Feuille de TD

Structures algébriques

Relations

Exercice 1.
On munit $E = \mathbb{Z} \times \mathbb{N}^*$ de la relation $\mathcal{R}$:
$(p_1, q_1)\,\mathcal{R}\,(p_2, q_2) \iff p_1 \cdot q_2 = p_2 \cdot q_1$.

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Déterminer la classe d'équivalence de $(1, 5)$.
3. On note $E/\mathcal{R}$ l'ensemble des classes d'équivalence pour la relation $\mathcal{R}$. Montrer que cet ensemble est en bijection avec l'ensemble des nombres rationnels $\mathbb{Q}$.

Remarque : Cette méthode est la façon la plus simple de construire l'ensemble $\mathbb{Q}$. La bijection prouve que toutes les constructions de $\mathbb{Q}$ possibles donnent le "même" ensemble.

---

1. On montre facilement que $\mathcal{R}$ est symétrique et réflexive.
   Reste la transitivité. Si $(p_1, q_1)\mathcal{R}(p_2, q_2)$ et $(p_2, q_2)\mathcal{R}(p_3, q_3)$, alors on a :
   $$p_1 q_3 = \frac{p_1 q_2 q_3}{q_2} = \frac{p_2 q_1 q_3}{q_2} = \frac{q_2 p_3 q_1}{q_2} = p_3 q_1,$$
   donc on a bien obtenu $(p_1, q_1)\mathcal{R}(p_3, q_3)$.
   Cette relation est bien une relation d'équivalence.
2. On a $(p, q)\mathcal{R}(1, 5)$ ssi $5p = q$.
   Comme on doit avoir $q > 0$, on a donc $C((1, 5)) = \{(p, 5p),\ p \in \mathbb{N}^*\}$.
3. On pose la fonction $f : E/\mathcal{R} \to \mathbb{Q}$ par $f(C((p, q))) = \frac{p}{q}$.
   Montrons que cette fonction est bien définie.
   Si $(p_1, q_1)\mathcal{R}(p_2, q_2)$, alors on a $q_1, q_2 \neq 0$, et par définition on obtient $\frac{p_1}{q_1} = \frac{p_2}{q_2}$.
   L'image d'une classe d'équivalence ne dépend pas du représentant de la classe d'équivalence que l'on choisit. Donc, la fonction f est bien définie.
   Montrons que f est bijective.
   On remarque que f est surjective, car pour $\frac{p}{q} \in \mathbb{Q}$ (avec $q > 0$) on a $\frac{p}{q} = f(C((p, q)))$.
   Ensuite, on a $f(C((p, q))) = f(C((p', q')))$ ssi $\frac{p}{q} = \frac{p'}{q'}$ ssi $pq' = p'q$, ssi $C((p, q)) = C((p', q'))$. Donc f est bien injective.
   Ainsi, la fonction f est bien une bijection.

Fonctions

Exercice 2.
Soient A et B deux parties de E et F. Soit f une application de E dans F. Déterminer si les propositions suivantes sont vraies ou fausses. Justifier.

1. Si A est une partie finie de E alors $f(A)$ est une partie finie de F.
2. Si $f(A)$ est une partie finie de F alors A est une partie finie de E.
3. Si B est une partie finie de F alors $f^{-1}(B)$ est une partie finie de E.
4. Si $f^{-1}(B)$ est une partie finie de E alors B est une partie finie de F.

---

1. Vrai. Notons n le cardinal de A. On peut alors écrire $A = \{x_1, \ldots, x_n\}$. Donc $f(A) = \{f(x_1), \ldots, f(x_n)\}$ et $\text{card}(f(A)) \leq n$. Donc $f(A)$ est une partie finie de F.
2. Faux. Il suffit de prendre E une partie infinie, $A = E$ et choisir une fonction constante. Dans ce cas, $f(A)$ est un singleton, de cardinal 1.
   Par exemple, on prend $E = F = \mathbb{N}$ et $f : \mathbb{N} \longrightarrow \mathbb{N}\ ;\ n \longmapsto 0$. Alors $f(E) = \{0\}$ est une partie finie (de cardinal 1) de F mais $\mathbb{N}$ est une partie infinie de $\mathbb{N}$.
3. Faux. Le même contre-exemple qu'à la question précédente convient. On prend $E = F = \mathbb{N}$, $f : \mathbb{N} \longrightarrow \mathbb{N}\ ;\ n \longmapsto 0$ et $B = \{0\} \subset \mathbb{N}$ de cardinal 1. On a $f^{-1}(B) = \mathbb{N}$ qui est une partie infinie de $\mathbb{N}$.
4. Faux. On prend $E = F = \mathbb{N}$, $f : \mathbb{N} \longrightarrow \mathbb{N}\ ;\ x \longmapsto \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ sinon} \end{cases}$ et $B = \mathbb{N}^*$. Alors $f^{-1}(B) = \{1\}$ est fini (de cardinal 1) et B est une partie infinie de $\mathbb{N}$.
   On pouvait aussi prendre pour f la fonction $n \longmapsto 0$ et $f^{-1}(\mathbb{N}^*) = \emptyset$ qui est une partie finie, de cardinal 0.

Dénombrement

Exercice 3.

1. Soit $n \in \mathbb{N}^*$.

(a) Calculer le nombre de couples d'entiers (i, j) tels que $1 \leq i \leq j \leq n$.

(b) Calculer le nombre de triplets d'entiers (i, j, k) tels que $1 \leq i \leq j \leq k \leq n$.
On pourra utiliser la formule $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) On lance 3 dés (à 6 faces) et on range les chiffres obtenus dans l'ordre croissant. Combien de résultats différents sont possibles ?

2. Soit $n \in \mathbb{N}$.

(a) Calculer le nombre de couples d'entiers naturels $(i, j) \in \mathbb{N}^2$ tels que $i + j = n$.

(b) Calculer le nombre de couples d'entiers naturels $(i, j) \in \mathbb{N}^2$ tels que $i + 2j = n$.

---

1. (a) Il y a n choix pour j, puis j choix pour i. Le nombre de possibilités est donc

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

(b) Soit T ce nombre de triplets. On choisit d'abord $k \in [\![1, n]\!]$, il reste à choisir un couple (i, j) tel que $1 \leq i \leq j \leq k$, on obtient

$$T = \sum_{k=1}^{n} \frac{k(k+1)}{2}.$$

On obtient donc

$$T = \frac{n(n+1)(2n+1)}{12} + \frac{n(n+1)}{4} = \frac{n(n+1)(n+2)}{6}.$$

Remarque : *On remarque que le résultat obtenu est égal à* $\binom{n+2}{3}$. *Voici une méthode combinatoire : on définit* $X = [\![1, n]\!] \cup \{a, b\}$ *et on choisit trois éléments dans* X, *il y a bien sûr* $\binom{n+2}{3}$ *possibilités. Ceci est équivalent à notre problème : si on choisit trois éléments dans* $[\![1, n]\!]$, *cela correspond à un triplet de trois chiffres distincts ; si on choisit deux éléments dans* $[\![1, n]\!]$ *et* a, *cela correspond à un triplet* (i, i, k) *; si on choisit deux éléments dans* $[\![1, n]\!]$ *et* b, *cela correspond à un triplet* (i, k, k) *; enfin si on choisit un élément dans* $[\![1, n]\!]$ *et* a, b, *cela correspond à un triplet* (i, i, i).

(c) Cela revient à chercher le nombre de triplets précédents, on applique donc la formule pour $n = 6$ et on trouve 56 possibilités.

2. (a) Il y a $n + 1$ choix possibles pour i. Une fois que i est choisi, il n'y a qu'une possibilité pour j. Au total, on a donc $n + 1$ couples.

(b) i doit être de la même parité que n.

— Si n est pair, on a $\frac{n}{2} + 1$ couples.

— Si n est impair, on a $\frac{n+1}{2}$ couples.

Exercice 4. 1. Soit $n \in \mathbb{N}^*$, $k \in [\![1, n]\!]$, on veut montrer la formule du pion :

$$k\binom{n}{k} = n\binom{n-1}{k-1}. \tag{1}$$

(a) Montrer (1) en utilisant la formule de $\binom{n}{k}$.

(b) Montrer (1) en comptant de deux façons différentes le nombre de couples (X, a) tels que $X \subset [\![1, n]\!]$ avec $|X| = k$ et $a \in X$.

2. Soit $n \in \mathbb{N}^*$. On veut montrer que

$$\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}. \tag{2}$$

(a) Montrer (2) en utilisant (1).

(b) Montrer (2) en dérivant $x \longmapsto (1 + x)^n$.

3. Calculer de deux façons la somme $\displaystyle\sum_{k=0}^{n} \frac{\binom{n}{k}}{k+1}$.

---

1. (a) On a

$$k\binom{n}{k} = \frac{k\,n!}{k!\,(n-k)!} = \frac{n!}{(k-1)!\,(n-k)!} = n\frac{(n-1)!}{(k-1)!\,(n-1-(k-1))!} = n\binom{n-1}{k-1}.$$

(b) La première méthode est de choisir X, on a $\binom{n}{k}$ possibilités, puis choisir a dans X, on a k possibilités. Au total $k\binom{n}{k}$ possibilités.
La deuxième méthode est de choisir d'abord $a \in [\![1, n]\!]$, on a n possibilités, puis de choisir $k - 1$ nombres dans $[\![1, n]\!] \setminus \{a\}$ pour compléter X, on a $\binom{n-1}{k-1}$ possibilités.
Au total $n\binom{n-1}{k-1}$ possibilités.

2. (a) En utilisant (1), on a

$$\sum_{k=1}^{n} k\binom{n}{k} = n\sum_{k=1}^{n} \binom{n-1}{k-1} = n\sum_{l=0}^{n-1} \binom{n-1}{l} = n2^{n-1}.$$

(b) D'après la formule du binôme, pour tout $x \in \mathbb{R}$,

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

En dérivant, on obtient

$$n(1+x)^{n-1} = \sum_{k=1}^{n} k\binom{n}{k} x^{k-1},$$

ce qui donne le résultat pour $x = 1$.

3. — La première méthode est d'utiliser (1), qui nous dit que

$$\frac{\binom{n}{k}}{k+1} = \frac{\binom{n+1}{k+1}}{n+1}.$$

Il reste à sommer pour obtenir $\dfrac{2^{n+1}-1}{n+1}$.

— La deuxième méthode consiste à intégrer la fonction $x \longmapsto (1+x)^n$ et à utiliser la formule du binôme.

Exercice 5. Déterminer les bornes supérieure et inférieure des parties suivantes, après avoir justifié leur existence. Ces parties admettent-elles un maximum ou un minimum ?

1. $A = \left\{ (-1)^n + \dfrac{1}{n+1} \mid n \in \mathbb{N} \right\}$.
2. $B = \left\{ \dfrac{1}{n} - \dfrac{1}{p} \mid (n,p) \in (\mathbb{N}^*)^2 \right\}$.

---

1. • A est non vide et pour tout $n \in \mathbb{N}^*$, comme $\dfrac{1}{n+1} > 0$, $-1 < (-1)^n + \dfrac{1}{n+1}$, donc A est minoré par -1. Donc A admet une borne inférieure.
   1. -1 minore A.
   2. Posons, pour tout $p \in \mathbb{N}$, $u_p = (-1)^{2p+1} + \dfrac{1}{2p+2}$. Alors, pour tout $p \in \mathbb{N}$, $u_p \in A$ (avec $n = 2p+1 \in \mathbb{N}$) et $u_p = -1 + \dfrac{1}{2p+2}$ tend vers -1 lorsque p tend vers $+\infty$.

   Donc d'après la caractérisation séquentielle de la borne inférieure, $\inf(A) = -1$.
   A n'admet pas de minimum car sinon, d'après le cours, ce serait $\inf(A) = -1$. Or pour tout $n \in \mathbb{N}^*$, $(-1)^n + \dfrac{1}{n+1} > -1$ donc $-1 \notin A$.

   • A est non vide et pour tout $n \in \mathbb{N}^*$, $(-1)^n + \dfrac{1}{n+1} \leq 1 + 1 = 2$. Donc A admet une borne supérieure.
   1. 2 majore A.
   2. On a $(-1)^0 + \dfrac{1}{0+1} = 2$ et $(-1)^0 + \dfrac{1}{0+1} \in A$, donc $2 \in A$.

   On en déduit que $2 = \max(A)$ et donc $2 = \sup(A) = \max(2)$.

2. • B est non vide et pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\dfrac{1}{n} - \dfrac{1}{p} < \dfrac{1}{n} \leq 1$ car $p > 0$ et $n \geq 1$. Donc B est une partie non vide et majorée de $\mathbb{R}$, elle admet donc une borne supérieure.
   1. 1 majore B.
   2. Posons, pour tout $p \in \mathbb{N}^*$, $u_p = \dfrac{1}{1} - \dfrac{1}{p}$. Alors, pour tout $p \in \mathbb{N}^*$, $u_p \in B$ (avec $n = 1$) et $u_p = 1 - \dfrac{1}{p}$ tend vers 1 lorsque p tend vers $+\infty$.

   Donc, d'après la caractérisation séquentielle de la borne supérieure, $\sup(B) = 1$.
   B n'a pas de maximum car sinon ce serait $\sup(B) = 1$ et donc $1 \in B$. Or pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\dfrac{1}{n} - \dfrac{1}{p} < 1$ donc $1 \notin B$.

   • B est non vide et pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\dfrac{1}{n} - \dfrac{1}{p} > -\dfrac{1}{p} \geq -1$ car $n > 0$ et $p \geq 1$. Donc B est une partie non vide et minorée de $\mathbb{R}$, elle admet donc une borne inférieure.
   1. -1 minore B.
   2. Posons, pour tout $n \in \mathbb{N}^*$, $v_n = \dfrac{1}{n} - \dfrac{1}{1}$. Alors, pour tout $n \in \mathbb{N}^*$, $v_n \in B$ (avec $p = 1$) et $v_n = \dfrac{1}{n} - 1$ tend vers -1 lorsque n tend vers $+\infty$.

   Donc, d'après la caractérisation séquentielle de la borne inférieure, $\inf(B) = -1$.
   B n'a pas de minimum car sinon ce serait $\inf(B) = -1$ et donc $-1 \in B$. Or pour tout $(n,p) \in (\mathbb{N}^*)^2$, $\dfrac{1}{n} - \dfrac{1}{p} > -1$ donc $-1 \notin B$.

Exercice 6.

1. Démontrer que $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-2}{p-1} + \ldots + \binom{p-1}{p-1}$.
2. Démontrer que $\displaystyle\binom{p+q}{p} = \sum_{k=0}^{p} \binom{p}{k}\binom{q}{p-k}$.

