

## FEUILLE DE TD

## Structures algébriques

## ■ Groupes ■

**Exercice 1.**

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.  $(\text{Fonct}(\mathbb{R}, \mathbb{C}), +)$
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 2.**

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 3.**

Soit  $(G, \star)$  un groupe fini dont le cardinal est pair.

Montrer qu'il existe  $x \in G$ , avec  $x \neq e_G$ , tel que  $x = x^{-1}$ .

On définit la relation  $R$  sur  $G$  par : pour  $x, y \in G$ ,  $xRy$  ssi  $x = y$  ou  $x^{-1} = y$ .

Cette relation est une relation d'équivalence, elle est réflexive, symétrique, et transitive.

Pour  $x \in G$ , la classe d'équivalence  $C_x$  est  $C_x = \{x, x^{-1}\}$ .

On a ainsi deux cas :  $\text{Card}(C_x) = 2$  ssi  $x^{-1} \neq x$ ,  $\text{Card}(C_x) = 1$  ssi  $x = x^{-1}$ .

Les classes d'équivalence de la relation  $R$  forment une partition de  $G$ , c'est-à-dire  $G = \cup_{C \in G/R} C$ .

En utilisant la fonction cardinal, on obtient :  $2n = \text{Card}(G) = \sum_{C \in G/R} \text{Card}(C) = \sum_{C \in G/R, \text{Card}(C)=2} 2 + \sum_{C \in G/R, \text{Card}(C)=1} 1 = 2\text{Card}(\{C \in G/R, \text{Card}(C) = 2\}) + \text{Card}(\{C \in G/R, \text{Card}(C) = 1\})$ .

Donc,  $\text{Card}(\{C \in G/R, \text{Card}(C) = 1\}) = 2(\text{Card}(G) - \text{Card}(\{C \in G/R, \text{Card}(C) = 2\}))$ .

Ainsi,  $\text{Card}(\{C \in G/R, \text{Card}(C) = 1\})$  est un nombre pair.

On sait de plus que  $C_{e_G} = \{e_G\}$ , donc  $\text{Card}(\{C \in G/R, \text{Card}(C) = 1\}) \geq 1$ .

Donc, on a  $\text{Card}(\{C \in G/R, \text{Card}(C) = 1\}) \geq 2$ . Ainsi, il existe  $x \in G$  avec  $x \neq e_G$  tel que  $x = x^{-1}$ .

**Exercice 4.**

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  $f \circ g$ ?

- 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  $pq$ .
- Non. Par exemple  $-I_n$  est d'ordre 2 dans  $GL_n(\mathbb{K})$ , et  $(-I_n)(-I_n) = I_n$  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.
- 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 5.

- Pour  $(G, \star)$  un groupe, quels sont les éléments de  $G$  d'ordre 1 ?
- Combien vaut  $ord(x^{-1})$  en fonction de  $ord(x)$  ?
- Trouver des matrices de  $GL_3(\mathbb{R})$  d'ordres 2 et 3.
- Soient  $n \geq 2$  et  $M \in GL_n(\mathbb{R})$  une matrice diagonale. On suppose que  $M$  est d'ordre fini.  
Déterminer  $ord(M)$ .
- Soit  $n \geq 2$ . On pose  $G = Bij(\{1, \dots, n\})$ . 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  $(G, \circ)$ .

- 
- Si  $x$  est d'ordre 1, alors il vérifie  $x^1 = e$ , donc  $x = e$ .
  - On a  $x^k = e$  si et seulement si on a  $e = x^{-k} = (x^{-1})^k$ . Donc,  $ord(x^{-1}) = ord(x)$ .
  - 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.
  - On a  $M = Diag(\lambda_1, \dots, \lambda_n)$ , 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  $\lambda_i$  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  $M^2 = I_n$ ).

- 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  $f^k(1) = f \circ \dots \circ f(1) = k + 1$ .  
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  $f^n = f \circ \dots \circ f = Id$ .  
Donc,  $f$  est un élément d'ordre  $n$  dans  $(G, \circ)$ .

### Exercice 6.

Les parties suivantes de  $GL_n(\mathbb{R})$  sont-elles des sous-groupes de  $GL_n(\mathbb{R})$ . ?

- $H_1 = \{A \in GL_n(\mathbb{R}); A \text{ diagonale avec tous ses coefficients diagonaux non-nuls}\}$ .
- $H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}; a > 0, b \in \mathbb{R} \right\}$  (ici,  $n = 2$ ).
- $H_3 = \left\{ \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}; a > 0, b \in \mathbb{R} \right\}$  (ici,  $n = 2$ ).

Oui.

Oui.

Non, il ne contient pas  $I_2$ .

### Exercice 7.

Montrer que l'ensemble  $G$  des matrices de la forme  $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$  est un groupe pour le produit matriciel. Déterminer son centre, c'est-à-dire les matrices  $A$  de  $G$  telles que  $AB = BA$  pour tout  $B \in G$ .

