

UNIVERSITÉ MOHAMMED I
Faculté Des Sciences
Département De Mathématiques
Et Informatique
O u j d a

Polycopié des Travaux Dirigés Corrigés d'Algèbre 1
Module Mathématiques 1
Filière SMIA / Semestre 1
Préparé par le Pr. M.C. Ismaili

Année Universitaire 2011/2012

Préface

Ce recueil d'exercices d'algèbre corrigés est destiné aux étudiants et étudiantes de première année de la filière SMIA (semestre 1). On y trouvera tous les exercices d'algèbre proposés durant l'année universitaire 2011/2012 aux étudiants de la section SMIA (semestre 1); soit 4 séries d'exercices avec leur corrigé détaillé.

Série d'Algèbre n°1

Exercice 1 Soient P , Q et R des propositions mathématiques. Sachant que :

$$(P \Rightarrow Q) \Leftrightarrow (\text{non}(P) \text{ ou } Q), \text{ et que } ((P \text{ et } R) \text{ ou } (Q \text{ et } R)) \Leftrightarrow ((P \text{ ou } Q) \text{ et } R),$$

et sans utiliser de table de vérité, montrer que :

$$((\text{non}(P) \Rightarrow Q) \text{ et } R) \Leftrightarrow ((\text{non}(P) \text{ ou } \text{non}(R)) \Rightarrow (Q \text{ et } R)),$$

et

$$(P \Rightarrow (Q \Rightarrow R)) \Leftrightarrow ((P \text{ et } Q) \Rightarrow R).$$

Exercice 2 Écrire les contraposées des implications suivantes et les démontrer. i , j , n et m appartiennent à \mathbb{N} , et x et y appartiennent à \mathbb{R} :

- a) n premier $\Rightarrow (n = 2 \text{ ou } n \text{ est impair})$.
- b) $x \neq y \Rightarrow (x + 1)(y - 1) \neq (x - 1)(y + 1)$.
- c) $i + j > n + m \Rightarrow (i > n \text{ ou } j > m)$.

Exercice 3

- 1) En raisonnant par l'absurde, montrer que si un entier $q > 1$ divise l'entier $n > 0$, alors q ne divise pas $n + 1$.
- 2) On note \mathcal{P} l'ensemble des nombres premiers. Le but de cet exercice est de montrer que cet ensemble est infini.
- a) On suppose que \mathcal{P} est fini, il existe donc p_1, \dots, p_m tels que $\mathcal{P} = \{p_1, \dots, p_m\}$. Montrer que pour tout i , $1 \leq i \leq m$, p_i ne divise pas $(p_1 \cdots p_m) + 1$.
- b) Conclure.

Exercice 4 Montrer que : $\forall n \in \mathbb{N}^*$, on a :

$$(1 + 2 + \cdots + n)^2 = 1^3 + 2^3 + \cdots + n^3.$$

Exercice 5 Pour $n \in \mathbb{N}$, on définit deux propriétés :

$$P_n : 3 \text{ divise } 4^n - 1 \text{ et } Q_n : 3 \text{ divise } 4^n + 1.$$

- 1) Prouver que pour tout $n \in \mathbb{N}$, $P_n \Rightarrow P_{n+1}$ et $Q_n \Rightarrow Q_{n+1}$.
- 2) Montrer que P_n est vraie pour tout $n \in \mathbb{N}$.
- 3) Que penser, alors, de la proposition : $\exists n_0 \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow Q_n$?

Exercice 6 Soit la suite $(S_n)_{n \geq 0}$ définie par $S_0 = 1$ et pour tout entier $n \geq 0$,

$$S_{n+1} = \sum_{k=0}^n C_n^k S_k = C_n^0 S_0 + C_n^1 S_1 + \cdots + C_n^{n-1} S_{n-1} + C_n^n S_n,$$

où $C_n^k = \frac{n!}{k!(n-k)!}$.

- 1) Calculer les quatre premiers termes de cette suite.
- 2) En utilisant la récurrence forte (ou complète), montrer que, pour tout entier $n \geq 0$, on a :

$$S_n \leq n!.$$

Exercice 7 Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications et soit $h = gof$ l'application composée.

- 1) Montrer que si h est injective alors f est injective. Si, de plus, f est surjective alors g est injective.
- 2) Montrer que si h est surjective alors g est surjective. Si en outre g est injective alors f est surjective.
- 3) Dédire de ce qui précède que : il existe une application $f' : F \rightarrow E$ telle que $f'of = \text{id}_E$ et $fof' = \text{id}_F$ si et seulement si f est bijective.

Exercice 8 Tout au long de cet exercice, E et F désigneront deux ensembles non vides, $f : E \rightarrow F$ une application, A un sous-ensemble de E et B un sous-ensemble de F .

- 1) Rappeler la définition de l'image directe $f(A)$ de A par f , ainsi que la définition de l'image réciproque $f^{-1}(B)$ de B par f .

- 2) Montrer que l'application f est surjective si et seulement si $f(E) = F$.

- 3) Montrer que pour toute partie B de F , on a :

$$f(f^{-1}(B)) = B \cap f(E).$$

- 4)a) Dédire de la question précédente que si f est surjective, alors $f(f^{-1}(B)) = B$ pour toute partie B de F .

b) Supposons f non surjective ; il existe donc $y \in F$ tel que $y \notin f(E)$. Posons $B = \{y\}$. Montrer que dans ce cas $f(f^{-1}(B)) \neq B$.

- c) Conclure.

Exercice 9 Soit E un ensemble et soit A une partie de E . On définit dans l'ensemble $\mathcal{P}(E)$ des parties de E , la relation \mathcal{R} , en posant, pour tout couple (X, Y) de parties de E :

$$X\mathcal{R}Y \Leftrightarrow A \cap X = A \cap Y.$$

- 1) Montrer que \mathcal{R} est une relation d'équivalence dans $\mathcal{P}(E)$.
- 2) Soit X une partie de E . On note \overline{X} la classe d'équivalence de X pour la relation \mathcal{R} . Calculer $\overline{\emptyset}$, \overline{E} , \overline{A} , et $\overline{C_E^A}$.
- 3) Soit h définie de $\mathcal{P}(E)/\mathcal{R}$ vers $\mathcal{P}(A)$ par :

$$\forall X \subset E, h(\overline{X}) = A \cap X.$$

- a) Montrer que h est une application, puis montrer qu'elle est bijective.
- b) Donner alors le cardinal de l'ensemble quotient $\mathcal{P}(E)/\mathcal{R}$ en fonction du cardinal de A .

Corrigé de la Série d'Algèbre n°1

Exercice 1 Soient P, Q, R trois propositions logiques. Sans utiliser la table de vérité et en utilisant les propositions suivantes :

$$(P \Rightarrow Q) \Longleftrightarrow ((\text{non } (P) \text{ ou } Q) \text{ et } (P \text{ et } R) \text{ ou } (Q \text{ et } R)) \Longleftrightarrow (((P \text{ ou } Q) \text{ et } R).$$

Nous montrons

I. $((\text{non } (P) \Rightarrow Q) \text{ et } R) \Longleftrightarrow ((\text{non } (P) \text{ ou } \text{non } (R)) \Rightarrow (Q \text{ et } R))$

II. $(P \Rightarrow (Q \Rightarrow R)) \Longleftrightarrow ((P \text{ et } Q) \Rightarrow R).$

I.

$$((\text{non } (P) \text{ ou } \text{non } (R)) \Rightarrow (Q \text{ et } R))$$

$$\Updownarrow$$

$$\text{non } ((\text{non } (P) \text{ ou } \text{non } (R)) \text{ ou } (Q \text{ et } R))$$

$$\Updownarrow$$

$$(P \text{ et } R) \text{ ou } (Q \text{ et } R)$$

$$\Updownarrow$$

$$(P \text{ ou } Q) \text{ et } R$$

$$\Updownarrow$$

$$(\text{non } (\text{non } (P)) \text{ ou } Q) \text{ et } R$$

$$\Updownarrow$$

$$((\text{non } (P) \Rightarrow Q) \text{ et } R)$$

II.

$$((P \text{ et } Q) \Rightarrow R)$$

$$\Updownarrow$$

$$(\text{non } (P \text{ et } Q) \text{ ou } R)$$

$$\Updownarrow$$

$$\text{non } (P) \text{ ou } (\text{non } (Q) \text{ ou } R)$$

$$\Updownarrow$$

$$\text{non } (P) \text{ ou } (Q \Rightarrow R)$$

$$\Updownarrow$$

$$P \Rightarrow (Q \Rightarrow R)$$

Exercice 2 Soient i, j, n et m appartenant à \mathbb{N} et x et y des nombres réels :

- a) ($n \neq 2$ et n est pair) $\Rightarrow n$ est non premier. En effet, si n est pair alors $n = 0$, ou n est de la forme $n = 2k$ avec $k \geq 2$, auquel cas, n admettra au moins trois diviseurs ; 1, 2 et n , donc dans tous les cas n n'est pas un nombre premier.
- b) $(x+1)(y-1) = (x-1)(y+1) \Rightarrow x = y$.
 $(x+1)(y-1) = (x-1)(y+1) \Rightarrow xy - x + y - 1 = xy + x - y - 1 \Rightarrow 2x = 2y \Rightarrow x = y$, d'où le résultat.
- c) ($i \leq n$ et $j \leq m$) $\Rightarrow i + j \leq n + m$. En effet : ($i \leq n$ et $j \leq m$) $\Rightarrow i + j \leq n + j \leq n + m$.

Exercice 3

- 1) Supposons que l'entier $q > 1$ divise l'entier $n > 0$, et que q divise aussi $n + 1$, alors q divisera $n + 1 - n = 1$; absurde, car $q > 1$.
- 2) On note \mathcal{P} l'ensemble des nombres premiers. Le but de cet exercice est de montrer que cet ensemble est infini.
- a) Pour tout $i, 1 \leq i \leq m, p_i$ divise $q = p_1 \cdots p_m$ et d'après la question précédente, p_i ne divise pas $q + 1 = (p_1 \cdots p_m) + 1$.
- b) L'entier $(p_1 \cdots p_m) + 1$ n'est divisible par aucun des nombres premiers p_i , Il est donc lui même un nombre premier différent de chaque p_i . Ce qui est absurde.
- Il existe donc une infinité de nombres premiers.

Exercice 4 Il est facile de vérifier la propriété pour $n = 1$. Soit $n \geq 1$ et supposons la propriété vraie à l'ordre n , alors

$$(1 + 2 + \cdots + n + n + 1)^2 = (1 + 2 + \cdots + n)^2 + 2(n + 1)(1 + 2 + \cdots + n) + (n + 1)^2 =$$

$$(1 + 2 + \cdots + n)^2 + (n + 1)[n(n + 1) + (n + 1)] = (1 + 2 + \cdots + n)^2 + (n + 1)(n + 1)^2 = 1^3 + 2^3 + \cdots + n^3 + (n + 1)^3,$$

à cause de l'hypothèse de récurrence et du fait que $1 + 2 + \cdots + n = \frac{n(n + 1)}{2}$. Ainsi, $\forall n \in \mathbb{N}^*$, on a :

$$(1 + 2 + \cdots + n)^2 = 1^3 + 2^3 + \cdots + n^3.$$

Exercice 5 Pour $n \in \mathbb{N}$, on définit deux propriétés :

$$P_n : 3 \text{ divise } 4^n - 1 \text{ et } Q_n : 3 \text{ divise } 4^n + 1.$$

- 1) Soit $n \in \mathbb{N}$, alors $4^{n+1} - 1 = 4 \cdot 4^n - 1 = 3 \cdot 4^n + 4^n - 1$, donc si 3 divise $4^n - 1$, alors 3 divise $4^{n+1} - 1$, cela signifie que pour tout $n \in \mathbb{N}$, $P_n \Rightarrow P_{n+1}$. Le même raisonnement permet de montrer que $Q_n \Rightarrow Q_{n+1}$.
- 2) P_0 est vraie puisque 3 divise $4^0 - 1 = 0$. Dans la question précédente on a montré que $P_n \Rightarrow P_{n+1}$, donc si on suppose que P_n est vraie, alors P_{n+1} est aussi vraie. Ainsi, P_n est vraie pour tout $n \in \mathbb{N}$.
- 3) Cette proposition est fausse, car sinon, s'il existe $n_0 \in \mathbb{N}$ tel que $\forall n \in \mathbb{N}, n \geq n_0 \Rightarrow Q_n$, alors pour tout $n \geq n_0$ on aura P_n et Q_n sont vraies, c'est-à-dire que pour tout $n \geq n_0$:

$$3 \text{ divise } 4^n - 1 \text{ et } 3 \text{ divise } 4^n + 1.$$

Donc 3 divisera $4^n + 1 - (4^n - 1) = 2$, est ceci est impossible.

Exercice 6 Soit la suite $(S_n)_{n \geq 0}$ définie par $S_0 = 1$ et pour tout entier $n \geq 0$,

$$S_{n+1} = \sum_{k=0}^n C_n^k S_k = C_n^0 S_0 + C_n^1 S_1 + \cdots + C_n^{n-1} S_{n-1} + C_n^n S_n,$$

où $C_n^k = \frac{n!}{k!(n-k)!}$.

- 1) $S_0 = 1, S_1 = C_0^0 S_0 = 1, S_2 = C_1^0 S_0 + C_1^1 S_1 = 2$ et $S_3 = C_2^0 S_0 + C_2^1 S_1 + C_2^2 S_2 = 5$.
- 2) Il est clair que les quatre premiers termes de la suite vérifient la propriété demandée.
- Soit $n \in \mathbb{N}$, et supposons que pour tout entier $k \leq n$ on a : $S_k \leq k!$, alors

$$S_{n+1} = \sum_{k=0}^n C_n^k S_k \leq \sum_{k=0}^n C_n^k k! = \sum_{k=0}^n \frac{n!}{(n-k)!} = n! \sum_{k=0}^n \frac{1}{(n-k)!} \leq n!(n+1) = (n+1)!,$$

d'où le résultat.

Exercice 7 Soient $f : E \rightarrow F$ et $g : F \rightarrow G$ deux applications et soit $h = g \circ f$ l'application composée.

1) Soient x et y deux éléments de E tels que $f(x) = f(y)$. Comme g est une application, alors $g(f(x)) = g(f(y))$, donc $h(x) = h(y)$, et comme h est injective alors $x = y$, donc f est injective.

