

GROUPES

Exercice 1. Montrer que les groupes $\mathbb{C}^*$ et $\mathbb{R}_+^* \times \mathbb{U}$ sont isomorphes

Exercice 2. Soit $(G, \cdot)$ un groupe

1. Montrer que l'ensemble des automorphismes de G muni de la loi $\circ$ est un groupe. Celui-ci sera noté $\text{Aut}(G)$.
2. On définit l'application : $\phi : g \in G \mapsto \phi_g \in \text{Aut}(G)$, où, pour tout $g \in G$, $\phi_g : x \in G \mapsto g.x.g^{-1} \in G$.
Montrer que ϕ est un morphisme de groupe. Déterminer son noyau.
3. Déterminer $\text{Aut}(\mathbb{Q})$ et $\text{Aut}(\mathbb{Z})$

Exercice 3. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.

Exercice 4. Théorème de Lagrange

Soit $(G, \cdot)$ un groupe fini. Soit H un sous-groupe de G . Pour $x \in G$, on note $xH = \{t \in G \mid \exists h \in H, t = xTh\}$

1. Montrer que pour tout $(x, y) \in G^2$, il existe une bijection de xH vers yH .
2. En déduire que le cardinal de H divise celui de G

Exercice 5. Soient G et H deux groupes, tel que G soit fini et $f : G \mapsto H$ un morphisme de groupes. Montrer que $\text{Card}(G) = \text{Card}(\ker f) \times \text{Card}(\text{Im } f)$

Exercice 6. Soit $(G, \cdot)$ un groupe fini de cardinal supérieur ou égal à 2 tel que : $\forall x \in G, x^2 = e$. Montrer que G est commutatif, puis qu'il existe $n \in \mathbb{N}^*$ tel que G soit isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.

Exercice 7. Montrer que le groupe $\mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Exercice 8. Soit $(G, \cdot)$ un groupe et H un sous-groupe de G . On dit que H est *distingué* dans G (et on note alors $H \triangleleft G$) si : $\forall x \in H, \forall z \in G, z.x.z^{-1} \in H$.

1. Soit $f : (G, \cdot) \mapsto (G', \cdot)$ un morphisme de groupes.
 - (a) Montrer que si $H' \triangleleft G'$, alors $f^{-1}(H') \triangleleft G$.
 - (b) Montrer que si $H \triangleleft G$ et si f est surjective, alors $f(H) \triangleleft G'$.
2. Soit $(G, \cdot)$ un groupe et H, K deux sous-groupes de G . On suppose $H \triangleleft G$. On définit l'ensemble HK par $HK = \{h.k \mid (h, k) \in H \times K\}$.
Montrer que HK est un sous-groupe de G .

Exercice 9. Soit $(G, \cdot)$ un groupe abélien.

1. Soient x, y deux éléments de G d'ordre respectifs p et q avec $p \wedge q = 1$. Montrer que xy est d'ordre pq .
2. On suppose que G est d'ordre pq où p, q sont deux nombres premiers distincts.
On veut montrer que G possède un élément d'ordre pq (c'est-à-dire que G est cyclique).
Par l'absurde, on suppose que G ne possède aucun élément d'ordre pq . Soit $x \in G \setminus \{e\}$.
 - (a) Quels sont les ordres possibles pour x ?
 - (b) On suppose que x est d'ordre p . Soit $y \in G \setminus \langle x \rangle$.
En considérant l'ensemble $H = \{x^i.y^j \mid (i, j) \in \llbracket 0, p-1 \rrbracket^2\}$, montrer que y ne peut pas être d'ordre p (On pourra utiliser le théorème de Lagrange).
 - (c) Conclure.

Exercice 10. Soit σ la permutation suivante (appartenant à S_{12}) :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 10 & 6 & 8 & 2 & 11 & 12 & 5 & 1 & 4 & 3 & 9 \end{pmatrix}$$

1. Décomposer σ en cycles disjoints.
2. Calculer son ordre, sa signature. Préciser σ^{1234} .

- Exercice 11.** 1. Soit $\sigma = (i_1 \ i_2 \ \dots \ i_k) \in S_n$.
Montrer que : $\forall \tau \in S_n, \tau \sigma \tau^{-1} = (\tau(i_1) \ \tau(i_2) \ \dots \ \tau(i_k))$
2. Soit $\sigma = (1 \ 2 \ \dots \ n) \in S_n$ et $\tau = (1 \ 2) \in S_n$.
Pour tout $k \in \mathbb{N}$, calculer $\sigma^k \tau \sigma^{-k}$. En déduire que $S_n = \langle \sigma, \tau \rangle$.

