Exercices du chapitre III (Structures algébriques)

✓ : exercice d'application des méthodes, ★ : exercice classique, ☢ : exercice difficile.

Groupes

Les groupes usuels sont munis de leur loi de composition interne usuelle, et les produits cartésiens de groupes usuels sont munis de la loi de composition interne définie par le produit « coordonnée par coordonnée ».

✓ **Exercice 1.** Déterminer les sous-groupes finis de $\mathbb{C}^*$ et $\mathbb{R}^*$.

★ **Exercice 2.**

1. Soit $(G, \cdot)$ un groupe commutatif. Montrer que si m et n sont deux entiers premiers entre eux, et si $a, b \in G$ sont deux éléments d'ordres m et n respectivement, alors $a \cdot b$ est d'ordre mn.
2. En déduire que si m et n sont deux entiers premiers entre eux, alors $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique (ne pas utiliser le théorème chinois). Donner un générateur explicite.
3. Montrer que le résultat de la première question est faux en général si m et n ne sont pas premiers entre eux.
4. Montrer que le résultat de la première question est faux en général si G n'est pas commutatif.

Exercice 3. Nous proposons une autre démonstration du fait que dans un groupe cyclique, tous les sous-groupes sont aussi cycliques. Soit G un tel groupe, dont on note a un générateur. Soit H un sous-groupe de G. On note k le plus entier naturel non nul tel que : $a^k \in H$.

1. Justifier que k existe.
2. Soit $x \in H$. Montrer qu'il existe $\ell \in \mathbb{Z}$ tel que : $x = a^{k\ell}$. Conclure.

★ **Exercice 4. (Exposant d'un groupe)** Soit G un groupe commutatif et fini. On appelle *exposant* de G le maximum des ordres de ses éléments. On note d l'exposant de G dans ce qui suit.

1. Montrer que pour tout $(a, b) \in G^2$, il existe $c \in G$ dont l'ordre est le ppcm des ordres de a et b.
2. En déduire que pour tout $g \in G$, on a : $g^d = 1_G$.

Exercice 5. Soit G un groupe commutatif et fini. Montrer que pour tout nombre premier p divisant $\mathrm{card}(G)$, il existe un élément d'ordre p. *À comparer avec la démonstration de l'exercice 40, qui n'utilise pas d'hypothèse de commutativité.*

Exercice 6. Soit G un groupe de cardinal impair. Montrer que pour tout $a \in G$, il existe un unique $b \in G$ tel que : $a = b^2$.

✓ **Exercice 7.** Soient G un groupe de $(x, y) \in G^2$. Montrer que si xy est d'ordre fini k, alors yx est aussi d'ordre k.

Exercice 8. Soient G un groupe et H_1, H_2 deux sous-groupes de G.

1. On suppose que $H_1 \cup H_2$ est un sous-groupe de G. Montrer : $H_1 \subseteq H_2$, ou : $H_2 \subseteq H_1$.
2. On suppose que les cardinaux de H_1 et H_2 sont finis et premiers entre eux. Décrire $H_1 \cap H_2$.

Exercice 9. Soient G un groupe fini et H, K deux sous-groupes de G. On note l'ensemble suivant : $HK = \{g \in G \mid \exists (h, k) \in H \times K,\ g = hk\}$. Montrer que HK est de cardinal $\dfrac{\mathrm{card}(H)\mathrm{card}(K)}{\mathrm{card}(H \cap K)}$.

Exercice 10. (Groupes commutatifs de cardinal p^2, avec p premier) Soit p un nombre premier. Montrer que tout groupe commutatif de cardinal p^2 est isomorphe soit à $(\mathbb{Z}/p^2\mathbb{Z})$, soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

L'exercice 39 démontre qu'en fait tout groupe de tel cardinal est nécessairement commutatif.