Soient z et t deux éléments de F tels que $g(z) = g(t)$. Comme f est surjective, alors il existe x et y deux éléments de E tels que $z = f(x)$ et $t = f(y)$, par suite, $g(z) = g(f(x)) = g(t) = g(f(y))$, c'est-à-dire que $h(x) = h(y)$, et comme h est injective, alors $x = y$, d'où $z = f(x) = f(y) = t$. Ainsi, g est injective.

2) Soit $y \in G$. Comme h est surjective, il existe $x \in E$ tel que $y = h(x) = g(f(x))$ donc $f(x)$ est un antécédent de y par g , d'où g est surjective.

Soit $z \in F$, alors $g(z) \in G$, et comme h est surjective, il existe $x \in E$ tel que $g(z) = h(x) = g(f(x))$, et puisque g est injective alors $z = f(x)$, cela signifie que f est surjective.

3) S'il existe une application $f' : F \rightarrow E$ telle que $f' \circ f = \text{id}_E$ et $f \circ f' = \text{id}_F$, alors comme id_E est injective f est injective d'après la question 1, et comme id_F est surjective, alors f l'est aussi à cause de la question 2. Ainsi, f est bijective.

Inversement, si f est bijective, on sait que son application réciproque $f' = f^{-1}$ vérifie les propriétés demandées.

Exercice 8 1) Par définition l'image directe de la partie A par f est $f(A) = \{f(x), x \in A\}$ et que l'image réciproque de la partie B par f est

$$f^{-1}(B) = \{x \in E \text{ tel que } f(x) \in B\}.$$

2) Dire que f est surjective c'est équivalent à dire que pour tout y dans F l'équation $f(x) = y$ possède au moins une solution en x dans E c-à-d pour tout $y \in F$ il existe $x \in E$ tel que $y = f(x)$, ce qui est équivalent à $\forall y \in F, y \in f(E)$ ou encore équivalent à $F = f(E)$.

3) Soit B une partie de F , soit $y \in f(f^{-1}(B))$, alors $\exists x \in f^{-1}(B)$ tel que $f(x) = y$ ce qui montre que $y \in f(E)$ et comme $x \in f^{-1}(B)$, $y = f(x) \in B$ donc $y \in B \cap f(E)$. Inversement soit $y \in B \cap f(E)$, alors $y \in B$ et $\exists x \in E$ tel que $y = f(x)$, par suite $x \in f^{-1}(B)$ et $y = f(x) \in f(f^{-1}(B))$. D'où l'égalité $f(f^{-1}(B)) = B \cap f(E)$.

4) a) Si f est surjective alors $f(E) = F$, donc d'après 3) $f(f^{-1}(B)) = B \cap f(E) = B \cap F = B$.

b) Supposons que f est non surjective, donc il existe $y \in F$ tel que $y \neq f(x) \forall x \in E$, posons $B = \{y\}$, donc l'image réciproque $f^{-1}(B)$ de B par f est \emptyset , par suite l'image directe de $f^{-1}(B)$ par f est $f(f^{-1}(B)) = \emptyset \neq B$.

c) Par contraposée, l'implication en b) montre que si $f(f^{-1}(B)) = B$ pour toute partie B de F , alors f est surjective. Donc d'après a) on a l'équivalence que f est surjective si et seulement si $f(f^{-1}(B)) = B \forall B, B$ partie de F .

Exercice 9 Soit E un ensemble et soit A une partie de E . On définit dans l'ensemble $\mathcal{P}(E)$ des parties de E , la relation \mathcal{R} , en posant, pour tout couple (X, Y) de parties de E :

$$X\mathcal{R}Y \Leftrightarrow A \cap X = A \cap Y.$$

1) Pour toute partie X de E on a $A \cap X = A \cap X$, d'où $X\mathcal{R}X$, donc \mathcal{R} est réflexive.

Si X et Y sont deux parties de E on a : $X\mathcal{R}Y \Leftrightarrow A \cap X = A \cap Y \Rightarrow A \cap Y = A \cap X \Rightarrow Y\mathcal{R}X$. Donc \mathcal{R} est symétrique.

Si X, Y et Z sont trois parties de E , telles que $X\mathcal{R}Y$ et $Y\mathcal{R}Z$, alors $A \cap X = A \cap Y$ et $A \cap Y = A \cap Z$, d'où $A \cap X = A \cap Z$, donc $X\mathcal{R}Z$, c-à-d. que \mathcal{R} est transitive. Ainsi, \mathcal{R} est une relation d'équivalence dans $\mathcal{P}(E)$.

2) Soit X une partie de E . On note \overline{X} la classe d'équivalence de X pour la relation \mathcal{R} .

\emptyset est, par définition d'une classe d'équivalence, l'ensemble des parties Y de E qui vérifient l'égalité $A \cap \emptyset = A \cap Y$. Comme $A \cap \emptyset$ est vide, \emptyset est l'ensemble des parties Y de E vérifiant $A \cap Y = \emptyset$. Or $A \cap Y = \emptyset$ est équivalent à $Y \subset C_E^A$. Donc \emptyset est l'ensemble $\mathcal{P}(C_E^A)$ des parties du complémentaire de A dans E .

\overline{E} est l'ensemble des parties Y de E qui vérifient l'égalité $A \cap E = A \cap Y$. Comme $A \cap E$ est égal à A ,

et comme les parties Y de E qui vérifient $A = A \cap Y$ sont les parties qui contiennent A , \overline{E} est donc l'ensemble des parties Y de E qui contiennent A .

\overline{A} est l'ensemble des parties Y de E qui vérifient l'égalité $A \cap A = A \cap Y$. Comme $A \cap A$ est égal à A , et comme les parties Y de E qui vérifient $A = A \cap Y$ sont les parties qui contiennent A , \overline{E} est l'ensemble des parties Y de E qui contiennent A , c'est \overline{E} .

$\overline{C_E^A}$ est l'ensemble des parties Y de E qui vérifient l'égalité $A \cap C_E^A = A \cap Y$. Comme $A \cap C_E^A$ est vide, et comme les parties Y de E qui vérifient $\emptyset = A \cap Y$ sont les parties contenues dans C_E^A , $\overline{C_E^A}$ est donc l'ensemble des parties Y de E qui ne rencontrent pas A , c'est l'ensemble $\mathcal{P}(C_E^A) = \overline{\emptyset}$.

3) Soit h définie de $\mathcal{P}(E)/\mathcal{R}$ vers $\mathcal{P}(A)$ par :

$$\forall X \subset E, \quad h(\overline{X}) = A \cap X.$$

a) Soient X et Y sont deux parties de E , alors d'après les propriétés fondamentales des classes d'équivalence, on a :

$$\overline{X} = \overline{Y} \Leftrightarrow X \mathcal{R} Y \Leftrightarrow A \cap X = A \cap Y \Leftrightarrow h(\overline{X}) = h(\overline{Y}).$$

Ainsi, on vient de montrer que h est une application et qu'elle est injective

Pour toute partie B de A , on a $B = A \cap B$, car $B \subset A$, d'où $B = A \cap B = h(\overline{B})$. Donc h est surjective.

Ainsi, h est bijective.

b) Comme h est une bijection de $\mathcal{P}(E)/\mathcal{R}$ vers $\mathcal{P}(A)$, ces deux ensembles sont équipotents. Ils ont donc le même cardinal. Ainsi :

$$\text{Card}(\mathcal{P}(E)/\mathcal{R}) = \text{Card}(\mathcal{P}(A)) = 2^{\text{Card}(A)}.$$

Série d'Algèbre n°2

Exercice 1 Soit $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$. On définit sur l'ensemble produit cartésien $E \times E$ la relation \mathcal{R} :

$$(p, q)\mathcal{R}(p', q') \Leftrightarrow (p - p' \text{ est pair et } q - q' \text{ est divisible par } 3).$$

- 1) Montrer que \mathcal{R} une relation d'équivalence sur $E \times E$.
- 2) On désigne par $\overline{(p, q)}$ la classe d'équivalence de (p, q) .
- a) Calculer le nombre d'éléments des classes suivantes : $\overline{(1, 1)}$, $\overline{(1, 2)}$ et $\overline{(1, 3)}$.
- b) Soit $q \in E$. Montrer que si $(x, y) \in \overline{(1, q)}$ alors $(x + 1, y) \in \overline{(2, q)}$.
- 3) En déduire une bijection de $\overline{(1, q)}$ vers $\overline{(2, q)}$.

Exercice 2 Dire si les relations suivantes sont réflexives, symétriques, antisymétriques, transitives :

- i) $E = \mathbb{N}$ et $x\mathcal{R}y \Leftrightarrow x = -y$.
- ii) $E = \mathbb{R}$ et $x\mathcal{R}y \Leftrightarrow \cos^2 x + \sin^2 y = 1$.
- iii) $E = \mathbb{N}$ et $x\mathcal{R}y \Leftrightarrow \exists p, q \geq 1, y = px^q$ (p et q sont des entiers).

Quelles sont parmi les exemples précédents les relations d'ordre et les relations d'équivalence ? Dans les cas où \mathcal{R} est une relation d'équivalence, calculer la classe d'équivalence de 0.

Exercice 3 Soit E un ensemble et soit A une partie de E . On désigne par χ_A l'application :

$$\chi_A : E \longrightarrow \{0, 1\}; \quad \chi_A(x) = 1 \text{ si } x \in A \text{ et } \chi_A(x) = 0 \text{ si } x \in E - A.$$

- 1) Montrer que l'application : $A \mapsto \chi_A$ est une bijection entre $\mathcal{P}(E)$ et $\{0, 1\}^E$, puis en déduire que $\text{Card}(\mathcal{P}(E)) = 2^{\text{Card}(E)}$.
- 2) On suppose que E et F sont deux ensembles finis non vides. Quel est le nombre de relations binaires qu'on peut définir de E vers F ?

Exercice 4 Soit n un entier naturel, soit $E_n = \{k \in \mathbb{N} \mid \frac{k(k+3)}{2} \geq n\}$, et soit m le plus petit élément de E_n .

- 1) Montrer que :

$$\frac{m(m+1)}{2} \leq n \leq \frac{m(m+3)}{2}.$$

- 2) Montrer que l'application :

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \times \mathbb{N} \\ n &\longmapsto \left(n - \frac{m(m+1)}{2}, \frac{m(m+3)}{2} - n\right) \end{aligned}$$

(où m est le plus petit élément de E_n) est bijective. Ainsi, $\mathbb{N} \times \mathbb{N}$ est dénombrable.

- 3) Construire une surjection de $\mathbb{N} \times \mathbb{N}^*$ dans \mathbb{Q} et en déduire que \mathbb{Q} est dénombrable.

Exercice 5 Soit n un entier naturel non nul.

- 1) Montrer que $\forall 1 \leq m \leq n$ on a : $C_n^m = C_{n-1}^{m-1} + C_{n-1}^m$ (propriété du triangle de Pascal).

2) Montrer par récurrence sur n que :

$$C_p^p + C_{p+1}^p + \cdots + C_n^p = C_{n+1}^{p+1}.$$

3)a) En déduire que :

$$\sum_{q=p}^n q(q-1) \cdots (q-p+1) = \frac{1}{p+1} (n+1)n(n-1) \cdots (n-p+1).$$

b) Retrouver ainsi les sommes $S_m = \sum_{q=1}^n q^m$ pour $m = 1, 2, 3$.

Exercice 6 Soit φ une application de \mathbb{R}^* dans \mathbb{R} . On définit sur l'ensemble $G = \mathbb{R}^* \times \mathbb{R}$ la loi de composition interne \star par :

$$\forall (a, b) \in G, \forall (c, d) \in G : (a, b) \star (c, d) = (ac, bc + \varphi(a)d).$$

- 1) Montrer que la loi \star est associative si et seulement si $\forall a, c \in \mathbb{R}^*, \varphi(ac) = \varphi(a)\varphi(c)$.
- 2)a) Montrer que si $\varphi(1) = 1$, alors la loi \star admet un élément neutre que l'on déterminera.
- b) Inversement, si la loi \star admet un élément neutre, est-ce que $\varphi(1) = 1$?

3) On suppose que l'application φ vérifie :
$$\begin{cases} \forall a, c \in \mathbb{R}^*, \varphi(ac) = \varphi(a)\varphi(c), \\ \varphi(1) = 1. \end{cases}$$

Montrer que tout élément $(a, b) \in G$ admet un symétrique pour la loi \star que l'on déterminera, puis en déduire que (G, \star) est un groupe.

4) Donner un exemple simple d'application φ tel que (G, \star) est un groupe.

Exercice 7 Soit (G, \cdot) un groupe fini de cardinal $2n$ ($n \geq 2$), d'élément neutre e et possédant 2 sous-groupes H et H' tels que :

$$\text{Card}(H) = \text{Card}(H') = n$$

et

$$H \cap H' = \{e\}.$$

- 1) Montrer que $G - (H \cup H')$ est un singleton, noté $\{a\}$.
- 2) Soit $h \in H - \{e\}$, montrer que $hH' \subset \{h, a\}$, en déduire que $hH' = \{h, a\}$ puis que $n = 2$. On rappelle que $hH' = \{hk \mid k \in H'\}$.
- 3) On écrit $G = \{e, a, h, h'\}$, donner la table de multiplication de G .

Exercice 8 Soient (G_1, \cdot) et (G_2, \star) deux groupes et $f : G_1 \rightarrow G_2$ un homomorphisme. Soit \mathcal{R} la relation d'équivalence associée à f , définie sur G_1 par : $\forall x, y \in G_1, x\mathcal{R}y \Leftrightarrow f(x) = f(y)$.

- 1) Montrer que $\ker f$ est un sous-groupe de G_1 et $\text{Im } f$ est un sous-groupe de G_2 .
 - 2) Montrer que la relation \mathcal{R} est compatible avec la loi de G_1 .
 - 3) Pour tous $x, y \in G_1$ on pose $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$, où \bar{x} désigne la classe de x modulo \mathcal{R} .
 - a) Montrer qu'on définit ainsi une loi de composition interne sur l'ensemble quotient G_1/\mathcal{R} (montrer que \cdot est bien définie).
 - b) Montrer que $(G_1/\mathcal{R}, \cdot)$ est un groupe.
 - 4) Montrer qu'il existe un isomorphisme entre les groupes $(G_1/\mathcal{R}, \cdot)$ et $(\text{Im } f, \star)$.
- Indication : penser à la décomposition canonique de f en tant qu'application.
- 5) Donner une autre façon de définir la relation \mathcal{R} moyennant $\ker f$.