---

1. On a la formule $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$, mais la même formule donne $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-2}{p-1} + \binom{n-2}{p}$ et on itère.

2. On considère un ensemble E à p éléments et un ensemble F à q éléments, avec $E \cap F = \emptyset$. On veut choisir p éléments dans $E \cup F$. Il y a $\binom{p+q}{p}$ possibilités. Mais on peut le faire de la façon suivante : pour $k \in [\![0, p]\!]$, on choisit k éléments dans E, ce qui fait $\binom{p}{k}$ possibilités, puis $p-k$ éléments dans F, ce qui fait $\binom{q}{p-k}$ possibilités.

   On peut aussi prouver cette formule en développant $(1+x)^{p+q}$ et $(1+x)^p(1+x)^q$, et en regardant le monôme x^p.

■ *Groupes* ■

Exercice 7.
Dire si ces ensembles avec ces lois de composition sont des groupes. Si oui, dire s'ils sont commutatifs ou non.

1. $(\mathbb{Z}, +)$
2. $(\mathbb{Z}, -)$
3. $(Fonct(\mathbb{R}, \mathbb{C}), +)$
4. $(\mathbb{K}[X] \setminus \{0\}, \times)$
5. $(P(E), \cup)$
6. $(P(E), \cap)$
7. $(P(E), \Delta)$, pour $A \Delta B = (A \cap \bar{B}) \cup (B \cap \bar{A})$

Tous les groupes ici sont commutatifs.

1. Oui.
2. Non. La loi n'est pas associative : $a - (b - c) \neq (a - b) - c$ pour certains entiers a, b, c.
3. Oui.
4. Non. Les polynômes non-constants n'ont pas d'inverse.
5. Non. L'élément neutre est $\emptyset$ mais toutes les parties non-vides n'ont pas d'inverse.
6. Non. L'élément neutre est E mais toutes les parties différentes de E n'ont pas d'inverse.
7. Oui. Le plus long est de montrer l'associativité. Ensuite, l'élément neutre est $\emptyset$, et l'inverse de A est A.

Exercice 8.
Soit $(G, \star)$ un groupe tel que $x^2 = e$ pour tout $x \in G$.
Montrer que le groupe G est commutatif.

Soient $x, y \in G$. Comme $x^2 = e = y^2$, on a $x^{-1} = x$ et $y^{-1} = y$.

On a aussi $(xy)^2 = e = xyxy$.

Ainsi, on en déduit que $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Donc G est commutatif.

Exercice 9.

1. Soit $(G, \star)$ un groupe commutatif. Soient $x \in G$ un élément d'ordre p et $y \in G$ un élément d'ordre q. Montrer que xy est d'ordre au plus pq.
2. xy est-il nécessairement d'ordre pq ? (donnez des exemples)
3. On pose $H = \text{Bij}(\mathbb{Z} \times \mathbb{Z})$.
   Montrer que $f : (m, n) \mapsto (-n, m)$ et $g : (m, n) \mapsto (n, -m - n)$ sont des éléments de $(H, \circ)$ d'ordres 4 et 3.
   Quel est l'ordre de $f \circ g$?

---

1. Le groupe G étant commutatif, on a : $(xy)^{pq} = (x^p)^q (y^q)^p = 1^q 1^p = 1$. Donc xy est d'ordre au plus pq.
2. Non. Par exemple $-I_n$ est d'ordre 2 dans $Gl_n(\mathbb{K})$, et $(-I_n)(-I_n) = iI_n$ n'est pas d'ordre 4 mais d'ordre 1.
   Par contre, dans $\mathbb{C}^*$, $a = \exp(i\pi)$ est d'ordre 2, $b = \exp(2i\pi/3)$ est d'ordre 3 et $ab = \exp(5i\pi/6)$ est d'ordre 6.
3. On trouve $f^4 = id$ et $g^3 = id$, ce qui prouve que f et g sont des bijections de $\mathbb{Z} \times \mathbb{Z}$ d'ordre respectif 4 et 3. Enfin, $f \circ g(m, n) = (m + n, n)$ et $(f \circ g)^k(1, 0) = (k, 0)$, donc $(f \circ g)^k \neq Id$ pour $k > 0$. On en déduit que $f \circ g$ est d'ordre infini et pas d'ordre au plus 6. Cela ne contredit pas la première question, car l''hypothèse G commutatif n'est pas vérifiée.

Exercice 10.

1. Pour $(G, \star)$ un groupe, quels sont les éléments de G d'ordre 1 ?
2. Combien vaut $ord(x^{-1})$ en fonction de $ord(x)$?
3. Trouver des matrices de $Gl_3(\mathbb{R})$ d'ordres 2 et 3.
4. Soient $n \geq 2$ et $M \in Gl_n(\mathbb{R})$ une matrice diagonale. On suppose que M est d'ordre fini.
   Déterminer $ord(M)$.
5. Soit $n \geq 2$. On pose $G = Bij(\{1, \ldots, n\})$. On prend $f \in G$ avec $f(i) = i+1$ pour $1 \leq i \leq n-1$ et $f(n) = 1$.
   Calculer l'ordre de f dans $(G, \circ)$.

---

1. Si x est d'ordre 1, alors il vérifie $x^1 = e$, donc $x = e$.
2. On a $x^k = e$ si et seulement si on a $e = x^{-k} = (x^{-1})^k$. Donc, $ord(x^{-1}) = ord(x)$.

3. La matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ est d'ordre 3.
   La matrice $-I_3$ est d'ordre 2.
4. On a $M = Diag(\lambda_1, \ldots, \lambda_n)$, avec $\lambda_i \neq 0$. M est d'ordre fini, donc il existe $k > 0$ tel que $M^k = I_n$.
   Cela veut dire que l'on a $\lambda_i^k = 1$, pour tout $1 \leq i \leq n$. Comme les λ_i sont réels, cela implique que $\lambda_i = 1$ ou -1.
   Ainsi, la diagonale de la matrice M est à valeurs dans $\{-1, 1\}$.
   On obtient que si $M = I_n$, alors M est d'ordre 1, et sinon M est d'ordre 2 (on a $M^2 = I_n$).
5. La fonction f est d'ordre n dans $(G, \circ)$.
   Montrons que $f^n = Id$ et que $f^k \neq Id$ pour $1 \leq k \leq n-1$.
   Pour $0 \leq k \leq n-1$, on a $f^k(1) = f \circ \ldots \circ f(1) = k+1$.
   Cela montre déjà que l'ordre de f est infini ou strictement supérieur à n.
   Ensuite, pour tout $1 \leq i \leq n$, on a $f^{n-i}(i) = f^{n-i}(f^i(1)) = f^n(1) = n$.
   Ainsi, on a $f^n(i) = f^i(f^{n-i}(i)) = f^i(n) = f^{i-1}(f(n)) = f^{i-1}(1) = i$.
   Cela montre que $f^n = f \circ \ldots \circ f = Id$.
   Donc, f est un élément d'ordre n dans $(G, \circ)$.

Exercice 11.
Dire si les groupes suivants sont isomorphes ou non. Le prouver.

1. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$
2. $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$
3. $\mathbb{Z}/13\mathbb{Z}$ et $\mathbb{Z}/15\mathbb{Z}$
4. $(\mathbb{Z}/2Z) \times (\mathbb{Z}/4\mathbb{Z})$ et U_8 (racines 8èmes de l'unité)
5. $\mathbb{Z}/n!\mathbb{Z}$ et $\mathcal{S}_n$, $n \geq 2$.
   Moins facile ...
6. $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$
7. $(\mathbb{Z}^n, +)$ et $(\mathbb{Z}^m, +)$, $n < m$
   On pourra utiliser la base canonique de $\mathbb{Q}^m$ et chercher une contradiction.
8. $(\mathbb{Q}, +)$ et $(\mathbb{Q}^2, +)$
9. $(\mathbb{R}, +)$ et $(\mathbb{R}^2, +)$. (Pas de preuve demandée.)
10. $(\mathbb{R}, +)$ et $(\mathbb{R}^n, +)$, $n > 0$.

---

1. Non. Pour $f : \mathbb{Z} \to \mathbb{Q}$ morphisme de groupe, posons $r = f(1)$.
   Pour tout $n \in \mathbb{Z}$, on a $f(n) = f(n.1) = n.f(1) = n.r$ (car f est un morphisme de groupes pour la loi $+$).
   Alors, on a $Im(f) = r.\mathbb{Z}$, l'ensemble des multiples du rationnel r.
   Ainsi, le rationnel $\frac{r}{2}$ (ou 1 si $r = 0$) n'est pas dans $Im(f)$. Donc le morphisme f n'est pas bijectif.
2. Non. $\mathbb{Q}$ est dénombrable et $\mathbb{R}$ est infini non-dénombrable, donc ces ensembles ne sont pas en bijection. Un isomorphisme est une bijection, donc il n'en existe pas entre $\mathbb{Q}$ et $\mathbb{R}$.
3. Non. Ces groupes n'ont pas le même cardinal. Ils ne peuvent pas être isomorphes.
4. Non. L'ordre des éléments de $\mathbb{Z}/2\mathbb{Z}$ est 1 ou 2. L'ordre des éléments de $\mathbb{Z}/4\mathbb{Z}$ est $1, 2$ ou 4. Les éléments de $(\mathbb{Z}/2Z) \times (\mathbb{Z}/4\mathbb{Z})$ sont de la forme $(\bar{a}, \bar{b})$. Leur ordre est alors $1, 2$ ou 4.
   Or, U_8 possède des éléments d'ordre 8 (comme $\exp(\frac{2i\pi}{8})$). Ces groupes ne sont donc pas isomorphes.
5. Non si $n \geq 3$.
   Ces groupes ont le même cardinal. Mais $\mathbb{Z}/n!\mathbb{Z}$ est un groupe commutatif, tandis que $\mathcal{S}_n$ n'est pas un groupe commutatif. En effet, on a $(1\,2) \circ (2\,3) = (1\,2\,3) \neq (1\,3\,2) = (2\,3) \circ (1\,2)$.
   Si $n = 2$, ces deux groupes sont des groupes à 2 éléments qui sont isomorphes.
6. Non.
   Soit $f : \mathbb{Z} \to \mathbb{Z}^2$ un morphisme de groupes. On pose $(a, b) = f(1)$.
   Si $(a, b) = 0$, alors f n'est pas injectif, donc pas un isomorphisme.
   Si $(a, b) \neq 0$, alors on a $f(n) = f(n.1) = n.f(1) = n(a, b)$.
   Donc $Im(f) = (a, b)\mathbb{Z}$.
   Comme $(a, b) \neq (0, 0)$, on a donc $(-b, a) \notin Im(f)$. Donc f n'est pas surjectif, donc pas un isomorphisme.
7. Non.
   Supposons par l'absurde avoir $f : \mathbb{Z}^n \to \mathbb{Z}^m$ un isomorphisme de groupes.
   On va utiliser les propriétés des $\mathbb{Q}$-espaces vectoriels de dimension finie, en faisant attention à se ramener à des coefficients entiers.
   Posons $e_1, \ldots, e_m$ la base canonique de $\mathbb{Q}^m$ (elle est dans $\mathbb{Z}^m$.
   Alors, il existe $x_1, \ldots, x_m \in \mathbb{Z}^n$ tels que $f(x_i) = e_i$ par surjectivité.
   La famille $(x_1, \ldots, x_m)$ est une famille à $m > n$ éléments dans $\mathbb{Q}^n$, qui est un $\mathbb{Q}$-ev de dimension n. Donc cette famille est liée.
   On a donc des rationnels non-tous nuls $r_1, \ldots, r_m \in \mathbb{Q}$ tels que $r_1x_1 + \ldots + r_mx_m = 0$.
   En multipliant ces rationnels $r_1, \ldots, r_m$ par leur dénominateur commun, on a ainsi des nombres entiers $k_1, \ldots, k_m$, non tous nuls, tels que $k_1x_1 + \ldots + k_mx_m = 0$.
   Mais alors, on a $0 = f(0) = f(k_1x_1 + \ldots + k_mx_m) = f(k_1x_1) + \ldots + f(k_mx_m)$, $0 = k_1f(x_1) + \ldots + k_mf(x_m) = k_1e_1 + \ldots + k_me_m$.
   Comme les k_i sont non tous nuls et que la famille $(e_1, \ldots, e_m)$ est libre dans $\mathbb{Q}^m$, le vecteur $k_1e_1 + \ldots + k_me_m$ est donc non-nul, ce qui est impossible.
8. Non.
   Soit $f : \mathbb{Q} \to \mathbb{Q}^2$ un morphisme de groupes. On pose $(a, b) = f(1)$.

Si $(a,b)=0$, alors f n'est pas injectif, donc pas un isomorphisme.
Si $(a,b)\neq 0$, alors on a $f(n)=f(n.1)=n.f(1)=n(a,b)$.
Pour tout $r\in\mathbb{Q}$, on a $r=\frac{p}{q}$, d'où $f(qr)=f(q.r)=q.f(r)$ et $f(qr)=f(p)=p.f(1)=p(a,b)$.
On en déduit que $f(r)=\frac{p}{q}(a,b)$.
Ainsi, on a $Im(f)=(a,b)\mathbb{Q}$. Comme $(a,b)\neq(0,0)$, on a donc $(-b,a)\notin Im(f)$. Donc f n'est pas surjectif, donc pas un isomorphisme.

9. Oui.
La preuve est difficile.
Les ensembles $\mathbb{R}$ et $\mathbb{R}^2$ sont des $\mathbb{Q}$-ev.
Ils possèdent des bases B et B' comme $\mathbb{Q}$-ev (des bases infinies).
Comme ces ensembles sont infinis non-dénombrables, B est en bijection avec $\mathbb{R}$ et B' en bijection avec $\mathbb{R}^2$.
Or, $\mathbb{R}$ est en bijection avec $\mathbb{R}^2$, donc B est en bijection avec B'.
Avec cette bijection entre bases, on peut construire un isomorphisme de $\mathbb{Q}$-ev entre $\mathbb{R}$ et $\mathbb{R}^2$.
Un isomorphisme de $\mathbb{Q}$-ev est entre autres un morphisme de groupes, ce qui donne le résultat.

10. Oui.
On montre cela par récurrence sur $n\geq 2$.
En effet, cela est vrai pour $n=2$. Et si cette proposition est vraie pour un $n\geq 2$, alors on a $\mathbb{R}^{n+1}=\mathbb{R}^n\times\mathbb{R}\simeq\mathbb{R}\times\mathbb{R}\simeq\mathbb{R}$.

Exercice 12.
Soient $(G,\star)$ et (H,Δ) des groupes, et $f:G\to H$ un morphisme de groupes.

