Feuille d'exercices d'algèbre

Relations binaires, lois de composition, applications

Exercice n°1

Soient E un ensemble et $A \subset E$. On définit la relation sur $\mathcal{P}(E)$: $X \sim Y \Leftrightarrow X \cup A = Y \cup A$.

1) Montrer que c'est une relation d'équivalence.

2) Soit $\varphi : \mathcal{P}(E) \to \mathcal{P}(E \setminus A)$, $X \mapsto X \setminus A$.
Montrer que φ est compatible avec $\sim$, et que l'application quotient associée est une bijection.

Exercice n°2

On définit dans le corps $\mathbb{C}$, la relation $\mathcal{R}$ par : $(x+iy)\mathcal{R}(x'+iy')$ si $(x < x')$ ou $(x = x'$ et $y \leq y')$. Montrer que c'est une relation d'ordre total, non compatible avec la multiplication. Déterminer l'ensemble des majorants de $U = \{z \in \mathbb{C},\ |z| = 1\}$. L'ensemble U admet-il une borne supérieure ?

Exercice n°3

On définit l'opération dans $\mathbb{Z}^2$: $(a,b) * (a',b') = (aa', ab'+b)$.

1) Étudier les propriétés de cette opération.

2) Pour $z \in \mathbb{Z}$, on pose $f_{a,b}(z) = az+b$. Montrer que $\varphi : \mathbb{Z}^2 \to \mathbb{Z}^{\mathbb{Z}}$, $(a,b) \mapsto f_{a,b}$ est un morphisme pour $*$ et $\circ$.

3) Est-ce un isomorphisme ?

Exercice n°4

Soient f une application de E dans F, g une application de F dans G et $h = g \circ f$.

1) Montrer que si h est surjective et g injective, alors f est surjective.

2) Montrer que si h est injective et f surjective alors g est injective.

Exercice n°5

Soient E et F deux ensembles non vides et f une application de E dans F. On note $\mathcal{F}$ l'ensemble des applications de F dans E.

1) Soient A_1 et A_2 deux parties de E. Montrer que $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$ avec égalité si f est injective.

2) Soient A une partie de E et B une partie de F. Montrer que

$A \subset f^{-1}(f(A))$ avec égalité si f est injective et $f\left(f^{-1}(B)\right) \subset B$ avec égalité si f est surjective

3) Montrer que f est injective si et seulement si : $\forall g \in \mathcal{F}, \forall h \in \mathcal{F}, (f \circ g = f \circ h \Rightarrow g = h)$

Arithmétique dans $\mathbb{Z}$

Exercice n°6

On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_n = 1 + 10 + 100 + \ldots + 10^n$

1) Trouver deux entiers naturels distincts n et p tels que $u_n - u_p$ soit divisible par 24.

2) Plus généralement, montrer que, pour tout nombre $a \in \mathbb{N}$, il existe un multiple non nul de a qui s'écrit en écriture décimale uniquement avec les chiffres 1 et 0.

Exercice n°7

Énoncer des critères de divisibilité par 6, par 2 et par 5 à partir de l'écriture en base six d'un nombre.

Exercice n°8 (*CAPES 2006, épreuve sur dossier*)

1) Soit m un entier relatif. On note (E_m) l'équation $11x + 13y = m$, d'inconnue (x, y). Trouver toutes les solutions (x, y) de (E_m) dans $\mathbb{Z} \times \mathbb{Z}$.

2) On suppose désormais que m est un entier naturel. Montrer qu'il y a autant de solutions (x, y) de l'équation (E_m) dans $\mathbb{N} \times \mathbb{N}$ qu'il y a d'entiers dans le segment $[\frac{5m}{11}, \frac{6m}{13}]$.

3) Montrer que si $m < 143$ (resp. $m \geq 143$), alors l'équation (E_m) possède au plus (resp. au moins) une solution (x, y) dans $\mathbb{N} \times \mathbb{N}$.

Exercice n°9

On cherche à résoudre dans $\mathbb{Z}$ l'équation $x^2 + 5y^2 = z^2$.

1) Montrer qu'il suffit de chercher les solutions telles que $pgcd(x, z) = 1$.