Corrigé de la Série d'Algèbre n°2

Exercice 1 Soit $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$. On définit sur l'ensemble produit cartésien $E \times E$ la relation \mathcal{R} :

$$(p, q)\mathcal{R}(p', q') \Leftrightarrow (p - p' \text{ est pair et } q - q' \text{ est divisible par } 3).$$

- 1) ★ Soient p et q dans E , alors $p - p = 0$ est pair et $q - q = 0$ est divisible par 3, donc $(p, q)\mathcal{R}(p, q)$, c'est-à-dire que la relation \mathcal{R} est réflexive.
- ★ $(p - p' \text{ est pair et } q - q' \text{ est divisible par } 3) \Rightarrow (p' - p = -(p - p') \text{ est pair et } q' - q = -(q - q') \text{ est divisible par } 3)$, donc $(p, q)\mathcal{R}(p', q') \Rightarrow (p', q')\mathcal{R}(p, q)$. Ainsi, \mathcal{R} est symétrique.
- ★ $[(p, q)\mathcal{R}(p', q') \text{ et } (p', q')\mathcal{R}(p'', q'')] \Rightarrow [(p - p' \text{ est pair et } q - q' \text{ est divisible par } 3 \text{ et } (p' - p'') \text{ est pair et } q' - q'' \text{ est divisible par } 3] \Rightarrow (p - p'' = p - p' + p' - p'' \text{ est pair et } q - q'' = q - q' + q' - q'' \text{ est divisible par } 3 \Rightarrow (p, q)\mathcal{R}(p'', q'')$, donc \mathcal{R} est transitive. Enfin, \mathcal{R} une relation d'équivalence sur $E \times E$.
- 2) On désigne par $\overline{(p, q)}$ la classe d'équivalence de (p, q) .
- a) $(p, q) \in \overline{(1, 1)} \Leftrightarrow (p, q)\mathcal{R}(1, 1) \Leftrightarrow (p - 1 \text{ est pair et } q - 1 \text{ est divisible par } 3) \Leftrightarrow (p \text{ est impair et } q \text{ est de la forme } 3k + 1) \Leftrightarrow p \in \{1, 3, 5, 7\} \text{ et } q \in \{1, 4, 7\}$. Donc le nombre d'éléments de la classe $\overline{(1, 1)}$ est $4 \cdot 3 = 12$.
- $(p, q) \in \overline{(1, 2)} \Leftrightarrow (p, q)\mathcal{R}(1, 2) \Leftrightarrow (p - 1 \text{ est pair et } q - 2 \text{ est divisible par } 3) \Leftrightarrow (p \text{ est impair et } q \text{ est de la forme } 3k + 2) \Leftrightarrow p \in \{1, 3, 5, 7\} \text{ et } q \in \{2, 5, 8\}$. Donc le nombre d'éléments de la classe $\overline{(1, 2)}$ est $4 \cdot 3 = 12$.
- $(p, q) \in \overline{(1, 3)} \Leftrightarrow (p, q)\mathcal{R}(1, 3) \Leftrightarrow (p - 1 \text{ est pair et } q - 3 \text{ est divisible par } 3) \Leftrightarrow (p \text{ est impair et } q \text{ est divisible par } 3) \Leftrightarrow p \in \{1, 3, 5, 7\} \text{ et } q \in \{3, 6\}$. Donc le nombre d'éléments de la classe $\overline{(1, 3)}$ est $4 \cdot 2 = 8$.
- b) Soit $q \in E$. On sait que $(x, y) \in \overline{(1, q)} \Leftrightarrow (x - 1 \text{ est pair et } y - q \text{ est divisible par } 3)$. On en déduit alors que x est impair, donc $x \in \{1, 3, 5, 7\}$, par suite, $x + 1 \in \{2, 4, 6, 8\}$, cela implique que $(x + 1, y) \in E \times E$, et comme $x - 1$ est pair implique que $x + 1 - 2 = x - 1$ est pair, alors $(x, y) \in \overline{(1, q)} \Rightarrow (x + 1, y) \in \overline{(2, q)}$.
- 3) La bijection de $\overline{(1, q)}$ vers $\overline{(2, q)}$ en question n'est rien d'autre que l'application $f : (x, y) \mapsto (x + 1, y)$, qui est injective de façon évidente. Le fait que f est surjective vient du fait que si (x', y) est dans la classe $\overline{(2, q)}$, alors $x' - 2$ est pair, donc $x' \in \{2, 4, 6, 8\}$, d'où $x' - 1 \in \{1, 3, 5, 7\}$ et $(x' - 1, y) \in \overline{(1, q)}$. De plus, on peut facilement vérifier que $(x', y) = f(x' - 1, y)$, c'est-à-dire que f est surjective, donc bijective.

Exercice 2 i) Sur \mathbb{N} la relation $x\mathcal{R}y \Leftrightarrow x = -y$ n'est pas réflexive car par exemple $1 \neq -1$ dans \mathbb{N} , mais elle est symétrique car si $x = -y$ dans \mathbb{N} alors $y = -x = 0$ dans \mathbb{N} . Cette relation est aussi antisymétrique.

Pour la transitivité, soit $x, y, z \in \mathbb{N}$ telle que $x = -y$ et $y = -z$ alors a-t-on $x = -z$? la réponse est oui car dans \mathbb{N} on a $a = -b$ implique $a = b = 0$, donc $x = y = z = -z = 0$ et \mathcal{R} est transitive. Conclusion : la relation \mathcal{R} n'est ni d'équivalence ni d'ordre par le fait que \mathcal{R} n'est réflexive.

ii) Soit $E = \mathbb{R}$ et \mathcal{R} la relation définie par $x\mathcal{R}y \Leftrightarrow \cos^2 x + \sin^2 y = 1$. Cette relation est réflexive par la formule bien connue $\cos^2 x + \sin^2 x = 1$ pour tout $x \in \mathbb{R}$. Remarquons que $(\cos^2 x + \sin^2 y = 1) \Leftrightarrow \cos^2 x + (1 - \cos^2 y) = 1 \Leftrightarrow \cos^2 x = \cos^2 y$, c'est donc $x\mathcal{R}y \Leftrightarrow \cos^2 x = \cos^2 y$ ce qui montre clairement que \mathcal{R} est une relation d'équivalence. Mais pas d'ordre car par exemple pour $y = x + 2\pi$ on a bien $\cos^2 x = \cos^2 y$ c-à-d $x\mathcal{R}y$ et $y\mathcal{R}x$ mais $y \neq x$. La classe de 0 est $\bar{0} = \{x \in E, \text{ tel que } \cos^2 x = \cos^2 0 = 1\} = \{k\pi, k \in \mathbb{Z}\}$.

iii) Soit $E = \mathbb{N}$ et la relation sur E définie par $x\mathcal{R}y \Leftrightarrow \exists p, q \geq 1$ tel que : $y = px^q$. La réflexivité : soit $p = q = 1$, alors $\forall x \in E$, $x = 1x^1$, donc $\exists p, q \geq 1$ tel que : $y = px^q$, par suite $x\mathcal{R}x \forall x \in E$. La symétrie : soit $x, y \in E$ tel que : $\exists p, q \geq 1$ tel que : $y = px^q$, comme $p, q \geq 1$ alors x divise y , donc de même une écriture de type $x = p'y^{q'}$ avec $p', q' \geq 1$ on aura y divise x ceci montre que \mathcal{R} est

antisymétrique mais non symétrique comme le montre le contre exemple $x = 2$ et $y = 4$ on a bien $x\mathcal{R}y$ mais pas $y\mathcal{R}x$. La transitivité : $x\mathcal{R}y$ et $y\mathcal{R}z$ implique $\exists p, q, p', q' \geq 1$ tel que : $y = px^q$ et $z = p'y^{q'}$, par substitution on obtient donc $z = p'(px^q)^{q'}$ c'est donc z est de la forme $z = mx^n$ où $m, n \geq 1$, autrement dit $x\mathcal{R}z$. La relation \mathcal{R} est une relation d'ordre mais pas d'équivalence.

Exercice 3 Soit E un ensemble. Pour chaque partie A de E soit χ_A la fonction indicatrice associée à A , à savoir la fonction définie par :

$$\begin{aligned}\chi_A : E &\rightarrow \{0, 1\} \\ x &\mapsto 1 \text{ si } x \in A \text{ et } 0 \text{ sinon}\end{aligned}$$

1) Soit $\{0, 1\}^E$ l'ensemble des applications de E dans $\{0, 1\}$. Montrons que l'application χ définie par :

$$\begin{aligned}\chi : \mathcal{P}(E) &\rightarrow \{0, 1\}^E \\ A &\mapsto \chi(A) = \chi_A\end{aligned}$$

est bijective.

L'injection : soit $A, B \in \mathcal{P}(E)$ tel que $\chi(A) = \chi(B)$, donc $\chi_A = \chi_B$, par suite $\forall x \in A$, $\chi_A(x) = \chi_B(x) = 1$, ainsi $A \subset B$. Le rôle symétrique que joue A et B permet de conclure que $B \subset A$, d'où l'égalité $A = B$ et que χ est injective.

La surjection : Soit $f \in \{0, 1\}^E$, posons $A = f^{-1}(\{1\})$ l'image réciproque de $\{1\}$ par f . Montrons alors que $f = \chi(A) = \chi_A$. Les deux applications ont même ensemble de départ et même ensemble d'arrivée, donc pour conclure l'égalité $f = \chi_A$ il suffit de montrer que $f(x) = \chi_A(x) \forall x \in E$. Soit $x \in E$, si $x \in A = f^{-1}(\{1\})$ alors $f(x) = 1 = \chi_A(x)$, sinon (c-à-d $x \notin A$), on a $f(x) = 0 = \chi_A(x)$. d'où $f = \chi_A$ et que χ est surjective.

Comme $\text{card}(\{0, 1\}^E) = \text{card}(\{0, 1\})^{\text{card}(E)} = 2^{\text{card}(E)}$ et que $\mathcal{P}(E)$ est équipotent à $\{0, 1\}^E$ par χ , on conclut que $\text{card}(\mathcal{P}(E)) = 2^{\text{card}(E)}$.

2) Soient E et F deux ensembles finis, donc $\text{card}(E \times F)$ est fini égal $\text{card}(E) \cdot \text{card}(F)$. Comme la donnée d'une relation binaire de E vers F est équivalent par définition à la donnée d'une partie (dite graphe de cette relation) de $E \times F$ on tire d'après 1) le nombre de ces relations est $\text{card}(\mathcal{P}(E \times F)) = 2^{\text{card}(E \times F)} = 2^{\text{card}(E) \cdot \text{card}(F)}$.

Exercice 4 Soit n un entier et $E_n = \{k \in \mathbb{N} \mid \frac{k(k+3)}{2} \geq n\}$. Soit m le plus petit élément de E_n .

I. Puisque m est le plus petit élément de E_n , donc l'inégalité

$$\frac{m(m+3)}{2} \geq n$$

est vérifiée.

Montrons l'autre inégalité, puisque m est le plus petit élément de E_n , donc $m-1$ n'appartient pas E_n et

$$\frac{(m-1)(m+2)}{2} < n.$$

Puisque

$$\frac{(m-1)(m+2)}{2} = \frac{m^2 + m - 2}{2} = \frac{m^2 + m}{2} - 1 < n.$$

Alors

$$\frac{m^2 + m}{2} - 1 + 1 = \frac{m^2 + m}{2} = \frac{m(m+1)}{2} \leq n.$$

L'autre inégalité est donc vérifiée. Nous avons donc

$$\frac{m(m+1)}{2} \leq n \leq \frac{m(m+3)}{2}.$$

- II. Soit $n \in \mathbb{N}$, d'après 1) il existe un unique m et par suite un unique couple $(x, y) \in \mathbb{N} \times \mathbb{N}$ tel $x = n - \frac{m(m+1)}{2} \in \mathbb{N}$ et $y = \frac{m(m+3)}{2} - n$. Donc l'application f est bien définie. Montrons qu'elle est bijective, Soit (x, y) un couple d'entiers de $\mathbb{N} \times \mathbb{N}$. Existe-il n et m dans \mathbb{N} tels que tel que $x = n - \frac{m(m+1)}{2}$ et $y = \frac{m(m+3)}{2} - n$? On doit donc résoudre dans \mathbb{N} le système suivant :

$$\begin{cases} x = n - \frac{m(m+1)}{2} \\ y = \frac{m(m+3)}{2} - n \end{cases}$$

où n et m sont les inconnues. La somme de la première et la deuxième équation nous donne $m = x + y$. De la première équation on tire aisément que $n = x + \frac{(x+y)(x+y+1)}{2}$. On vérifie facilement que la deuxième équation est satisfaite. Comme x et y sont des entiers positifs, on en déduit que les solutions trouvées n et m le sont aussi. Il en découle que :

$$\frac{m(m+1)}{2} \leq n \leq \frac{m(m+3)}{2}.$$

Cela signifie exactement que m est le plus petit élément de E_n et donc que $(x, y) = f(n)$. Ainsi, f est surjective. Pour l'injectivité, soit n et n' de \mathbb{N} tels que $f(n) = f(n')$, c'est à dire

$$n - \frac{m(m+1)}{2} = n' - \frac{m'(m'+1)}{2}$$

et

$$\frac{m(m+3)}{2} - n = \frac{m'(m'+3)}{2} - n'.$$

Donc, en faisant la somme des deux dernières égalités nous obtenons $m = m'$ et par suite $n = n'$. Donc f est injective. finalement f est une bijection. Ainsi $\mathbb{N} \times \mathbb{N}$ est dénombrable.

- III. Nous considérons l'application g de $\mathbb{N} \times \mathbb{N}^*$ dans \mathbb{Q} qui au couple $(2p, q)$ fait correspondre la fraction $\frac{p}{q}$, et au couple $(2p+1, q)$ fait correspondre la fraction $-\frac{p}{q}$. C'est une application surjective. Donc $\mathbb{Q} = g(\mathbb{N} \times \mathbb{N}^*)$ est un ensemble dénombrable car c'est l'image d'un dénombrable par une application surjective.

Exercice 5 Soit n un entier naturel non nul.