Exercice 11. Soient $n \in \mathbb{N} \setminus \{0\}$ et $k \in \mathbb{Z}$. Montrer que $\bar{k}$ et $\overline{\mathrm{pgcd}(n, k)}$ ont même ordre dans $\mathbb{Z}/n\mathbb{Z}$.

★ **Exercice 12.** Soit φ l'indicatrice d'Euler. Montrer : $\forall n \in \mathbb{N} \setminus \{0\},\ n = \displaystyle\sum_{d|n} \varphi(d)$. La somme est indexée par les diviseurs *positifs* de n.

Exercice 13. Soient K un corps et G un sous-groupe fini de $(K^*, \times)$. Montrer que G est cyclique. *Utiliser l'exercice 4.*

Exercice 14. Soit K un corps. On veut montrer que les groupes $(K, +)$ et $(K^*, \times)$ ne sont pas isomorphes.

1. Justifier que le résultat de l'exercice est évident si K est fini.

On suppose désormais que K est un corps infini.

2. Compter le nombre de solutions des équations $x^2 = 1$ et $2x = 0$, d'inconnue $x \in K$, et en déduire que $(K, +)$ et $(K^*, \times)$ ne sont pas isomorphes.

★ **Exercice 15.** Soit G un groupe tel que : $\forall g \in G,\ g^2 = 1_G$.

1. Montrer que G est commutatif.
2. On suppose de plus que G est fini et non réduit à l'élément neutre. Montrer qu'il existe $s \in \mathbb{N} \setminus \{0\}$ tel que G soit isomorphe à $(\mathbb{Z}/2\mathbb{Z})^s$.

✓ **Exercice 16.** Soit $(a, b) \in (\mathbb{N} \setminus \{0\})^2$.

1. Expliciter $\mathbb{U}_a \cap \mathbb{U}_b$ par des arguments de théorie des groupes.
2. Montrer que l'application $z \mapsto (z^b, z^a)$ est un isomorphisme de $\mathbb{U}_{ab}$ dans $\mathbb{U}_a \times \mathbb{U}_b$ si et seulement si a et b sont premiers entre eux.

1896-1934

Exercice 17. (Groupe quasi-cyclique de Prüfer) Soit p un nombre premier. On pose : $G = \bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}$.

1. Montrer que G est un groupe non monogène.
2. Montrer que tout sous-groupe strict de G est cyclique.

★ **Exercice 18.** Montrer que $\mathbb{Q}$ n'admet pas de partie génératrice finie.

★ **Exercice 19.** Soit $(a, b) \in (\mathbb{N} \setminus \{0\})^2$. Déterminer les morphismes de groupes de $\mathbb{Z}/a\mathbb{Z}$ dans $\mathbb{Z}/b\mathbb{Z}$.

Exercice 20. Soit $n \in \mathbb{N} \setminus \{0\}$.

1. Déterminer les morphismes de groupes de $\mathbb{Z}$ dans lui-même.
2. Déterminer les morphismes de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$.
3. Déterminer les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^*$.
4. Déterminer les morphismes de groupes de $\mathbb{U}_n$ dans $\mathbb{C}^*$.

✓ **Exercice 21.** Montrer que $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*)$ sont isomorphes, mais que $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*)$ ne le sont pas.

★ **Exercice 22.** Soient G un groupe fini et $f : G \to \mathbb{C}^*$ un morphisme de groupes. Calculer : $\sum_{g \in G} f(g)$.

Exercice 23. Soient G un groupe fini et $f : G \to G$ un morphisme de groupes. Montrer que $\ker(f) = \ker(f^2)$ si et seulement si $\mathrm{im}(f) = \mathrm{im}(f^2)$.

✓ **Exercice 24.** Montrer que si G et G' sont deux groupes isomorphes, alors $\mathrm{Aut}(G)$ et $\mathrm{Aut}(G')$ le sont aussi.

Exercice 25. Soient G un groupe commutatif de cardinal n et k un entier premier avec n. Montrer que l'application $x \mapsto x^k$ est un automorphisme de G.