2) Soit (x, y, z) une telle solution. On note $d = pgcd(z - x, z + x)$. Montrer que d divise 2.

a) On suppose que $d = 1$. Montrer qu'il existe deux entiers impairs u et v tels que $y = uv$ et $2z = 5u^2 + v^2$.

b) On suppose que $d = 2$. Montrer qu'il existe deux entiers u et v l'un pair, l'autre impair tels que $y = 2uv$ et $z = 5u^2 + v^2$.

3) Résoudre l'équation de départ.

Exercice n°10

Quel est le nombre de diviseurs de 192 080 000 ?
Par combien de zéros se termine l'écriture décimale de 126! ?
Quel est le chiffre des unités dans l'écriture en base 10 du nombre $7^{7^{7^{7^{7^7}}}}$?
Le 26 mai 2001 était un samedi. Quel jour de la semaine était le 26 mai 1981 ?

Exercice n°11

1) Soit $n \in \mathbb{N}$. Montrer que l'on peut trouver n entiers consécutifs dont aucun n'est premier.

2) Montrer que si un produit d'entiers naturels est de la forme $4n - 1$ alors au moins l'un des facteurs est de la même forme. En déduire qu'il existe une infinité de nombres premiers de la forme $4n - 1$.

3) Soient $n \in \mathbb{N}$ et $p \geq 3$ un diviseur premier de $n^2 + 1$. Montrer que $p \equiv 1\,[4]$. En déduire qu'il y a une infinité de nombres premiers de la forme $4k + 1$.

Exercice n°12 (*Nombres de Mersenne et nombres parfaits*)

1) Soient $p, q \in \mathbb{N}$. Montrer que $2^{pq} - 1$ est divisible par $2^p - 1$ et par $2^q - 1$. En déduire que si n n'est pas premier, il en est de même de $2^n - 1$.

2) On suppose que $2^n - 1$ est premier et on pose $a = 2^{n-1}(2^n - 1)$. Montrer qu'un diviseur de a est nécessairement soit de la forme $2^k(2^n - 1)$ soit de la forme 2^k, k étant un entier compris entre 0 et $n - 1$. En déduire que a est parfait, c'est à dire que la somme de ses diviseurs est égale à $2a$.
Montrer réciproquement que si un entier naturel pair a est parfait alors on peut l'écrire sous la forme $a = 2^{n-1}(2^n - 1)$ avec $2^n - 1$ premier.

3) Montrer que si on fait la somme des chiffres d'un nombre parfait pair a, puis si on fait la somme des chiffres du nombre obtenu etc ... , on obtient toujours 1 sauf pour $a = 6$. On pourra remarquer que si $p > 3$ est un nombre premier, alors p est de la forme $6k + 1$ ou $6k + 5$ et observer alors la congruence modulo 9.

Exercice n°13 (*Théorème de Wilson*)

Soit $p \in \mathbb{N}^*$. Montrer p est un nombre premier, si et seulement si : $(p - 1)! \equiv -1\,(n)$.

Exercice n°14 (*Petit théorème de Fermat*)

1) Soit p un nombre premier. Montrer que, pour tout entier k de $[1, p - 1]$, p divise $\begin{pmatrix} p \\ k \end{pmatrix}$.

2) En déduire que pour $a, b \in \mathbb{Z}$ on a $(a + b)^p \equiv a^p + b^p \bmod p$, puis que $a^p \equiv a \bmod p$.

Exercice n°15

Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs positifs de n.

1) Montrer que si $n = ab$ avec $a \wedge b = 1$, alors $d_n = d_a d_b$.

2) Montrer que n est un carré parfait si et seulement si d_n est impair.

3) Montrer que : $\prod_{d|n} d = \sqrt{n}^{d_n}$.

Exercice n°16

Soit $n \in \mathbb{N}^*$. Montrer que le cardinal de $\{(a,b) \in (\mathbb{N}^*)^2,\ a \vee b = n\}$ est égal au nombre de diviseurs de n^2.

Exercice n°17

Soit $p > 3$ un nombre premier.

1) Montrer qu'une équation du second degré : $x^2 + ax + b = \dot{0}$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si son discriminant : $a^2 - 4b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

2) On suppose que $p \equiv 1\ [3]$: $p = 3q + 1$. Montrer qu'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a^q \neq \dot{1}$. En déduire que $-\dot{3}$ est un carré.

3) Réciproquement, on suppose que $-\dot{3}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Montrer que $p \equiv 1\ [3]$.