On vérifie que  $G$  contient la matrice identité  $I_3$ , et est stable pour le produit matriciel et pour l'inverse de matrices.

Pour déterminer le centre de  $G$ , on pose  $A \in G$  et  $B \in G$ , on calcule  $AB - BA$ , et on regarde à quelle condition sur  $A$  on a  $AB - BA = 0$  pour tout  $B \in G$ .

On obtient que  $Z(G)$  est l'ensemble des matrices de la forme  $\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ .

### Exercice 8.

Démontrer pour chaque question que  $H$  est un sous-groupe de  $(G, *)$ .

1.  $(\mathbb{C}^*, \times)$  et  $H = \{z \in \mathbb{C}^* : \exists n \in \mathbb{N}, z^n = 1\}$ .
2.  $(\mathbb{R}^*, \times)$  et  $H = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, (a, b) \neq (0, 0)\}$ .
3.  $(\mathbb{R}_+^*, \times)$  et  $H = \{x + y\sqrt{3}; x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\}$ .

Plusieurs méthodes sont possibles.

1. On montre que  $H$  est un sous-groupe multiplicatif en vérifiant la définition des sous-groupes (neutre, stabilité par produit, stabilité par inverse).
2. On montre que  $H$  est un sous-groupe multiplicatif en vérifiant la définition des sous-groupes (neutre, stabilité par produit, stabilité par somme).  
Ou bien, on peut vérifier que  $Q[\sqrt{2}]$  est un corps (un sous-corps de  $\mathbb{R}$ ) et que  $H$  est le groupe des inversibles de  $Q[\sqrt{2}]$ , autrement dit que  $(H, \times)$  est un groupe.
3. On montre que  $H$  est un sous-groupe multiplicatif en vérifiant la définition des sous-groupes (neutre, stabilité par produit, stabilité par somme).

### Exercice 9.

Traduire en termes de morphismes de groupes les propriétés bien connues suivantes (dont le domaine de validité a volontairement été omis) :

1.  $\ln(xy) = \ln(x) + \ln(y)$  ;
2.  $|zz'| = |z||z'|$  ;
3.  $\sqrt{xy} = \sqrt{x}\sqrt{y}$  ;
4.  $e^{x+y} = e^x e^y$  ;

1. Morphisme de  $(\mathbb{R}_+^*, \times)$  vers  $(\mathbb{R}, +)$ . (bijectif)
2. Morphisme de  $(\mathbb{C}^*, \times)$  vers  $(\mathbb{R}_+^*, \times)$  (surjectif, non injectif)
3. Morphisme de  $(\mathbb{R}_+^*, \times)$  vers  $(\mathbb{R}_+^*, \times)$  (bijectif)
4. Morphisme de  $(\mathbb{R}, +)$  vers  $(\mathbb{R}_+^*, \times)$ . (bijectif)

### Exercice 10.

Soit  $(G, \times)$  un groupe commutatif. Pour  $n \in \mathbb{N}^*$  on pose  $G_n = \{x \in G \text{ t.q. } x^n = e_G\}$  et  $G_\infty = \{x \in G \text{ t.q. } \exists k \in \mathbb{N} \text{ t.q. } x^k = e_G\}$ .

1. Montrer que pour tout  $n \in \mathbb{N}$ ,  $G_n$  est un sous-groupe de  $G$ .
2. Montrer que  $G_\infty$  est un sous-groupe de  $G$ . Quelle est la relation entre  $G_\infty$  et les  $G_n$  ?

3. Soient  $m_1$  et  $m_2$  des entiers premiers entre eux.  
Montrer alors que  $G_{m_1 m_2} = G_{m_1} G_{m_2} = \{xy, x \in G_{m_1}, y \in G_{m_2}\}$ .  
On s'aidera d'une relation de Bézout.
4. Soit  $n \in \mathbb{N}^*$ . Pour  $x \in G_n$ , que peut-on dire sur  $\text{ord}(x)$  ?
5. Montrer que si  $G_n$  est cyclique, alors  $\text{Card}(G_n) \mid n$ .
6. Soient  $m_1, m_2 \in \mathbb{N}^*$  premiers entre eux. On suppose qu'il existe  $x, y \in G$  tels que  $G_{m_1} = \langle x \rangle$  et  $G_{m_2} = \langle y \rangle$ .  
Montrer qu'alors on a  $G_{m_1 m_2} = \langle xy \rangle$ .  
On pourra exprimer  $x$  et  $y$  comme une puissance de  $xy$ .
7. Soit  $p$  premier, et soit  $k \in \mathbb{N}^*$ .  
Montrer que l'on a soit  $G_{p^k} = G_{p^{k-1}}$  ou bien  $\text{Card}(G_{p^k}) \geq p^k$ .  
On pourra regarder l'ordre des éléments du sous-groupe.
8. On suppose que pour tout  $n \in \mathbb{N}^*$ , l'équation  $x^n = e_G$  possède au plus  $n$  solutions.  
Montrer alors que pour tout  $m \in \mathbb{N}^*$  le sous-groupe  $G_m$  est cyclique.
9. Soit  $\mathbb{K}$  un corps. On considère  $G$  le groupe des inversibles de  $\mathbb{K}$  ( $G = \mathbb{K}^*$ ).  
Montrer que pour tout  $m \in \mathbb{N}^*$  on a  $G_m$  cyclique.
10. Soit  $\mathbb{K}$  un corps fini. Montrer que  $(\mathbb{K}^*, \times)$  est un groupe cyclique.