- I. Montrons que $\forall 1 \leq m \leq n: C_n^m = C_{n-1}^{m-1} + C_{n-1}^m$

$$\begin{aligned} C_{n-1}^{m-1} + C_{n-1}^m &= \frac{(n-1)!}{(n-m)!(m-1)!} + \frac{(n-1)!}{(n-1-m)!m!} \\ &= \frac{(n-1)!}{(n-m-1)!(m-1)!} \left[\frac{1}{n-m} + \frac{1}{m} \right] \\ &= \frac{(n-1)!}{(n-m-1)!(m-1)!} \left[\frac{n}{m(n-m)} \right] \\ &= \frac{n!}{(n-m)!m!} = C_n^m. \end{aligned}$$

- II. Montrons par récurrence sur n que :

$$C_p^p + C_{p+1}^p + \dots + C_n^p = C_{n+1}^{p+1}.$$

Pour $n = 0$, $C_0^0 = C_1^1$. Donc la proposition à démontrer est vraie pour $n = 0$. Supposons qu'elle est vraie pour l'ordre n , c'est à dire que

$$C_p^p + C_{p+1}^p + \dots + C_n^p = C_{n+1}^{p+1},$$

et montrons qu'elle est vraie pour $n+1$.

$$\begin{aligned} C_p^p + C_{p+1}^p + \dots + C_n^p + C_{n+1}^p &= C_{n+1}^{p+1} + C_{n+1}^p \\ &= C_{n+2}^{p+1}. \end{aligned}$$

La proposition est donc vraie pour l'ordre $n+1$.

III. (1) Puisque

$$\begin{aligned} C_p^p + C_{p+1}^p + \dots + C_n^p &= \sum_{q=p}^n C_q^p \\ &= \sum_{q=p}^n \frac{q!}{p!(n-p)!} \\ &= \frac{1}{p!} \sum_{q=p}^n \frac{q!}{(n-p)!} \\ &= \frac{1}{p!} \sum_{q=p}^n q(q-1)\dots(q-p+1), \end{aligned}$$

et

$$\begin{aligned} C_{n+1}^{p+1} &= \frac{(n+1)!}{(p+1)!(n-p)!} \\ &= \frac{1}{p!} \frac{(p+1)(n+1)!}{(n-p)!} \\ &= \frac{1}{p!} \frac{1}{p+1} (n+1)n\dots(n-p+1). \end{aligned}$$

Comme

$$C_p^p + C_{p+1}^p + \dots + C_n^p = C_{n+1}^{p+1},$$

(voir question 2 du même exercice) nous déduisons

$$\sum_{q=p}^n q(q-1)\dots(q-p+1) = \frac{1}{p+1} (n+1)n\dots(n-p+1).$$

(2) Calcul de $S_1 = \sum_1^n q$.

$$\text{Puisque } p = 1, S_1 = \sum_1^n q = \frac{1}{2}(n+1)n.$$

Calcul de $S_2 = \sum_1^n q^2$.

$S_2 = \sum_1^n (q^2 - q) + q = \sum_1^n (q^2 - q) + \sum_1^n q = \sum_2^n q(q-1) + \sum_1^n q$. Pour terminer il suffit de connaître le terme $\sum_2^n q(q-1)$ qui se calcule en remplaçant p par 2, c'est à dire $\sum_2^n q(q-1) = \frac{1}{3}(n+1)n(n-1)$. Donc

$$S_2 = \frac{1}{6}n(n+1)(2n+1)$$

Calcul de $S_3 = \sum_1^n q^3$.

Puisque $q(q-1)(q-2) = q^3 - 3q^2 + 2q$, alors

$$\sum_{q=1}^n q(q-1)(q-2) = \sum_{q=1}^n q^3 - 3 \sum_{q=1}^n q^2 + 2 \sum_{q=1}^n q.$$

Donc

$$\begin{aligned} S_3 &= \sum_{q=1}^n q(q-1)(q-2) + 3 \sum_{q=1}^n q^2 - 2 \sum_{q=1}^n q \\ &= \sum_{q=1}^n q(q-1)(q-2) + 3S_2 - 2S_1 \\ &= \frac{1}{4}(n+1)n(n-1)(n-2) + 3\frac{1}{2}n(n+1)(2n+1) - 2\frac{1}{2}n(n+1) \\ &= \frac{n^2(n+1)^2}{4}. \end{aligned}$$

Exercice 6 Soit φ une application de \mathbb{R}^* dans \mathbb{R} . On définit sur l'ensemble $G = \mathbb{R}^* \times \mathbb{R}$ la loi de composition interne \star par :

$$\forall (a, b) \in G, \forall (c, d) \in G : (a, b) \star (c, d) = (ac, bc + \varphi(a)d).$$

1) La loi \star est associative si et seulement si $\forall (a, b) \in G, \forall (c, d) \in G, \forall (e, f) \in G : [(a, b) \star (c, d)] \star (e, f) = (a, b) \star [(c, d) \star (e, f)]$ si et seulement si $\forall (a, b) \in G, \forall (c, d) \in G, \forall (e, f) \in G : [(ac, bc + \varphi(a)d)] \star (e, f) = (ace, (bc + \varphi(a)d)e + \varphi(ac)f) = (a, b) \star [(ce, de + \varphi(c)f)] = (ace, bce + \varphi(a)(de + \varphi(c)f)) =$ si et seulement si $\forall (a, b) \in G, \forall (c, d) \in G, \forall (e, f) \in G : (ace, (bc + \varphi(a)d)e + \varphi(ac)f) = (ace, bce + \varphi(a)(de + \varphi(c)f))$ si et

seulement si $\forall a, c, e \in \mathbb{R}^*, \forall b, d, f \in \mathbb{R} : ace = ace$ et $(bc + \varphi(a)d)e + \varphi(ac)f = bce + \varphi(a)(de + \varphi(c)f)$ si et seulement si $\forall a, c \in \mathbb{R}^*, \forall f \in \mathbb{R} : \varphi(ac)f = \varphi(a)\varphi(c)f$ si et seulement si $\forall a, c \in \mathbb{R}^*, \varphi(ac) = \varphi(a)\varphi(c)$.

2)a) Soit $\varphi(1) = 1$. L'élément $(c, d) \in G$ est l'élément neutre de la loi \star si et seulement si $\forall (a, b) \in G$, on a $(a, b) \star (c, d) = (c, d) \star (a, b) = (a, b)$ si et seulement si $\forall (a, b) \in G, (ac, bc + \varphi(a)d) = (ca, da + \varphi(c)b) = (a, b)$ si et seulement si

$$\forall (a, b) \in G \begin{cases} ac = ca = a \\ bc + \varphi(a)d = b \\ da + \varphi(c)b = b \end{cases} \Leftrightarrow \forall (a, b) \in G \begin{cases} c = 1 \\ b + \varphi(a)d = b \\ da + \varphi(1)b = b \end{cases} \Leftrightarrow \forall (a, b) \in G \begin{cases} c = 1 \\ \varphi(a)d = 0 \\ da = b(1 - \varphi(1)) = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} c = 1 \\ d = 0 \end{cases}, \text{ car } a \neq 0. \text{ Donc } \varphi(1) = 1 \text{ implique que la loi } \star \text{ admet un élément neutre qui est } (1, 0).$$

b) Inversement, si la loi \star admet un élément neutre $(c, d) \in G$, alors d'après les calculs précédents, on trouve que $\forall (a, b) \in G, (a, b) \star (c, d) = (c, d) \star (a, b) = (a, b)$ si et seulement si

$$\forall (a, b) \in G \begin{cases} c = 1 \\ \varphi(a)d = 0 \\ da = b(1 - \varphi(1)) \end{cases}.$$

La dernière égalité doit être valable pour tout $a \in \mathbb{R}^*$ et tout $b \in \mathbb{R}$, en particulier pour $b = 0$, ce qui donne $da = 0$, donc $d = 0$, par suite $0 = b(1 - \varphi(1))$ pour tout $b \in \mathbb{R}$, ceci n'est possible que si $\varphi(1) = 1$. Conclusion : la loi \star admet un élément neutre si et seulement si $\varphi(1) = 1$.

3) On suppose que l'application φ vérifie : $\begin{cases} \forall a, c \in \mathbb{R}^*, \varphi(ac) = \varphi(a)\varphi(c), \\ \varphi(1) = 1. \end{cases}$

On sait que cela signifie que la loi \star est associative et qu'elle admet un élément neutre qui est $(1, 0)$. Montrer que l'élément $(a, b) \in G$ admet un symétrique pour la loi \star revient à résoudre l'équation $(a, b) \star (c, d) = (c, d) \star (a, b) = (1, 0)$, c.-à-d. l'équation $(ac, bc + \varphi(a)d) = (ca, da + \varphi(c)b) = (1, 0)$ ce qui conduit au système :

$$\begin{cases} ac = ca = 1 \\ bc + \varphi(a)d = 0 \\ da + \varphi(c)b = 0 \end{cases}.$$

Ce système est équivalent à

$$\begin{aligned} \begin{cases} c = \frac{1}{a} \\ d = -\frac{\varphi(c)b}{a} \\ bc + \varphi(a)d = 0 \end{cases} &\Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{\varphi(c)b}{a} \\ bc + \varphi(a)[-\frac{\varphi(c)b}{a}] = 0 \end{cases} \Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{\varphi(c)b}{a} \\ bc - \frac{\varphi(a)\varphi(c)b}{a} = 0 \end{cases} \Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{\varphi(c)b}{a} \\ \frac{abc - \varphi(a)\varphi(c)b}{a} = 0 \end{cases} \\ &\Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{\varphi(c)b}{a} \\ \frac{abc - \varphi(ac)b}{a} = 0 \end{cases} \Leftrightarrow \begin{cases} c = \frac{1}{a} \\ d = -\frac{\varphi(c)b}{a} \\ \frac{b}{a}[ac - \varphi(ac)] = \frac{b}{a}[1 - \varphi(1)] = \frac{b}{a} \times 0 = 0 \end{cases} \end{aligned}$$

Le système admet donc une solution et le symétrique de (a, b) est $(\frac{1}{a}, -\frac{\varphi(c)b}{a})$ et si l'on remarque que $ac = 1$ implique que $\varphi(ac) = \varphi(a)\varphi(c) = \varphi(1) = 1$, on déduit que $\varphi(c) = \varphi(\frac{1}{a}) = \frac{1}{\varphi(a)}$. On peut donc écrire :

$$(a, b)^{-1} = (\frac{1}{a}, -\frac{b}{a\varphi(a)}).$$

Les trois axiomes qui permettent de dire que (G, \star) est un groupe sont vérifiés, d'où la conclusion.

4) Comme exemple, on peut citer l'application φ définie par $\varphi(a) = a$ pour tout $a \in \mathbb{R}^*$, ce qui donne la loi \star définie sur G par : $(a, b) \star (c, d) = (ac, bc + ad)$.

Exercice 7 Soit (G, \cdot) un groupe fini de cardinal $2n$ ($n \geq 2$), d'élément neutre e et possédant 2 sous-groupes H et H' tels que :

$$\text{Card}(H) = \text{Card}(H') = n$$

et

$$H \cap H' = \{e\}.$$

1) Comme $\text{Card}(H \cup H') = \text{Card}(H) + \text{Card}(H') - \text{Card}(H \cap H') = 2n - 1$, alors $\text{Card}(G - (H \cup H')) = 1$, donc $G - (H \cup H')$ est un singleton qu'on notera par $\{a\}$.

2) Soit $h \in H - \{e\}$, et soit $h' \in H'$. Si $h' = e$, alors $hh' = h$, et si $h' \neq e$, alors $hh' = a$ ou $hh' \in (H \cup H')$. Si $hh' \in H$, alors $h' = h^{-1}hh'$ sera dans H , donc dans $H \cap H'$, par suite $h' = e$ et ceci est impossible. Si par contre $hh' \in H'$, alors $h = hh'(h')^{-1}$ sera dans H' , donc dans $H \cap H'$, par suite $h = e$ et ceci est encore impossible. Donc $hH' \subset \{h, a\}$.

Comme $\text{Card}(H') = n \geq 2$, alors il existe $h' \in H'$ et différent de e , et d'après ce qui précède, $a = hh' \in hH'$. Donc $hH' = \{h, a\}$, et comme l'application τ définie de H' vers hH' par $\tau(h') = hh'$ est une bijection, alors H' et hH' ont même cardinal qui est celui de l'ensemble $\{h, a\}$, ce cardinal est 2, car $a \neq h$ puisque a est dans G est n'est pas dans H . Donc le cardinal de H est $n = 2$.

3) On écrit $G = \{e, a, h, h'\}$. Comme H et H' jouent des rôles symétriques, alors $h'H = \{h', a\}$. On en déduit que $hh' = h'h = a$, et comme h et H' sont d'ordre 2, alors $h^2 = (h')^2 = e$, d'où $a^2 = hh'h'h = h^2 = e$, $ah = h^{h^2} = h'$ et $ha = h^2h' = h'$. Les produits qui restent se traitent de la même manière et la table de multiplication de G est donnée par :

\cdot	e	a	h	h'
e	e	a	h	h'
a	a	e	h'	h
h	h	h'	e	a
h'	h'	h	a	e

Il faut noter que G est un groupe commutatif non cyclique d'ordre 4.

Exercice 8 Soient (G_1, \bullet) et (G_2, \star) deux groupes et $f: G_1 \rightarrow G_2$ un homomorphisme de groupes. Soit \mathcal{R} la relation d'équivalence associée à f .

I. $\ker f$ est un sous groupe car

- $\ker f \neq \emptyset$ car il contient au moins e_1 (élément neutre de G_1), $f(e_1) = e_2$.
- soient x, y deux éléments de $\ker f$. Montrons que $x \bullet y^{-1}$ est un élément de $\ker f$.

$$f(x \bullet y^{-1}) = f(x) \star f(y^{-1}) = e_2 \star e_2^{-1} = e_2.$$

Donc $x \bullet y^{-1}$ est un élément de $\ker f$.

$\text{Im } f$ est un sous groupe car

- $\text{Im } f \neq \emptyset$ car il contient au moins $e_2 = f(e_1)$ (élément neutre de G_2).
- soient x, y deux éléments de $\text{Im } f$. Montrons que $x \bullet y^{-1}$ est un élément de $\text{Im } f$. Puisque $x \in \text{Im } f$ et $y \in \text{Im } f$, alors il existe r, s de G_1 tels que $x = f(r)$ et $y = f(s)$. Montrons que $x \bullet y^{-1}$ est un élément de $\text{Im } f$.
Calculons $x \star y^{-1} = f(r) \star f(s)^{-1} = f(r \bullet s^{-1})$. Donc $x \star y^{-1}$ s'écrit comme image d'un élément de G_1 . Donc $x \star y^{-1}$ est un élément de $\text{Im } f$.

II. Montrons que la relation \mathcal{R} est compatible avec la loi du groupe. Si $x\mathcal{R}y$ et $x'\mathcal{R}y'$ alors $f(x) = f(y)$ et $f(x') = f(y')$. Donc $f(x \bullet x') = f(x) \star f(x') = f(y) \star f(y') = f(y \bullet y')$ et par suite $(x \bullet x')\mathcal{R}(y \bullet y')$.