- Exercice 12.** 1. Soit $\sigma = (a_1 \ a_2 \ \dots \ a_r) \in S_n$ un cycle d'ordre r .
Pour quelles valeurs de $k \in \llbracket 1, n-1 \rrbracket$, la permutation σ^k est-elle un cycle ?

ARITHMÉTIQUE

- Exercice 13.** 1. Montrer que, pour tout $n \in \mathbb{N}$, $5 \mid 2^{3n+5} + 3^{n+1}$
2. Montrer que, pour tout $n \in \mathbb{N}$, $30 \mid n^5 - n$
3. Déterminer le reste de la division euclidienne de $16^{2^{1000}}$ par 7.
4. Quel est le dernier chiffre (dans l'écriture décimale) de 7^{7^7} ?

Exercice 14. Calculer le pgcd, le ppcm et un couple de coefficients de Bézout de $a = 270$ et $b = 105$.

Exercice 15. Résoudre dans $\mathbb{Z}^2$ l'équation : $47u + 111v = 1$.

Exercice 16. Résoudre le système :
$$\begin{cases} 3x \equiv 2 \ [5] \\ 5x \equiv 1 \ [6] \end{cases}$$

- Exercice 17.** 1. Soit $a \geq 2$ et $n \geq 2$ deux entiers tels que $a^n - 1$ soit un nombre premier. Montrer que $a = 2$ et que n est un nombre premier.
2. Soit $n \in \mathbb{N}^*$ tel que $2^n + 1$ soit un nombre premier. Montrer que n est une puissance de 2.

Exercice 18. Nombres de Fermat

On pose, pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$.

1. Pour tout $n \in \mathbb{N}$ et pour tout $k \in \mathbb{N}^*$, montrer que $F_{n+k} - 2 \equiv 0 \ [F_n]$.
2. Montrer que les $(F_n)_{n \in \mathbb{N}}$ sont premiers entre eux deux à deux.
3. En déduire une autre démonstration du fait qu'il existe une infinité de nombres premiers.

Exercice 19. Calculer $\varphi(100)$ et en déduire les deux derniers chiffres de l'écriture décimale de 3^{4321} .

Exercice 20. Montrer que pour tout $n \in \mathbb{N}^*$, $n = \sum_{d \mid n} \varphi(d)$

(on commencera par montrer que $\mathbb{U}_n$ possède exactement $\varphi(n)$ éléments d'ordre n .)

POLYNÔMES

Exercice 21. Soit $n \in \mathbb{N}^*$ et $P_n = \sum_{k=0}^n X^k = 1 + X + \dots + X^n$.

1. Décomposer P_n en produit d'irréductibles dans $\mathbb{C}[X]$
2. En déduire la valeur de $\prod_{k=1}^n \sin\left(\frac{k\pi}{n+1}\right)$. (On pourra évaluer P_n en 1.)

- Exercice 22.** 1. Soit $a \in \mathbb{R}$. Déterminer le reste de la division euclidienne de $(X \sin a + \cos a)^n$ par $X^2 + 1$.
2. Montrer que pour tout $n \in \mathbb{N}$, le polynôme $P_n = (X-1)^{n+2} + X^{2n+1} \in \mathbb{C}[X]$ est divisible par $X^2 - X + 1$

Exercice 23. Soit $P \in \mathbb{R}[X]$ unitaire de degré $d \geq 1$.

