de $\bar{b}$. En particulier

$$\overline{b^k} = (\bar{b})^k = \bar{1} \ \text{ dans } (\mathbb{Z}/a\mathbb{Z})^*$$

Autrement dit $b^k \equiv 1$ modulo a.

c. On veut montrer que si un entier n est premier avec 10, alors il existe un multiple de n qui s'écrit $11 \cdots 1$.

i. Montrer que $9n$ est premier avec 10. En déduire qu'il existe un entier positif k tel que $10^k \equiv 1$ (mod $9n$).

Nous avons $10 \wedge 9 = 1$ et $10 \wedge n = 1$. On déduit de question a. que $10 \wedge 9n = 1$. Utilisant question b., voir équation (1), on sait qu'il existe un entier naturel k tel que $10^k \equiv 1$ modulo $9n$.

ii. Montrer que 9 divise $10^k - 1$. Quel est la valeur du quotient ?

On peut remarquer que

$$10^k - 1 = \underbrace{99 \cdots 9}_{k \text{ fois}} = 9 \times \underbrace{11 \cdots 1}_{k \text{ fois}} \tag{2}$$

Donc $\boxed{\text{le quotient de } 10^k - 1 \text{ divisé par 9 est } \underbrace{11 \cdots 1}_{k \text{ fois}}.}$

iii. Conclure.

Nous savons que $10^k \equiv 1$ modulo $9n$. Autrement dit il existe $l \in \mathbb{Z}$ tel que $10^k - 1 = 9nl$. Or utilisant l'équation (2) on obtient

$$\begin{aligned} 10^k - 1 = 9nl &\iff 9 \times \underbrace{11 \cdots 1}_{k \text{ fois}} = 9nl \\ &\iff \underbrace{11 \cdots 1}_{k \text{ fois}} = nl \end{aligned}$$

Autrement un multiple de n s'écrit $11 \cdots 1$.

<u>**Exercice 3 :**</u> **Soit le groupe $G = (\mathbb{Z}/30\mathbb{Z}, +)$.**

a. Quel est l'ordre de l'élément $\bar{9}$?

Nous savons que $\bar{9} = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{9 \text{ fois}}$ et que $o(\bar{1}) = 10$.

Or pour tout élément g d'un groupe $o(g^k) = \dfrac{o(g)}{o(g) \wedge k}$. Donc $\boxed{o(\bar{9}) = \dfrac{o(\bar{1})}{o(\bar{1}) \wedge 9} = \dfrac{30}{30 \wedge 9} = 10}$.

b. Déterminer les éléments $\bar{k} \in G$ tels que $G = \langle \bar{k} \rangle$.

$G = \langle \bar{k} \rangle$ si et seulement si $o(\bar{k}) = 30$. Or, puisque $\bar{k} = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{k \text{ fois}}$, on a

$$o(\bar{k}) = \frac{o(\bar{1})}{o(\bar{1}) \wedge k} = \frac{30}{30 \wedge k}$$

Donc nous cherchons les entiers naturel $k \in [\![1, 30]\!]$ tels que $k \wedge 30 = 1$. Ils sont $\{1, 7, 11, 13, 17, 19, 23, 29\}$.

c. Déterminer le plus petit sous-groupe H de G qui contient $\bar{6}$ et $\bar{8}$.

Nous voulons montrer que $H = \langle \bar{2} \rangle$.

- $\subset$: Puisque $\bar{6} = \bar{2} + \bar{2} + \bar{2}$ alors alors $\bar{6} \in \langle \bar{2} \rangle$. De même puisque 8 $\bar{8} = \bar{2} + \bar{2} + \bar{2} + \bar{2}$, alors $\bar{6} \in \langle \bar{2} \rangle$. Donc $H \subset \langle \bar{2} \rangle$.
- $\supset$: Puisque $\bar{2} = \bar{8} - \bar{6}$, tout élément de $\bar{2}$ est un élément de H car H est un sous-groupe.