- III. Pour tout $x, y \in G_1$, nous posons $\bar{x}\bar{\bullet}\bar{y} = \overline{x\bullet y}$.
- Montrons que \bullet est une loi de composition interne sur G_1/\mathcal{R} , l'ensemble des classes d'équivalences modulo \mathcal{R} , c'est à dire une application de $G_1/\mathcal{R} \times G_1/\mathcal{R}$ dans G_1/\mathcal{R} . Soient \bar{x} et \bar{y} deux éléments de G_1/\mathcal{R} . Si x' et y' sont deux éléments de G_1 tels que $\bar{x} = \bar{x'}$ et $\bar{y} = \bar{y'}$, alors $\bar{x}\bar{\bullet}\bar{y} = \overline{x\bullet y} = \overline{x'\bullet y'} = \overline{x'\bullet y'}$, car la relation \mathcal{R} est compatible avec la loi de G_1 . Donc \bullet est une loi de composition interne sur G_1/\mathcal{R} .
 - Montrons que G_1/\mathcal{R} , muni de \bullet , est un groupe. La loi est associative, il reste à vérifier deux points.
Le premier est $\bar{\bullet}$ admet un élément neutre qui est la classe de e_1 pour la relation \mathcal{R} , c'est à dire \bar{e}_1 car $\bar{x}\bar{\bullet}\bar{e}_1 = \overline{x\bullet e_1} = \bar{x}$.
Le deuxième est que tout élément \bar{x} , admet un inverse pour $\bar{\bullet}$, qui est la classe de x^{-1} pour la relation \mathcal{R} , c'est dire \bar{x}^{-1} .
- IV. Montrer qu'il existe un isomorphisme de groupes de $(G_1/\mathcal{R}, \bar{\bullet})$ dans $(\text{Im } f, \star)$. Soit $\phi: (G_1/\mathcal{R}, \bar{\bullet}) \rightarrow (\text{Im } f, \star)$ qui à \bar{x} associe $f(x)$. Montrons que ϕ est homomorphisme bijective.
- ϕ est un homomorphisme car pour tout \bar{x} et \bar{y} deux éléments de G_1/\mathcal{R} , calculons $\phi(\bar{x}\bar{\bullet}\bar{y})$.
- $$\begin{aligned}\phi(\bar{x}\bar{\bullet}\bar{y}) &= \phi(\overline{x\bullet y}) \\ &= f(x\bullet y) \\ &= f(x) \star f(y) \\ &= \phi(\bar{x}) \star \phi(\bar{y}).\end{aligned}$$
- Elle est surjective car soit $y \in \text{Im } f$, il existe $x \in G_1$ tel que $y = f(x)$. \bar{x} est l'antécédent de y car $\phi(\bar{x}) = f(x) = y$.
 - Elle est injective, car soient \bar{x} et \bar{y} deux éléments de G_1/\mathcal{R} tels que $\phi(\bar{x}) = \phi(\bar{y})$. Montrons que $\bar{x} = \bar{y}$. Puisque $\phi(\bar{x}) = \phi(\bar{y})$ alors $f(x) = f(y)$ ce qui veut dire que $x\mathcal{R}y$ et $\bar{x} = \bar{y}$.
- Conclusion ϕ est un isomorphisme de groupes et $(G_1/\mathcal{R}, \bar{\bullet})$ et $(\text{Im } f, \star)$ sont deux groupes isomorphes.
- V. x est en relation avec y si et seulement si $f(x) = f(y)$, ce qui est équivalent à $f(x\bullet y^{-1}) = e_2$ ce qui est aussi équivalent à $x\bullet y^{-1} \in \ker f$, c'est-à-dire que x est congru à y modulo $\ker f$.

Série d'Algèbre n°3

Exercice 1 Soit (G, \cdot) un groupe et H_1 et H_2 deux sous-groupes de G . Montrer que :

$$H_1 \cup H_2 \text{ est un sous-groupe de } G \text{ si et seulement si } (H_1 \subset H_2 \text{ ou } H_2 \subset H_1).$$

Exercice 2 Soit (G, \cdot) un groupe d'élément neutre e et soit $Z(G)$ l'ensemble défini par :

$$Z(G) = \{a \in G \mid \forall y \in G, ay = ya\}.$$

1) Montrer que $Z(G)$ est un sous-groupe de G et que $Z(G)$ est commutatif.

Dans la suite, on suppose qu'il existe $n \in \mathbb{N}^*$ tel que l'application $f : G \rightarrow G$ définie par : $\forall u \in G, f(u) = u^n$ soit un automorphisme de G .

2) Soient x et y deux éléments quelconques de G .

a) Montrer qu'il existe $z \in G$ tel que $y = xz$.

b) En utilisant le fait que f est surjective, montrer qu'il existe $u \in G$ tel que $y = xu^n$.

c) Montrer par récurrence sur k que :

$$\forall k \in \mathbb{N}, (xu)^k = x(ux)^k x^{-1}.$$

d) En utilisant les questions précédentes et le fait que f est un automorphisme de G , montrer que :

$$x^{n-1}y = yx^{n-1}.$$

e) Conclure.

On rappelle qu'un automorphisme de G est un homomorphisme bijectif de G vers G .

Le sous-groupe $Z(G)$ s'appelle le centre de G .

Exercice 3 Soit (G, \cdot) un groupe d'élément neutre e . Soit $d \in \mathbb{N}^*$ et soit $f_d : G \rightarrow G$ l'application définie par : $\forall u \in G, f_d(u) = u^d$.

1) Montrer que f_2 est un endomorphisme de G si et seulement si le groupe G est commutatif.

Dans la suite, on suppose que (G, \cdot) est un groupe commutatif d'ordre n (c.-à-d. que $|G| = n$).

2) Montrer que pour tout $d \in \mathbb{N}^*$, f_d est un endomorphisme de G .

3) On suppose que d et n sont premiers entre eux.

a) Montrer que f_d est un automorphisme de G .

Indication : pour montrer que $\ker f_d = \{e\}$, utiliser le fait que si $x \in \ker f_d$, alors $x^d = x^n = e$, puis utiliser l'identité de Bézout entre n et d .

b) En déduire que si n est impair, alors : $\forall y \in G, \exists u \in G$ tel que $y = u^2$.

On rappelle qu'un endomorphisme de G est un homomorphisme de G vers G , lorsqu'il est de plus bijectif, on dit que c'est un automorphisme de G .

Exercice 4 Soit $(A, +, \cdot)$ un anneau commutatif. Soient I et J deux idéaux de A . On pose :

$$I + J = \{i + j \mid i \in I \text{ et } j \in J\}$$

- 1) Montrer que $I + J$ est un idéal de A et que $I + J = (I \cup J)$.
- 2) On pose $IJ = (\{ij \mid i \in I, j \in J\})$. Montrer que IJ est l'ensemble des sommes finies d'éléments de la forme ij où $i \in I$ et $j \in J$.
- 3) On dit que deux idéaux I et J sont premiers entre eux si $I + J = A$.
 - a) Montrer que si I est premier avec J_1 et J_2 , alors il est premier avec $J_1 J_2$.
 - b) On suppose que I et J sont premiers entre eux. Montrer que $\forall a, b \in A, \exists x \in A$ tel que $x \equiv a \pmod{I}$ et $x \equiv b \pmod{J}$.
 - c) Montrer que si I et J sont premiers entre eux, alors $IJ = I \cap J$ et $A/IJ \simeq A/I \times A/J$. Ce dernier résultat est connu sous le nom du théorème du reste chinois.

Exercice 5 1) Soit A un anneau commutatif. Un idéal M de A est dit maximal si pour tout idéal I de A tel que $M \subset I \subset A$ et $M \neq I$ on ait $I = A$.

- a) Montrer qu'un idéal M de A est maximal si et seulement si A/M est un corps.
- b) En déduire que l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est un nombre premier.

2) Un idéal propre P de A est dit premier si :

$$\forall a, b \in A, (ab \in P \Rightarrow a \in P \text{ ou } b \in P).$$

- a) Montrer qu'un idéal P de A est premier si et seulement si A/P est un anneau intègre.
- b) En déduire que tout idéal maximal M de A est premier.

Exercice 6 Soit $(A, +, \cdot)$ un anneau commutatif tel que $A \neq \{0\}$. On rappelle que le groupe multiplicatif des éléments inversibles (des unités) de A est $\mathcal{U}(A) = \{u \in A \mid \exists u' \in A \text{ et } uu' = 1\}$.

- 1) Soit I un idéal de A . Montrer que s'il existe $u \in \mathcal{U}(A)$ tel que $u \in I$, alors $I = A$.
Dans toute la suite, on pose p un nombre premier et $A = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ et } n \text{ et } p \text{ premiers entre eux}\}$.
- 2) Montrer que $(A, +, \cdot)$ est un sous-anneau de $(\mathbb{Q}, +, \cdot)$.
- 3) Montrer qu'un élément $x = \frac{m}{n}$ de A est une unité de A si et seulement si m et p sont premiers entre eux.
- 4) Soit I un idéal non trivial de A , c'est-à-dire $I \neq \{0\}$ et $I \neq A$. Soit $x = \frac{m}{n}$ un élément de I .
 - a) Montrer que p divise m (remarquer que dans le cas contraire, x sera une unité puis utiliser 1)).
 - b) En déduire que $I \subset pA$, où pA est l'idéal principal engendré par p .
 - c) Montrer alors que pA est l'unique idéal maximal de A .

Exercice 7 Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, où $i \in \mathbb{C}$ vérifie $i^2 = -1$. Soient m et $n \in \mathbb{N}^*$ tels que $m < n$.

- 1) Montrer que $(\mathbb{Z}[i], +, \cdot)$ est un sous-anneau de $(\mathbb{C}, +, \cdot)$.
- 2) Soit l'application φ définie de $\mathbb{Z}[i]$ vers $\mathbb{Z}/n\mathbb{Z}$ par :

$$\forall a, b \in \mathbb{Z}, \varphi(a + ib) = \overline{a + mb},$$

où $\bar{x} = x + n\mathbb{Z}$ désigne la classe d'équivalence de x modulo n dans \mathbb{Z} .

Montrer que si $m^2 + 1 \equiv 0 \pmod{n}$, alors φ est un homomorphisme d'anneaux.

Dans la suite, on suppose que $m^2 + 1 = (2m + 1 - n)n$. Dans ce cas, l'application φ est un homomorphisme d'anneaux.

- 3) a) Montrer que φ est surjectif (utiliser la division euclidienne par m).
- b) Montrer que $n - m + i$ appartient à $\ker \varphi$.
- 4) Soit $a + ib$ un élément de $\ker \varphi$.
 - a) Montrer qu'il existe $k \in \mathbb{Z}$ tel que $a + mb = kn$.
 - b) Montrer que $(n - m)^2 + 1 = n$.
 - c) En déduire que $a + ib = (n - m + i)(c + id)$, où $c = b - (b - k)(n - m)$ et $d = b - k$, puis que $\ker \varphi = (n - m + i)$; l'idéal principal de $\mathbb{Z}[i]$ engendré par $n - m + i$.
 - d) Montrer alors que l'anneau quotient $\mathbb{Z}[i]/\ker \varphi$ est un corps si et seulement si n est un nombre premier (utiliser le fait que $\mathbb{Z}[i]/\ker \varphi$ est isomorphe à $\text{Im } \varphi$).

Corrigé de la Série d'Algèbre n°3

Exercice 1 Soit (G, \cdot) un groupe et H_1 et H_2 deux sous-groupes de G .

Si $(H_1 \subset H_2 \text{ ou } H_2 \subset H_1)$, alors $H_1 \cup H_2 = H_2$ ou $H_1 \cup H_2 = H_1$ et dans les deux cas, $H_1 \cup H_2$ est un sous-groupe de G .

On montre la réciproque en utilisant le raisonnement par l'absurde. Supposons que $H_1 \cup H_2$ est un sous-groupe de G et que $(H_1 \not\subset H_2 \text{ et } H_2 \not\subset H_1)$. Il existe donc $x_1 \in H_1 - H_2$ et $x_2 \in H_2 - H_1$. Comme x_1 et x_2 sont dans $H_1 \cup H_2$, et comme ce dernier est un sous-groupe, alors $x_1 x_2 \in H_1 \cup H_2$. Si $x_1 x_2$ est dans H_1 , alors $x_2 = x_1^{-1} x_1 x_2 \in H_1$, ce qui est absurde. Si $x_1 x_2$ est dans H_2 , alors $x_1 = x_1 x_2 x_2^{-1} \in H_2$, ce qui est encore impossible, d'où le résultat.

Exercice 2 Soit (G, \cdot) un groupe d'élément neutre e et soit $Z(G)$ l'ensemble défini par :

$$Z(G) = \{a \in G \mid \forall y \in G, ay = ya\}.$$

1) Pour tout y dans G , on a : $ey = y = ye$, donc $e \in Z(G)$, d'où $Z(G) \neq \emptyset$.

Soient a et b dans $Z(G)$, et soit $y \in G$, alors $ay = ya$ et $by = yb$, d'où $(ab)y = a(by) = a(yb) = (ay)b = (ya)b = y(ab)$, donc $ab \in Z(G)$.

Si $a \in Z(G)$ et $y \in G$, alors $ay = ya \Rightarrow a^{-1}ay = a^{-1}ya = y \Rightarrow ya^{-1} = a^{-1}yaa^{-1} = a^{-1}y$, d'où $a^{-1} \in Z(G)$.

Conclusion : $Z(G)$ est un sous-groupe de G .

$\forall a, b \in Z(G)$, on a $ab = ba$ car $a \in Z(G)$, donc $Z(G)$ est commutatif.

Dans la suite, on suppose qu'il existe $n \in \mathbb{N}^*$ tel que l'application $f : G \rightarrow G$ définie par : $\forall u \in G, f(u) = u^n$ soit un automorphisme de G .

2) Soient x et y deux éléments quelconques de G .

a) Une solution évidente de l'équation $y = xz$ est $z = x^{-1}y$.

b) Comme f est surjective, il existe $u \in G$ tel que $z = u^n$, d'où il existe $u \in G$ tel que $y = xu^n$.

c) La propriété est vraie à l'ordre 0 puisque $(xu)^0 = e$ et $x(ux)^0 x^{-1} = xex^{-1} = xx^{-1} = e$.