1. Soit  $n \in \mathbb{N}$ . On a  $e_G^n = e_G$ , donc  $e_G \in G_n$ .  
Pour  $x, y \in G_n$ , par commutativité dans  $G$  on a  $(x.y^{-1})^n = x^n(y^{-1})^n = e_G.(y^n)^{-1} = e_G$ , donc  $xy^{-1} \in G_n$ . Ainsi,  $G_n$  est un sous-groupe de  $G$ .
2. Pour  $x = e_G$  on a  $x^1 = e_G$ , donc  $e_G \in G_\infty$ .  
Pour  $x, y \in G_\infty$ , soient  $n, m \in \mathbb{N}$  t.q.  $x^n = e_G$  et  $y^m = e_G$ .  
On a alors  $(xy^{-1})^{nm} = x^{nm}(y^{-1})^{nm} = (x^n)^m.(y^m)^{-n} = e_G.e_G = e_G$ .  
Donc,  $xy^{-1} \in G_\infty$ .  
Pour tout  $n \in \mathbb{N}$ , on a  $G_n \subset G_\infty$ . Et, on a  $G_\infty = \bigcup_{n \geq 1} G_n$ .
3. Pour  $x \in G_{m_1}$  et  $y \in G_{m_2}$  on a  $(xy)^{m_1 m_2} = (x^{m_1})^{m_2} (y^{m_2})^{m_1} = e_G.e_G = e_G$ .  
Donc, on a  $G_{m_1} G_{m_2} \subset G_{m_1 m_2}$ .  
Réciproquement, d'après le Théorème de Bézout, soient  $u, v \in \mathbb{Z}$  tels que  $m_1 u + m_2 v = 1$ .  
Pour  $z \in G_{m_1 m_2}$  on a  $z = z^1 = z^{m_1 u + m_2 v} = z^{m_1 u} z^{m_2 v}$ .  
On a  $(z^{m_1 u})^{m_2} = e_G$  et  $(z^{m_2 v})^{m_1} = e_G$ , donc  $z^{m_1 u} \in G_{m_2}$  et  $z^{m_2 v} \in G_{m_1}$ . Donc, on a  $G_{m_1 m_2} \subset G_{m_1} G_{m_2}$ , ce qui conclut pour l'égalité.
4. Pour  $x \in G_n$ , on a  $\text{ord}(x) \mid n$  car  $x^n = e_G$ .
5. Soit  $x \in G_n$  tel que  $\langle x \rangle = G_n$ . Alors on a  $\text{Card}(G_n) = \text{ord}(x)$ , et  $\text{ord}(x) \mid n$ .

6. D'une part, on a  $xy \in G_{m_1 m_2}$ , donc  $\langle xy \rangle \subset G_{m_1 m_2}$ .  
Réciproquement, on réutilise la relation de Bézout précédente.  
On a  $(xy)^{vm_2} = x^{vm_2} y^{vm_2} = x^{1-um_1} .e_G = x(x^{m_1})^{-u} = x.e_G = x$ .  
De même, on a  $(xy)^{um_1} = x^{um_1} y^{um_1} = e_G .y^{1-vm_2} = y(y^{m_2})^{-v} = y.e_G = y$ .  
Ainsi, on a  $x, y \in \langle xy \rangle$ , donc  $G_{m_1 m_2} = G_{m_1} G_{m_2} = \langle x \rangle \langle y \rangle \subset \langle xy \rangle$ , ce qui conclut.

7. Soit  $x \in G_{p^k}$ .  
On a  $ord(x) \mid p^k$ . Si  $ord(x) = p^k$  on a  $Card(G_{p^k}) \geq ord(x) \geq p^k$ .  
Sinon on a  $ord(x) < p^k$ . Comme  $p$  est premier, on a donc  $ord(x) \mid p^{k-1}$ , donc  $x \in G_{p^{k-1}}$ .  
Ainsi, soit  $G_{p^k}$  ne possède aucun élément d'ordre  $p^k$ , auquel on a  $G_{p^k} \subset G_{p^{k-1}}$ .  
Sinon, le sous-groupe possède au moins un élément d'ordre  $p^k$ , auquel cas il contient au moins  $p^k$  éléments.

8. On commence par montrer cela pour  $p^k$ , pour tout nombre premier  $p$  et pour tout entier  $k \in \mathbb{N}$ .

Fixons  $p$  premier. On pose  $HR_k : "G_{p^k}$  est cyclique.