Montrer que P est scindé sur $\mathbb{R}$ si et seulement si pour tout $z \in \mathbb{C}$, $|P(z)| \geq |\operatorname{Im}(z)|^d$

Exercice 24. Soit $(A, B) \in (\mathbb{C}[X] \setminus \{0\})^2$. Montrer l'équivalence suivante :

A et B ne sont pas premiers entre eux $\iff \exists (U, V) \in (\mathbb{C}[X] \setminus \{0\})^2$ tq
$$\begin{cases} AU + BV = 0 \\ \deg(U) < \deg(B) \\ \deg(V) < \deg(A) \end{cases}.$$

ENSEMBLES $\mathbb{Z}/n\mathbb{Z}$

Exercice 25. Résoudre dans $\mathbb{Z}/37\mathbb{Z}$

$$1. \begin{cases} \overline{3}x + \overline{7}y = \overline{3} \\ \overline{6}x - \overline{7}y = \overline{0} \end{cases} \quad 2. x^2 + \overline{31}x + \overline{18} = \overline{0} \quad \text{Indication : } (\overline{6})^2 = \overline{-1}.$$

Exercice 26. Donner l'ensemble G des inversibles de l'anneau $\mathbb{Z}/20\mathbb{Z}$.
Montrer que $(G, \times)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$.

Exercice 27. Soit $n \in \mathbb{N}^*$. On note $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des automorphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ (cf exercice 2).
Démontrer que les groupes $(\text{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$ et $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ sont isomorphes.

Exercice 28. Déterminer tous les morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{Z}/m\mathbb{Z}, +)$. Combien y en-a-t-il ?

Exercice 29. Soit p un nombre premier supérieur ou égal à 3.

1. Quel est le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$?
2. On suppose $p \equiv 1 \pmod{4}$. En calculant $(p-1)!$ de deux façons, montrer que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
3. On suppose $p \equiv 3 \pmod{4}$. Montrer que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 30. Théorème de Wilson

Soit $p \in \mathbb{N} \setminus \{0, 1\}$. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

ANNEAUX , CORPS, ALGÈBRES

Exercice 31. Soit $A = \left\{ \frac{m}{2^n} \mid m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$.

Montrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$. Quels en sont les éléments inversibles ?

Exercice 32. On considère $\mathbb{Z}[i] = \{u + iv \mid (u, v) \in \mathbb{Z}^2\}$ et $\varphi : a \in \mathbb{Z}[i] \mapsto a\bar{a} \in \mathbb{N}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.
2. Déterminer le groupe multiplicatif des éléments inversibles de $\mathbb{Z}[i]$.
(on pourra commencer par caractériser ce groupe à l'aide de φ)
3. Montrer que, pour tout $(a, b) \in \mathbb{Z}[i] \times (\mathbb{Z}[i] \setminus \{0\})$, il existe $(q, r) \in (\mathbb{Z}[i])^2$ tel que $a = bq + r$ avec $\varphi(r) < \varphi(b)$.
4. En déduire que $\mathbb{Z}[i]$ est principal.

Exercice 33. Soit $E = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\}$. Montrer que $(E, +, \times)$ est un corps, et déterminer ses automorphismes.

Exercice 34. Soit I un idéal d'un anneau commutatif A . On appelle radical de I l'ensemble noté $\sqrt{I}$ défini par : $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N}^*; x^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A .
2. Déterminer le radical d'un idéal de $\mathbb{Z}$.

Exercice 35. Montrer que toute suite croissante (pour l'inclusion) d'idéaux de $\mathbb{Z}$ est stationnaire.
Le résultat se généralise-t-il aux idéaux de $\mathbb{K}[X]$?

Exercice 36. Soit $\alpha \in \mathbb{R}$ et soit $E_\alpha = \left\{ \begin{pmatrix} x & \alpha y \\ y & x \end{pmatrix} \mid (x, y) \in \mathbb{R}^2 \right\}$.

1. Montrer que E_α est une sous-algèbre commutative de $\mathcal{M}_2(\mathbb{R})$.
2. Si $\alpha < 0$, montrer que E_α est un corps, isomorphe à $\mathbb{C}$.
Si $\alpha \geq 0$, montrer que E_α est un anneau non intègre.

Exercice 37. Soit $P = X^3 - X + 1$.

1. Montrer que P a une unique racine réelle θ , que $\theta \notin \mathbb{Q}$ et que P est irréductible sur $\mathbb{Q}$.
2. On pose $\mathbb{Q}[\theta] = \{A(\theta) \mid A \in \mathbb{Q}[X]\}$. Montrer que $\mathbb{Q}[\theta]$ est un corps.
3. Calculer l'inverse de $\theta^2 - 2\theta - 3$.