Supposons qu'à l'ordre k on ait $(xu)^k = x(ux)^k x^{-1}$, alors $(xu)^{k+1} = (xu)(xu)^k = (xu)x(ux)^k x^{-1} = x(ux)(ux)^k x^{-1} = x(ux)^{k+1} x^{-1}$, donc la propriété est vraie aussi à l'ordre $k+1$, d'où le résultat.

d) D'après les questions précédentes il existe u dans G tel que :

$$x^{n-1}y = x^{n-1}xu^n = x^nu^n = f(x)f(u) = f(xu) = (xu)^n =$$

$$x(ux)^nx^{-1} = xf(ux)x^{-1} = xf(u)f(x)x^{-1} = xu^nx^n x^{-1} = yx^{n-1},$$

grâce au fait que f est un automorphisme de G .

e) La question précédente montre que $\forall x \in G, x^{n-1} \in Z(G)$.

Exercice 3 Soit (G, \cdot) un groupe d'élément neutre e . Soit $d \in \mathbb{N}^*$ et soit $f_d : G \rightarrow G$ l'application définie par : $\forall u \in G, f_d(u) = u^d$.

1) Si f_2 est un endomorphisme de G , alors $\forall x, y \in G$, on a $f_2(xy) = f_2(x)f_2(y)$, d'où :

$$\forall x, y \in G, (xy)^2 = x^2y^2 = (xy)(xy) = x(yx)y = x(xy)y \Rightarrow (yx)y = (xy)y \Rightarrow yx = xy,$$

car x et y sont réguliers. Donc G est commutatif.

Inversement, si le groupe G est commutatif, alors $\forall x, y \in G, xy = yx$, d'où $\forall x, y \in G, (xy)^2 = x^2y^2$,

donc $\forall x, y \in G, f_2(xy) = f_2(x)f_2(y)$. Ainsi, f_2 est un endomorphisme de G .

Dans la suite, on suppose que (G, \cdot) est un groupe commutatif d'ordre n (c.-à-d. que $|G| = n$).

2) Soit $d \in \mathbb{N}^*$. Comme G est commutatif, alors : $\forall x, y \in G, xy = yx$, d'où $\forall x, y \in G, (xy)^d = x^d y^d$, donc $\forall x, y \in G, f_d(xy) = f_d(x)f_d(y)$. Ainsi, pour tout $d \in \mathbb{N}^*$, f_d est un endomorphisme de G .

3) On suppose que d et n sont premiers entre eux.

a) Comme n et d sont premiers entre eux, il existe a et b dans \mathbb{Z} tel que $an + bd = 1$. Soit $x \in \ker f_d$, alors $f_d(x) = x^d = e$. Comme $x^n = e$, alors $x = x^1 = x^{an+bd} = (x^n)^a (x^d)^b = e^a e^b = e$. Donc $\ker f_d = \{e\}$, d'où f_d est injective. Comme G est fini, alors f_d est surjective (toute injection d'un ensemble fini vers lui-même est surjective). Donc f_d est un automorphisme de G .

b) Si n est impair, alors $d = 2$ est premier avec n , d'où f_2 est un automorphisme de G , f_2 est donc surjective, d'où : $\forall y \in G, \exists u \in G$ tel que $y = f_2(u) = u^2$.

Exercice 4 Soit $(A, +, \cdot)$ un anneau commutatif. Soient I et J deux idéaux de A . On pose $I + J = \{i + j \mid i \in I \text{ et } j \in J\}$.

1) • On a $0 = 0 + 0 \in I + J$, donc $I + J$ est non vide.

• Soient x et y deux éléments de $I + J$, alors $\exists i_1, i_2 \in I$ et $j_1, j_2 \in J$ tels que $x = i_1 + j_1$ et $y = i_2 + j_2$, d'où $x - y = (i_1 - i_2) + (j_1 - j_2) \in I + J$, car $(i_1 - i_2) \in I$ et $(j_1 - j_2) \in J$ puisque ce sont des idéaux de A . Ainsi, $I + J$ est un sous-groupe de $(A, +)$.

• Soient $a \in A$ et $x = i + j \in I + J$, alors $ax = ai + aj \in I + J$, car $ai \in I$ et $aj \in J$.

Donc $I + J$ est un idéal de A .

• Il est clair que $I \cup J \subset I + J$. Si K est un idéal contenant $I \cup J$, alors K contient tout élément de la forme $i + j$ où $i \in I$ et $j \in J$, d'où $I + J \subset K$. Ainsi, $I + J$ est le plus petit idéal contenant $I \cup J$, donc $I + J = (I \cup J)$.

2) Nous posons $IJ = \{ij \text{ tel que } i \in I, j \in J\}$. Notons aussi S_f l'ensemble des sommes finies des éléments de la forme ij . Montrons que S_f est un idéal,

– $S_f \neq \emptyset$ car $0 = 0 \cdot 0 \in S_f$.

– Montrons que S_f est un sous-groupe de $(A, +)$. Soient x, y des éléments de S_f , $x = \sum_{k=1}^n i_k j_k$ et

$y = \sum_{l=1}^m i'_l j'_l$. Donc $x - y = \sum_{k=1}^n i_k j_k + \sum_{l=1}^m (-i'_l) j'_l$ qui est une somme finie d'éléments de la forme ij , d'où $x - y \in S_f$.

– $\forall a \in A$, montrons que pour tout x de S_f , $ax = xa$ sont aussi des éléments de S_f . Puisque $x \in S_f$

alors $x = \sum_{k=1}^n i_k j_k$ et $xa = \sum_{k=1}^n i_k (j_k a) \in S_f$, car $j_k a \in J$ pour tout k puisque J est un idéal.

Puisque

$$\{ij \text{ tel que } i \in I, j \in J\} \subset S_f,$$

alors l'idéal engendré par

$$\{ij \text{ tel que } i \in I, j \in J\}$$

qui est IJ est dans S_f .

Soit $x = \sum_{k=1}^n i_k j_k \in S_f$. Donc $x \in IJ$ car IJ est un idéal et par suite $S_f \subset IJ$. Donc $IJ = S_f$.

3) On dit que deux idéaux I et J sont premiers entre eux si $I + J = A$.

a) Comme $I + J_1 = I + J_2 = A$, il existe $i_1, i_2 \in I$ et $(j_1, j_2) \in J_1 \times J_2$ tels que $1 = i_1 + j_1 = i_2 + j_2$, d'où :

$$1 \cdot 1 = (i_1 + j_1)(i_2 + j_2) = i_1(i_2 + j_2) + i_2 j_1 + j_1 j_2 = 1 \in I + J_1 J_2,$$

car $i_1(i_2 + j_2) + i_2 j_1 \in I$ et $j_1 j_2 \in J_1 J_2$. On en déduit que $\forall a \in A, a = a \cdot 1 \in I + J_1 J_2$, par suite, $I + J_1 J_2 = A$, d'où I est premier avec $J_1 J_2$.

b) Pour tous $a, b \in A$, puisque I, J sont premiers entre eux, il existe $i_a, i_b \in I$ et $j_a, j_b \in J$ tels que $a = i_a + j_a$ et $b = i_b + j_b$. Si on pose $i = i_b - i_a$ et $j = j_a - j_b$, alors, $a - b = j - i$, d'où, $a + i = b + j$. Posons $x = a + i$, x est aussi égal à $b + j$. Donc x est congru à a modulo I et x est congru à b modulo J .

c) Montrons que $IJ = I \cap J$. Si $(i, j) \in I \times J$, alors $i \cdot j \in I \cap J$ et par construction $IJ \subset I \cap J$. Puisque

il existe $i \in I, j \in J$ tels que $i + j = 1$. Soit $x \in I \cap J$, $x = xi + xj$ donc $x \in IJ$ car xi est le produit d'un élément de I et d'un élément de J et de même pour xj d'où l'égalité $IJ = I \cap J$.

Soit $f: x \in A \rightarrow (\bar{x}_I, \bar{x}_J) \in (A/I) \times (A/J)$. Montrons que f est un homomorphisme d'anneaux surjectif de noyau IJ . Il est immédiat que f est un morphisme d'anneaux. Le noyau de f est l'ensemble des $x \in A$ tel que $\bar{x}_I = 0$ et $\bar{x}_J = 0$, c'est à dire $x \in I \cap J = IJ$ car $I + J = A$. Montrons qu'elle est aussi surjective. Soit $(X, Y) \in (A/I) \times (A/J)$ et soit a un représentant de X et b un représentant de Y . D'après **b)**, il existe $x \in A$ tel que x est congru à a modulo I et x est congru à b modulo J , c'est-à-dire que $f(x) = (X, Y)$. Donc f est surjective. Donc $A/IJ \simeq (A/I) \times (A/J)$.

Exercice 5 1) Soit A un anneau commutatif. Un idéal M de A est dit maximal si pour tout idéal I de A tel que $M \subset I \subset A$ et $M \neq I$ on ait $I = A$.

a) Supposons M est maximal et soit $\bar{x} \neq \bar{0}$ un élément de A/M , alors $x \notin M$ d'où l'idéal engendré par x et M est l'anneau A tout entier, donc $1 \in A$ peut s'écrire $1 = \lambda x + m$ ou $m \in M$. Ce qui nous donne dans l'anneau quotient A/M , $\bar{1} = \bar{\lambda}\bar{x}$, c'est à dire \bar{x} admet dans A/M un inverse qui est $\bar{\lambda}$. Donc A/M est un corps.

Inversement, supposons que A/M est un corps. Considérons un idéal propre I de A et supposons aussi que $I \supset M$ strictement, alors il existe $x \in I$, tel que $x \notin M$. Puisque A/M est un corps, il existe donc dans A/M un inverse de \bar{x} c'est à dire $\bar{x}\bar{y} = \bar{1}$. Ce qui se traduit dans A par $xy - 1 \in M$ ou encore $1 = xy + m$ avec $m \in M$. Mais $m \in M$ et $x \in I$, donc $xy \in I$ ce qui implique que $1 \in I$, d'où $I = A$.

b) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si l'idéal $(n) = n\mathbb{Z}$ est maximal si et seulement si n est irréductible dans \mathbb{Z} (voir cours) si et seulement si n est un nombre premier.

2) Un idéal propre P de A est dit premier si :

$$\forall a, b \in A, (ab \in P \Rightarrow a \in P \text{ ou } b \in P).$$

a) Soit P un idéal de A . Supposons que P est premier, alors dans A/P , $\bar{x}\bar{y} = \bar{0} \Rightarrow xy \in P$, ce qui implique que $x \in P$ ou $y \in P$, d'où $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$.

Inversement, Si A/P est intègre, nous avons $xy \in P \Rightarrow \bar{x}\bar{y} = \bar{0}$ dans l'anneau quotient, d'où $\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0}$, c'est à dire $x \in P$ ou $y \in P$.

b) Supposons P maximal donc A/P est un corps et par suite il est intègre et P est premier.

Exercice 6 Soit $(A, +, \cdot)$ un anneau commutatif tel que $A \neq \{0\}$. On rappelle qu'un élément u de A est dit une unité de A , s'il existe $u' \in A$ tel que $uu' = 1$

1) Soit I un idéal de A tel qu'il existe unité u de A et $u \in I$. Il existe donc $u' \in A$ tel que $uu' = 1$. Comme $u \in I$ et I est un idéal, alors $uu' = 1 \in I$, d'où $\forall a \in A, a = a \cdot 1 \in I$, c.-à-d. $A \subset I$. Donc $I = A$.

Dans toute la suite, on pose p un nombre premier et $A = \{\frac{m}{n} \mid m, n \in \mathbb{Z} \text{ et } n \text{ et } p \text{ premiers entre eux}\}$.

2) $1 = \frac{1}{1} \in A$.

Soient $x = \frac{m}{n}$ et $y = \frac{m'}{n'}$ deux éléments de A , avec m, m', n et n' dans \mathbb{Z} et p est premier avec n et n' , alors p ne divise ni n ni n' , par suite, $x - y = \frac{m}{n} - \frac{m'}{n'} = \frac{mn' - m'n}{nn'}$ et $xy = \frac{mm'}{nn'}$. Comme p est un nombre premier qui est premier avec n et n' , alors p est premier avec le produit nn' , d'où $x - y$ et xy sont dans A . Ainsi, $(A, +, \cdot)$ est un sous-anneau de $(\mathbb{Q}, +, \cdot)$.

3) Si $x = \frac{m}{n}$ est une unité de A , alors il existe $x' = \frac{m'}{n'} \in A$ tel que $xx' = 1 = \frac{mm'}{nn'}$, d'où $mm' = nn'$. Comme x et x' sont dans A , p est premier avec n et n' donc avec $nn' = mm'$, par suite p ne divise pas m , donc m et p sont premiers entre eux.

Inversement, si m et p sont premiers entre eux, alors $x' = \frac{n}{m} \in A$ et $xx' = \frac{m}{n} \cdot \frac{n}{m} = 1$, donc x est une unité de A .

4) Soit I un idéal non trivial de A , c'est-à-dire $I \neq \{0\}$ et $I \neq A$. Soit $x = \frac{m}{n}$ un élément de I .

a) Si p ne divise pas m , alors m et p sont premiers entre eux, d'où x est une unité de A qui appartient à I et d'après **1)**), on a $I = A$, absurde, car $I \neq A$, d'où le résultat.

b) $x = \frac{m}{n}$ un élément de I . Comme p divise m , il existe $m' \in \mathbb{Z}$ tel que $m = pm'$ d'où, $x = \frac{m}{n} =$

$\frac{pm'}{n} = p \cdot \frac{m'}{n} \in pA$, car $pA = \{pa \mid a \in A\}$ et $\frac{m'}{n} \in A$. Donc tout élément x de I est dans pA . Ainsi, $I \subset pA$,

c) Tout idéal $I \neq A$ est inclus dans pA , donc pA est l'unique idéal maximal de A .

Exercice 7 Soit $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, où $i \in \mathbb{C}$ vérifie $i^2 = -1$. Soient m et $n \in \mathbb{N}^*$ tels que $m < n$.

1) Soient a, b, c et d dans \mathbb{Z} , alors $(a + ib) - (c + id) = (a - c) + i(b - d)$ est dans $\mathbb{Z}[i]$. De même, $(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc)$ appartient à $\mathbb{Z}[i]$. Enfin $1 + i0 = 1 \in \mathbb{Z}[i]$. Donc $(\mathbb{Z}[i], +, \cdot)$ est un sous-anneau de $(\mathbb{C}, +, \cdot)$.

