Exercices du chapitre III (Structures algébriques) – Indications

L'icône « (🗎) » indique que les documents *Méthodes* donnent des conseils plus généraux.

L'indication « **(G/H)** », dans les indications ou commentaires d'un exercice, indique des approfondissements sur la structure d'ensemble quotient, hors programme mais susceptibles d'intéresser le féru d'algèbre.

Groupes

Exercice 1. (🗎) Utiliser le théorème de Lagrange pour montrer que ces sous-groupes sont inclus dans des sous-groupes ✓ de racines de l'unité, et conclure par égalité des cardinaux.

> **Commentaires.** On remarquera que dans un groupe fini, tous les éléments sont des « racines de l'unité » (du moins si le neutre est noté 1_G). Phénomène à peine remarqué dans le cas général, cela rend triviale la détermination des sous-groupes finis des groupes $\mathbb{C}^*$ et $\mathbb{R}^*$ dont vous connaissez les racines de l'unité depuis longtemps.
> Remarquons que dans $\mathbb{C}^*$, il y a exactement n racines n^{es} de l'unité : ce n'est évidemment pas le cas dans $\mathbb{R}^*$, et on peut avoir strictement plus que n racines de l'unité dans d'autres situations : chercher des contre-exemples dans $\mathrm{GL}_n(K)$, S_n (où l'élément neutre est Id), etc. Le fait d'être dans un corps est central : $X^n - 1$ ne peut pas avoir plus de n racines. Ce lien entre des éléments et racines d'un polynôme revient dans l'exercice 13 puis à plusieurs reprises dans le chapitre IV.
> Le résultat de cet exercice se généralise : tout sous-groupe fini de K^*, lorsque K est un corps, est cyclique (c'est en particulier le cas pour K^* lui-même si K est fini). voir l'exercice 13. Nous exploiterons cette observation avec $\mathbb{Z}/p\mathbb{Z}$ dans le chapitre IV.

★ **Exercice 2.** (🗎)

1. Montrer que l'ordre de ab (noté d ici) divise mn. Ensuite, montrer que les ordres de a et b divisent d, et conclure grâce à l'hypothèse sur m et n.
2. Trouver un élément d'ordre mn en dénichant un élément d'ordre m, un autre d'ordre n, et en les additionnant (la loi est additive, attention).
3. Choisir intelligemment a et b de même ordre et dont le produit se simplifie trivialement.
4. Prendre un élément d'ordre 3 et un autre d'ordre 2 dans S_3.

> **Commentaires.** Comme l'ordre est défini comme le plus petit élément d'un certain ensemble (au sens de la relation de divisibilité), les égalités sur l'ordre s'obtiennent souvent par double divisibilité. Observation faite fréquemment (avec des bornes supérieures, des normes infinies, et plus tard avec les pgcds, ppcms, intérieurs et adhérences de parties, etc.).
> Lorsque deux nombres sont premiers, ou premiers entre eux, cela permet de raisonner « facteur par facteur » pour obtenir des relations de divisibilité : on montre que ab divise c en montrant que a et b divisent c. C'est parfois plus commode, selon les hypothèses sur les quantités.
> Lorsqu'il apparaît un pgcd dans un contexte non arithmétique (il apparaît ici implicitement, puisque des éléments sont premiers entre eux), une relation de Bézout permet souvent de l'exploiter dans des identités algébriques, même si ce n'est pas crucial ici.

Exercice 3.

1. Utiliser le fait que $\mathbb{N}$ admette un bon ordre.
2. Comme x est aussi dans G, il est une puissance de a. Effectuer la division euclidienne de l'exposant par k, et utiliser la minimalité de k pour simplifier le reste.

> **Commentaires.** Noter que lorsqu'on veut montrer qu'un certain élément est multiple d'un autre, c'est la division euclidienne qui s'impose : elle permet en effet de mesurer l'écart de n'importe quel entier aux multiples d'un autre.