Exercice n°18

Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. On note $\bar{k}$ le classe de k modulo n. Montrer que les propriétés suivantes sont équivalentes :
(i) $\text{pgcd}(n,k) = 1$
(ii) $\bar{k}$ est un générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$
(iii) $\bar{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ (c'est à dire que $\bar{k}$ est élément du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$).

Exercice n°19

Soit $n = pq$ où p et q sont deux nombres premiers distincts. Soient a, b deux entiers naturels tels que $ab \equiv 1 \quad [\varphi(n)]$. Montrer que les applications f et g de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même définies respectivement par $x \mapsto x^a$ et $x \mapsto x^b$ sont réciproques l'une de l'autre.

Exercice n°20 *(Propriété universelle de $\mathbb{Z}/n\mathbb{Z}$)*

Soient n dans $\mathbb{N}$ et Γ un groupe.

1) Montrer que l'application $\begin{array}{ccc} \text{Hom}_{\text{groupes}}(\mathbb{Z}/n\mathbb{Z}, \Gamma) & \longrightarrow & \{\gamma \in \Gamma | \gamma^n = e\} \\ f & \longmapsto & f(1 \bmod n) \end{array}$ est une bijection.

Est-ce un isomorphisme de groupes ?

2) Déterminer l'application réciproque de f.

Exercice n°21

1) Déterminer tous les endomorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$.

2) Montrer que l'ensemble des automorphismes de $\mathbb{Z}/n\mathbb{Z}$, muni de la composition, est un groupe isomorphe au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice n°22

Pour tout n de $\mathbb{N}^*$, on note μ_n le groupe des racines nièmes de l'unité dans $\mathbb{C}$. Soient $m, n \in \mathbb{N}^*$.

1) Montrer que $G = \mu_n \cap \mu_m$ est cyclique et en donner un générateur.

2) Soit H le sous-groupe de $(\mathbb{C}^*, \times)$ engendré par $\mu_n \cup \mu_m$. Montrer que H est cyclique et en donner un générateur.

Exercice n°23

1) Montrer que 2 est un générateur de $(\mathbb{Z}/13\mathbb{Z})^*$. Dresser une table donnant pour tout x de $(\mathbb{Z}/13\mathbb{Z})^*$ l'unique entier n tel que $x = 2^n$ et $0 \leq n < 12$ (n est appelé *logarithme discret* de x).

2) Résoudre l'équation $6x^2 \equiv 5 \quad [13]$ en cherchant x sous la forme 2^n à l'aide de la table précédente.

Exercice n°24

Soient p un nombre premier impair et x dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

1) Montrer que $x^{\frac{p-1}{2}} = \pm 1$.

2) Montrer que $x^{\frac{p-1}{2}} = 1$ si et seulement si x est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

3) En déduire que si $p = 1 \bmod 4$ alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

4) Montrer que dans $(\mathbb{Z}/p\mathbb{Z})^\times$ il y a exactement $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés.

Exercice n°25

Pour tout entier $n \geq 1$, on note $\varphi(n)$ le nombre d'entiers k premiers avec n et tels que $1 \leq k \leq n$. La fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ ainsi définie est appelée *fonction d'Euler*.

1) Soit $n \geq 1$ un entier. Montrer que $\varphi(n)$ est égal au nombre de générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$.

2) Soient m et n deux entiers naturels non nuls et premiers entre eux. Montrer que $\varphi(mn) = \varphi(m)\varphi(n)$.

3) Soient $p > 1$ un nombre premier et $\alpha > 0$ un entier. Montrer que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

4) Soient $n \geq 2$ un entier et $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Montrer que :

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$$

5) Soient $n > 0$ un entier et $D_n = \{d \in \mathbb{N}^* | d \text{ divise } n\}$. Montrer que $\sum_{d \in D_n} \varphi(d) = n$ (on pourra considérer l'application g définie sur $E_n = \{1, 2 \cdots, n\}$ par $g(x) = \text{pgcd}(x, n)$).

Exercice n°26

Soient a et b deux entiers strictement positifs. On note d le PGCD de a et b, m leur PPCM, et l'on pose $a = da'$ et $b = db'$. On considère l'homomorphime de groupes :

$$\varphi : \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z},\ x \mapsto (x \bmod a, x \bmod b)$$

1) Déterminer le noyau de φ. En déduire le cardinal de l'image de φ et une condition nécessaire et suffisante sur a et b pour que φ soit surjectif.