1. Soit G_1 un sous-groupe de G. Montrer que $f(G_1)$ est un sous-groupe de H.
2. Soit H_1 un sous-groupe de H. Montrer que $f^{-1}(H_1)$ est un sous-groupe de G.
3. Soit $x\in G$. Montrer que $f(\langle x\rangle)=\langle f(x)\rangle$.
4. Soit $S\subset G$ une partie de G.
Montrer que $f(\langle S\rangle)=\langle f(S)\rangle$.
5. Soit $S'\subset H$. Montrer qu'en général on a $f^{-1}(\langle S'\rangle)\neq\langle f^{-1}(S)\rangle$.

---

1. On montre que $f(G_1)$ contient e_H, et que pour $x,y\in f(G_1)$ on a $xy\in f(G_1)$ et $x^{-1}\in f(G_1)$.
2. On montre que $f^{-1}(H_1)$ contient e_G, et que pour $x,y\in f^{-1}(H_1)$ on a $xy\in f^{-1}(H_1)$ et $x^{-1}\in f^{-1}(H_1)$.
3. On a $\langle y\rangle=\{y^n,\ n\in\mathbb{Z}\}$. Or, on a vu en cours que $f(x^n)=f(x)^n$.
Donc, $f(\langle x\rangle)=\{f(x^n),\ n\in\mathbb{Z}\}=\{f(x)^n,\ n\in\mathbb{Z}\}=\langle f(x)\rangle$.
4. Le sous-groupe $\langle S\rangle$ est formé de tous les éléments de G de la forme $a_1\star\ldots\star a_m$, avec $m\geq 1$, et ($a_i\in S$ ou $a_i^{-1}\in S$).
Or, on a $f(a_1\star\ldots\star a_m)=f(a_1)\Delta\ldots\Delta f(a_m)$.
On obtient donc l'égalité : $f(\langle S\langle)=\langle f(S)\rangle$.
5. On prend $G=H=\mathbb{Z}$ et $f(n)=2n$. On prend $S'=\{3\}$.
Alors, on a $\langle S'\rangle=3\mathbb{Z}$. On a $\langle S'\rangle\cap Im(f)=6\mathbb{Z}$.
Cela donne : $f^{-1}(\langle S'\rangle)=3\mathbb{Z}$, et $\langle f^{-1}(S)\rangle=\langle\emptyset\rangle=\{0\}$.

Exercice 13. Soit G un groupe fini.
Pour tout $a\in G$, on pose $\Phi_a:x\in G\mapsto axa^{-1}\in G$.

1. Vérifier que Φ_a est un automorphisme de G (un isomorphisme de G dans G.
2. Montrer que pour $Aut(G)=\{f:G\to G, f \text{ automorphisme }\}$, $(Aut(G),\circ)$ est un groupe.
3. On pose $I=\{\Phi_a\mid a\in G\}$. Montrer que I est un sous-groupe de $Aut(G)$.
4. Montrer que $h:a\in G\mapsto\Phi_a\in I$ est un morphisme de groupes.
Déterminer $Ker(h)$.
5. On suppose que G est un groupe commutatif.
Déterminer I.
6. On suppose que I est un groupe cyclique (engendré par un seul élément, $I=\langle x\rangle$.
Montrer que G est un groupe commutatif.
7. En déduire que les ensembles I et $Aut(G)$ ne sont en général pas égaux.

---

1. Pour $a,b\in G$, on vérifique que $\Phi_a\circ\Phi_b=\Phi_{ab}$. On a de plus $\Phi_e=id_G$.
On en déduit que la fonction Φ_a est bijective, et que $\Phi_a^{-1}=\Phi_{a^{-1}}$.
Il reste à montrer que $\Phi_a:G\to G$ est un morphisme :
$$\forall x,y\in G,\ \Phi_a(xy)=axya^{-1}=(axa^{-1}aya^{-1}=\Phi_a(x)\Phi_a(y).$$
Cela est donc vrai.
2. La fonction Id_G est un automorphisme de G. Pour f,g deux automorphismes de G, on a vu en cours que f^{-1} est aussi un automorphisme.
On montre alors que $f\circ g$ est aussi un automorphisme. (fonction bijective, et morphisme de groupes). Cela montre que $(Aut(G),\circ)$ est un sous-groupe de $(Bij(G),\circ)$. Donc, $(Aut(G),\circ)$ est un groupe.

3. A la première question, on a montré que I est stable par multiplication, contient Id_G, et que tout élément possède un inverse dans I. C'est bien un sous-groupe de $Aut(G)$.
4. A la première question on a montré que $\Phi_a \circ \Phi_b = \Phi_{ab}$.
   Cela démontre que $h : a \mapsto \Phi_a$ est un morphisme de groupes.
   Son noyau est l'ensemble des $a \in G$ tels que $\Phi_a = Id_G$.
   Soit $b \in G$. On a $\Phi_a(b) = b$ ssi $aba^{-1} = b$, ssi $ab = ba$, ssi a et b commutent.
   Donc, on a $\Phi_a = Id_G$ ssi a commute avec tous les éléments de G.
   Ainsi, $Ker(h) = \{a \in G \text{ t.q. } ab = ba \, \forall b \in G\}$.
5. On a $I = \langle x \rangle$. Soit $a \in G$ tel que $\Phi_a = x$.
   Soit $b \in G$. Alors il existe n tel que $\Phi_b = \Phi_a^n = \Phi_{a^n}$.
   Alors, on a $a = \Phi_{a^n}(a) = \Phi_b(a)$, donc $a = bab^{-1}$, donc $ab = ba$.
   Ainsi a commute avec tous les éléments de G, donc $\Phi_a = id_G$, donc $I = \{id_G\}$, donc G est commutatif.
6. Prenons un contre-exemple. Pour $(G, \star) = (\mathbb{Z}, +)$, on a $I = \{Id_{\mathbb{Z}}\}$ car ce groupe est commutatif.
   Pourtant, $f : n \in \mathbb{Z} \mapsto -n \in \mathbb{Z}$ est un automorphisme de $\mathbb{Z}$.
   Ainsi, on a $Aut(\mathbb{Z}) \neq I$.

Exercice 14.
Soit $n \in \mathbb{N}^*$. Soient i, j, $k \in [\![1, n]\!]$.

1. Calculer $\begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix}$.
2. Calculer $\begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix} \begin{pmatrix} i & j \end{pmatrix}$.
3. Soit $\sigma \in \mathcal{S}_n$, que vaut $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$?

---

1. On note $\gamma = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix}$. Pour tout $x \in [\![1, n]\!] \setminus \{i, j, k\}$, $\gamma(x) = x$. De plus, $\gamma(i) = k$, $\gamma(k) = j$ et $\gamma(j) = i$. On dit que γ est un 3-cycle et on note $\gamma = \begin{pmatrix} i & k & j \end{pmatrix}$.
2. On note $\delta = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} i & k \end{pmatrix} \begin{pmatrix} i & j \end{pmatrix}$, on a $\delta(i) = i$, $\delta(j) = k$ et $\delta(k) = j$. Tous les autres points sont fixes donc $\delta = \begin{pmatrix} j & k \end{pmatrix}$.
3. Soit $\theta = \sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$. Si $x \in [\![1, n]\!]$ avec $\sigma^{-1}(x) \notin \{i, j\}$, on a $\theta(x) = \sigma(\sigma^{-1}(x)) = x$. Maintenant, $\theta(\sigma(i)) = \sigma(j)$ et $\theta(\sigma(j)) = \sigma(i)$. Finalement, $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(i) & \sigma(j) \end{pmatrix}$.

Exercice 15.
Décomposer les permutations suivantes en produit de cycles à supports disjoints, ainsi qu'en produit de transpositions, calculer leur ordre. Calculer enfin σ_1^{1000} et σ_2^{1000}.

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{bmatrix} \quad \text{et} \quad \sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{bmatrix}.$$

On a

$$\sigma_1 = \begin{pmatrix} 1 & 3 & 4 & 6 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix},$$

donc σ_1 est d'ordre 4. En effet, le 4-cycle $\begin{pmatrix} 1 & 3 & 4 & 6 \end{pmatrix}$ est d'ordre 4 donc l'ordre de σ_1 est plus grand que 4, et on peut vérifier que $\sigma_1^4 = \text{Id}$. Ainsi $\sigma_1^{1000} = \text{Id}$. Une décomposition de σ_1 en produit de transpositions est

$$\sigma_1 = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix}.$$

On a

$$\sigma_2 = \begin{pmatrix} 1 & 4 & 7 & 8 \end{pmatrix} \begin{pmatrix} 2 & 6 & 5 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix},$$

donc σ_2 est d'ordre 12. En effet, $\sigma_2^k = \begin{pmatrix} 1 & 4 & 7 & 8 \end{pmatrix}^k \begin{pmatrix} 2 & 6 & 5 \end{pmatrix}^k \begin{pmatrix} 3 & 9 \end{pmatrix}^k$. Si $\sigma_2^k = \text{Id}$ alors $\begin{pmatrix} 1 & 4 & 7 & 8 \end{pmatrix}^k = \text{Id}$ donc k est un multiple de 4, $\begin{pmatrix} 2 & 6 & 5 \end{pmatrix}^k = \text{Id}$ donc k est un multiple de 3, et $\begin{pmatrix} 3 & 9 \end{pmatrix}^k = \text{Id}$ donc k est un multiple de 2. Ainsi, k est un multiple de 12. On peut vérifier que $\sigma_2^{12} = \text{Id}$. Ainsi, $\sigma_2^{1000} = \sigma_2^{12 \times 83 + 4} = \sigma_2^4 = \begin{pmatrix} 2 & 6 & 5 \end{pmatrix}^4 = \begin{pmatrix} 2 & 6 & 5 \end{pmatrix}$. Une décomposition de σ_2 en produit de transpositions est

$$\sigma_2 = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix} \begin{pmatrix} 7 & 8 \end{pmatrix} \begin{pmatrix} 2 & 6 \end{pmatrix} \begin{pmatrix} 6 & 5 \end{pmatrix} \begin{pmatrix} 3 & 9 \end{pmatrix}.$$

Exercice 16.

1. Montrer que les doubles transpositions de la forme $\begin{pmatrix} 1 & i \end{pmatrix} \begin{pmatrix} 1 & j \end{pmatrix}$ engendrent le groupe alterné $\mathcal{A}_n$.
2. Montrer que les 3-cycles engendrent le groupe alterné $\mathcal{A}_n$.

---

1. On a montré dans le TD précédent que les transpositions de la forme $\begin{pmatrix} 1 & i \end{pmatrix}$ engendrent $\mathcal{S}_n$. Toute permutation de $\mathcal{A}_n$ s'écrit donc comme un produit de transpositions $\begin{pmatrix} 1 & i \end{pmatrix}$. Or un élément de $\mathcal{A}_n$ doit avoir une signature égale à 1, c'est-à-dire que le nombre de transpositions dans sa décomposition doit être pair. Cette permutation est donc un produit de doubles transpositions $\begin{pmatrix} 1 & i \end{pmatrix} \begin{pmatrix} 1 & j \end{pmatrix}$.
2. On a $\begin{pmatrix} 1 & i \end{pmatrix} \begin{pmatrix} 1 & j \end{pmatrix} = \begin{pmatrix} 1 & j & i \end{pmatrix}$, ce qui montre le résultat. *On a même montré mieux : le groupe alterné est engendré par les 3-cycles de la forme* $\begin{pmatrix} 1 & i & j \end{pmatrix}$.

Exercice 17. Soit $n \geq 2$. Soit $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$.
Déterminer l'ordre de $\overline{m}$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$.
Quels sont tous les ordres possibles ?
Pour chaque ordre r, trouver un élément $\overline{m}$ d'ordre r.

Pour déterminer cet ordre, on cherche tous les entiers $k \geq 1$ tels que $k.\overline{m} = \overline{0}$. (on regarde

l'équation $x^k = e$)
On a $k.\overline{m} = \overline{m} + \ldots + \overline{m} = \overline{km}$.
Et $\overline{km} = \overline{0}$ si et seulement si n divise km.
Comme n et m sont fixés, on a $n \mid km$ si et seulement si k est un multiple de $\frac{n}{pgcd(n,m)}$.
Ainsi, par minimalité de l'ordre d'un élément, on en déduit que $ord(\overline{m}) = \frac{n}{pgcd(n,m)}$.
On remarque que les ordres des éléments de $\mathbb{Z}/n\mathbb{Z}$ divisent n.
Réciproquement, pour tout d divisant n, on pose $m = \frac{n}{d}$.
Alors, $\text{pgcd}(n,m) = \frac{n}{d}$, et donc $ord(\overline{m}) = \frac{n}{\frac{n}{d}} = d$.
Les ordres des éléments de $\mathbb{Z}/n\mathbb{Z}$ sont exactement tous les diviseurs de n.

Exercice 18.
Décrire (cardinal, commutatif ou non, cyclique ou non, ordre des éléments) les groupes suivants :

1. $\mathbb{Z}/7\mathbb{Z}$
2. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
3. $\mathbb{Z}/8\mathbb{Z}$
4. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$ sont-ils isomorphes ?

---

1. C'est un groupe à 8 éléments. Il est commutatif. Il est cyclique, car engendré par $\bar{1}$.
   Il a 1 élément d'ordre 1, et 6 élément d'ordre 7.
2. C'est un groupe à 8 éléments. Il est commutatif.
   Il a 1 élément d'ordre 1, 3 éléments d'ordre 2, 4 éléments d'ordre 4.
   Ce groupe n'est donc pas cyclique, car il ne possède pas d'éléments d'ordre 8.
3. C'est un groupe à 8 éléments. Il est commutatif. Il est cyclique, car engendré par $\bar{1}$.
   Il a 1 élément d'ordre 1, 1 élément d'ordre 2, 2 éléments d'ordre 4, 4 éléments d'ordre 8.
4. Non, l'un a des éléments d'ordre 8 et l'autre n'en a pas.

Exercice 19.

1. Développer $(x^2 + x - \bar{1})(x^2 - x - \bar{1})$ et $(x^2 + \bar{2})(x^2 - \bar{2})$ dans $\mathbb{Z}/3\mathbb{Z}$.
2. Développer $(x^2 + x - \bar{1})(x^2 - x - \bar{1})$ et $(x^2 + \bar{2})(x^2 - \bar{2})$ dans $\mathbb{Z}/5\mathbb{Z}$
   Que remarque-t-on ?