Initialisation : Pour  $k = 0$ , on a  $G_1 = \{e_G\}$ , qui est cyclique.

Hérédité : Soit  $k \in \mathbb{N}$  tel que  $HR_k$  est vraie.

D'après la question précédente, on a alors soit  $G_{p^{k+1}} = G_{p^k}$ , auquel cas ce groupe est cyclique d'après  $HR_k$ , soit  $G_{p^{k+1}}$  possède un élément  $x$  d'ordre  $p^{k+1}$ .

Vu que le sous-groupe  $G_{p^{k+1}}$  ne contient qu'au plus  $p^{k+1}$  éléments, et que le sous-groupe  $\langle x \rangle$  en contient exactement  $p^{k+1}$ , on a alors  $G_{p^{k+1}} = \langle x \rangle$ , donc ce sous-groupe est cyclique.

Donc  $HR_{k+1}$  est vraie, ce qui termine la récurrence.

Soit  $r \in \mathbb{N}^*$  et soient  $m_1, \dots, m_r \in \mathbb{N}^*$  des entiers premiers entre eux deux à deux tels que chaque  $G_{m_i}$  est cyclique, pour  $1 \leq i \leq r$ .

On pose  $HR_r : "G_{m_1 \dots m_r}$  est cyclique".

Démontrons par récurrence que pour tout  $r \in \mathbb{N}^*$ ,  $HR_r$  est vraie.

Initialisation : Pour  $r = 1$  cela est vrai,  $G_{m_1}$  est cyclique.

Hérédité : Soit  $r \geq 1$  tel que  $HR_r$  est vraie.

D'après les questions précédentes, on a  $G_{m_1 \dots m_r m_{r+1}} = G_{m_1 \dots m_r} . G_{m_{r+1}}$ .

D'après  $HR_r$  et d'après l'hypothèse initiale, les deux sous-groupes de gauche sont cycliques.

Comme  $m_1 \dots m_r$  et  $m_{r+1}$  sont premiers entre eux, on sait d'après une question précédente que le produit de ces sous-groupes est encore cyclique. Donc,  $G_{m_1 \dots m_r m_{r+1}}$  est cyclique.

Donc  $HR_{r+1}$  est vraie, ce qui termine la récurrence.

Soit maintenant  $n \in \mathbb{N}^*$ . D'après le théorème de décomposition en produit de facteurs premiers, on a  $r \in \mathbb{N}^*$  et  $p_1, \dots, p_r \in \mathcal{P}$ , et  $a_1, \dots, a_r \in \mathbb{N}$  tels que  $n = \prod_{i=1}^r p_i^{a_i}$ .

D'après les deux résultats précédents, on a alors que  $G_n = G_{p_1^{a_1} \dots p_r^{a_r}}$  est cyclique.

9. Un corps est en particulier un anneau commutatif unitaire et intègre. Dans un tel anneau, une équation polynomiale de degré  $n$  possède au plus  $n$  solutions.  
En particulier, pour tout  $n \in \mathbb{N}$ , l'équation  $x^n = 1$  possède au plus  $n$  solutions.

Le groupe des inversibles  $\mathbb{K}^*$  du corps  $\mathbb{K}$  est donc un corps commutatif tel que chaque équation  $x^n = 1$  possède au plus  $n$  solutions.

D'après la question précédente, on en déduit que chaque sous-groupe  $G_n$  est cyclique, pour tout  $n \in \mathbb{N}$ .

10. Si  $\mathbb{K}$  est de plus fini, alors  $\mathbb{K}^*$  est fini. D'après le théorème de Lagrange, pour  $x \in \mathbb{K}^*$  on a  $ord(x) \mid Card(\mathbb{K}^*)$ .

Ainsi, on obtient que  $\mathbb{K}^* = G_{Card(\mathbb{K}^*)}$ .

Le sous-groupe  $G_{Card(\mathbb{K}^*)}$  étant cyclique, on en déduit que  $\mathbb{K}^*$  est cyclique.

**Remarque :** Le sous-groupe  $G_\infty$  n'est en général pas cyclique. L'exemple fondamental est celui des racines de l'unité dans  $\mathbb{C}$ .