Exercice 26. (Automorphismes de $\mathbb{Z}/n\mathbb{Z}$) Soit $n \in \mathbb{N} \setminus \{0\}$. Décrire l'ensemble $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, et en déduire que $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$ est isomorphe à $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$.

Groupe symétrique

★ **Exercice 27.** Soient $n \in \mathbb{N} \setminus \{0\}$ et $p \in [\![1, n]\!]$. Donner le nombre de p-cycles dans S_n.

★ **Exercice 28.** Soient k et n deux entiers naturels non nuls. Montrer que si σ est un n-cycle de S_n, alors σ^k est un produit de $d = \mathrm{pgcd}(k, n)$ cycles de longueur $\frac{n}{d}$.

Exercice 29. Soit n un entier congru à 2 modulo 3. Montrer que l'application $\bar{x} \mapsto \overline{3x}$ est une permutation de $\mathbb{Z}/n\mathbb{Z}$ et donner sa signature.

☢ **Exercice 30.** Soit $n \in \mathbb{N} \setminus \{0,1\}$. Montrer que $A_n = \ker(\varepsilon)$ est l'unique sous-groupe de S_n de cardinal $\dfrac{n!}{2}$.

Exercice 31. (Commutant d'un p-cycle) Soient $n \in \mathbb{N} \setminus \{0\}$ et $p \in [\![1, n]\!]$. Soit σ un p-cycle de S_n. Montrer que l'ensemble : $C(\sigma) = \{\tau \in S_n \mid \sigma\tau = \tau\sigma\}$, appelé le *commutant* de σ, est un groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times S_{n-p}$.

★ **Exercice 32. (Parties génératrices de S_n)** Soit $n \in \mathbb{N} \setminus \{0,1\}$.

1. Montrer que $\{(i\ i+1) \mid i \in [\![1, n-1]\!]\}$ engendre S_n.
2. Montrer que $\{(1\ 2), (1\ 2\ \cdots\ n)\}$ engendre S_n.
3. ☢ On suppose que n est un nombre premier. Montrer que pour toute transposition τ et tout n-cycle σ, l'ensemble $\{\tau, \sigma\}$ engendre S_n.

★ **Exercice 33. (Groupe dérivé de S_n)** Soit $n \in \mathbb{N} \setminus \{0\}$. On appelle *groupe dérivé* de S_n le sous-groupe de S_n engendré par : $\{\sigma\tau\sigma^{-1}\tau^{-1} \mid (\sigma,\tau) \in S_n^2\}$. Il est noté $D(S_n)$.

1. Montrer : $D(S_n) \subseteq A_n$, où A_n est le noyau du morphisme de signature $\varepsilon : S_n \to \{-1,1\}$.
2. Supposons dans cette question : $n \geqslant 3$. Écrire tout 3-cycle sous la forme $\sigma\tau\sigma^{-1}\tau^{-1}$ avec $(\sigma,\tau) \in S_n^2$.
3. En déduire : $D(S_n) = A_n$.
4. Montrer que si $f : S_n \to \mathbb{C}^*$ est un morphisme de groupes, alors il est constant égal à 1 ou égal au morphisme de signature.

Exercice 34. Soit $n \in \mathbb{N} \setminus \{0\}$. Soit A_n le noyau du morphisme de signature $\varepsilon : S_n \to \{-1,1\}$. Montrer qu'il existe un morphisme injectif de S_n dans A_{n+2}.

Exercice 35. Soit $\mathrm{Aut}(S_3)$ l'ensemble des automorphismes de S_3. Montrer que $\mathrm{Aut}(S_3)$ est isomorphe à S_3.

Initiation aux actions de groupe (sans le dire)

On remarquera que le point commun entre toutes les exercices de cette partie réside dans la construction d'un morphisme de groupes $G \to S_X$ noté $g \mapsto \varphi_g$, avec X un ensemble (G agit sur X), puis dans l'étude d'ensembles de la forme $\{g \in G \mid \varphi_g(x) = x\}$ (stabilisateur de x sous l'action de G) ou $\{\varphi_g(x) \mid g \in H\}$ (orbite de x sous l'action de H).