---

1. On a $(x^2 + x - \bar{1})(x^2 - x - \bar{1}) = x^4 + \bar{1}$ et $(x^2 + \bar{2})(x^2 - \bar{2}) = x^4 - \bar{1}$
2. On a $(x^2 + x - \bar{1})(x^2 - x - \bar{1}) = x^4 + 2\bar{x}^2 + \bar{1}$ et $(x^2 + \bar{2})(x^2 - \bar{2}) = x^4 + \bar{1}$.
   On a des produits de polynômes de degré 2 qui donnent des résultats différents selon l'ensemble $\mathbb{Z}/n\mathbb{Z}$ choisi.

Exercice 20.

1. Résoudre l'équation diophantienne modulaire : $x \equiv 4 \bmod (6)$ et $x \equiv 7 \bmod 11$.

Trouver un isomorphisme entre les groupes suivants :

1. $\mathbb{Z}/15\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
2. $\mathbb{Z}/100\mathbb{Z}$ et $\mathbb{Z}/4Z \times \mathbb{Z}/25\mathbb{Z}$

On écrira à chaque fois ϕ et sa bijection réciproque ϕ^{-1}.

---

1. On utilise le théorème d'isomorphisme chinois.
   On recherche d'abord une solution particulière x_0.
   Les entiers 6 et 11 sont premiers entre eux.
   On trouve comme relation de Bézout : $2.6 - 11 = 1$.
   Ainsi, une solution particulière est $x_0 = 4.(-11) + 7.(12) = -44 + 84 = 40$.
   On a donc : ($x \equiv 4 \bmod (6)$ et $x \equiv 7 \bmod 11$) ssi $x \equiv 40 \bmod (66)$.
   Donc, l'ensemble des solutions est $40 + 66\mathbb{Z}$.
2. On a $\phi(\bar{c}) = (\bar{c}, \bar{c})$ et $\phi^{-1}(\bar{a}, \bar{b}) = 10a \bar{+} 6b$.
   Pour déterminer ϕ^{-1} il faut déterminer l'image de $(\bar{1}, \bar{0})$ et $(\bar{0}, \bar{1})$ (ici $\bar{10}$ et $\bar{6}$).
   On les détermine soit en testant certaines valeurs, soit avec l'algorithme d'Euclide.
   Comme on a $2.3 + (-1).5 = 1$, on obtient d'après le cours les valeurs de $\bar{-5} = \bar{10}$ et $\bar{6}$ dans $\mathbb{Z}/15\mathbb{Z}$.
3. On a $\phi(\bar{c}) = (\bar{c}, \bar{c})$ et $\phi^{-1}(\bar{a}, \bar{b}) = 76a \bar{+} 25b$.
   Pour déterminer ϕ^{-1} il faut déterminer l'image de $(\bar{1}, \bar{0})$ et $(\bar{0}, \bar{1})$ (ici $\bar{76}$ et $\bar{25}$).
   On les détermine soit en testant certaines valeurs, soit avec l'algorithme d'Euclide.
   Comme on a $1.25 + (-6).4 = 1$, on obtient d'après le cours les valeurs de $-\bar{24} = \bar{76}$ et $\bar{25}$ dans $\mathbb{Z}/100\mathbb{Z}$.

Exercice 21. Soit $n \geq 2$. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui ont un inverse pour $\times$.

1. Quels sont les éléments $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$?
2. Montrer que $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un groupe commutatif.
3. Trouver un produit de groupes $\mathbb{Z}/m\mathbb{Z}$ isomorphe à $(\mathbb{Z}/7\mathbb{Z})^\times$.
4. Trouver un produit de groupes $\mathbb{Z}/m\mathbb{Z}$ isomorphe à $(\mathbb{Z}/8\mathbb{Z})^\times$.
5. Trouver un produit de groupes $\mathbb{Z}/m\mathbb{Z}$ isomorphe à $(\mathbb{Z}/9\mathbb{Z})^\times$.

1. Ce sont les $\overline{a}$ tels que a est premier avec n.
2. Cet ensemble est stable pour la loi multiplication $\times$. En effet, si a et b sont premiers avec n, alors ab aussi.
   Cet ensemble contient l'élément neutre pour $\times$, qui est $\overline{1}$.
   On sait que la loi $\times$ est associative et commutative.
   Enfin, tout élément de cet ensemble possède un inverse pour $\times$.
   Donc, $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est bien un groupe commutatif.
3. Ce groupe est $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$. Il a 6 éléments.
   On montre que $\overline{3}$ est d'ordre 6 pour $\times$. Donc, $(\mathbb{Z}/7\mathbb{Z})^\times = \langle\overline{3}\rangle$. Ce groupe est donc un groupe cyclique à 6 éléments. Il est isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$.
4. Ce groupe est $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Il a 4 éléments.
   On montre que $\overline{3}, \overline{5}, \overline{7}$ sont d'ordre 2 pour $\times$. Donc, $(\mathbb{Z}/8\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/2Z) \times (\mathbb{Z}/2\mathbb{Z})$.
5. Ce groupe est $\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Il a 6 éléments.
   On montre que $\overline{2}$ est d'ordre 6 pour $\times$. Donc, $(\mathbb{Z}/9\mathbb{Z})^\times = \langle\overline{2}\rangle$. Ce groupe est donc un groupe cyclique à 6 éléments. Il est isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$.

■ *Anneaux* ■

Exercice 22.
Pour chaque anneau A, donner son groupe des inversibles $A^\times$, et résoudre (si l'on peut) l'équation $a^2 = 1_A$.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. $\mathbb{K}[X]$
3. $M_n(\mathbb{K})$
4. $\mathcal{F}(E, \mathbb{C})$, pour E un ensemble.
5. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$

Dans quelle famille d'anneaux l'équivalence "$a^2 = 1_A$ ssi $a = \pm 1_A$" est-elle forcément vraie ?

1. $\mathbb{Z}^\times = \{1, -1\}$. $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{C}^\times = \mathbb{C}^*$.
   Dans ces anneaux, on a $a^2 = 1$ ssi $a = \pm 1$.
2. $\mathbb{K}[X]^\times = \mathbb{K}^*$. On a $a^2 = 1$ ssi $a = \pm 1$.
3. $M_n(\mathbb{K})^\times = Gl_n(\mathbb{K})$. On a $A^2 = I_n$ ssi $(A - I_n)(A + I_n) = 0$.
   Cette équation possède énormément de solutions. Toutes les matrices diagonales $B = Diag(\lambda_1, \ldots, \lambda_n)$ avec $\lambda_i \in \{-1, 1\}$ sont des solutions.
   Pour toute matrice inversible P, la matrice PBP^{-1} est aussi une solution. En effet on a $(PBP^{-1})^2 = PB^2P^{-1} = PP^{-1} = I_n$.
4. On a $f \in \mathcal{F}(E, \mathbb{C})^\times$ si et seulement si $f(x) \neq 0$ pour tout $x \in E$. L'ensemble des fonctions inversibles pour $\times$ est donc l'ensemble des fonctions qui ne s'annulent jamais.
   On a $f^2 = 1$ si et seulement si $f(x) = \pm 1$ pour tout $x \in E$.
5. On a $\mathbb{Q}[\sqrt{2}]^\times = \mathbb{Q}[\sqrt{2}]^*$. En effet, on a $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}[\sqrt{2}]$.
   On a $a^2 = 1$ ssi $a = \pm 1$.

Si l'anneau A est intègre, on a $a^2 = 1$ ssi $(a-1)(a+1) = 0$ ssi ($a - 1 = 0$ ou $a + 1 = 0$) ssi $a = \pm 1$.

Exercice 23.
• Donner le groupe des inversibles de l'anneau $\mathbb{Z}/20\mathbb{Z}$. Quel est son cardinal ?
• Donner un isomorphisme de groupes ϕ entre $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$ et $((\mathbb{Z}/20\mathbb{Z})^\times, \times)$. On ne demande pas de vérifier que ϕ est bien un isomorphisme de groupes.

Les inversibles sont obtenus à partir des nombres premiers avec 20

$$G = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

C'est un groupe à 8 éléments.
3 est un élément d'ordre 4 dans $(G, \times)$ avec

$$\langle 3\rangle = \{1, 3, 9, 7\}$$

et 11 est un élément d'ordre 2 n'appartenant pas à $\langle 3\rangle$.
La fonction $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to G$ telle que

$$\varphi(\overline{k}, \overline{\ell}) = 11^k \times 3^\ell$$

est bien définie. On peut montrer que c'est un morphisme de groupes, injectif, entre deux groupes à 6 éléments. C'est donc bien un morphisme de groupes.

Exercice 24. On pose $j := e^{\frac{2i\pi}{3}}$. et $\mathbb{Z}[j] := \{a + jb \in \mathbb{C}/(a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $1 + j + j^2 = 0$
2. Est-ce que $(\mathbb{Z}[j], +, \times)$ est un anneau ? Dire pourquoi.
3. Soit $z \in \mathbb{Z}[j]$.
   Montrer que $z \in \mathbb{Z}[j]^\times \Leftrightarrow |z| = 1$

4. Soit $z = a + jb \in \mathbb{Z}[j]$.
   Montrer que $z \in \mathbb{Z}[j]^\times \Rightarrow (a, b) \in \{-1, 0, 1\}^2$
5. En déduire l'ensemble $\mathbb{Z}[j]^\times$.

---

1. On a $1 + j + j^2 = \dfrac{1 - j^3}{1 - j} = 0$ car $j^3 = 1$ et $j \neq 1$.
2. $\mathbb{Z}[j]$ est un sous-groupe de $\mathbb{C}$ pour l'addition $+$.
   Dans $\mathbb{C}$, la multiplication $\times$ est associative, admet un élément neutre, et est distributive sur $+$.
   On a $1 \in \mathbb{Z}[j]$ car $1 = 1 + 0j$.
   Et pour tous a, b, a', $b' \in \mathbb{Z}$, on a
   $$(a + jb)(a' + jb') = (aa' - bb') + (ab' + ba' - bb')j \in \mathbb{Z}[j].$$
   Cela montre que $(\mathbb{Z}[j], +, \times)$ est un anneau.
3. On calcule : $|a + jb|^2 = (a - \dfrac{b}{2})^2 + \dfrac{3b^2}{4} = a^2 + b^2 - ab \in \mathbb{Z}$.
   On en déduit que si $a + jb$ est inversible dans $\mathbb{Z}[j]$, alors $|a + b|^2$, $|a + jb|^{-2} \in \mathbb{Z}$, d'où $|a + jb| = 1$.
   Réciproquement, si $|a + jb| = 1$, alors $(a + jb)^{-1} = \overline{a + jb} = a + \bar{j}b = a - b - bj \in \mathbb{Z}[j]$, car $\bar{j} = j^2 = -1 - j$.
4. On doit résoudre $a^2 - ab + b^2 - 1 = 0$, que l'on considère comme une équation du second degré d'inconnue a.
   On calcule son discriminant : $\Delta = b^2 - 4(b^2 - 1) = 4 - 3b^2$ qui est positif ssi $b \in \{-1, 0, 1\}$ puisque $b \in \mathbb{Z}$. De même pour a.
5. On a ± 1, $\pm j$, $\pm(1 + j) = \pm j^2$ inversibles, soit 6 éléments inversibles. $\pm(1 - j)$ et 0 ne sont pas de module 1 !

---

1. On pose $a' = a^{n-1}$. On a alors $aa' = a'a = 1$, donc a est inversible, et $a^{-1} = a^{n-1}$.
2. Le polynôme s'écrit $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, avec $a_0, \ldots, a_{n-1} \in A$.
   On a $a_0 = P(0) \in A^\times$.
   On a $0 = P(b) = b^n + \ldots + a_1b + a_0 = b(b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1) + a_0$.
   Donc, on a $-a_0 = b(b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1)$.
   Comme a_0 est inversible, on a $1 = b(b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1)(-a_0^{-1})$. En posant $b' = (b^{n-1} + b^{n-2}a_{n-1} + \ldots + a_1)(-a_0^{-1})$, on a $b'b = bb' = 1$.
   Donc b est inversible, d'inverse b'.
3. Si $A^\times$ est fini, on a donc un groupe fini. Pour $Card(A^\times) = n$, le chapitre sur les Groupes nous dit que pour $c \in A^\times$, on a $c^n = 1$.
   Donc, $P(X) = X^n - 1$ convient.

Exercice 25.

1. Soit A un anneau commutatif fini. Trouver un polynôme P tel que $P(a) = 0$ pour tout $a \in A$.
2. Dans $\mathbb{Z}/p\mathbb{Z}$, montrer que $Q(X) = X^p - X$ convient.
   On pourra s'aider de l'exercice précédent.
3. Dans $\mathbb{Z}/6\mathbb{Z}$, trouver un polynôme R, avec $\deg(R) < 6$, tel que $R(a) = 0$ pour tout $a \in \mathbb{Z}/6\mathbb{Z}$.
   On pourra chercher un polynôme qui ressemble à Q.

---

1. Comme A est fini on écrit $A = \{a_0, \ldots, a_n\}$. On pose alors $P(X) = (X - a_0)(X - a_1)\ldots(X - a_n)$. Ce polynôme P convient.
2. Dans $\mathbb{Z}/p\mathbb{Z}$, tout élément non-nul est inversible. $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup (\mathbb{Z}/p\mathbb{Z})^\times$.
   On a vu dans l'exercice précédent que pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, a est annulé par le polynôme $X^{p-1} - 1$.
   Il reste 0, qui est annulé par le polynôme X.
   Donc, le polynôme $X(X^{p-1} - 1) = X^p - X$ est un polynôme qui est annulé par tous les éléments de $\mathbb{Z}/p\mathbb{Z}$.
3. Dans $\mathbb{Z}/6\mathbb{Z}$, on cherche un polynôme de la forme $X^m - X$. On regarde donc les puissances de chaque élément.
   On remarque que $\overline{k}^3 = \overline{k}$, pour tout $\overline{k}$.
   Donc, le polynôme $R(X) = X^3 - X$ convient.

Exercice 26. Soit A un anneau commutatif. Soit $x \in A$. On dit que x est **nilpotent** s'il existe $n \geq 1$ tel que $x^n = 0$.

1. Soit $x \in A$ nilpotent, et $a \in A$.
   Montrer que ax est nilpotent.
2. Soit $y \in A$ nilpotent. Montrer que $x + y$ est nilpotent.
3. En déduire que $N = \{x \in A \text{ t.q. } x \text{ nilpotent}\}$ est un idéal de A.
4. Quels sont les éléments nilpotents dans un anneau intègre ?
5. Donner un exemple d'anneau A qui a des éléments nilpotents non-nuls.
6. Donner un exemple d'anneau A commutatif qui a des éléments nilpotents non-nuls.
7. Montrer que le résultat de 1) est faux si A n'est pas commutatif.
   On cherchera un contre-exemple.
8. Est-ce qu'il existe des anneaux A non-intègres tels que $N = \{0\}$?
9. Montrer que $1 - x$ est inversible, et donner son inverse.