2) Soit l'application φ définie de $\mathbb{Z}[i]$ vers $\mathbb{Z}/n\mathbb{Z}$ par :

$$\forall a, b \in \mathbb{Z}, \quad \varphi(a + ib) = \overline{a + mb},$$

Soient a, b, c et d dans \mathbb{Z} , alors $\varphi(a + ib) + \varphi(c + id) = \overline{a + mb} + \overline{c + md} = \overline{(a + c) + m(b + d)} = \varphi(a + c + i(b + d)) = \varphi((a + ib) + (c + id))$. On a aussi, $\varphi(1) = \overline{1}$ qui est l'élément neutre de la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Montrons que si $m^2 + 1 \equiv 0 \pmod{n}$, alors $\varphi((a + ib) \cdot (c + id)) = \varphi(a + ib) \cdot \varphi(c + id)$. On a :

$$\varphi((a + ib) \cdot (c + id)) = \varphi((ac - bd) + i(ad + bc)) = \overline{(ac - bd) + m(ad + bc)},$$

et

$$\varphi(a + ib) \cdot \varphi(c + id) = \overline{a + mb} \cdot \overline{c + md} = \overline{ac + m(ad + bc) + m^2bd}.$$

Pour montrer l'égalité entre ces deux expressions il suffit de remarquer que :

$$m^2 + 1 \equiv 0 \pmod{n} \Rightarrow m^2 \equiv -1 \pmod{n} \Rightarrow m^2bd \equiv -bd \pmod{n} \Rightarrow$$

$$ac + m(ad + bc) + m^2bd \equiv (ac - bd) + m(ad + bc) \pmod{n}.$$

On en déduit donc que φ est un homomorphisme d'anneaux.

Dans la suite, on suppose que $m^2 + 1 = (2m + 1 - n)n$. Dans ce cas, l'application φ est un homomorphisme d'anneaux.

3a) Soit $\bar{s} \in \mathbb{Z}/n\mathbb{Z}$, le théorème de la division euclidienne de s par m dans \mathbb{Z} assure le fait qu'il existe q et r dans \mathbb{Z} tel que $s = mq + r$, d'où $\bar{s} = \bar{r} + m\bar{q} = \varphi(r + iq)$, donc φ est surjectif.

b) $\varphi(n - m + i) = \overline{n - m + m} = \bar{n} = \bar{0}$, donc $n - m + i$ appartient à $\ker \varphi$.

4) Soit $a + ib$ un élément de $\ker \varphi$.

a) $(a + ib) \in \ker \varphi \Rightarrow \varphi(a + ib) = \overline{a + mb} = \bar{0}$, cela veut dire que n divise $a + mb$ dans \mathbb{Z} , donc il existe $k \in \mathbb{Z}$ tel que $a + mb = kn$.

b) $m^2 + 1 = (2m + 1 - n)n = 2mn + n - n^2 \Rightarrow n^2 - 2mn + m^2 + 1 = n \Rightarrow (n - m)^2 + 1 = n$.

c) $(n - m + i)(c + id) = (n - m + i)(b - (b - k)(n - m) + i(b - k)) = (n - m)(b - (b - k)(n - m)) - (b - k) + i(b - (b - k)(n - m) + (n - m)(b - k)) = (n - m)b - (b - k)(n - m)^2 - (b - k) + ib = (n - m)b - (b - k)((n - m)^2 + 1) + ib = (n - m)b - n(b - k) + ib = nk - mb + ib = a + ib$.

L'égalité qu'on vient juste d'établir montre que tout élément $a + ib$ de $\ker \varphi$ appartient à l'idéal principal de $\mathbb{Z}[i]$ engendré par $n + m - i$. De plus, $n + m - i \in \ker \varphi \Rightarrow (n - m + i) \subset \ker \varphi$, d'où $\ker \varphi = (n - m + i)$.

d) Comme $\mathbb{Z}[i]/\ker \varphi$ est isomorphe à $\text{Im } \varphi$ et comme φ est surjective, alors $\text{Im } \varphi = \mathbb{Z}/n\mathbb{Z}$, d'où $\mathbb{Z}[i]/\ker \varphi$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Ainsi, $\mathbb{Z}[i]/\ker \varphi$ est un corps si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Série d'Algèbre n°4

Exercice 1

- 1) Calculer le reste de la division euclidienne de 17^{17} par 4.
- 2) En utilisant la question précédente, déterminer le reste de la division euclidienne de

$$23^{17^{17}} \text{ et de } 17^{17^{17}}$$

par 10.

Exercice 2 Soit n un entier naturel. Le but de l'exercice est de montrer que 30 divise toujours $n^5 - n$.

- 1) En remarquant que $n^5 - n = n(n^4 - 1)$, montrer que 2 divise $n^5 - n$.
- 2) Montrer que $n^5 - n = (n^3 - n)(n^2 + 1)$, puis en déduire, en utilisant le petit théorème de Fermat, que 3 divise $n^5 - n$.
- 3) Montrer alors que :

$$\forall n \in \mathbb{N}, 30 \mid (n^5 - n).$$

Exercice 3

- 1) En utilisant l'algorithme d'euclide, montrer que 31 et 14 sont premiers entre eux.
- 2) En faisant le chemin inverse de l'algorithme d'euclide, trouver u et v tels que :

$$u \times 14 + v \times 31 = 1.$$

- 3) Résoudre le système de congruences

$$(SC) \quad \begin{cases} x \equiv 9 & (\text{mod } 14) \\ x \equiv 13 & (\text{mod } 31) \end{cases}$$

dans \mathbb{Z} ,

- a) En utilisant la relation de Bézout.
- b) En écrivant le système dans \mathbb{Z} , puis dans l'un des groupes $\mathbb{Z}/14\mathbb{Z}$ ou $\mathbb{Z}/31\mathbb{Z}$.

Exercice 4 Nombres de Fermat.

- 1) Soient b et p deux entiers naturels. Montrer que :

$$b^{2p+1} + 1 = (b + 1)(b^{2p} - b^{2p-1} + \dots - b + 1) \text{ puis en déduire que } b^{2p+1} + 1 \equiv 0 \pmod{b + 1}.$$

- 2) En déduire que pour tous $a, p, q \in \mathbb{N}$, et $a \geq 2$, on a :

$$a^{q(2p+1)} + 1 \equiv 0 \pmod{a^q + 1}.$$

- 3) Soit maintenant $a \in \mathbb{N}$, $a \geq 2$. On va montrer que si $a^m + 1$ est premier, alors m est une puissance de 2. On sait que tout entier naturel non nul m s'écrit de façon unique sous la forme $m = 2^n(2p + 1)$, avec $n, p \in \mathbb{N}$.

a) Montrer que $a^m + 1 \equiv 0 \pmod{a^{2^n} + 1}$.

b) En déduire que si $a^m + 1$ est premier, alors m est une puissance de 2.

En particulier, pour $a = 2$, si $2^m + 1$ est premier, alors m est une puissance de 2. Les nombres de la forme $2^{2^n} + 1$ s'appellent *les nombres de Fermat*.

- 4) Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (F_n est appelé le $n^{\text{ème}}$ nombre de Fermat).

- a) Montrer que, pour tout $k \in \mathbb{N}^*$, $(F_n - 1)^{2^k} + 1 = F_{n+k}$.
b) En déduire que pour tout $k \in \mathbb{N}^*$, $F_{n+k} \equiv 2 \pmod{F_n}$.
5) Soient m et n dans \mathbb{N} avec $m > n$. En utilisant ce qui précède, montrer que F_m et F_n sont premiers entre eux.

Indication : poser $k = m - n$ et si d désigne le pgcd de F_m et F_n montrer que d divise 2.

Exercice 5 Cet exercice propose une démonstration du petit théorème de Fermat. Soit p un nombre premier et a un entier relatif non divisible par p . On note E l'ensemble $E = \{1, 2, \dots, p-1\}$.

- 1) Pour tout k élément de E , on note r_k le reste de la division euclidienne de ka par p . Montrer que :

$$\forall k \in E, r_k \neq 0 \text{ et } ka \equiv r_k \pmod{p}.$$

- 2) Soient k et l deux éléments de E tels que $r_k = r_l$. Montrer que $(k-l)a$ est divisible par p , puis que $k = l$.

- 3) On considère F l'ensemble $F = \{r_k \mid k \in E\}$. Déduire de la question précédente que F est un ensemble ayant $(p-1)$ éléments, puis que $F = E$ (remarquer que $F \subset E$).

- 4) En considérant le produit $a \times 2a \times \dots \times (p-1)a$ et en remarquant que le produit $r_1 \times r_2 \times \dots \times r_{p-1} = 1 \times 2 \times \dots \times (p-1)$; montrer que :

$$(a^{p-1} - 1)(1 \times 2 \times \dots \times (p-1)) \equiv 0 \pmod{p}.$$

- 5) En déduire que p divise $a^{p-1} - 1$, puis le petit théorème de Fermat.

Exercice 6 Soient P et Q deux polynômes non constants de $K[X]$, premiers entre eux.

- 1) Montrer alors que P^n et Q^m sont premiers entre eux, où n et m sont des entiers positifs.
2) Montrer de même que $P + Q$ et PQ sont premiers entre eux.

Exercice 7 Soit $(P_n)_{n \geq 0}$ la suite de polynômes de $\mathbb{R}[X]$, définie par : $P_0 = 0$, $P_1 = 1$ et

$$\forall n \in \mathbb{N}, P_{n+2} = XP_{n+1} - P_n.$$

- 1) Calculer P_2 , P_3 et P_4 .
2) Montrer par récurrence sur n que : $\forall n \in \mathbb{N}, P_{n+1}^2 = 1 + P_n P_{n+2}$.
3) En déduire que pour tout $n \in \mathbb{N}$, les polynômes P_n et P_{n+1} sont premiers entre eux.

Exercice 8 Soit $n \in \mathbb{N}^*$ et soit $P_n = (X-2)^{2n} + (X-1)^n - 1$.

- 1) Montrer que P_n est divisible par $X-1$ et par $X-2$.

On note Q_1 et Q_2 les quotients correspondants.

- 2) Montrer que P_n est divisible par $(X-1)(X-2)$ et que le quotient est $Q_2 - Q_1$.
3) Montrer que ce quotient est égal à :

$$\left((X-2)^{2n-2} - (X-2)^{2n-3} + \dots - (X-2) + 1 \right) + \left((X-1)^{n-2} + (X-1)^{n-3} + \dots + (X-1) + 1 \right).$$

Exercice 9 Effectuer les divisions suivant les puissances croissantes de :

- i) $P = 1$ par $Q = 1 - X$, à l'ordre n ,
ii) $P = 1 + X$ par $Q = 1 + X^2$ à l'ordre 5.

Corrigé de la série d'Algèbre $n^{\circ}4$ **Exercice 1**

1) On a $17 \equiv 1 \pmod{4}$, d'où $17^{17} \equiv 1^{17} = 1 \pmod{4}$, et comme $0 \leq 1 < 4$, alors 1 est le reste de la division euclidienne de 17^{17} par 4.

2) D'après la question précédente, il existe $q \in \mathbb{N}$ tel que $17^{17} = 4q + 1$. D'autre part, $23 \equiv 3 \pmod{10}$ d'où $23^{17^{17}} \equiv 3^{17^{17}} = 3^{4q+1} = 3^{4q}3 = 81^q3 \pmod{10}$. Comme $81 \equiv 1 \pmod{10}$, on trouve $23^{17^{17}} \equiv 1^q3 = 3 \pmod{10}$, et puisque $0 \leq 3 < 10$, alors 3 est le reste de la division euclidienne de $23^{17^{17}}$ par 10. De la même manière, $17 \equiv 7 \pmod{10}$ implique que $17^{17^{17}} \equiv 7^{17^{17}} = 7^{4q+1} = 7^{4q}7 \pmod{10}$. Comme $7^4 = 49 \times 49$ et comme $49 \equiv -1 \pmod{10}$, alors $7^4 = (49)^2 \equiv (-1)^2 = 1 \pmod{10}$, d'où $7^{4q}7 \equiv 1^q7 = 7 \pmod{10}$. Ainsi, $17^{17^{17}} \equiv 7 \pmod{10}$, et puisque $0 \leq 7 < 10$, alors 7 est le reste cherché.

Exercice 2 Soit n un entier naturel. Le but de l'exercice est de montrer que 30 divise toujours $n^5 - n$.

1) Comme $n^5 - n = n(n^4 - 1)$, alors 2 divise n si n est pair et divise $n^4 - 1$ si n est impair puisque dans ce cas n^4 est impair, ce qui fait que $n^4 - 1$ est pair. Donc dans tous les cas, 2 divise $n^5 - n$.

2) $(n^3 - n)(n^2 + 1) = n^5 - n^3 + n^3 - n = n^5 - n$. D'après le petit théorème de Fermat, $n^3 \equiv n \pmod{3}$, donc 3 divise $n^3 - n$, par suite, 3 divise $n^5 - n$.

3) Pour montrer que $30 \mid (n^5 - n)$, il suffit de prouver que $5 \mid (n^5 - n)$, car $30 = 2 \times 3 \times 5$ et 2, 3 et 5 sont premiers entre eux deux à deux. Or on sait, d'après le petit théorème de Fermat, que $5 \mid (n^5 - n)$, d'où le résultat.

Exercice 3

1) L'algorithme d'Euclide donne :

$$\begin{cases} 31 = 14 \times 2 + 3, \\ 14 = 3 \times 4 + 2, \\ 3 = 2 + 1. \end{cases}$$

Donc le dernier reste non nul est 1 et c'est le pgcd de 31 et 14. Ainsi, 31 et 14 sont premiers entre eux.

