

---

Examen - Session 1 - 16 mai 2024

---

**Durée : 2h00. Aucun document ni calculatrice autorisé**

Toute réponse non justifiée est considérée comme zéro

**Exercice 1 :** On note  $P(X) = -X^3 + 1$  et  $Q(X) = X^2 + X$ .

1. Calculer le polynôme  $P \circ Q(X)$ . Quel est son degré ?
2. Montrer que 1 est une racine de  $P$ .  
En déduire une factorisation de  $P$  comme un polynôme de  $\mathbb{R}[X]$ .
3. Montrer que  $P$  et  $Q$  sont premiers entre eux.

**Exercice 2 :**

1. Soient  $a, b, c$  des entiers non nuls tels que  $a \wedge b = 1$  et  $a \wedge c = 1$ . Montrer que  $a \wedge bc = 1$ .
2. (Ordre d'un entier modulo  $a$ ) Soient  $a, b \geq 2$  deux entiers. Montrer l'équivalence suivante :

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

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

3. On veut montrer que si un entier  $n$  est premier avec 10, alors il existe un multiple de  $n$  qui s'écrit  $11 \dots 1$ .
  - a. Montrer que  $9n$  est premier avec 10. En déduire qu'il existe un entier positif  $k$  tel que  $10^k \equiv 1 \pmod{9n}$ .
  - b. Montrer que 9 divise  $10^k - 1$ . Quel est la valeur du quotient ?
  - c. Conclure.

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

- a. Quel est l'ordre de l'élément  $\bar{9}$  ?
- b. Déterminer les éléments  $\bar{k} \in G$  tels que  $G = \langle \bar{k} \rangle$ .
- c. Déterminer le plus petit sous-groupe  $H$  de  $G$  qui contient  $\bar{6}$  et  $\bar{8}$ .

**Exercice 4 :** Soit  $\sigma : \{1, 2, \dots, 11, 12\} \rightarrow \{1, 2, \dots, 11, 12\}$  la permutation :

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

1. Donnez l'image par  $\sigma$  de chacun des entiers de 1 à 12.
2. Déterminer les orbites de  $\sigma$ . En déduire la décomposition de  $\sigma$  comme produit des cycles disjoints.
3. Donner l'ordre de  $\sigma$ .
4. 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.
5. A quel groupe est isomorphe  $\langle \sigma^7 \rangle$  ? et le groupe  $\langle \sigma^8 \rangle$  ? Dans chaque cas donner un isomorphisme.

**Exercice 5 :** (Bonus)

1. Justifier que l'équation  $18u + 23v = 1$  admet des solutions et donner une solution particulière.
2. Déterminer toutes les solutions entières de  $18x \equiv b \pmod{23}$  où  $b \in \mathbb{Z}$ .