### 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.  $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$  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  $f : \mathbb{Z} \rightarrow \mathbb{Q}$  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  $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$  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  $S_n$  n'est pas un groupe commutatif. En effet, on a  $(12) \circ (23) = (123) \neq (132) = (23) \circ (12)$ .  
Si  $n = 2$ , ces deux groupes sont des groupes à 2 éléments qui sont isomorphes.
6. Non.  
Soit  $f : \mathbb{Z} \rightarrow \mathbb{Z}^2$  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  $f(n) = f(n \cdot 1) = n \cdot f(1) = n(a, b)$ .  
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  $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$  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  $e_1, \dots, e_m$  la base canonique de  $\mathbb{Q}^m$  (elle est dans  $\mathbb{Z}^m$ ).  
Alors, il existe  $x_1, \dots, x_m \in \mathbb{Z}^n$  tels que  $f(x_i) = e_i$  par surjectivité.  
La famille  $(x_1, \dots, x_m)$  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  $r_1, \dots, r_m \in \mathbb{Q}$  tels que  $r_1 x_1 + \dots + r_m x_m = 0$ .  
En multipliant ces rationnels  $r_1, \dots, r_m$  par leur dénominateur commun, on a ainsi des nombres entiers  $k_1, \dots, k_m$ , non tous nuls, tels que  $k_1 x_1 + \dots + k_m x_m = 0$ .  
Mais alors, on a  $0 = f(0) = f(k_1 x_1 + \dots + k_m x_m) = f(k_1 x_1) + \dots + f(k_m x_m)$ ,  
 $0 = k_1 f(x_1) + \dots + k_m f(x_m) = k_1 e_1 + \dots + k_m e_m$ .  
Comme les  $k_i$  sont non tous nuls et que la famille  $(e_1, \dots, e_m)$  est libre dans  $\mathbb{Q}^m$ , le vecteur  $k_1 e_1 + \dots + k_m e_m$  est donc non-nul, ce qui est impossible.
8. Non.  
Soit  $f : \mathbb{Q} \rightarrow \mathbb{Q}^2$  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  $f(n) = f(n \cdot 1) = n \cdot f(1) = n(a, b)$ .  
Pour tout  $r \in \mathbb{Q}$ , on a  $r = \frac{p}{q}$ , d'où  $f(qr) = f(q \cdot r) = q \cdot f(r)$  et  $f(qr) = f(p) = p \cdot f(1) = p(a, b)$ .  
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  $(H, \Delta)$  des groupes, et  $f : G \rightarrow H$  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,  $f(\langle x \rangle) = \{f(x)^n, n \in \mathbb{Z}\} = \langle f(x) \rangle$ .
  4. Le sous-groupe  $\langle S \rangle$  est formé de tous les éléments de  $G$  de la forme  $a_1 \star \dots \star a_m$ , avec  $m \geq 1$ , et  $(a_i \in S$  ou  $a_i^{-1} \in S)$ .  
Or, on a  $f(a_1 \star \dots \star a_m) = f(a_1)\Delta \dots \Delta f(a_m)$ .  
On obtient donc l'égalité :  $f(\langle S \rangle) = \langle f(S) \rangle$ .
  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  $\Phi_a : x \in G \mapsto axa^{-1} \in G$ .

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

- Pour  $a, b \in G$ , on vérifie que  $\Phi_a \circ \Phi_b = \Phi_{ab}$ . On a de plus  $\Phi_e = \text{id}_G$ . On en déduit que la fonction  $\Phi_a$  est bijective, et que  $\Phi_a^{-1} = \Phi_{a^{-1}}$ . Il reste à montrer que  $\Phi_a : G \rightarrow G$  est un morphisme :

$$\forall x, y \in G, \Phi_a(xy) = axya^{-1} = (axa^{-1})ya^{-1} = \Phi_a(x)\Phi_a(y).$$

Cela est donc vrai.

- La fonction  $\text{Id}_G$  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  $(\text{Aut}(G), \circ)$  est un sous-groupe de  $(\text{Bij}(G), \circ)$ . Donc,  $(\text{Aut}(G), \circ)$  est un groupe.
- A la première question, on a montré que  $I$  est stable par multiplication, contient  $\text{Id}_G$ , et que tout élément possède un inverse dans  $I$ . C'est bien un sous-groupe de  $\text{Aut}(G)$ .
- 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  $\Phi_a = \text{Id}_G$ . 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  $\Phi_a = \text{Id}_G$  ssi  $a$  commute avec tous les éléments de  $G$ . Ainsi,  $\text{Ker}(h) = \{a \in G \text{ t.q. } ab = ba \forall b \in G\}$ .

- 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  $\Phi_a = \text{id}_G$ , donc  $I = \{\text{id}_G\}$ , donc  $G$  est commutatif.

- Prenons un contre-exemple. Pour  $(G, \star) = (\mathbb{Z}, +)$ , on a  $I = \{\text{Id}_{\mathbb{Z}}\}$  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  $\text{Aut}(\mathbb{Z}) \neq I$ .

**Exercice 14.**

Soit  $n \in \mathbb{N}^*$ . Soient  $i, j, k \in \llbracket 1, n \rrbracket$ .

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

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

**Exercice 15.**

Décomposer les permutations suivantes en produit de cycles à supports disjoints, ainsi qu'en produit de transpositions, calculer leur ordre. Calculer enfin  $\sigma_1^{1000}$  et  $\sigma_2^{1000}$ .