10. Montrer que $1 + N \subset A^\times$.

---

1. L'anneau A est commutatif. On a $(ax)^n = a^n x^n = 0$.
2. Pour n tel que $x^n = 0$, et m tel que $y^m = 0$, on regarde $(x+y)^{n+m}$.
   Par commutativité, la formule du binôme donne $(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$.
   Pour tout $0 \leq k \leq n+m$, on a soit $k \geq n$ soit $n+m-k \geq m$, donc $(x+y)^{n+m} = 0$.
3. L'ensemble N contient 0, est stable par multiplication par tout élément de A, et est stable par addition.
   C'est donc un idéal de A.
4. Dans un anneau intègre, on a $x^n = 0$ si et seulement si $x = 0$. Donc $N = \{0\}$.
5. Dans $M_2(\mathbb{R})$ on a $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ qui vérifie $M^2 = 0$.
6. Dans $\mathbb{Z}/4\mathbb{Z}$, on a $x = \overline{2}$ qui vérifie $x^2 = 0$.
7. Dans $M_2(\mathbb{R})$ pour $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $N = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, on a M nilpotente, mais $NM = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ n'est pas une matrice nilpotente.
8. Oui. Pour $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, l'anneau A n'est pas intègre (on a $(1,0) \times (0,1) = (0,0)$), mais son seul élément nilpotent est $(0,0)$.
9. Comme on a $x^n = 0$, on a $(1-x)(1+x+\ldots+x^{n-1}) = 1 - x^n = 1$.
   Et $1-x$ commute avec $1+x+\ldots+x^{n-1}$.
   Donc, $1-x$ est inversible, d'inverse $1+x+\ldots+x^{n-1}$.
10. On a $1 + N = \{1+x,\ x \in N\}$.
    Soit $x \in N$. Comme N est un idéal, on a $y = -x$ qui est nilpotent. Donc $1 - y = 1 + x$ est inversible.
    Ainsi, on a $1 + N \subset A^\times$.

Exercice 27 (Quaternions)**.** Dans $M_2(\mathbb{C})$, on pose $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$.

1. Calculer $i^2, j^2, k^2, ij, jk, ik$.
2. Combien valent ijk, et ji, kj, ki ?
3. On pose $A = Vect_{\mathbb{R}}(I_2, i, j, k)$, le sous-ev **réel** engendré par ces 4 matrices. Montrer que A est un sous-anneau de $M_2(\mathbb{C})$.
4. Est-ce que A est commutatif ?
5. Soit $x = aI_2 + bi + cj + dk \in A$, $a, b, c, d \in \mathbb{R}$.
   Pourquoi a-t-on $x = 0$ si et seulement si $a = b = c = d = 0$?
   Penser au cours de Géométrie.
6. On pose $\overline{x} = aI_2 - bi - cj - dk$.
   Calculer $x\overline{x}$.
7. Montrer que $A^\times = A^*$.
8. En déduire que l'anneau A est intègre.
9. Résoudre l'équation $x^2 = -1_A$.
   On pourra s'aider de la question 6).
10. L'anneau A est intègre, mais l'équation polynomiale $x^2 = -1_A$ possède plus de 2 solutions dans A.
    Qu'est-ce que cet anneau a de particulier ?

---

1. On trouve $i^2 = j^2 = k^2 = -I_2$. $ij = k$, $jk = i$, $ik = -j$.
2. On a $ijk = (ij)k = k^2 = -I_2$.
   On a $jij = jk = i$, donc $-ji = jij^2 = ij$. Ainsi, $ji = -ij = -k$.
   De même, $jkj = ij = k$, donc $-kj = j^2kj = jk = i$. Ainsi, $kj = -jk = -i$.
   De même, on trouve $ki = -ik = j$.
3. Comme A est un sous-ev de $M_4(\mathbb{R})$, $(A, +)$ est un sous-groupe de $M_4(\mathbb{R})$.
   On a bien $I_2 \in A$.
   Soient $x, y \in A$. D'après les questions précédentes, on a $xy \in A$ (par distributivité, le produit de combinaisons linéaires de I_2, i, j, k est encore une combinaison linéaire de I_2, i, j, k).
   C'est donc bien un sous-anneau de $M_2(\mathbb{C})$.
4. Cet anneau n'est pas commutatif, on a $ij = -ji \neq ij$.
5. La famille (I_2, i, j, k) est une famille libre de matrices dans le $\mathbb{R}$-espace vectoriel $M_2(\mathbb{C})$. Donc, on a $aI_2 + bi + cj + dk = 0$ si et seulement si $a = b = c = d = 0$. (Cela vient du chapitre e.v. en Géométrie 1)
6. Avec les premières questions, on trouve que $x\overline{x} = (a^2 + b^2 + c^2 + d^2)I_2$.
7. On a $A^\times \subset A^*$. Montrons l'inclusion réciproque.
   Soit $x \in A^*$. On a $x = aI_2 + bi + cj + dk$.
   D'après la question précédente, on a donc un des coefficients a, b, c, d qui est non-nul.
   Donc, $a^2 + b^2 + c^2 + d^2 \neq 0$.
   En posant $y = \overline{x} \frac{1}{a^2+b^2+c^2+d^2}$, on a $xy = I_2$.
   D'après le cours d'Algèbre 1 (chapitre Matrices), on sait directement que la matrice x est inversible, d'inverse y (pas besoin de calculer yx).
   Comme $y \in A$, on a donc $x \in A^\times$ (l'inverse de x est bien un élément de A).
   Donc, on a $A^\times = A^*$.

8. Soient $x, y \in A$.
   Si $x, y \neq 0$, alors x et y sont inversibles, donc xy est inversible, donc $xy = 0$.
   Ainsi, on a $xy = 0$ si et seulement si $x = 0$ ou $y = 0$.
   Donc, l'anneau A est intègre.
9. Soit $x \in A$ tel que $x^2 = -1_A = -I_2$.
   On a alors $x(-x) = I_2$, donc x est inversible d'inverse $-x$. Or, on a vu que l'inverse de x est $\frac{1}{a^2+b^2+c^2+d^2}\overline{x}$.
   On a donc $-x = \frac{1}{a^2+b^2+c^2+d^2}\overline{x}$.
   Comme la famille (I_2, i, j, k) est libre, cela est équivalent aux 4 équations : $-a = \frac{a}{a^2+b^2+c^2+d^2}$ et $-b = \frac{-b}{a^2+b^2+c^2+d^2}$ et $-c = \frac{-c}{a^2+b^2+c^2+d^2}$ et $-d = \frac{-d}{a^2+b^2+c^2+d^2}$.
   Cela est équivalent à $a = 0$ et $1 = a^2 + b^2 + c^2 + d^2 = b^2 + c^2 + d^2$.
   Ainsi, on a $x^2 = -I_2$ si et seulement si $x = bi + cj + dk$ avec $b^2 + c^2 + d^2 = 1$.
   Remarque : D'un point de vue géométrique, l'ensemble des racines carrées de $-I_2$ dans A forme une sphère. On peut paramétrer cet ensemble avec $(\cos(t), \sin(t)\cos(s), \sin(t)\sin(s))$, pour $s, t \in [0, 2\pi[$.
10. L'équation polynomiale de degré 2 $x^2 = -1_A$ possède une infinité de solutions.
    Cela ne contredit pas le cours d'Algèbre 2, car l'anneau A est intègre mais est **non commutatif**.

    Une équation polynômiale comme $(x - i)(x + i) = 0$ possède exactement 2 solutions dans un anneau intègre.
    Mais, comme A n'est pas commutatif, x ne commute pas avec i en général. Cette équation est équivalente à $x^2+xi-ix-i^2 = 0$, et en général on a $x^2+xi-ix-i^2 \neq x^2-i^2 = x^2+1_A$.
    Ainsi, l'équation polynômiale $x^2+1_A = 0$, qui est aussi $x^2-i^2 = 0$, n'est pas équivalente à $(x - i)(x + i) = 0$.
    Le calcul dans les anneaux non commutatifs est beaucoup plus compliqué que dans les anneaux commutatifs. C'est pour cela que le cours étudie surtout les anneaux commutatifs. On commence par le plus simple avant d'aller au plus difficile.

Exercice 28 ($\mathbb{Z}[i]$ et somme de deux carrés)**.** On étudie $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[i], +, \times)$ est un sous-anneau de $\mathbb{C}$.
2. Quelles sont ses propriétés ? (commutatif ? intègre ?)
3. Soit $z = x + iy \in \mathbb{Z}[i]$.
   En utilisant la fonction $|z|^2 = z\overline{z}$, Montrer que l'on a $z \in \mathbb{Z}[i]^\times$ ssi $|z| = 1$.
4. En déduire que $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.
5. Soit $z \in \mathbb{Z}[i]$ tel que $|z|^2 = p$, avec p premier.
   Montrer que z est irréductible dans $\mathbb{Z}[i]$.
6. Soit q un nombre premier, tel que $q \equiv 3 \bmod (4)$. On veut montrer que q est irréductible dans $\mathbb{Z}[i]$.
   (a) Supposons par l'absurde que q est réductible dans $\mathbb{Z}[i]$.
   On écrit alors $q = zz'$, avec z, z' qui ne sont pas inversibles.
   Combien vaut $|z|^2$? Et $|z'|^2$?
   (b) Montrer que pour $z = x + iy$, on a $x, y \neq 0$.
   On pourra démontrer cela par l'absurde.
   (c) Trouver une relation entre $arg(z)$ et $arg(z')$.
   (d) Montrer que $z' = \overline{z}$.
   (e) En déduire que q est la somme de deux carrés.
   Conclure.
7. On admet que l'anneau $\mathbb{Z}[i]$ est principal. (On démontre cela en prouvant qu'il existe une division euclidienne sur $\mathbb{Z}[i]$.)
   Dire si les éléments $1 + 2i$, 5, 13, $3 + 4i$, sont irréductibles dans $\mathbb{Z}[i]$.
   Si non, donner leur factorisation en produit d'éléments irréductibles.

---

1. Cela a été traité en cours, il faut vérifier que $\mathbb{Z}[i]$ contient 1, et que pour $z, z' \in \mathbb{Z}[i]$ on a $z - z'$ et zz' dans $\mathbb{Z}[i]$.
2. Cet anneau est commutatif et intègre, comme sous-anneau d'un anneau commutatif intègre.
3. Soit $z = x + iy \in \mathbb{Z}[i]$. Si $|z| = 1$ alors $z\overline{z} = |z|^2 = 1$. Comme $\overline{z} = x - iy \in \mathbb{Z}[i]$, z est bien inversible dans $\mathbb{Z}[i]$.
   Réciproquement, soit $z \in \mathbb{Z}[i]^\times$. On a $z' = x' + iy'$ tel que $zz' = 1$. Alors, $1 = |zz'|^2 = |z|^2|z'|^2 = (x^2 + y^2)(x'^2 + y'^2)$.
   Comme x, y, x', y' sont des entiers, $|z|^2$ et $|z'|^2$ sont des entiers.
   Comme cet entiers divisent 1 et sont positifs, on a donc $|z|^2 = 1$, d'où $|z| = 1$.
4. On a $x^2 + y^2 = 1$ avec $x, y \in \mathbb{Z}$ si et seulement si ($x = \pm 1$ et $y = 0$) ou ($x = 0$ et $y = \pm 1$).
   Cela donne les 4 éléments de $\mathbb{Z}[i]$, $1, -1, i, -i$.
5. Soient $a, b \in \mathbb{Z}[i]$ tels que $z = ab$.
   Alors, on a $p = |z|^2 = |ab|^2 = |a|^2|b|^2$.
   Comme p est un nombre premier et $|a|^2, |b|^2$ sont entiers positifs, on a donc ($|a|^2 = 1$ et $|b|^2 = p$) ou ($|a|^2 = p$ et $|b|^2 = 1$).
   Ainsi, on a a inversible ou b inversible, d'après la question précédente.
   Cela prouve que z est un élément irréductible de $\mathbb{Z}[i]$.
6. (a) On a $q^2 = |zz'|^2 = |z|^2|z'|^2$.
   Comme q est premier, on en déduit donc que $|z|^2 = 1, q, q^2$.
   Comme z et z' ne sont pas inversibles, on a $|z| \neq 1$ et $|z'| \neq 1$, d'après une question précédente.
   Donc, le seul cas possible est $|z|^2 = |z'|^2 = q$.

(b) Pour $z = x + iy$.
Si $y = 0$, on a $z = x$. On a ainsi $q = xz'$.
Cela implique que z' est un nombre réel, donc un entier naturel. Ainsi, $x \mid q$ avec x entier. Cela donne $x = \pm 1$ ou $x = \pm q$.
Cela donne $x^2 = 1$ ou $x^2 = q^2$.
Mais on a obtenu $|z|^2 = |x|^2 = q$ à la question précédente. Contradiction.
Si $x = 0$, on a $z = iy$. On a ainsi $q = y(iz')$.
Cela implique que iz' est un nombre réel, donc un entier naturel. Ainsi, $y \mid q$ avec y entier. Cela donne $y = \pm 1$ ou $y = \pm q$.
Cela donne $y^2 = 1$ ou $y^2 = q^2$.
Mais on a obtenu $|z|^2 = |y|^2 = q$ à la question précédente. Contradiction.

(c) Comme zz' est un nombre réel positif, on a $arg(z') = -arg(z)$.

(d) Ainsi, pour $z = Re^{it}$, on a $R = \sqrt{q}$.
Pour $z' = R'e^{it'}$, on a $R' = R = \sqrt{q}$ et $t' = -t$, donc $z' = Re^{-it} = \overline{z}$.

(e) Pour $z = x + iy$, avec les questions précédentes on a $x, y \neq 0$ et $x^2 + y^2 = |z|^2 = z\overline{z} = zz' = q$.
Donc, q est la somme de deux carrés.

(f) Or, modulo 4 cela est impossible. La somme de deux carrés est congue à 0,1, ou 2, mais pas à 3.
On obtient donc une contradiction. Le nombre q est donc irréductible dans $\mathbb{Z}[i]$.

