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.

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.

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 $i + 2j = n$.

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 $\displaystyle\sum_{k=0}^{n} \frac{\binom{n}{k}}{k+1}$.

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

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 $\dbinom{p+q}{p} = \displaystyle\sum_{k=0}^{p} \binom{p}{k}\binom{q}{p-k}$.

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 $A \Delta B = (A \cap \bar{B}) \cup (B \cap \bar{A})$

Exercice 8.
Soit $(G, \star)$ un groupe tel que $x^2 = e$ pour tout $x \in G$.
Montrer que le groupe 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 $H = \mathrm{Bij}\,(\mathbb{Z} \times \mathbb{Z})$.
   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 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 $(G, \circ)$.

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 $(x^2 + x - \overline{1})(x^2 - x - \overline{1})$ et $(x^2 + \overline{2})(x^2 - \overline{2})$ dans $\mathbb{Z}/3\mathbb{Z}$.
2. Développer $(x^2 + x - \overline{1})(x^2 - x - \overline{1})$ et $(x^2 + \overline{2})(x^2 - \overline{2})$ 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 $q \equiv 3 \bmod (4)$. 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.

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).

■ *Polynômes* ■

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

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

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

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 ?

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

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

Exercice 38.
Déterminer tous les polynômes P tels que :

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

et :

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

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 $n \geq 1$

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 $P(a) = P(b) = 0$.

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 $\mathbb{C}[X]$: $X^3 - 1$, $X^n - 1$ $n \geq 1$, $X^2 - 5X + 2$, $X^2 + 1$, $X^n - z$ $n \geq 1$ $z = r.e^{it}$.

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.

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 $\mathbb{Q}[X]$?

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 $]-1, 1[$.

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.)

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 $X^2 + 1$.