2) On considère l'homomorphisme naturel de groupes :

$$\psi : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z},\ (y, z) \mapsto (y \bmod d) - (z \bmod d)$$

Montrer que ψ est surjectif. En déduire le cardinal du noyau de ψ. Calculer $\psi \circ \varphi$ et en déduire (en utilisant les questions précédentes) que Im φ = Ker ψ.

3) Etant donnés deux entiers α et β, donner une condition nécessaire et suffisante sur d, α et β pour que le système $(*) \quad x \equiv \alpha \pmod a \quad x \equiv \beta \pmod b$
admette au moins une solution $x \in \mathbb{Z}$. Si x_0 est une solution de $(*)$, décrire l'ensemble de toutes les solutions.

Exercice n°27

Soit p un nombre premier et soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1) Soient $x, y \in \mathbb{F}_p$. Montrer que si ni x ni y est un carré, alors xy est un carré (dans $\mathbb{F}_p$). En déduire que au moins un des éléments $\overline{-1}$, $\overline{2}$, $\overline{-2}$ est un carré.

2) Montrer que $X^4 + 1$ est réductible dans $\mathbb{F}_p$.

Polynômes et arithmétique

Exercice n°28

Calculer le PGCD de $P_1 = 2X^4 - 3X^2 + 1$ et de $P_2 = X^3 + X^2 - X - 1$ dans $\mathbb{Q}[X]$ ainsi que $S,\ T \in \mathbb{Q}[X]$ tel que $PGCD(P_1, P_2) = P_1.S + P_2.T$

Exercice n°29

Soit $P = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ avec $n \geq 1$ et $a_n \neq 0$. Montrer que si $r = \dfrac{c}{d} \in \mathbb{Q}$, avec $pgcd(c, d) = 1$ est une racine de P alors c divise a_0 et d divise a_n.
Trouver les racines de $2X^5 - 5X^4 - 21X^3 - 15X^2 - 23X - 10$ dans $\mathbb{Q}$.

Exercice n°30

Soit p un nombre premier et $P = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ un polynôme de degré $n \geq 1$ à coefficients entiers tel que a_n n'est pas divisible par p, montrer que parmi les nombres $\{0, 1, 2, \ldots, p-1\}$, il n'existe pas plus de n nombres x pour lesquels $P(x)$ soit divisible par p.
Montrer par un contre exemple, que ce résultat n'est plus vrai si p n'est pas premier.

Exercice n°31

1) Quel est le reste dans la division euclidienne de $X^9 + 4X^6 + 3X^5 + X + 1$ par $X^2 + X + 1$ dans $\mathbb{R}[X]$?

2) Montrer que si trois polynômes P, Q, R de $\mathbb{R}[X]$ vérifient la relation $P^2 - XQ^2 = XR^2$, ils sont nuls. Est-ce encore vrai dans $\mathbb{C}[X]$?

3) Trouver tous les polynômes P de $\mathbb{R}[X]$ vérifiant $P(X^2) + P(X)P(X + 1) = 0$

4) Montrer que pour tout polynôme P de $\mathbb{C}[X]$, le polynôme $P[P(x)] - X$ est divisible par $P(X) - X$.

Exercice n°32

Soit P un polynôme de $\mathbb{R}[X]$ tel que $\forall x \in \mathbb{R},\ P(x) \geq 0$. Montrer qu'il existe des polynômes A et B de $\mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Exercice n°33

1) Décomposer $P = (X^2 + 1)^2 - 3X^2$ en facteurs irréductibles dans $\mathbb{R}[X]$. En déduire que P est irréductible dans $\mathbb{Q}[X]$.

2) On note α la classe de X dans $A = \mathbb{Q}[X]/(P)$. Montrer que $\alpha + 1$ est inversible dans A. Exprimer α^6, α^{12} et $1/(\alpha + 1)$ dans la $\mathbb{Q}$-base $(1, \alpha, \alpha^2, \alpha^3)$ de A. En déduire le reste dans la division de $X^6 + 1$ par P.

Espaces vectoriels, applications linéaires, matrices

Exercice n°34

Soient F et G deux sous-espaces d'un espace vectoriel $\mathbb{E}$.

