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

Exercice 2.
Soit $(G, \star)$ un groupe tel que $x^2 = e$ pour tout $x \in G$.
Montrer que le groupe 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 $x = x^{-1}$.

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 $f \circ g$?

Exercice 5.

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 $(G, \circ)$.

Exercice 6.
Les parties suivantes de $GL_n(\mathbb{R})$ sont-elles des sous-groupes de $GL_n(\mathbb{R})$. ?

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

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 $B \in G$.

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 $H = \{x + y\sqrt{3};\ x \in \mathbb{N},\ y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$.

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. $e^{x+y} = e^x e^y$;

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_∞ est un sous-groupe de G. Quelle est la relation entre G_∞ 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 $ord(x)$?
5. Montrer que si G_n est cyclique, alors $Card(G_n) \mid n$.
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 $Card(G_{p^k}) \geq p^k$.
   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.

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 $(\mathbb{R}^n, +)$, $n > 0$.

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 $f^{-1}(\langle S' \rangle) \neq \langle f^{-1}(S) \rangle$.

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.

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 $\sigma \begin{pmatrix} i & j \end{pmatrix} \sigma^{-1}$?

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}.

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

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 $\mathcal{A}_n$.

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.

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 ?

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 ?

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}.

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 $(\mathbb{Z}/9\mathbb{Z})^\times$.

■ *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 ?

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.

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 $\mathbb{Z}[j]^\times$.

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.

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 $1 + N \subset A^\times$.

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 ?

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 $q \equiv 3 \mathrm{mod}\ (4)$. 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.

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 $M_2(\mathbb{Q})$

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 $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

■ *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.

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 $\mathbb{R}[J]$.

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).