<u>**Exercice 4 :**</u> **Soit $\sigma : \{1, 2, \ldots, 11, 12\} \longrightarrow \{1, 2, \ldots, 11, 12\}$ la permutation :**

$$\sigma = (1 \;\; 2 \;\; 5 \;\; 7)(3 \;\; 1 \;\; 12 \;\; 5 \;\; 6)(2 \;\; 6 \;\; 11 \;\; 10 \;\; 9 \;\; 8)(11 \;\; 12)(5 \;\; 7 \;\; 2 \;\; 12 \;\; 3)$$

a. Donnez l'image par σ de chacun des entiers de 1 à 12.

Notons

$$\alpha = (1 \;\; 2 \;\; 5 \;\; 7) \;,\; \beta = (3 \;\; 1 \;\; 12 \;\; 5 \;\; 6) \;,\; \tau = (2 \;\; 6 \;\; 11 \;\; 10 \;\; 9 \;\; 8)$$

$$\gamma = (11 \;\; 12) \;,\; \delta = (5 \;\; 7 \;\; 2 \;\; 12 \;\; 3)$$

$\sigma(1) = \alpha(\beta(\tau(\gamma(\delta(1))))) = \alpha(\beta(\tau(\gamma(1)))) = \alpha(\beta(\tau(1))) = \alpha(\beta(1)) = \alpha(12) = 12.$
$\sigma(2) = \alpha(\beta(\tau(\gamma(\delta(2))))) = \alpha(\beta(\tau(\gamma(12)))) = \alpha(\beta(\tau(11))) = \alpha(\beta(10)) = \alpha(10) = 10.$
$\sigma(3) = \alpha(\beta(\tau(\gamma(\delta(3))))) = \alpha(\beta(\tau(\gamma(5)))) = \alpha(\beta(\tau(5))) = \alpha(\beta(5)) = \alpha(6) = 6.$
$\sigma(4) = \alpha(\beta(\tau(\gamma(\delta(4))))) = \alpha(\beta(\tau(\gamma(4)))) = \alpha(\beta(\tau(4))) = \alpha(\beta(4)) = \alpha(4) = 4.$
$\sigma(5) = \alpha(\beta(\tau(\gamma(\delta(5))))) = \alpha(\beta(\tau(\gamma(7)))) = \alpha(\beta(\tau(7))) = \alpha(\beta(7)) = \alpha(7) = 1.$
$\sigma(6) = \alpha(\beta(\tau(\gamma(\delta(6))))) = \alpha(\beta(\tau(\gamma(6)))) = \alpha(\beta(\tau(6))) = \alpha(\beta(11)) = \alpha(11) = 11.$
$\sigma(7) = \alpha(\beta(\tau(\gamma(\delta(7))))) = \alpha(\beta(\tau(\gamma(2)))) = \alpha(\beta(\tau(2))) = \alpha(\beta(6)) = \alpha(3) = 3.$
$\sigma(8) = \alpha(\beta(\tau(\gamma(\delta(8))))) = \alpha(\beta(\tau(\gamma(8)))) = \alpha(\beta(\tau(8))) = \alpha(\beta(2)) = \alpha(2) = 5.$
$\sigma(9) = \alpha(\beta(\tau(\gamma(\delta(9))))) = \alpha(\beta(\tau(\gamma(9)))) = \alpha(\beta(\tau(9))) = \alpha(\beta(8)) = \alpha(8) = 8.$
$\sigma(10) = \alpha(\beta(\tau(\gamma(\delta(10))))) = \alpha(\beta(\tau(\gamma(10)))) = \alpha(\beta(\tau(10))) = \alpha(\beta(9)) = \alpha(9) = 9.$
$\sigma(11) = \alpha(\beta(\tau(\gamma(\delta(11))))) = \alpha(\beta(\tau(\gamma(11)))) = \alpha(\beta(\tau(12))) = \alpha(\beta(12)) = \alpha(5) = 7.$
$\sigma(12) = \alpha(\beta(\tau(\gamma(\delta(12))))) = \alpha(\beta(\tau(\gamma(3)))) = \alpha(\beta(\tau(3))) = \alpha(\beta(3)) = \alpha(1) = 2.$

b. Déterminer les orbites de σ. En déduire la décomposition de σ comme produit des cycles disjoints.