Exercice 38. Soit $E = \left\{ M(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \mid (a, b, c) \in \mathbb{R}^3 \right\}$. Montrer que E est une sous-algèbre commutative de $\mathcal{M}_3(\mathbb{R})$ dont on déterminera la dimension.

EXERCICES DE BANQUE CCINP

EXERCICE 65 algèbre

Soit u un endomorphisme d'un espace vectoriel E sur le corps $\mathbb{K}$ ($= \mathbb{R}$ ou $\mathbb{C}$). On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

1. Démontrer que : $\forall (P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X], (PQ)(u) = P(u) \circ Q(u)$.
2. (a) Démontrer que : $\forall (P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X], P(u) \circ Q(u) = Q(u) \circ P(u)$.
(b) Démontrer que, pour tout $(P, Q) \in \mathbb{K}[X] \times \mathbb{K}[X] : (P \text{ polynôme annulateur de } u) \implies (PQ \text{ polynôme annulateur de } u)$
3. Soit $A = \begin{pmatrix} -1 & -2 \\ 1 & 2 \end{pmatrix}$.

Écrire le polynôme caractéristique de A , puis en déduire que le polynôme $R = X^4 + 2X^3 + X^2 - 4X$ est un polynôme annulateur de A .

EXERCICE 85 algèbre

1. Soient $n \in \mathbb{N}^*, P \in \mathbb{R}_n[X]$ et $a \in \mathbb{R}$.
(a) Donner sans démonstration, en utilisant la formule de Taylor, la décomposition de $P(X)$ dans la base $(1, X - a, (X - a)^2, \dots)$.
(b) Soit $r \in \mathbb{N}^*$. En déduire que :
 a est une racine de P d'ordre de multiplicité r si et seulement si $P^{(r)}(a) \neq 0$ et $\forall k \in \llbracket 0, r - 1 \rrbracket, P^{(k)}(a) = 0$.
2. Déterminer deux réels a et b pour que 1 soit racine double du polynôme $P = X^5 + aX^2 + bX$ et factoriser alors ce polynôme dans $\mathbb{R}[X]$.

EXERCICE 86 algèbre

1. Soit $(a, b, p) \in \mathbb{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
2. Soit p un nombre premier.
(a) Prouver que $\forall k \in \llbracket 1, p - 1 \rrbracket, p$ divise $\binom{p}{k} k!$ puis en déduire que p divise $\binom{p}{k}$.
(b) Prouver que : $\forall n \in \mathbb{N}, n^p \equiv n \pmod{p}$.
Indication : procéder par récurrence.
(c) En déduire, pour tout entier naturel n , que : p ne divise pas $n \implies n^{p-1} \equiv 1 \pmod{p}$.

EXERCICE 87 algèbre

Soient $a_0, a_1, \dots, a_n, n + 1$ réels deux à deux distincts.

1. Montrer que si $b_0, b_1, \dots, b_n$ sont $n + 1$ réels quelconques, alors il existe un unique polynôme P vérifiant
 $\deg P \leq n$ et $\forall i \in \llbracket 0, n \rrbracket, P(a_i) = b_i$.

2. Soit $k \in \llbracket 0, n \rrbracket$.

Expliciter ce polynôme P , que l'on notera L_k , lorsque :

$$\forall i \in \llbracket 0, n \rrbracket, b_i = \begin{cases} 0 & \text{si } i \neq k \\ 1 & \text{si } i = k \end{cases}$$

3. Prouver que $\forall p \in \llbracket 0, n \rrbracket, \sum_{k=0}^n a_k^p L_k = X^p$.

EXERCICE 94 algèbre

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux.
Soit $c \in \mathbb{N}$.
Prouver que : $(a|c \text{ et } b|c) \iff ab|c$.
3. On considère le système $(S) : \begin{cases} x \equiv 6 & [17] \\ x \equiv 4 & [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.
(a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
(b) Déduire des questions précédentes la résolution dans $\mathbb{Z}$ du système (S) .