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

On a

$$\sigma_1 = (1 \ 3 \ 4 \ 6) (2 \ 5),$$

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

$$\sigma_1 = (1 \ 3) (3 \ 4) (4 \ 6) (2 \ 5).$$

On a

$$\sigma_2 = (1 \ 4 \ 7 \ 8) (2 \ 6 \ 5) (3 \ 9),$$

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

$$\sigma_2 = (1 \ 4) (4 \ 7) (7 \ 8) (2 \ 6) (6 \ 5) (3 \ 9).$$

### Exercice 16.

1. Montrer que les doubles transpositions de la forme  $(1 \ i) (1 \ j)$  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  $(1 \ i)$  engendrent  $\mathcal{S}_n$ . Toute permutation de  $\mathcal{A}_n$  s'écrit donc comme un produit de transpositions  $(1 \ i)$ . 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  $(1 \ i) (1 \ j)$ .
  2. On a  $(1 \ i) (1 \ j) = (1 \ j \ i)$ , ce qui montre le résultat. On a même montré mieux : le groupe alterné est engendré par les 3-cycles de la forme  $(1 \ i \ j)$ .

**Exercice 17.** Soit  $n \geq 2$ . Soit  $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ .

Déterminer l'ordre de  $\bar{m}$  dans  $(\mathbb{Z}/n\mathbb{Z}, +)$ .

Quels sont tous les ordres possibles ?

Pour chaque ordre  $r$ , trouver un élément  $\bar{m}$  d'ordre  $r$ .

---

Pour déterminer cet ordre, on cherche tous les entiers  $k \geq 1$  tels que  $k \cdot \bar{m} = \bar{0}$ . (on regarde l'équation  $x^k = e$ )

On a  $k \cdot \bar{m} = \bar{m} + \dots + \bar{m} = \overline{km}$ .

Et  $\overline{km} = \bar{0}$  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  $\frac{n}{\text{pgcd}(n,m)}$ . Ainsi, par minimalité de l'ordre d'un élément, on en déduit que  $\text{ord}(\bar{m}) = \frac{n}{\text{pgcd}(n,m)}$ .

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  $\text{ord}(\bar{m}) = \frac{n}{\frac{n}{d}} = d$ .

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 :  $x \equiv 4 \pmod{6}$  et  $x \equiv 7 \pmod{11}$ .

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  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$

On écrira à chaque fois  $\phi$  et sa bijection réciproque  $\phi^{-1}$ .

- 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 :  $2 \cdot 6 - 11 = 1$ .  
Ainsi, une solution particulière est  $x_0 = 4 \cdot (-11) + 7 \cdot (12) = -44 + 84 = 40$ .  
On a donc :  $(x \equiv 4 \pmod{6})$  et  $(x \equiv 7 \pmod{11})$  ssi  $x \equiv 40 \pmod{66}$ .  
Donc, l'ensemble des solutions est  $40 + 66\mathbb{Z}$ .
- On a  $\phi(\bar{c}) = (\bar{c}, \bar{c})$  et  $\phi^{-1}(\bar{a}, \bar{b}) = 10\bar{a} + 6\bar{b}$ .  
Pour déterminer  $\phi^{-1}$  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  $2 \cdot 3 + (-1) \cdot 5 = 1$ , on obtient d'après le cours les valeurs de  $\bar{-5} = \bar{10}$  et  $\bar{6}$  dans  $\mathbb{Z}/15\mathbb{Z}$ .
- On a  $\phi(\bar{c}) = (\bar{c}, \bar{c})$  et  $\phi^{-1}(\bar{a}, \bar{b}) = 76\bar{a} + 25\bar{b}$ .  
Pour déterminer  $\phi^{-1}$  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  $1 \cdot 25 + (-6) \cdot 4 = 1$ , 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  $\times$ .

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

- Ce sont les  $\bar{a}$  tels que  $a$  est premier avec  $n$ .
- 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  $\bar{1}$ .  
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.
- Ce groupe est  $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ . Il a 6 éléments.  
On montre que  $\bar{3}$  est d'ordre 6 pour  $\times$ . Donc,  $(\mathbb{Z}/7\mathbb{Z})^\times = \langle \bar{3} \rangle$ . Ce groupe est donc un groupe cyclique à 6 éléments. Il est isomorphe à  $(\mathbb{Z}/6\mathbb{Z}, +)$ .

- Ce groupe est  $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Il a 4 éléments.  
On montre que  $\bar{3}, \bar{5}, \bar{7}$  sont d'ordre 2 pour  $\times$ . Donc,  $(\mathbb{Z}/8\mathbb{Z})^\times$  est isomorphe à  $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ .
- Ce groupe est  $\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ . Il a 6 éléments.  
On montre que  $\bar{2}$  est d'ordre 6 pour  $\times$ . Donc,  $(\mathbb{Z}/9\mathbb{Z})^\times = \langle \bar{2} \rangle$ . 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  $a^2 = 1_A$ .