$$1 \xrightarrow{\sigma} 12 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 10 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 1$$

Donc $O_1 = O_{12} = O_2 = O_{10} = O_9 = O_8 = O_5 = \{1, 2, 5, 8, 9, 10, 12\}$.
$\sigma(4) = 4$. Donc $O_4 = \{4\}$.

$$3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 11 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 3$$

Donc $O_3 = O_6 = O_{11} = O_7 = \{3, 6, 7, 11\}$.
La décomposition de σ en cycles disjoints est :

$$\sigma = (1 \; 12 \; 2 \; 10 \; 9 \; 8 \; 5) \; (3 \; 6 \; 11 \; 7) \tag{3}$$

c. Donner l'ordre de σ.

Puisque la décomposition de σ dans l'équation (3) est en cycle disjoint, on sait que $o(\sigma)$ est le ppcm des longueurs des cycles dans la décomposition. Dans ce cas on obtient que $\boxed{o(\sigma) = 7 \vee 4 = 26}$.

d. Déterminer un élément de $\langle\sigma\rangle$ d'ordre n pour $n = 2, 4, 5, 6$ ou expliquer pourquoi il n'y en a pas.

Nous utilisons la formule

$$\forall k \in \mathbb{N} \quad o(\sigma^k) = \frac{o(\sigma)}{o(\sigma) \wedge k} = \frac{28}{28 \wedge k}.$$

Donc $o(\sigma^{14}) = 2$ et $o(\sigma^7) = 4$.
On a $\mathrm{Card}(\langle\sigma\rangle) = o(\sigma) = 28$. Or l'ordre de tout élément de $\langle\sigma\rangle$ doit diviser le cardinal de ce groupe (c'est-à-dire 28). Puisque 5 ne divise pas 28, le groupe $\langle\sigma\rangle$ n'admet aucun élément d'ordre 5.
De même manière il n'existe aucun élément de $\langle\sigma\rangle$ d'ordre 6.

e. A quel groupe est isomorphe $\langle\sigma^7\rangle$? et le groupe $\langle\sigma^8\rangle$? Dans chaque cas donner un isomorphisme.

$\langle\sigma^7\rangle$ est un groupe cyclique de cardinal $o(\sigma^7)$. Or $o(\sigma^7) = 4$, donc $\langle\sigma^7\rangle$ est isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$ où l'isomorphisme est donné par $\boxed{(\sigma^7)^k \mapsto \bar{k}}$ où $\bar{k}$ désigne la classe de congruence de k dans $\mathbb{Z}/4\mathbb{Z}$.
De même $\langle\sigma^8\rangle$ est un groupe cyclique de cardinal $o(\sigma^8)$. Or $o(\sigma^8) = 7$, donc $\langle\sigma^8\rangle$ est isomorphe à $(\mathbb{Z}/7\mathbb{Z}, +)$ où l'isomorphisme est donné par $\boxed{(\sigma^8)^m \mapsto \tilde{m}}$ où $\tilde{m}$ désigne la classe de congruence de m dans $\mathbb{Z}/7\mathbb{Z}$.

<u>**Exercice 5 :**</u> **(Bonus)**

a. Justifier que l'équation $18u + 23v = 1$ admet des solutions et donner une solution particulière.

18 et 23 sont premiers entre eux. D'après le théorème de Bézout on sait que l'équation diophantienne $18u + 23v = 1$ admet des solutions. Une solution particulière est $18 \times 9 - 23 \times 7 = 1$.

b. Déterminer toutes les solutions entières de $18x \equiv b$ [mod 23] où $b \in \mathbb{Z}$.

Puisque $18 \times 9 - 23 \times 7 = 1$, on a $9 \times 18 \equiv 1$ [mod 23]. Donc

$$9 \times 18x \equiv 9 \times b \ [\mathrm{mod}\ 23] \implies x \equiv 9 \times b \ [\mathrm{mod}\ 23]$$