7. On a $5 = 4 + 1 = (1 + 2i)(1 - 2i)$, donc 5 est réductible.
On a $|1 + 2i|^2 = 1 + 4 = 5$, donc $1 + 2i$ est irréductible. Cela donne la décomposition en facteurs irréductibles de 5.
On a $13 = 4 + 9 = (2 + 3i)(2 - 3i)$, donc 13 est réductible. Les nombres $2 + 3i$ et $2 - 3i$ sont irréductibles dans $\mathbb{Z}[i]$ car leur norme au carré est un nombre premier.
On a $3^2 + 4^2 = 9 + 16 = 25$. Donc, $(3 + 4i)(3 - 4i) = 5x5 = (1 + 2i)^2(1 - 2i)^2$.
L'élément irréductible $1 + 2i$ divise donc $3 + 4i$ ou $3 - 4i$, d'après le théorème d'Euclide.
Ce nombre n'est donc pas irréductible dans $\mathbb{Z}[i]$.
On a $(1 + 2i)^2 = -3 + 4i$, donc $3 + 4i = (-i)(1 + 2i)(1 + 2i) = (2 - i)(1 + 2i)$.

Exercice 29. Existe-t-il un morphisme d'anneaux entre les anneaux suivants ? Si oui, en donner un. Si non, prouver qu'il n'en existe pas.

1. $\mathbb{Z}$ et $\mathbb{Q}$
2. $\mathbb{Q}$ et $\mathbb{Z}$
3. $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, pour $n \geq 2$
4. $\mathbb{Q}$ et $M_n(\mathbb{R})$, pour $n \geq 2$
5. $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{C}$
   Plus durs :
6. $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$, pour $n, m \geq 2$
7. $\mathbb{Q}[\sqrt{2}]$ et $M_2(\mathbb{Q})$

---

1. Oui, $n \in \mathbb{Z} \mapsto n \in \mathbb{Q}$.
   On l'appelle le morphisme d'inclusion. On le note souvent i.
2. Non. Dans $\mathbb{Q}$, pour $x = \frac{1}{2}$, on a $2x = 1$.
   Donc, pour f un morphisme d'anneaux, on aurait $1 = f(1) = f(2x) = f(x + x) = f(x) + f(x) = 2f(x)$.
   Or, il n'y a aucun élément y dans $\mathbb{Z}$ tel que $2y = 1$. Un tel morphisme f n'existe non pas.
3. Oui, c'est $f : a \in \mathbb{Z} \mapsto \overline{a} \in \mathbb{Z}/n\mathbb{Z}$.
   On a vu que f est un morphisme de groupes. On a $f(1) = \overline{1}$. Et, pour $x, y \in \mathbb{Z}$ on a $\overline{xy} = \overline{xy}$.
4. Oui, c'est $f : r \in \mathbb{Q} \mapsto rI_n \in M_n(\mathbb{R})$.
5. Non.
   Pour f un morphisme d'anneaux, on a $f(\overline{n}) = f(n.\overline{1}) = f(\overline{1} + \ldots + \overline{1}) = f(\overline{1}) + \ldots + f(\overline{1}) = n.f(\overline{1})$.
   Or, on a $\overline{n} = \overline{0}$, donc $f(\overline{0}) = 0$.
   D'autre part, on a $f(\overline{1}) = 1$, et $n.f(\overline{1}) = n$.
   Et, dans $\mathbb{C}$, on a $n \neq 0$. Donc un tel morphisme f n'existe pas.
6. Oui, si et seulement si m divise n.
   D'une part, si $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ existe, comme dans la question précédente on aura $0 = f(\overline{n}) = f(n.\overline{1}) = n.\overline{1}$.
   On a $0 = n.\overline{1}$ dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si m divise n.
   Réciproquement, si $n = mn''$, alors la fonction $f : (a \bmod (mn')) \in \mathbb{Z}/(mn')\mathbb{Z} \mapsto (a \bmod (m)) \in \mathbb{Z}/m\mathbb{Z}$ est bien définie.
   On peut vérifier que f est bien un morphisme d'anneaux.
7. Oui. On peut prendre $f : a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}] \mapsto aI_2 + b\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Q})$. Pour $B = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, on a $B^2 = 2I_2$. La matrice B est une racine carrée de $2I_2$.
   On peut vérifier que f est bien un morphisme d'anneaux.

Exercice 30. Les anneaux suivants sont-ils isomorphes ?
Si oui, trouver un isomorphisme. Si non, montrer qu'il n'en existe pas.
On pourra utiliser les propriétés des anneaux, leurs groupes des inversibles, et l'exercice précédent.

1. $\mathbb{Z}$ et $\mathbb{Q}$
2. $\mathbb{Q}$ et $\mathbb{R}$
3. $\mathbb{R}$ et $\mathbb{C}$

4. $\mathbb{R}$ et l'anneau produit $\mathbb{R} \times \mathbb{R}$
5. $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[i]$
6. $\mathbb{C}$ et $\mathbb{R}[A]$, avec $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
7. $\mathbb{C}$ et $\mathbb{R}[A]$, avec $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

---

1. Non, $\mathbb{Z}$ ne contient que 2 éléments inversibles alors que $\mathbb{Q}$ en a une infinité. Un isomorphisme $f : A \to B$ donne une bijection entre $A^\times$ et $B^\times$.
2. Non. Dans $\mathbb{R}$, on a $\sqrt{2}$ qui est une racine de $x^2 - 2 = 0$, alors que dans $\mathbb{Q}$ le polynôme $X^2 - 2$ n'a pas de racines.
   D'après l'exercice précédent, il n'existe pas de morphisme d'anneaux $f : \mathbb{R} \to \mathbb{Q}$.
3. Non. Dans $\mathbb{C}$ on a i qui est une racine de $x^2 + 10$, alors que dans $\mathbb{R}$ le polynôme $X^2 + 1$ n'a pas de racines.
   D'après l'exercice précédent, il n'existe pas de morphisme d'anneaux $f : \mathbb{C} \to \mathbb{R}$.
4. Non. L'anneau $\mathbb{R}$ est intègre, et $\mathbb{R} \times \mathbb{R}$ n'est pas intègre.
   Pour $f : A \to B$ un isomorphisme, si A possède des diviseurs de 0, alors B aussi. (Si $ab = 0$ avec $a, b \neq 0$, alors $f(a)f(b) = 0$ avec $f(a), f(b) \neq 0$)
5. Non. Dans $\mathbb{Q}[i]$ on a i qui est une racine de $x^2 + 10$, alors que dans $\mathbb{Q}[\sqrt{2}]$ le polynôme $X^2 + 1$ n'a pas de racines.
   D'après l'exercice précédent, il n'existe pas de morphisme d'anneaux $f : \mathbb{Q}[i] \to \mathbb{Q}[\sqrt{2}]$.
   Pourtant, ces deux anneaux sont isomorphes en tant que $\mathbb{Q}$-espaces vectoriels de dimension 2.
6. Oui.
   On a $A^2 = -I_2$. Ainsi, $\mathbb{R}[A] = Vect(I_2, A) = \{xI_2 + yA,\ x, y \in \mathbb{R}\}$.
   En posant $f(x + iy) = xI_2 + yA$ (c'est-à-dire $f(1) = I_2$ et $f(i) = A$), on montre que f est un morphisme d'anneaux ($f(x - y) = f(x) - f(y)$, $f(xy) = f(x)f(y)$).
   La fonction f est de plus bijective, donc f est un isomorphisme d'anneaux.
7. Non.
   On a $B^2 = I_2$, donc l'anneau $\mathbb{R}[B]$ n'est pas intègre car l'équation $z^2 = I_2$ possède au moins 4 solutions.
   Or, $\mathbb{C}$ est un anneau intègre.
   En fait, on a $\mathbb{R}[B]$ isomorphe à $\mathbb{R}^2$. ($(xI_2 + yB) \mapsto (x, y) \in \mathbb{R}^2$).

Corps

Exercice 31. Soient $A = \{a + b\sqrt{7},\ (a, b) \in \mathbb{Q}^2\}$ et $B = \{a + b\sqrt{11},\ (a, b) \in \mathbb{Q}^2\}$.

1. Démontrer que A et B sont des sous-corps de $(\mathbb{R}, +, \times)$.
2. Montrer que la fonction $\varphi : a + b\sqrt{7} \in A \mapsto a + b\sqrt{11} \in A$ est un morphisme de groupes, mais pas un morphisme d'anneaux.

---

1. On a $A = \mathbb{Q}(\sqrt{7})$ et $B = \mathbb{Q}(\sqrt{11})$.
   On fait la la preuve pour A. On a $A \subset \mathbb{R}$.
   Il faut montrer que A est un sous-anneau de $\mathbb{R}$, et que l'on a $A^\times = A^*$.
   On a vu dans un TD précédent que $\mathbb{Q}(\sqrt{2})$ est un sous-anneau de $\mathbb{R}$, la preuve est la même. (On a $1 \in A$, et pour tous $x, y \in A$, on a $x - y \in A$ et $xy \in A$).
   On montre ensuite que pour $a + b\sqrt{7}$ non-nul, on a $\frac{1}{a+b\sqrt{7}} = \frac{a-b\sqrt{7}}{a^2-7b^2}$. Cet élément est encore dans A.
   Donc, A est un sous-corps de $\mathbb{R}$.
   La preuve pour B est identique.
2. On doit vérifier que $\varphi(x + y) = \varphi(x) + \varphi(y)$, pour tous $x, y \in A$. Cela est vrai.
   Mais, on n'a pas $\varphi(xy) = \varphi(x)\varphi(y)$. En effet, on a $\varphi(\sqrt{7}^2) = \varphi(7) = 7 \neq 11 = \sqrt{11}^2 = \varphi(\sqrt{7})^2$.
   Ce n'est donc pas un morphisme d'anneaux.

Exercice 32. Soit $J = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$.

1. Rappeler la définition de $\mathbb{Q}[J]$.
2. Montrer que $\mathbb{Q}[J] = \{aI_2 + bJ,\ a, b \in \mathbb{Q}\}$.
   On pourra calculer J^2.
3. Montrer que l'on a $aI_2 + bJ = 0$ ssi $a = b = 0$.
4. L'anneau $\mathbb{Q}[J]$ est-il commutatif, intègre, principal, un corps ?
5. Reprendre les mêmes questions avec $\mathbb{R}[J]$.

---

1. On a $\mathbb{Q}[J] = Vect(I_2, J, J^2, \ldots) = Vect(J^n,\ n \geq 0)$.
2. On a $J^2 = 2I_2$. Ainsi, on en déduit que I_2, J est une famille génératrice de $Vect(J^n,\ n \geq 0)$. Donc, $\mathbb{Q}[J] = Vect(I_2, J)$.
3. Comme cette famille est libre, c'est une base de $\mathbb{Q}[J]$. Donc, on a $aI_2 + bJ = 0$ ssi $a = b = 0$.
4. L'annau $\mathbb{Q}[J]$ est commutatif (vu en cours). C'est un corps, donc il est aussi intègre et principal.
   Démontrons cela.
   Soit $x = aI_2 + bJ \in \mathbb{Q}[J]$. En posant $y = aI_2 - bJ$, on a $xy = a^2I_2 - b^2J^2 = (a^2 - 2b^2)I_2$.
   Comme $a, b \in \mathbb{Q}$, on a $a^2 - 2b^2 = 0$ ssi $a = b = 0$.
   Donc, si $x \neq 0$, on a $a^2 - 2b^2 \neq 0$, et donc $x.(\frac{1}{a^2-2b^2}y) = I_2$.
   La matrice x est donc inversible, d'inverse $\frac{1}{a^2-2b^2}y$.
   Ainsi, tout élément non-nul de $\mathbb{Q}[J]$ est inversible, c'est bien un corps.

5. Avec $\mathbb{R}[J]$, on a encore que $\mathbb{R}[J] = Vect(I_2, J)$ (mais en tant que $\mathbb{R}$-espace vectoriel).
On a encore $aI_2 + bJ = 0$ ssi $a = b = 0$.
L'anneau est encore commutatif.
Mais, cet anneau n'est plus intègre. Il n'est donc ni intègre, ni principal, ni un corps.
En effet, pour $a = \sqrt{2}$, $b = 1$, $x = aI_2 + b$, et $y = aI_2 - bJ$, on a $x, y \neq 0$, mais $xy = (a^2 - 2b^2)I_2 = 0$.
Dans $\mathbb{Q}[J]$, la matrice J agit comme une "racine carrée de 2" (c'est une solution de l'équation polynomiale $X^2 = 2$).
Dans $\mathbb{R}[J]$, il existe déjà $\sqrt{2}$ et $-\sqrt{2}$. Ajouter J ajoute de nouvelles "racines carrées de 2" (l'équation $X^2 = 2$ possède une infinité de solutions dans $\mathbb{R}[J]$).
Cet anneau ne peut alors pas être intègre, car dans un anneau intègre une équation polynomiale de degré 2 a au plus 2 racines.

Exercice 33. Soit A un anneau commutatif, intègre. On suppose que A est fini.
Indication : Dans cet exercice, toutes les propriétés de l'anneau A sont utilisées.

1. **Première partie**
Soit $f : n \in \mathbb{Z} \mapsto n.1_A \in A$. f est un morphisme d'anneaux de $\mathbb{Z}$ vers A.
Montrer qu'il existe $p \in \mathbb{Z}$ tel que $Ker(f) = p\mathbb{Z}$.
2. Montrer que l'on a $p \neq 0, 1, -1$, et montrer que l'on peut choisir p positif.
3. Soient $n, m \in \mathbb{Z}$ tels que $\overline{n} = \overline{m}$ dans $\mathbb{Z}/p\mathbb{Z}$.
Montrer que dans A on a $n.1_A = m.1_A$.
4. En déduire que la fonction $h : \overline{n} \in \mathbb{Z}/p\mathbb{Z} \mapsto n.1_A \in A$ est bien définie.
5. Montrer que le nombre entier positif p est premier.
On pourra raisonner par l'absurde.
Bonus : Montrer qu'en posant $\overline{n} \cdot a = h(\overline{n}).a \in A$, l'ensemble $(A, +, \cdot)$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.
6. Montrer que $(A, +, \cdot)$ est un $\mathbb{Z}/p\mathbb{Z}$-ev de dimension finie.
7. On pose $r = \dim(A)$. En posant $(e_1, \ldots, e_r)$ une base de A, calculer $Card(A)$.
8. **Deuxième partie**
Soit $x \in A$ non-nul. On pose $g_x : a \in A \mapsto ax \in A$.
Montrer que g_x est une fonction injective.
9. Montrer que x possède un inverse dans A.
10. En déduire que A est un corps.

Conclusion : On vient de démontrer que pour tout anneau A qui est commutatif, intègre, et fini, alors A est un corps et il existe p premier et $r \geq 1$ tels que $Card(A) = p^r$.
En algèbre, un tel corps est noté $\mathbb{F}_{p^r}$. On l'appelle corps fini.
Les corps finis sont très utiles en informatique (par ex : codes correcteurs d'erreurs, cryptographie).