Exercice 36. (Théorème de Cayley) Soit G un groupe. Pour tout $g \in G$, on note φ_g l'application $x \mapsto gx$ définie de G dans lui-même. Montrer que l'application $g \mapsto \varphi_g$ définit un morphisme injectif de G dans S_G.

Exercice 37. (Les actions de groupe donnent des générateurs) Soit $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. On pose : $\forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, $\forall z \in \mathcal{H}$, $\varphi_M(z) = \dfrac{az+b}{cz+d}$ (on rappelle que $\mathrm{SL}_2(\mathbb{R})$ est le noyau de $\det : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^*$).

1. Montrer que l'application $M \mapsto \varphi_M$ est un morphisme de groupes de $\mathrm{SL}_2(\mathbb{R})$ dans $S_{\mathcal{H}}$.
2. Montrer : $\{M \in \mathrm{SL}_2(\mathbb{R}) \mid \varphi_M(i) = i\} = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$. On note $\mathrm{O}_2(\mathbb{R})$ cet ensemble.
3. On note $\mathrm{T}_2(\mathbb{R})$ le sous-groupe des matrices triangulaires supérieures. Décrire : $\{\varphi_T(i) \mid T \in \mathrm{T}_2(\mathbb{R})\}$.
4. En déduire la *décomposition d'Iwasawa* : $\forall M \in \mathrm{SL}_2(\mathbb{R})$, $\exists (T,O) \in \mathrm{T}_2(\mathbb{R}) \times \mathrm{O}_2(\mathbb{R})$, $M = TO$.


1917-1998

Exercice 38. (Les actions de groupe permettent le dénombrement) Soit $E = [\![1,n]\!]$. Soit $k \in [\![0,n]\!]$. Notons $\mathcal{P}_k(E) \subseteq \mathcal{P}(E)$ l'ensemble de ses parties à k éléments. Nous voulons redémontrer : $\mathrm{card}(\mathcal{P}_k(E)) = \dfrac{n!}{(n-k)!k!}$.

1. Décrire les ensembles $G = \{\sigma \in S_n \mid \sigma([\![1,k]\!]) = [\![1,k]\!]\}$ et $O = \{\sigma([\![1,k]\!]) \mid \sigma \in S_n\} \subseteq \mathcal{P}(E)$.
2. Donner une relation entre les cardinaux de G et O.
3. Montrer l'existence d'une bijection entre G et $S_k \times S_{n-k}$, et conclure.

On pourra s'inspirer de cet exercice pour trouver une nouvelle méthode de calcul de A_n^k.

Exercice 39. (Le centre d'un p-groupe est non trivial) Soient G un groupe de cardinal p^k avec p un nombre premier et k un entier naturel non nul. On note $Z(G) = \{x \in G \mid \forall y \in G,\ xy = yx\}$ le centre de G, et pour tout $x \in G$, on note : $O(x) = \left\{y \in G \mid \exists g \in G,\ y = gxg^{-1}\right\}$.

1. Montrer que la relation binaire définie par : $\forall (x,y) \in G^2$, $x \sim y \iff y \in O(x)$, est une relation d'équivalence.
2. Montrer que le cardinal de $O(x)$ divise le cardinal de G pour tout $x \in G$.
3. Montrer : $\mathrm{card}(G) \equiv \mathrm{card}(Z(G)) \bmod p$, et en déduire que le centre de G n'est pas réduit à l'élément neutre.
4. Supposons $k = 2$. Montrer que s'il existe $x \in G \setminus Z(G)$, alors $S_x = \{y \in G \mid xy = yx\}$ est un ensemble de cardinal supérieur ou égal à $p+1$, et en déduire une contradiction.