★ **Exercice 4. (Exposant d'un groupe)**

1. Utiliser le résultat de la première question de l'exercice 2, mais pas avec a et b (puisque leurs ordres ne sont pas supposés premiers entre eux) : plutôt avec des puissances bien choisies de a et b, dont les ordres sont premiers entre eux et dont le produit est le ppcm demandé. Se souvenir que le ppcm de deux entiers s'écrit explicitement à l'aide des valuations p-adiques de ces deux entiers.
2. Appliquer la question précédente avec $g \in G$ et un élément d'ordre maximal (il en existe).

> **Commentaires.** Il est très utile de remarquer que si l'on connaît l'ordre de x, alors on connaît l'ordre de x^k pour tout k (attention, cela dépend selon que k divise l'ordre de x ou non). Cela permet à moindre frais de fabriquer des éléments « de l'ordre qu'on veut », tant que c'est un diviseur de l'ordre d'un élément connu.

Exercice 5. (🗎) Utiliser le théorème d'isomorphisme avec un morphisme bien choisi à valeurs dans G et surjectif, dont le cardinal du groupe de départ dépend des ordres d'éléments de G (d'abord se demander comment écrire explicitement tout élément de G d'une manière aussi simple que possible, et dont la quantification fait intervenir

des ordres d'éléments ; utiliser cette description explicite pour fabriquer le morphisme). Ce théorème d'isomorphisme permet d'en déduire que $\mathrm{card}(G)$ divise les ordres d'éléments de G. On en déduit (comment ?) que p divise l'ordre d'un des éléments de G. En considérant $x \in G$ l'élément en question, r son ordre, et en posant $r = pm$ avec m entier, construire un élément d'ordre exactement p.

Commentaires. Il est très utile de remarquer que si l'on connaît l'ordre de x, alors on connaît l'ordre de x^k pour tout k (attention, cela dépend selon que k divise l'ordre de x ou non). Cela permet à moindre frais de fabriquer des éléments « de l'ordre qu'on veut », tant que c'est un diviseur de l'ordre d'un élément connu.
Pour donner plus de hauteur à cette idée : en fait, il n'est pas difficile de constater que tout groupe commutatif $(G, +)$ serait un « $\mathbb{Z}$-espace vectoriel » si cela avait un sens, c'est-à-dire si $\mathbb{Z}$ était un corps : on a déjà la stabilité par combinaison linéaire (entière), la distributivité, l'associativité, etc. La multiplication externe par un entier est définie classiquement : $k \cdot g = g + \cdots + g$ (k fois) si $k \geqslant 0$, et $k \cdot g = (-g) + \cdots + (-g)$ ($-k$ fois) sinon. Je l'écris ici additivement pour renforcer l'analogie avec les espaces vectoriels, mais cela vaut aussi en notation multiplicative (même si vous le remarquez moins naturellement).
Même sans structure d'espace vectoriel, ce raisonnement par analogie peut être fructueux : de la même manière qu'une famille libre (resp. une famille génératrice, une base) d'un espace vectoriel E équivaut à la donnée d'un morphisme injectif (resp. surjectif, bijectif) $K^n \to E$, une partie génératrice d'un groupe commutatif G permet d'écrire un morphisme surjectif $\mathbb{Z}^n \to G$. Si la partie génératrice est bien choisie, ce morphisme induit un isomorphisme par le théorème de factorisation : $\prod_i \mathbb{Z}/d_i\mathbb{Z} \to G$, où les d_i sont les ordres des éléments des générateurs. C'est l'idée exploitée dans cet exercice.
Ce constat vaut aussi pour les anneaux commutatifs et les corps. Pour les corps, ce sont même des « vrais » espaces vectoriels sur leur sous-corps premier : voir l'exercice 50 pour une application de cette idée.
En fait, dans la littérature, on parle de $\mathbb{Z}$-module, ou plus généralement de A-module, lorsque les axiomes définissant un espace vectoriel sont vérifiés sur un anneau A qui n'est pas un corps. Tout groupe commutatif est un $\mathbb{Z}$-module, et réciproquement.