2) En remontant l'algorithme d'Euclide, on trouve :

$$1 = 3 - 2 = 3 - (14 - 3 \times 4) = 3 \times 5 - 14 = (31 - 14 \times 2) \times 5 - 14 = (-11) \times 14 + 5 \times 31; \text{ d'où :}$$

$$(-11) \times 14 + 5 \times 31 = 1.$$

3) Comme 14 et 31 sont premiers entre eux, alors le théorème du reste chinois assure le fait que le système de congruences

$$(SC) \quad \begin{cases} x \equiv 9 \pmod{14} \\ x \equiv 13 \pmod{31} \end{cases}$$

admet une infinité de solutions dans \mathbb{Z} .

a) On sait qu'une solution particulière peut être donnée en utilisant l'identité de Bézout ; c'est :

$$c = 13 \times (-11) \times 14 + 9 \times 5 \times 31 = -607.$$

Les autres solutions sont $x_k = -607 + 14 \times 31 \times k = -607 + 434q$ avec $q \in \mathbb{Z}$. La plus petite solution positive correspond à $q = 2$, et c'est $x_0 = 868 - 607 = 261$.

b) En écrivant le système dans \mathbb{Z} , puis dans $\mathbb{Z}/14\mathbb{Z}$ par exemple, cela donne :

$$\begin{cases} x &= 9 + 14k, \\ x &= 13 + 31l, \end{cases} \implies \begin{cases} \bar{x} &= \bar{9}, \\ \bar{x} &= \bar{13} + \bar{31}l = \bar{13} + \bar{3}l, \end{cases}$$

d'où l'on tire :

$$\bar{3}l = \bar{9} - \bar{13} = \bar{-4} = \bar{10}.$$

Comme 14 et 3 sont premiers entre eux, alors 3 est inversible modulo 14. L'inverse de $\bar{3}$ dans $\mathbb{Z}/14\mathbb{Z}$ est $\bar{5}$, ce qui donne $\bar{l} = \bar{5}\bar{10} = \bar{8}$. En posant $l = 8 + 14q$, avec q variant dans \mathbb{Z} , on obtient :

$$x = 13 + 31l = 13 + 31 \times 8 + (14 \times 31)q = 261 + (14 \times 31)q.$$

Exercice 4 Nombres de Fermat.

1) Soient b et p deux entiers naturels. On a :

$$(b+1)(b^{2p} - b^{2p-1} + \dots - b + 1) = b^{2p+1} - b^{2p} + \dots - b^2 + b + b^{2p} - b^{2p-1} + \dots - b + 1 = b^{2p+1} + 1,$$

donc $b+1$ divise $b^{2p+1} + 1$, par suite, $b^{2p+1} + 1 \equiv 0 \pmod{b+1}$.

2) Pour tous $a, p, q \in \mathbb{N}$, et $a \geq 2$, on pose $b = a^q$ et en utilisant la question précédente, on a :

$$a^{q(2p+1)} + 1 = (a^q)^{2p+1} + 1 \equiv 0 \pmod{a^q + 1}.$$

3) Soit maintenant $a \in \mathbb{N}$, $a \geq 2$, et soit m un entier naturel non nul qu'on écrit de façon unique sous la forme $m = 2^n(2p+1)$, avec $n, p \in \mathbb{N}$.

a) En posant $q = 2^n$ et en utilisant ce qui précède, on a facilement : $a^m + 1 \equiv 0 \pmod{a^{2^n} + 1}$.

b) On peut donc dire que $a^{2^n} + 1$ est un diviseur de $a^m + 1$ strictement plus grand que 1. Si on suppose que $a^m + 1$ est premier, alors $a^m + 1 = a^{2^n} + 1$, d'où $a^m = a^{2^n}$, et ceci n'est possible que si $p = 0$ et $m = 2^n$, d'où le résultat.

4) Pour tout $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$ (F_n est appelé le $n^{\text{ème}}$ nombre de Fermat).

a) Pour tout $k \in \mathbb{N}^*$, $(F_n - 1)^{2^k} + 1 = (2^{2^n})^{2^k} + 1 = 2^{2^n \cdot 2^k} + 1 = 2^{2^{n+k}} + 1 = F_{n+k}$.

b) Pour tout $k \in \mathbb{N}^*$, on a :

$$F_n - 1 \equiv -1 \pmod{F_n} \Rightarrow (F_n - 1)^{2^k} \equiv (-1)^{2^k} \pmod{F_n} \Rightarrow (F_n - 1)^{2^k} + 1 \equiv (-1)^{2^k} + 1 \pmod{F_n},$$

et comme $k > 0$, alors 2^k est pair, d'où $(-1)^{2^k} = 1$, par suite, $F_{n+k} = (F_n - 1)^{2^k} + 1 \equiv 2 \pmod{F_n}$.

5) Soient m et n dans \mathbb{N} avec $m > n$. Si on pose $k = m - n$, alors $k > 0$ et d'après ce qui précède :

$$F_m = F_{n+k} \equiv 2 \pmod{F_n}.$$

Il existe donc $q \in \mathbb{Z}$ tel que $F_m = qF_n + 2$, et si d est le pgcd de F_m et F_n , alors d divise $F_m - qF_n = 2$ car d divise à la fois F_m et F_n . Ainsi, d divise 2, donc $d = 1$ ou 2. Comme les nombres de Fermat sont des entiers impairs, $d = 1$, d'où F_m et F_n sont premiers entre eux.

Exercice 5 Cet exercice propose une démonstration du petit théorème de Fermat. Soit p un nombre premier et a un entier relatif non divisible par p . On note E l'ensemble $E = \{1, 2, \dots, p-1\}$.

1) Comme $1 \leq k \leq p-1$, alors p est premier avec k , et comme p premier avec a , alors p est premier avec ka , donc p ne divise pas ka , d'où $r_k \neq 0$.

D'après le théorème de la division euclidienne, il existe q et r_k dans \mathbb{Z} tel que $ka = pq + r_k$, où $0 < r_k < p$, d'où p divise $ka - r_k$, donc $ka \equiv r_k \pmod{p}$.

2) Soient k et l deux éléments de E tels que $r_k = r_l$. On sait que $ka \equiv r_k$ et $la \equiv r_l \pmod{p}$, d'où $ka - la = (k-l)a \equiv r_k - r_l \pmod{p}$, c.-à-d. $(k-l)a \equiv 0 \pmod{p}$. Ainsi, p divise $(k-l)a$. Comme p est premier avec a , alors d'après le théorème de Gauss, p divise $k-l$. Or $|k-l| < \max(k, l) < p$, et p

divise $|k - l|$, donc $|k - l| = 0$, d'où $k = l$.

3) On a montré que $r_k = r_l \Rightarrow k = l$, donc $\forall k, l \in E, k \neq l \Rightarrow r_k \neq r_l$. Donc il y a autant de restes $r_k \in F$ que d'éléments $k \in E$. Ainsi, F est un ensemble ayant $(p - 1)$ éléments. On a montré que $\forall k \in E, 0 < r_k < p$, donc $\forall k \in E, r_k \in E$, d'où $F \subset E$, et comme ils ont même cardinal, alors $F = E$.

4) Comme $F = E$, alors $r_1 \times r_2 \times \dots \times r_{p-1} = 1 \times 2 \times \dots \times (p - 1)$, et comme $ka \equiv r_k \pmod{p}$ pour tout $k \in E$, alors $a^{p-1}(1 \times 2 \times \dots \times (p - 1)) = a \times 2a \times \dots \times (p - 1)a \equiv r_1 \times r_2 \times \dots \times r_{p-1} = 1 \times 2 \times \dots \times (p - 1) \pmod{p}$. On a donc :

$$(a^{p-1} - 1)(1 \times 2 \times \dots \times (p - 1)) \equiv 0 \pmod{p}.$$

5) On a montré que p divise $(a^{p-1} - 1)(1 \times 2 \times \dots \times (p - 1))$, et comme p est premier avec $(1 \times 2 \times \dots \times (p - 1))$ (car p est premier avec tout élément k de E), alors, d'après le théorème de Gauss, p divise $a^{p-1} - 1$.

Conclusion : Pour tout entier $a \in \mathbb{Z}$ premier avec p on a : $a^{p-1} \equiv 1 \pmod{p}$, donc $a^p \equiv a \pmod{p}$. Si $a \in \mathbb{Z}$ est tel que p divise a , alors p divise aussi a^p , donc $a^p \equiv 0 \equiv a \pmod{p}$. Cela termine la démonstration du petit théorème de Fermat.

Exercice 6

1) Montrons par récurrence sur n que P^n et Q sont premiers entre eux.

La propriété est vraie pour $n = 1$, (c'est la donnée de base).

Soit $n \geq 1$ tel que P^n et Q soient premiers entre eux. Comme P et Q sont premiers entre eux par hypothèse, alors d'après le théorème de Bézout, il existe des polynômes U, V, U_n et V_n de $K[X]$ tels que :

$$\begin{cases} UP + VQ = 1 \\ U_n P^n + V_n Q = 1 \end{cases}$$

On en déduit alors (en multipliant la deuxième égalité par UP) que :

$$UU_n P^{n+1} + UV_n PQ = UP = 1 - VQ,$$

d'où :

$$(UU_n)P^{n+1} + (V + UPV_n)Q = 1.$$

Ainsi, P^{n+1} et Q vérifient l'identité de Bézout ; ils sont donc premiers entre eux.

Soient maintenant n et m deux entiers positifs. On sait que $R = P^n$ et Q sont premiers entre eux, et d'après ce qui précède on a : R et Q^m sont premiers entre eux, d'où le résultat.

2) Comme P et Q sont premiers entre eux, alors d'après le théorème de Bézout, il existe des polynômes U et V de $K[X]$ tels que : $UP + VQ = 1$, d'où

$$UP + UQ - UQ + VQ = UP + VQ = 1 = U(P + Q) + (V - U)Q.$$

Donc $P + Q$ et Q sont premiers entre eux.

Exercice 7 Soit $(P_n)_{n \geq 0}$ la suite de polynômes de $\mathbb{R}[X]$, définie par : $P_0 = 0, P_1 = 1$ et

$$\forall n \in \mathbb{N}, P_{n+2} = XP_{n+1} - P_n.$$

1) • $P_2 = XP_1 - P_0 = X, P_3 = XP_2 - P_1 = X^2 - 1$ et $P_4 = XP_3 - P_2 = X^3 - 2X$.

2) • Pour $n = 0$, on a : $P_1^2 = 1$ et $P_0 P_2 = 0 \cdot X = 0$, d'où $P_1^2 = 1 = 1 + P_0 P_{2+2}$. Donc la propriété est vraie à l'ordre 0.

• Soit $n \geq 0$, supposons qu'à l'ordre n on ait : $P_{n+1}^2 = 1 + P_n P_{n+2}$, alors :

$$\begin{aligned} 1 + P_{n+1} P_{n+3} &= 1 + P_{n+1}(XP_{n+2} - P_{n+1}) = 1 - P_{n+1}^2 + XP_{n+1} P_{n+2} \stackrel{\text{HR}}{=} \\ &= -P_n P_{n+2} + XP_{n+1} P_{n+2} = P_{n+2}(XP_{n+1} - P_n) = P_{n+2}^2. \end{aligned}$$

Donc la propriété est vraie à l'ordre $n + 1$, d'où le résultat.

3) • Pour tout $n \in \mathbb{N}$, les polynômes P_n et P_{n+1} sont liés par l'identité : $P_{n+1}^2 = 1 + P_n P_{n+2}$, qui conduit

à l'identité : $P_{n+1}^2 - P_n P_{n+2} = 1$; qui n'est rien d'autre que l'identité de Bézout : $UP_n + VP_{n+1} = 1$, où $U = -P_{n+2}$ et $V = P_{n+1}$. Donc pour tout $n \in \mathbb{N}$, les polynômes P_n et P_{n+1} sont premiers entre eux.

Exercice 8 Soit $n \in \mathbb{N}^*$ et soit $P_n = (X-2)^{2n} + (X-1)^n - 1$.

1) On a $P(1) = (-1)^{2n} - 1 = 1 - 1 = 0$ et $P(2) = (2-1)^n - 1 = 1 - 1 = 0$, donc 1 et 2 sont des racines de P_n , d'où P_n est divisible par $X-1$ et par $X-2$.

On note Q_1 et Q_2 les quotients correspondants.

2) Comme $P_n = (X-1)Q_1 = (X-2)Q_2$, alors :

$$(X-1)(X-2)(Q_2 - Q_1) = (X-1)P_n - (X-2)P_n = P_n.$$

Donc P_n est divisible par $(X-1)(X-2)$ et le quotient est $Q_2 - Q_1$.

3) En multipliant le quotient proposé par $(X-1)(X-2)$, on obtient :

$$\begin{aligned} (X-1)(X-2) & \left[\left((X-2)^{2n-2} - (X-2)^{2n-3} + \dots - (X-2) + 1 \right) + \left((X-1)^{n-2} + (X-1)^{n-3} + \dots + (X-1) + 1 \right) \right] = \\ & (X-2) \left[(X-2+1) \left((X-2)^{2n-2} - (X-2)^{2n-3} + \dots - (X-2) + 1 \right) \right] + \\ & (X-1) \left[(X-1-1) \left((X-1)^{n-2} + (X-1)^{n-3} + \dots + (X-1) + 1 \right) \right]. \end{aligned}$$

Il est facile de remarquer que $(X-1-1) \left((X-1)^{n-2} + (X-1)^{n-3} + \dots + (X-1) + 1 \right) = (X-1)^{n-1} - 1$.

On utilise ensuite l'identité :

$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$ qui, lorsque k est impair et $b = -1$, donne : $a^k + 1 = a^k - (-1)^k = (a+1)(a^{k-1} - a^{k-2} + \dots - a + 1)$. Donc, si on pose $k = 2n-1$ et $a = X-2$, on obtient : $(X-2+1) \left((X-2)^{2n-2} - (X-2)^{2n-3} + \dots - (X-2) + 1 \right) = (X-2)^{2n-1} - (-1)^{2n-1} = (X-2)^{2n-1} + 1$.

On arrive donc au résultat suivant :

$$\begin{aligned} (X-1)(X-2) & \left[\left((X-2)^{2n-2} - (X-2)^{2n-3} + \dots - (X-2) + 1 \right) + \left((X-1)^{n-2} + (X-1)^{n-3} + \dots + (X-1) + 1 \right) \right] = \\ & (X-2) \left((X-2)^{2n-1} + 1 \right) + (X-1) \left((X-1)^{n-1} - 1 \right) = (X-2)^{2n} + X - 2 + (X-1)^n - X + 1 = \\ & (X-2)^{2n} + (X-1)^n - 1 = P_n. \end{aligned}$$

Exercice 9

i) On remarque que $X^{n+1} - 1 = (X-1)(1+X+\dots+X^n)$, d'où : $(1-X)(1+X+\dots+X^n) + X^{n+1} = 1$. Ainsi, le quotient de la DSPC de $P = 1$ par $Q = 1-X$, à l'ordre n est $1+X+\dots+X^n$ et le reste est X^{n+1} .

ii) En effectuant les calculs appropriés, on trouve :

$$1+X = (1+X^2)(1+X-X^2-X^3+X^4+X^5) - X^6(1+X).$$

Donc le quotient de la DSPC de $P = 1+X$ par $Q = 1+X^2$ à l'ordre 5 est $1+X-X^2-X^3+X^4+X^5$ et le reste est $-X^6(1+X)$.