On a démontré qu'un groupe de cardinal p^2 est nécessairement commutatif. Ceci complète l'étude de l'exercice 10.

Exercice 40. (Lemme de Cauchy) L'objectif de cet exercice est de montrer que si n est un entier naturel non nul, et si p est un diviseur premier de n, alors tout groupe G de cardinal n admet au moins un élément d'ordre p. On pose : $X = \{(g_1,\dots,g_p) \in G^p \mid g_1 \cdots g_p = 1_G\}$.

1. Donner le cardinal de X.
2. Soit $\sigma = (1\ 2\ \cdots\ p) \in S_p$. Montrer qu'en posant : $\forall \gamma \in \langle\sigma\rangle$, $\forall (g_0,\dots,g_{p-1}) \in X$, $\varphi_\gamma((g_1,\dots,g_p)) = (g_{\gamma(1)},\dots,g_{\gamma(p)})$, on définit un morphisme $\gamma \mapsto \varphi_\gamma$ de $\langle\sigma\rangle$ dans S_X.
3. Montrer que si $x \in X$, alors le cardinal de $O(x) = \{\varphi_\gamma(x) \mid \gamma \in \langle\sigma\rangle\}$ est égal à 1 ou p.
4. On pose : $F = \{x \in X \mid \forall \gamma \in \langle\sigma\rangle,\ \varphi_\gamma(x) = x\}$. Décrire les éléments de F.
5. En écrivant X comme réunion disjointe faisant intervenir des ensembles de la forme $O(x)$, montrer : $\mathrm{card}(X) \equiv \mathrm{card}(F) \bmod p$. Conclure.

Anneaux et corps

✓ **Exercice 41.** Soient A et B deux anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux.

1. Pour tout idéal J de B, montrer que $f^{-1}(J)$ est un idéal de A.
2. On suppose f surjectif. Montrer que pour tout I idéal de A, l'ensemble $f(I)$ est un idéal de B. Proposer un contre-exemple si f n'est pas surjectif.

★ **Exercice 42.** Soit A un anneau commutatif.

1. Montrer que A est un corps si et seulement si ses seuls idéaux sont $\{0_A\}$ et A.
2. On suppose que A est intègre et admet un nombre fini d'idéaux. Montrer que A est un corps.
3. Déduire de cet exercice qu'un morphisme de corps est toujours injectif.

Exercice 43. Soient A un anneau commutatif et I un idéal de A. On pose : $\sqrt{I} = \left\{x \in A \mid \exists k \in \mathbb{N} \setminus \{0\},\ x^k \in I\right\}$.

1. Montrer que $\sqrt{I}$ est un idéal de A et que : $\sqrt{\sqrt{I}} = \sqrt{I}$.
2. Si I et J sont deux idéaux de A, montrer : $\sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$, et : $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

✓ **Exercice 44.** Soit $A = \mathrm{C}^0([0,1], \mathbb{R})$. Pour tout $x \in [0,1]$, on pose : $I_x = \{f \in A \mid f(x) = 0\}$. Montrer que pour tout $x \in [0,1]$, l'ensemble I_x est un idéal de A. Est-il principal ?

★ **Exercice 45. (Diviseurs de zéro et éléments nilpotents dans $\mathbb{Z}/n\mathbb{Z}$)** Soit $n \in \mathbb{N} \setminus \{0\}$.

1. Déterminer le nombre d'éléments $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ tels que : $\exists y \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\},\ \bar{x}\bar{y} = \bar{0}$.
2. Déterminer le nombre d'éléments $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ tels que : $\exists k \in \mathbb{N} \setminus \{0\},\ \bar{x}^k = \bar{0}$.

★ **Exercice 46.** Soit A un anneau. On rappelle qu'un élément $x \in A$ est *nilpotent* s'il existe $n \in \mathbb{N} \setminus \{0\}$ tel que : $x^n = 0_A$.