---

1. Le noyau d'un morphisme d'anneaux est un idéal.
Les idéaux de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$, avec $p \in \mathbb{Z}$ ($\mathbb{Z}$ est un anneau principal). Cela donne le résultat.
2. Si $p = 1$ ou -1 on a $Ker(f) = \mathbb{Z}$. Comme $f(1) = 1_A$, cela n'est pas possible.
Si $p = 0$ alors $Ker(f) = \{0\}$, donc f est injectif. Comme A est fini et $\mathbb{Z}$ infini, cela est impossible.
3. Supposons par l'absurde que p n'est pas premier. Comme on a $|p| \geq 2$, on écrit $p = ab$ avec $a, b \neq p, -p$.
Comme f est un morphisme d'anneaux, on a alors $f(p) = f(ab) = f(a)f(b)$.
D'un côté on a $f(p)0$, car $p \in p\mathbb{Z} = Ker(f)$.
De l'autre, on a $f(a), f(b) \neq 0$ car $a, b \notin p\mathbb{Z} = Ker(f)$.
On a donc deux éléments non-nuls de A dont le produit est nul.
Cela est impossible car A est intègre. Contradiction.
Donc, le nombre p est premier.
4. Si on a $\overline{n} = \overline{m}$, alors $n \equiv m \bmod (p)$. Donc $n = m + kp$, pour un $k \in \mathbb{Z}$.
Comme f est un morphisme d'anneaux, cela donne $f(n) = f(m+kp) = f(m)+f(kp) = f(m) + f(k).f(p) = f(m)$. Ainsi, dans A on a $n.1_A = m.1_A$.
5. D'après la question précédente, l'élément $n.1_A$ ne dépend pas du représentant de la classe d'équivalence $\overline{n}$ que l'on choisit. Donc, on peut poser $h(\overline{n}) = f(n) = n.1_A$.
Pour démontrer que $(A, +, \cdot)$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel, il faut montrer que cet ensemble vérifie toutes les propriétés d'un espace vectoriel, comme vous le faisiez en Géométrie 1.
6. L'ensemble A est fini. Pour $A = \{a_0, a_1, \ldots, a_{Card(A)}\}$, on a $A = Vect(a_0, a_1, \ldots, a_{Card(A)})$. Donc A possède une famille génératrice finie.
D'après le cours de Géométrie 1, A est donc un $\mathbb{Z}/p\mathbb{Z}$-ev de dimension finie.
7. Soit $r = \dim(A)$. Soit $(e_1, \ldots, e_r)$ une base de A.
Alors, d'après le cours de Géométrie 1, on a une bijection entre $(\mathbb{Z}/p\mathbb{Z})^r$ et A, avec : $(x_1, \ldots, x_r) \in (\mathbb{Z}/p\mathbb{Z})^r \mapsto x_1e_1 + x_2e_2 + \ldots + x_re_r \in A$. (C'est même un isomorphisme d'ev).
Donc, on a $Card(A) = Card((\mathbb{Z}/p\mathbb{Z})^r) = p^r$.
8. Soient $y, z \in A$. On a $g_x(y) = g_x(z)$ ssi $yx = zx$ ssi $(y - z)x = 0$.
Comme x est non-nul et comme A est intègre, on a $(y - z)x = 0$ ssi $y - z = 0$ ssi $y = z$.
Donc, g_x est une fonction injective.
9. La fonction g_x est une fonction injective de A dans A. Comme A est un ensemble fini, cette fonction est aussi surjective.
Donc, il existe $y \in A$ tel que $xy = 1_A$. Comme A est commutatif, on a aussi $yx = xy =$

1_A.
Ainsi, x est inversible dans A.

10. Tous les éléments non-nuls de A sont inversibles, donc A est un corps.

■ *Polynômes* ■

Exercice 34.
Soient $a \in \mathbb{K}$ et $n \geq 1$.
La famille $(1, X-a, (X-a)^2, \dots, (X-a)^n)$ est-elle une base de $\mathbb{K}_n[X]$?

Oui. Cette famille est libre avec $n+1$ vecteurs, et est donc une base de $\mathbb{K}_n[X]$.
Pour cela, on montre par récurrence sur $n \geq 0$ que $(1, X-a, (X-a)^2, \dots, (X-a)^n)$ est libre.
En effet, cela est vrai pour $n = 0$.
Supposons cela vrai pour un certain $n \geq 0$. La famille $(1, X-a, (X-a)^2, \dots, (X-a)^n)$ est contenue dans le sous-ev $\mathbb{K}_n[X]$. Le polynôme $(X-a)^{n+1}$ est de degré $n+1$, donc n'appartient pas à $\mathbb{K}_n[X]$, donc il n'est pas combinaison linéaire des $(X-a)^k$, $0 \leq k \leq n$.
Ainsi, la famille $(1, X-a, (X-a)^2, \dots, (X-a)^{n+1})$ reste libre.
Cela termine la récurrence.

Exercice 35.
Résoudre dans $\mathbb{K}[X]$:

$$P(X^2) = (X^2+1)P(X).$$

Soit P tel que $P(X^2) = (X^2+1)P(X)$.
En regardant les degrés, on a :

$$2.\deg(P) = \deg(P(X^2)) = \deg((X^2+1)P(X)) = 2 + \deg(P)$$

On en déduit donc que l'on a soit $P = 0$ ($\deg(P) = -\infty$), soit $\deg(P) = 2$.
Supposons P de degré 2. Pour $P(X) = aX^2 + bX + c$, on a : $0 = P(X^2) - (X^2+1)P(X) = aX^4+bX^2+c-(X^2+1)(aX^2+bX+c) = (aX^4+bX^2+c)-(aX^4+bX^3+(a+c)X^2+bX+c)$

$$\Leftrightarrow 0 = -bX^3 + (-a+b-c)X^2 - bX \Leftrightarrow \left\{ \begin{array}{rcl} -b & = & 0 \\ -a+b-c & = & 0 \\ -b & = & 0 \end{array} \right.$$

$\Leftrightarrow b = 0$ et $c = -a$
$\Leftrightarrow P(X) = a(X^2-1)$
L'ensemble des solutions de cette équation est ainsi $Vect(X^2-1)$.

Exercice 36.
Soit f l'endomorphisme de $\mathbb{K}[X]$ qui, à tout polynôme P, associe sa dérivée P'.
Soit g l'endomorphisme de $\mathbb{K}[X]$ défini par $P(X^k) = \frac{1}{k+1}X^{k+1}$. Déterminer $\ker(f \circ g)$ et $\ker(g \circ f)$.
Est-ce que $f \circ g$ est injectif ? surjectif ? bijectif ?
Est-ce que $g \circ f$ est injectif ? surjectif ? bijectif ?

Pour $P(X) = \sum_{k=0}^n a_k X^k$, on a $g(P) = \sum_{k=0}^n \frac{a_k}{k+1} X^{k+1}$ par linéarité de g. Donc $f(g(P)) = \sum_{k=0}^n a_k X^k$, c'est-à-dire $f \circ g = Id_{\mathbb{K}[X]}$.
On a $f(P) = \sum_{k=1}^n k a_k X^{k-1}$, donc $g(f(P)) = \sum_{k=1}^n a_k X^k = P(X) - P(0)$. Ainsi, $g \circ f = Id_{\mathbb{K}[X]} - (P \mapsto P(0))$.
Ainsi, on a $f \circ g(P) = 0$ ssi $P(X) = 0$, et $g \circ f(P) = 0$ ssi $P(X) = P(0)$.
Donc $Ker(f \circ g) = \{0\}$ et $Ker(g \circ f) = Vect(1)$.
L'endomorphisme $f \circ g$ est bijectif.
L'endomorphisme $g \circ f$ n'est pas injectif. Il n'est pas surjectif non plus car $1 \notin Im(g \circ f)$. Il n'est donc pas bijectif.

Exercice 37.
Pour $n \in \mathbb{N}^*$, développer le polynôme

$$P_n(X) = (1+X)(1+X^2)(1+X^4)\dots(1+X^{2^{n-1}})$$

On démontre par récurrence sur $n \geq 1$ que $P_n(X) = \sum_{k=0}^{2^n-1} X^k$.
Initialisation : Pour $n = 1$, c'est vrai.
Hérédité : Supposons le résultat vrai pour un $n \geq 1$.
On a alors $P_{n+1}(X) = P_n(X)(1+X^{2^n}) = \sum_{k=0}^{2^n-1} X^k + \sum_{k=0}^{2^n-1} X^{2^n} X^k$
$P_{n+1}(X) = \sum_{k=0}^{2^n-1} X^k + \sum_{k=0}^{2^n-1} X^{2^n+k} = \sum_{m=0}^{2^{n+1}-1} X^m$.
Cela termine la récurrence.

Exercice 38.
Déterminer tous les polynômes P tels que :

$$P(2) = 6,\ P'(2) = 1 \quad \text{et} \quad P''(2) = 4$$

et :

$$\forall n \geqslant 3 \quad P^{(n)}(2) = 0.$$

On a $\deg(P) \geq 2$. On décompose P dans la base $((X-2)^k,\ k \geq 0)$.
Pour $\deg(P) = n$, on a $P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(2)}{k!}(X-2)^k$.
On en déduit que le polynôme P est unique, et vaut $P(X) = 2(X-2)^2 + (X-2) + 6$.

Exercice 39.
Effectuer les divisions euclidiennes suivantes :

1. $X^3 - X^2 + X - 1$ par $X + 1$
2. $X^4 - 3X^3 + 2$ par $X^2 + 2$
3. $3X^5 + 2X^2 + X - 4$ par $X^2 + X + 1$
4. $X^n - 1$ par $X - 1$, pour $n \geq 1$

1. On a $X^3 - X^2 + X - 1 = (X^2 - 2X + 3)(X + 1) + (-4)$
2. On a $X^4 - 3X^3 + 2 = (X^2 - 3X - 2)(X^2 + 2) + (6X + 6)$
3. On a $3X^5 + 2X^2 + X - 4 = (3X^3 - 3X^2 + 5)(X^2 + X + 1) + (-4X - 9)$
4. On a $X^n - 1 = (X-1)(1 + X + \ldots + X^{n-1})$. Donc le quotient de la division euclidienne vaut $1 + X + \ldots + X^{n-1}$ et le reste vaut 0.

Exercice 40. Soient $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$.
• Déterminer le reste de la division euclidienne de $P(X)$ par $X - a$.
• Montrer que l'on a $X - a \mid P$ si et seulement si $P(a) = 0$.
• Soit $b \in \mathbb{K}$. Montrer que l'on a $(X-a)(X-b) \mid P$ si et seulement si $P(a) = P(b) = 0$.

• Soit $P(X) = Q(X)(X-a) + R(X)$ la division euclidienne de P par $X - a$.
On a $\deg(R) < 1$, donc $R(x) = b$ avec $b \in \mathbb{K}$.
D'après les propriétés des fonctions polynômiales, on a :

$$P(a) = Q(a)(a-a) + b = 0 + b = b,$$

donc on a $R(X) = b = P(a)$.
Le reste de la div. eucl. de P par $(X-a)$ est $P(a)$.
• Le polynôme $X - a$ divise P si et seulement si le reste dans la division euclidienne de $X - a$ par P vaut 0, si et seulement si $P(a) = 0$.
• Si $P(X) = Q(X)(X-a)(X-b)$, on trouve alors que $P(a) = Q(a)(a-a)(a-b) = 0$ et $P(b) = Q(b)(b-a)(b-b) = 0$.
Réciproquement, supposons que $P(a) = P(b) = 0$.
On a donc $(X-a) \mid P$, donc $P(X) = Q_1(X)(X-a)$.
Comme $P(b) = 0$, on a $0 = Q_1(b)(b-a)$. Donc, on a $Q_1(b) = 0$.
Ainsi, $(X-b)$ divise Q_1, d'où $Q_1(X) = Q_2(X)(X-b)$.
On obtient alors $P(X) = Q_2(X)(X-b)(X-a)$.

Exercice 41.

1. Calculer $pgcd(X^2, (X-1)^3)$, $pgcd(X^2-1, X^3-1)$, $pgcd(X^4-1, X^6-1)$, $pgcd(X^4 - 2X^2 + 3, X^2 + X)$.
2. Factoriser dans $\mathbb{R}[X]$: $X^2 - 1$, $X^3 - 1$, $X^2 - 5X + 2$,$X^2 + 1$, $X^4 + 1$.
3. Factoriser dans $\mathbb{C}[X]$: $X^3 - 1$, $X^n - 1$ $n \geq 1$, $X^2 - 5X + 2$, $X^2 + 1$, $X^n - z$ $n \geq 1$ $z = r.e^{it}$.

1. $pgcd(X^2, (X-1)^3) = 1$, $pgcd(X^2-1, X^3-1) = (X-1)$.
$pgcd(X^4 - 2X^2 + 3, X^2 + X) = X + 1$ car $X^2 + X = X(X+1)$, et X ne divise pas $X^4 - 2X^2 + 3$ mais $(-1)^4 - 2.(-1)^2 + 3 = 0$ donc $X + 1 \mid X^4 - 2X^2 + 3$.
$pgcd(X^4 - 1, X^6 - 1) = X^2 - 1$ car $X^4 - 1 = (X-1)(X+1)(X^2+1)$ et $X^6 - 1 = (X^3-1)(X^3+1) = (X-1)(X^2+X+1)(X+1)(X^2-X+1)$, et $pgcd(X^2+1, X^2+X+1) = pgcd(X^2+1, X^2-X+1) = 1$.
2. $X^2-1 = (X-1)(X+1)$. $X^3-1 = (X-1)(1+X+X^2)$. $X^2-5X+2 = (X - \frac{5+\sqrt{17}}{2})(X - \frac{5-\sqrt{17}}{2})$. $X^2+1 = X^2+1$ (polynôme irréductible). $X^4+1 = X^4+2X^2+1-2X^2 = (X^2+1)^2 - 2X^2 = (X^2+1-\sqrt{2}X)(X^2+1+\sqrt{2}X)$, et ces deux polynômes sont irréductibles dans $\mathbb{R}[X]$.
3. $X^3 - 1 = (X-1)(X-j)(X-j^2)$. $X^n - 1 = \Pi_{k=1}^{n}(X - e^{2i\pi\frac{k}{n}})$. $X^2 - 5X + 2 = (X - \frac{5+\sqrt{17}}{2})(X - \frac{5-\sqrt{17}}{2})$. $X^2+1 = (X-i)(X+i)$. $X^n - z = \Pi_{k=1}^{n}(X - r^{\frac{1}{n}} e^{2i\pi\frac{k}{n} + \frac{t}{n}})$.

Exercice 42. Soit $P \in \mathbb{C}[X]$ vérifiant $P(X^2) = P(X-1)P(X+1)$.
Soit $z \in \mathbb{C}$ une racine de P. On admet que P possède alors une racine w telle que $|w| > |z|$.
En déduire les polynômes $P \in \mathbb{C}[X]$ solutions de l'équation.