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

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

- $\mathbb{Z}^\times = \{1, -1\}$ .  $\mathbb{Q}^\times = \mathbb{Q}^*$ ,  $\mathbb{R}^\times = \mathbb{R}^*$ ,  $\mathbb{C}^\times = \mathbb{C}^*$ .  
Dans ces anneaux, on a  $a^2 = 1$  ssi  $a = \pm 1$ .
- $\mathbb{K}[X]^\times = \mathbb{K}^*$ . On a  $a^2 = 1$  ssi  $a = \pm 1$ .
- $M_n(\mathbb{K})^\times = GL_n(\mathbb{K})$ . On a  $A^2 = I_n$  ssi  $(A - I_n)(A + I_n) = 0$ .  
Cette équation possède énormément de solutions. Toutes les matrices diagonales  $B = \text{Diag}(\lambda_1, \dots, \lambda_n)$  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  $(PBP^{-1})^2 = PB^2P^{-1} = PP^{-1} = I_n$ .
- 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  $x \in E$ .
- 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  $\phi$  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  $\phi$  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  $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \rightarrow G$  telle que

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

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  $1 + j + j^2 = \frac{1-j^3}{1-j} = 0$  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 :  $|a + jb|^2 = (a - \frac{b}{2})^2 + \frac{3b^2}{4} = a^2 + b^2 - ab \in \mathbb{Z}$ .

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  $\pm 1, \pm j, \pm(1 + j) = \pm j^2$  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  $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$ , avec  $a_0, \dots, a_{n-1} \in A$ .  
On a  $a_0 = P(0) \in A^\times$ .  
On a  $0 = P(b) = b^n + \dots + a_1b + a_0 = b(b^{n-1} + b^{n-2}a_{n-1} + \dots + a_1) + a_0$ .  
Donc, on a  $-a_0 = b(b^{n-1} + b^{n-2}a_{n-1} + \dots + a_1)$ .  
Comme  $a_0$  est inversible, on a  $1 = b(b^{n-1} + b^{n-2}a_{n-1} + \dots + a_1)(-a_0^{-1})$ . En posant  $b' = (b^{n-1} + b^{n-2}a_{n-1} + \dots + a_1)(-a_0^{-1})$ , 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  $A = \{a_0, \dots, a_n\}$ . On pose alors  $P(X) = (X - a_0)(X - a_1) \dots (X - a_n)$ . 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  $\bar{k}^3 = \bar{k}$ , pour tout  $\bar{k}$ .

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  $x = \bar{2}$  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  $(1 - x)(1 + x + \dots + x^{n-1}) = 1 - x^n = 1$ .

Et  $1 - x$  commute avec  $1 + x + \dots + x^{n-1}$ .

Donc,  $1 - x$  est inversible, d'inverse  $1 + x + \dots + x^{n-1}$ .

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  $\bar{x} = aI_2 - bi - cj - dk$ .  
Calculer  $x\bar{x}$ .
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  $x\bar{x} = (a^2 + b^2 + c^2 + d^2)I_2$ .
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  $y = \bar{x} \frac{1}{a^2 + b^2 + c^2 + d^2}$ , 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  $xy \neq 0$ .  
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  $\frac{1}{a^2 + b^2 + c^2 + d^2} \bar{x}$ .  
On a donc  $-x = \frac{1}{a^2 + b^2 + c^2 + d^2} \bar{x}$ .  
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 polynomiale 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 polynomiale  $x^2 + 1_A = 0$ , 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  $|z|^2 = z\bar{z}$ , 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  $q \equiv 3 \pmod{4}$ . 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) Dans l'écriture exponentielle de  $z, z'$ , montrer que  $\arg(z') = \arg(\bar{z})$ .
  - (d) Montrer que  $z' = \bar{z}$ .
  - (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  $z\bar{z} = |z|^2 = 1$ . Comme  $\bar{z} = x - iy \in \mathbb{Z}[i]$ ,  $z$  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 ces 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  $(x = \pm 1 \text{ et } y = 0)$  ou  $(x = 0 \text{ et } y = \pm 1)$ .  
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  $(|a|^2 = 1 \text{ et } |b|^2 = p)$  ou  $(|a|^2 = p \text{ et } |b|^2 = 1)$ .  
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  $z' = Re^{-it} = \bar{z}$ .

- (e) Pour  $z = x + iy$ , avec les questions précédentes on a  $x, y \neq 0$  et  $x^2 + y^2 = |z|^2 = z\bar{z} = zz' = q$ .  
Donc,  $q$  est la somme de deux carrés.
- (f) Or, modulo 4 cela est impossible. La somme de deux carrés est congrue 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,  $(3 + 4i)(3 - 4i) = 5 \times 5 = (1 + 2i)^2(1 - 2i)^2$ .  
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  $f : a \in \mathbb{Z} \mapsto \bar{a} \in \mathbb{Z}/n\mathbb{Z}$ .  
On a vu que  $f$  est un morphisme de groupes. On a  $f(1) = \bar{1}$ . Et, pour  $x, y \in \mathbb{Z}$  on a  $\overline{xy} = \bar{x}\bar{y}$ .
  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  $f(\bar{n}) = f(n\bar{1}) = f(\bar{1} + \dots + \bar{1}) = f(\bar{1}) + \dots + f(\bar{1}) = n.f(\bar{1})$ .  
 Or, on a  $\bar{n} = \bar{0}$ , donc  $f(\bar{0}) = 0$ .  
 D'autre part, on a  $f(\bar{1}) = 1$ , et  $n.f(\bar{1}) = n$ .  
 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  $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$  existe, comme dans la question précédente on aura  $0 = f(\bar{n}) = f(n\bar{1}) = n.\bar{1}$ .  
 On a  $0 = n.\bar{1}$  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  $f : A \rightarrow B$  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  $f : \mathbb{R} \rightarrow \mathbb{Q}$ .