1. Montrer que si A est intègre, alors 0_A est l'unique élément nilpotent de A.
2. Soit $(a, b) \in A^2$ tel que : $ab = ba$, avec a et b nilpotents. Montrer que $a + b$ et ab sont nilpotents.
3. Pour tout $u \in A$ inversible et tout $v \in A$ nilpotent qui commute avec u, montrer que $u + v$ est inversible.

Exercice 47. Soit A un anneau tel que : $\forall x \in A,\ x^3 = x$.

1. Déterminer les éléments nilpotents de A.
2. Soit $b \in A$ tel que : $b^2 = b$. Montrer que b et a commutent pour tout $a \in A$. *Considérer* $b(1-b)a$.
3. En déduire que les éléments de la forme a^2, avec $a \in A$, commutent avec tous les éléments de A.
4. Montrer que A est commutatif.

Exercice 48. Soit A un anneau commutatif. Déterminer $A[X]^\times$.


1882-1935

Exercice 49. (Anneaux noethériens) Soit A un anneau commutatif, dont on note $\mathcal{I}$ l'ensemble des idéaux. Montrer que les propositions suivantes sont équivalentes :

(i) Pour tout idéal I de A, il existe $k \in \mathbb{N} \setminus \{0\}$ et $(a_i)_{1 \leqslant i \leqslant k} \in A^k$ tel que : $I = \sum_{i=1}^{k} a_i A$.

(ii) Toute suite croissante d'idéaux de A (au sens de l'inclusion) est stationnaire.

(iii) Toute partie non vide de $\mathcal{I}$ admet un élément maximal (au sens de l'inclusion).

★ **Exercice 50. (Caractéristique d'un anneau)** Soient A un anneau et $f_A : \mathbb{Z} \to A$ l'application $k \mapsto k \cdot 1_A$.

1. Montrer qu'il existe $n \in \mathbb{N}$ tel que : $\ker(f_A) = n\mathbb{Z}$. L'entier n est appelé *caractéristique* de l'anneau A.
2. Montrer que si $n = 0$, alors A contient un sous-anneau isomorphe à $\mathbb{Z}$, tandis que si $n \geqslant 2$, alors A contient un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
3. Soit B un autre anneau tel que : $A \subseteq B$. Montrer que A et B ont même caractéristique.
4. Montrer que si A est intègre, alors sa caractéristique est nulle ou est un nombre premier.
5. Montrer que si A est un corps de caractéristique nulle, alors il contient un sous-corps isomorphe à $\mathbb{Q}$.

En résumé, si A est un corps, alors il contient un sous-corps isomorphe à $\mathbb{Q}$ ou $\mathbb{Z}/p\mathbb{Z}$ avec $p > 0$ la caractéristique : on l'appelle *sous-corps premier* de A.

Exercice 51. (Un morphisme de corps est linéaire) On utilisera librement les résultats de l'exercice 50. Montrer que si K est un corps et $k \subseteq K$ son sous-corps premier (c'est-à-dire $k = \mathbb{Q}$ si K est de caractéristique nulle, et $k = \mathbb{Z}/p\mathbb{Z}$ si K est de caractéristique $p > 0$), alors tout morphisme de corps $f : K \to K$ est aussi une application k-linéaire.

✓ **Exercice 52. (Propriétés invariantes par isomorphisme)** Soit $f : K \to L$ un isomorphisme de corps.