Si P admet une racine (complexe), alors il en admet d'après la question précédente une infinité. C'est donc le polynôme nul. Les polynômes qui sont solutions de l'équation ne peuvent donc être que des polynômes constants, et les seuls polynômes constants solutions sont les polynômes $P(X) = 0$ et $P(X) = 1$.

Exercice 43.

1. Montrer qu'un polynôme de $\mathbb{K}[X]$, de degré 3, qui n'a pas de racines dans $\mathbb{Q}$, est irréductible dans $\mathbb{K}[X]$.
2. Soit $n \in \mathbb{N}$. Est-ce que le polynôme X^2+X+1 divise $X^{3n+8}+X^{3n+4}+X^{3n}$ dans $\mathbb{Q}[X]$?

---

1. Soit $P \in \mathbb{K}[X]$ avec $\deg(P) = 3$ et P sans racines.
   On suppose par l'absurde que P est réductible dans $\mathbb{K}[X]$.
   On aurait alors $P = Q_1Q_2$ avec Q_1 et Q_2 des polynômes non-constants.
   On aurait alors $\deg(P) = 3 = \deg(Q_1) + \deg(Q_2)$, donc $\deg(Q_1) = 1$ et $\deg(Q_2) = 2$ ou $\deg(Q_1) = 2$ ou $\deg(Q_2) = 1$.
   Or, un polynôme de degré 1 est de la forme $aX + b$ avec $a \neq 0$, et admet comme racine $\frac{-b}{a}$. Ainsi, Q_1 ou Q_2 a une racine dans $\mathbb{K}$, donc P a une racine dans $\mathbb{K}$, contradiction.
   Donc P est irréductible dans $\mathbb{K}$.
2. On a $X^{3n+8} + X^{3n+4} + X^{3n} = X^{3n}(X^8 + X^4 + 1)$.
   On se place dans $\mathbb{C}[X]$. On a alors $X^2 + X + 1 = (X - j)(X - j^2)$. On a $j^3 = 1$ et $j^2 + j + 1 = 0$. Cela donne $j^8 + j^4 + 1 = j^2 + j + 1 = 0$, et $j^{16} + j^8 + 1 = j + j^2 + 1 = 0$.
   Donc, $X^2 + X + 1$ divise $X^8 + X^4 + 1$ dans $\mathbb{C}$. Donc, d'après l'exercice précédent, $X^2 + X + 1$ divise $X^8 + X^4 + 1$ dans $\mathbb{Q}$.
   Ainsi, $X^2 + X + 1$ divise bien $X^{3n+8} + X^{3n+4} + X^{3n}$.

Exercice 44. Soit $n \geq 1$. Dans $\mathbb{R}[X]$, on définit $P(X) = (X^2 - 1)^n$.

1. Montrer que pour tout $k \geq 0$, le polynôme $P^{(k)}$ est scindé (ou nul).
2. Quelle est la multiplicité de -1 et 1 dans $P^{(k)}$, pour $k \leq n$?
3. Montrer que pour tout $0 \leq k \leq n-1$, $P^{(k)}$ possède au moins $2+k$ racines distinctes, situées dans l'intervalle $[-1, 1]$.
4. En déduire que pour tout $0 \leq k \leq n-1$, $P^{(k)}$ possède exactement $2+k$ racines distinctes, situées dans l'intervalle $[-1, 1]$.
5. En déduire que $P^{(n)}$ est scindé à racines simples, à racines dans $]-1, 1[$.

---

1. Le polynôme P est scindé et à coefficients réels. Donc, d'après le cours, P' est scindé (ou $P' = 0$).
   On montre alors par récurrence sur $k \geq 0$ que $P^{(k)}$ est scindé ou $P^{(k)} = 0$.
2. -1 et 1 sont des racines de P de multiplicité n.
   Donc, d'après le cours, pour $0 \leq k \leq n-1$, -1 et 1 sont des racines de $P^{(k)}$ de multiplicité $n - k$.
3. Démontrons donc le résiltat par récurrence sur $0 \leq k \leq n-1$.
   Pour $k = 0$ c'est vrai.
   Supposons le résultat vrai pour $0 \leq k < n-1$.
   Alors, $P^{(k)}$ possède au moins $2 + k$ racines distinctes $a_1 < a_2 < \ldots < a_{2+k}$, qui sont toutes dans $[-1, 1]$.
   Comme -1 et 1 sont des racines de $P^{(k)}$, on en déduit que $a_1 = -1$ et $a_{2+k} = 1$.
   D'après le théorème de Rolle, il existe donc $b_1 < \ldots < b_{k+1}$ des réels, avec $b_i \in]a_i, a_{i+1}[$ tels que $P^{(k+1)}(b_i) = 0$.
   D'après la question précédente, -1 et 1 sont aussi des racines de $P^{(k+1)}$. On a donc trouvé $k + 3 = (k + 1) + 2$ racines distinctes de $P^{[k+1)}$, dans $[-1, 1]$.
   Cela termine la récurrence.
4. D'après les deux questions précédentes, $P^{(k)}$ possède -1 et 1 comme racines de multiplicité $n - k$, et il possède k autres racines dans $]-1, 1[$.
   Or, $P^{(k)}$ est de degré $2n - k$. Comme $(n - k) + (n - k) + k = 2n - k$, on a trouvé toutes les racines de $P^{(k)}$ comptées avec multiplicité.
5. Pour $k = n - 1$, on a $P^{(n-1)}$, polynôme de degré $n + 1$, qui possède $k + 2 = n + 1$ racines distinctes dans $[-1, 1]$.
   Donc $P^{(n-1)}$ est scindé à racines simples.
   D'après le cours, son polynôme dérivé, qui vaut $P^{(n)}$, est lui aussi à racines simples, situées dans $]-1, 1[$.

Exercice 45.

1. Soit $n \geq 1$. Le polynôme $P(X) = \sum_{k=0}^{n} \frac{1}{k!} X^k$ a-t-il des racines multiples ?
2. Soit $P \in \mathbb{R}[X]$ non-nul tel que $P' \mid P$. Montrer que P ne possède qu'un seul facteur irréductible P_1.
   Que peut-on dire sur $\deg(P_1)$?.
   Trouver tous les polynômes $P \in \mathbb{K}[X]$ non-nuls tels que $P' \mid P$.
3. Soit $Q \in \mathbb{R}[X]$, de degré n. Montrer que $Q(X + 1) = \sum_{k=0}^{n} \frac{Q^{(k)}(X)}{k!}$. (On pourra utiliser des applications linéaires, ou des bases.)

---

1. On a $P'(X) = \sum_{k=1}^{n} \frac{k}{k!} X^{k-1} = \sum_{m=0}^{n-1} \frac{1}{m!} X^m$.
   Le polynôme P a des racines multiples si et seulement si P et P' ont des racines communes.
   Or, on a $P(X) - P'(X) = \frac{1}{n!} X^n$, dont la seule racine est 0. Ainsi, si x est une racine commune à P et à P', on doit avoir $\frac{x^n}{n!} P(x) - P'(x) = 0 - 0 = 0$. x doit être une racine de X^n, c'est-à-dire $x = 0$.
   Comme 0 n'est pas racine du polynôme P, ce polynôme n'a donc pas de racines multiples.

2. Si P est un polynôme constant, on a $P'(X) = 0$ et cela n'est pas vrai. On a donc $\deg(P) = n > 0$.
On écrit $P = a_n P_1^{\alpha_1} \dots P_r^{\alpha_r}$ la décomposition de P en produit de facteurs irréductibles.
D'après le cours, on a $pgcd(P', P) = P_1^{\alpha_1 - 1} \dots P_r^{\alpha_r - 1}$.
Si $P' \mid P$ on a donc $pgcd(P', P)$ associé à P' (égaux à un scalaire près).
Comme $\deg(P) = n > 0$, on a $\deg(P') = n - 1 \geq 0$. Cela implique donc que $P_1^{\alpha_1 - 1} \dots P_r^{\alpha_r - 1}$ est de degré $n - 1$.
Or, ce polynôme est de degré $n - \deg(P_1) - \deg(P_2) - \dots - \deg(P_r)$.
Comme $\deg(P_1) \geq 1$, on doit donc avoir $r = 1$ et $\deg(P_1) = 1$.
Ainsi, P ne possède qu'un seul facteur irréductible, et ce facteur est de degré 1 : $P(X) = a_n(X - b)^{\alpha_1}$.
Réciproquement, si P est de cette forme, on a $P'(X) = a_n.\alpha_1(X - b)^{\alpha_1 - 1}$.
On trouve bien que P' divise P (et que P' et $pgcd(P', P)$ sont associés).

Autre méthode : Comme P' divise P et comme $\deg(P) \geq 1$, on a $\deg(P') = \deg(P) - 1$, et donc la division de P par P' donne $P(X) = a(X - b)P'(X)$, pour des $a, b \in \mathbb{R}$ avec $a \neq 0$. Ce nombre b est donc une racine de P.
Le coefficient dominant de $P(X)$ est a_n. Le coefficient dominant de $P'(X)$ est na_n. On a donc $a = \frac{1}{n}$.
On écrit $P(X) = a_n(X - b)^k Q(X)$, avec $Q(b) = 0$.
On a alors $P'(X) = a_n(X - b)^k Q'(X) + a_n k(X - b)^{k-1} Q(X) = a_n(X - b)^{k-1}((X - b)Q'(X) + kQ(X))$. On a alors $\frac{1}{n}(X - b)P'(X) = a_n(X - b)^k(\frac{1}{n}(X - b)Q'(X) + \frac{k}{n}Q(X))$.
Cela donne donc $Q(X) = \frac{1}{n}(X - b)Q'(X) + \frac{k}{n}Q(X)$.
On obtient : $nQ(X) = (X - b)Q'(X) + kQ(X)$.
Ainsi, $(n - k)Q(X) = (X - b)Q'(X)$.
Si $n = 1$ on a $k = 1$, et donc $P(X) = a_n(X - b)$, $P'(X) = a_n$, donc P' divise P.
Si $n > 1$, et si on a $k < n$, alors on aurait $X - b$ divise $Q(X)$ et donc $Q(b) = 0$, ce qui est impossible.
Quand $n > 1$, on a donc $k = n$, c'est-à-dire $Q(X) = 1$.
On obtient ainsi $P(X) = a_n(X - b)^n$.
Réciproquement, pour P un polynôme de cette forme, on a $P'(X) = a_n n(X - b)^{n-1}$ et donc P' divise P.

3. La fonction $f : Q \mapsto \sum_{k=0}^{n} \frac{Q^{(k)}(X)}{k!}$ est une application linéaire sur $\mathbb{R}_n[X]$ (la fonction $Q \mapsto Q'$ est une application linéaire, et f est une combinaison linéaire de composées de $Q \mapsto Q'$).
On veut en fait montrer que pour tout $Q \in \mathbb{R}_n[X]$, on a $f(Q) = Q$, c'est-à-dire que $f = Id_{\mathbb{R}_n[X]}$.
Pour cela, il suffit de le montrer sur une base de $\mathbb{R}_n[X]$. On prend la base canonique $(1, X, \dots, X^n)$.
Pour $0 \leq m \leq n$, on a
$(X + 1)^m = \sum_{k=0}^{m} \binom{m}{k} 1^k X^{m-k} = \sum_{k=0}^{m} \frac{m(m-1)\dots(m-k+1)}{k!} X^{m-k}$.
Comme on a $(X^m)^{(k)} = X^{m-k} m(m - 1) \dots (m - k + 1)$, on obtient $(X + 1)^m = \sum_{k=0}^{m} \frac{1}{k!}(X^m)^{(k)}$.
Comme on a $(X^m)^{(k)} = 0$ pour $k \geq m + 1$, et comme $m \leq n$, on obtient $(X + 1)^m = \sum_{k=0}^{n} \frac{1}{k!}(X^m)^{(k)}$.
On a donc montré que $f(X^m) = X^m$ pour tout $0 \leq m \leq n$. Donc les applications linéaires f et Id sont égales sur une base de $\mathbb{R}_n[X]$, donc ces applications linéaires sont égales.

Exercice 46. Soit $P \in \mathbb{K}[X]$. Soient $a, b \in \mathbb{K}$ avec $a \neq b$.

1. Déterminer le reste de la division euclidienne de P par $(X - a)(X - b)$.
2. Soient $n \geq 1$ et $t \in \mathbb{R}$.
Déterminer le reste dans la division euclidienne, dans $\mathbb{R}[X]$, de $P(X) = (X\cos(t) + \sin(t))^n$ par $X^2 + 1$.

---

1. On a $P(X) = Q(X)(X - a) + P(a)$. On a $Q(X) = Q_2(X)(X - b) + Q(b)$.
Donc, $P(X) = Q_2(X)(X - a)(X - b) + Q(b)(X - a) + P(a)$. On a bien obtenu une division euclidienne.
Maintenant, on a $P(b) = Q(b)(b - a) + P(a)$, donc $Q(b) = \frac{P(b) - P(a)}{b - a}$.
Donc, le reste vaut $\frac{P(b) - P(a)}{b - a}(X - a) + P(a)$.
2. Comme $P(X)$ et $X^2 + 1$ sont à coefficients réels, leur division euclidienne dans $\mathbb{C}[X]$ est identique à leur division euclidienne dans $\mathbb{R}[X]$. (la div. eucl. dans $\mathbb{R}$ peut être vue dans $\mathbb{C}$, et il y a unicité).
On effectue donc tous les calculs dans $\mathbb{C}[X]$.
On a alors $X^2 + 1 = (X - i)(X + i)$.
Donc, le reste de $P(X)$ dans la division euclidienne par X^+1, dans $\mathbb{C}[X]$, vaut :
$R(X) = \frac{P(i) - P(-i)}{i - (-i)}(X - (-i)) + P(-i) = -i\frac{P(i) - P(-i)}{2}(X + i) + P(-i)$.
$R(X) = -i\frac{P(i) - P(-i)}{2}X + P(-i) + i(-i)\frac{P(i) - P(-i)}{2} = -i\frac{P(i) - P(-i)}{2}X + \frac{P(i) + P(-i)}{2}$.
Comme $P \in \mathbb{R}[X]$, on a $P(-i) = \overline{P(i)}$, donc :
$R(X) = Im(P(i))X + Re(P(i))$. On a $P(i) = (i\cos(t) + \sin(t))^n = \exp(it - \frac{i\pi}{2})^n = \exp(ni(t - \frac{\pi}{2}))$,
donc $R(X) = \sin(n(t - \frac{\pi}{2})X + \cos(n(t - \frac{\pi}{2}))$.