1) Montrer que $F \cup G$ est un sous-espace de $\mathbb{E}$ si et seulement si $F \subset G$ ou $G \subset F$.

2) En déduire que si $F \neq E$ et $G \neq E$, alors $F \cup G \neq E$.

Exercice n°35

1) Soit u un endomorphisme d'un espace vectoriel E. Montrer que si pour tout x de E, x et $u(x)$ sont colinéaires alors u est une homothétie.

2) Soient E un espace vectoriel euclidien et f une isométrie linéaire de E (i.e. un élément de $\mathcal{O}(E)$) qui commute avec toutes les autres isométries linéaires.
Montrer que f préserve toutes les droites de E. En déduire la nature de f.

Exercice n°36

On appelle projecteur d'un $\mathbb{K}$-espace vectoriel E, tout endomorphisme p de E vérifiant $p \circ p = p$. Montrer que si p est un projecteur de E alors $E = \text{Ker } p \oplus \text{Im } p$ et $\text{Im } p = \text{Ker } (id_E - p)$.
En déduire qu'en dimension finie un projecteur est toujours diagonalisable. Pouvait-on obtenir ce résultat plus rapidement ?

Exercice n°37

Soient f et g deux endomorphismes d'un $\mathbb{K}$-espace vectoriel de dimension finie E, vérifiant $f \circ g - g \circ f = id_E$.

1) Montrer que $\forall Q \in \mathbb{K}[X],\ f \circ Q(g) - Q(g) \circ f = Q'(g)$.

2) Montrer que : $\exists P \in \mathbb{K}[X],\ P \neq 0$ et $P(g) = 0$.

3) Que peut-on en déduire lorsque $\mathbb{K}$ est de caractéristique nulle ?

Exercice n°38

Montrer que deux matrices de $\mathcal{M}(n, \mathbb{R})$ semblables dans $\mathcal{M}(n, \mathbb{C})$ sont semblables dans $\mathcal{M}(n, \mathbb{R})$.

Exercice n°39

Soit $A \in \mathcal{M}(n, \mathbb{C})$ ayant toutes ses valeurs propres deux à deux distinctes.
Montrer que la famille $(I, A, A^2, \cdots, A^{n-1})$ est libre.

Exercice n°40

Soit $A \in \mathcal{M}(n, \mathbb{C})$. Montrer que tout vecteur propre de A est vecteur propre de ${}^t com\, A$ (transposée de la comatrice de A).

Polynômes d'endomorphismes - Réduction

Exercice n°41

Soit u un endomorphisme d'un espace vectoriel sur un corps K et P un polynôme annulateur de u.

1) Montrer que $E = \text{Ker } P(u)$ et que toute valeur propre de u est racine de P.

2) Montrer que si $P(0) \neq 0$ alors u est bijectif.

Exercice n°42

Soient u un endomorphisme d'un espace vectoriel sur un corps K et P, Q_1, Q_2 dans $K[X]$ tels que $P = Q_1 \times Q_2$. Montrer que $P(u) = Q_1(u) \circ Q_2(u) = Q_2(u) \circ Q_1(u)$. Montrer que si de plus Q_1 et Q_2 sont premiers entre eux, alors $\text{Ker } P(u) = \text{Ker } Q_1(u) \oplus \text{Ker } Q_2(u)$.

Exercice n°43

Soit u un endomorphisme de $\mathbb{R}^2$ tel que $\det u = 0$ et $\text{tr } (u) = 0$. Montrer que u est nilpotent. La réciproque est-elle vraie ?

Exercice n°44

Soit E un $\mathbb{K}$-ev de dimension n. Soient $u \in \mathcal{L}(E)$, P son polynôme minimal et p le plus petit exposant de X dans l'écriture de P. On suppose $p \neq 0$. Montrer que $E = \text{Im } u^p \oplus \text{Ker } u^p$. Que se passe-t-il si $p = 0$?

Exercice n°45

Soit E un $\mathbb{K}$-ev de dimension finie et $f \in \mathcal{L}(E)$. On suppose qu'il existe $P \in \mathbb{K}[X]$ tel que $P(f) = 0$ et $P'(0) \neq 0$. Montrer que $\text{Ker } f \oplus \text{Im } f = E$.