1. Montrer que K est commutatif si et seulement si L est commutatif.
2. Montrer que si $x, y \in K^*$, alors x est l'inverse de y si et seulement si $f(x)$ est l'inverse de $f(y)$.
3. Montrer que les *groupes* $(K, +)$ et $(L, +)$ sont isomorphes, ainsi que les groupes $(K^*, \times)$ et $(L^*, \times)$.
4. Montrer que $g : K \to K$ est un automorphisme de corps si et seulement si $f \circ g \circ f^{-1} : L \to L$ est un automorphisme de corps, et en déduire que les groupes $\mathrm{Aut}(K)$ et $\mathrm{Aut}(L)$ sont isomorphes.
5. Montrer que K et L ont même caractéristique (voir exercice 50).
6. Soit $P = \sum_{i=0}^{n} a_i X^i \in K[X]$. On *définit* $f(P)$ par : $f(P) = \sum_{i=0}^{n} f(a_i) X^i \in L[X]$. Soit $x \in K$. Montrer que x est une racine de P si et seulement si $f(x)$ est une racine de $f(P)$.
7. Montrer que P et $f(P)$ ont le même nombre de racines, avec des ordres de multiplicité correspondants (c'est-à-dire : $x \in K$ est une racine de P d'ordre de multiplicité k si et seulement si $f(x) \in L$ est une racine de $f(P)$ d'ordre de multiplicité k).

★ **Exercice 53.**

1. Déterminer les automorphismes de corps de $\mathbb{R}$.
2. Déterminer les automorphismes de corps de $\mathbb{C}$ dont la restriction à $\mathbb{R}$ est l'identité.

Exercice 54. Soient K un corps fini et $f : \mathbb{Z} \to K$ l'application $k \mapsto k \cdot 1_K$.

1. Montrer qu'il existe un nombre premier p tel que : $\ker(f) = p\mathbb{Z}$.
2. Montrer que la loi de composition externe $\mathbb{Z}/p\mathbb{Z} \times K \to K$ donnée par $(\bar{k}, x) \mapsto f(k)x$ est correctement définie, et donne à K une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.
3. Montrer qu'il existe $d \in \mathbb{N} \setminus \{0\}$ tel que : $\mathrm{card}(K) = p^d$.

On en déduit par exemple qu'il n'existe pas de corps de cardinal 6.

Exercice 55. (Quelques exemples de corps finis)

1. Vérifier que $\mathbb{Z}/3\mathbb{Z}$ est un corps.
2. On pose : $K = \mathrm{Vect}_{\mathbb{Z}/3\mathbb{Z}} \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & -\bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right\}$. Montrer que K est un corps, dont on donnera le cardinal.
3. On munit $K = (\mathbb{Z}/2\mathbb{Z})^2$ des lois $+$ et $\times$ définies ainsi : $\forall (\bar{a}, \bar{b}, \bar{c}, \bar{d}) \in (\mathbb{Z}/2\mathbb{Z})^4$, $(\bar{a}, \bar{b}) + (\bar{c}, \bar{d}) = (\bar{a} + \bar{c}, \bar{b} + \bar{d})$, et : $(\bar{a}, \bar{b}) \times (\bar{c}, \bar{d}) = (\overline{ad} + \overline{bc} + \overline{ac}, \overline{bd} + \overline{ac})$. Montrer que K est un corps.
   Ce corps est construit de manière complètement artificielle. La construction la plus naturelle des corps finis est par adjonction de racines via *un anneau-quotient, comme pour* $\mathbb{C}$. *Ici :* $K = \mathbb{Z}/2\mathbb{Z}[X]/(X^2 + X + 1)\mathbb{Z}/2\mathbb{Z}[X]$.
4. Montrer que tout corps fini à quatre éléments est isomorphe au *corps* $(\mathbb{Z}/2\mathbb{Z})^2$ muni des deux lois définies dans la question précédente.

Exercice 56. Soit K un corps fini. Montrer : $\sum_{x \in K^*} x = 0$ (sauf si $K = \mathbb{Z}/2\mathbb{Z}$), et : $\prod_{x \in K^*} x = -1$ (ce dernier produit généralise le théorème de Wilson, qui correspond à $K = \mathbb{Z}/p\mathbb{Z}$).

Exercice 57. Soit K un corps fini à q éléments, et soit m un entier. Montrer que si $q - 1$ ne divise pas m, alors : $\sum_{x \in K^*} x^m = 0$, tandis que si $q - 1$ divise m, alors : $\sum_{x \in K^*} x^m = q - 1$.