3. Non. Dans  $\mathbb{C}$  on a  $i$  qui est une racine de  $x^2 + 10$ , alors que dans  $\mathbb{R}$  le polynôme  $X^2 + 10$  n'a pas de racines.  
 D'après l'exercice précédent, il n'existe pas de morphisme d'anneaux  $f : \mathbb{C} \rightarrow \mathbb{R}$ .
4. Non. L'anneau  $\mathbb{R}$  est intègre, et  $\mathbb{R} \times \mathbb{R}$  n'est pas intègre.  
 Pour  $f : A \rightarrow B$  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  $X^2 + 10$  n'a pas de racines.  
 D'après l'exercice précédent, il n'existe pas de morphisme d'anneaux  $f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[\sqrt{2}]$ .  
 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,  $\mathbb{R}[A] = \text{Vect}(I_2, A) = \{xI_2 + yA, x, y \in \mathbb{R}\}$ .  
 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  $J = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ .

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

- On a  $\mathbb{Q}[J] = Vect(I_2, J, J^2, \dots) = Vect(J^n, n \geq 0)$ .
- 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,  $\mathbb{Q}[J] = Vect(I_2, J)$ .
- Comme cette famille est libre, c'est une base de  $\mathbb{Q}[J]$ . Donc, on a  $aI_2 + bJ = 0$  ssi  $a = b = 0$ .
- L'anneau  $\mathbb{Q}[J]$  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  $x \cdot (\frac{1}{a^2 - 2b^2}y) = I_2$ .  
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.
- 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  $a = \sqrt{2}, b = 1, x = aI_2 + bJ$ , 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  $f : n \in \mathbb{Z} \mapsto n \cdot 1_A \in A$ .  $f$  est un morphisme d'anneaux de  $\mathbb{Z}$  vers  $A$ .  
Montrer qu'il existe  $p \in \mathbb{Z}$  tel que  $Ker(f) = p\mathbb{Z}$ .

- Montrer que l'on a  $p \neq 0, 1, -1$ , et montrer que l'on peut choisir  $p$  positif.
- Soient  $n, m \in \mathbb{Z}$  tels que  $\bar{n} = \bar{m}$  dans  $\mathbb{Z}/p\mathbb{Z}$ .  
Montrer que dans  $A$  on a  $n \cdot 1_A = m \cdot 1_A$ .
- En déduire que la fonction  $h : \bar{n} \in \mathbb{Z}/p\mathbb{Z} \mapsto n \cdot 1_A \in A$  est bien définie.
- Montrer que le nombre entier positif  $p$  est premier.  
On pourra raisonner par l'absurde.  
*Bonus :* Montrer qu'en posant  $\bar{n} \cdot a = h(\bar{n}) \cdot a \in A$ , l'ensemble  $(A, +, \cdot)$  est un  $\mathbb{Z}/p\mathbb{Z}$ -espace vectoriel.
- Montrer que  $(A, +, \cdot)$  est un  $\mathbb{Z}/p\mathbb{Z}$ -ev de dimension finie.
- On pose  $r = \dim(A)$ . En posant  $(e_1, \dots, e_r)$  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.

- Montrer que  $x$  possède un inverse dans  $A$ .
- 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).

- 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.
- 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  $p \in p\mathbb{Z} = \text{Ker}(f)$ .  
De l'autre, on a  $f(a), f(b) \neq 0$  car  $a, b \notin p\mathbb{Z} = \text{Ker}(f)$ .  
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  $\bar{n} = \bar{m}$ , alors  $n \equiv m \pmod{p}$ . 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  $\bar{n}$  que l'on choisit. Donc, on peut poser  $h(\bar{n}) = f(n) = n.1_A$ .  
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  $A = \{a_0, a_1, \dots, a_{\text{Card}(A)}\}$ , on a  $A = \text{Vect}(a_0, a_1, \dots, a_{\text{Card}(A)})$ . 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  $(e_1, \dots, e_r)$  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 :  
 $(x_1, \dots, x_r) \in (\mathbb{Z}/p\mathbb{Z})^r \mapsto x_1e_1 + x_2e_2 + \dots + x_re_r \in A$ . (C'est même un isomorphisme d'ev).  
Donc, on a  $\text{Card}(A) = \text{Card}((\mathbb{Z}/p\mathbb{Z})^r) = p^r$ .
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.