Exercice 6. (📄) Utiliser le théorème de Lagrange pour écrire $a = a^\bigstar$ avec $\bigstar$ pair.

Commentaires. Le théorème de Lagrange est le lien le plus direct entre une hypothèse sur le cardinal du groupe et une conclusion sur la puissance d'un élément.
On se demandera pourquoi je ne propose pas de montrer que $x \mapsto x^2$ est un automorphisme en montrant que $\ker(f)$ est trivial : cela semble pourtant très efficace.

✓ **Exercice 7.** (📄) Exprimer $(xy)^\ell$ en fonction d'une puissance de yx pour tout ℓ, et inversement, à l'aide de l'associativité du produit.

Commentaires. Comme l'ordre est défini comme le plus petit élément d'un certain ensemble (au sens de la relation de divisibilité), les égalités sur l'ordre s'obtiennent souvent par double divisibilité. Observation faite fréquemment (avec des bornes supérieures, des normes infinies, et plus tard avec les pgcds, ppcms, intérieurs et adhérences de parties, etc.).

Exercice 8. (📄)

1. Montrer que si les deux inclusions sont fausses, alors $H_1 \cup H_2$ n'est pas stable par produit : prendre deux éléments adéquats de H_1 et H_2.
2. Utiliser le théorème de Lagrange.

Commentaires. Le théorème de Lagrange donne des informations très contraignantes sur le cardinal d'un sous-groupe : ce doit être le PREMIER RÉFLEXE lorsqu'on n'est pas en mesure d'expliciter le sous-groupe aisément.

Exercice 9. Introduire une application surjective naturelle de $H \times K$ dans HK et montrer que chaque élément de son image a $\mathrm{card}(H \cap K)$ antécédents. Vous aurez besoin d'identifier à quelle condition l'égalité $hk = h'k'$ avec $(h, h', k, k') \in H^2 \times K^2$ est possible.

Commentaires. Grâce au principe des bergers (ou à l'application $\tilde{f} : E/R \to F$ induite par $f : E \to F$, où R est la relation d'équivalence mesurant le défaut d'injectivité de f), on voit qu'il n'est pas nécessaire d'avoir une bijection dans les questions de dénombrement, bien que ce soit ce qu'on pense en premier lieu : une surjection f dont les fibres $f^{-1}(\{y\})$ sont de cardinal constant suffit. Et c'est parfois plus naturel à construire.

Exercice 10. (Groupes commutatifs de cardinal p^2, avec p premier) (📄) S'il existe un élément d'ordre p^2 alors l'exercice est terminé. Sinon : remarquer que l'ordre d'un élément est soit 1, soit p. Montrer que si on choisit arbitrairement un élément d'ordre x, puis y un élément « indépendant » de x en un sens que je vous laisse comprendre, alors x et y engendrent G. Cela vous permettra de construire aisément une application surjective de $(\mathbb{Z}/p\mathbb{Z})^2$ dans G. Conclure par cardinalité.

Commentaires. On le sait grâce au théorème de Lagrange et on l'illustre encore ici : le cardinal d'un groupe conditionne BEAUCOUP sa structure. On a vu dans le cours qu'il n'y a qu'un seul groupe de cardinal premier à isomorphisme près (c'est $\mathbb{Z}/p\mathbb{Z}$), et cet exercice (conjointement à l'exercice 39) montre qu'il n'y en a que deux de cardinal p^2. Et ils sont très simples ! En maîtrisant $(\mathbb{Z}/p\mathbb{Z})^2$ et $\mathbb{Z}/p^2\mathbb{Z}$, vous maîtrisez tous les groupes de cardinal 4, 9, 25, etc. Avoir cette classification en tête est très utile.

Exercice 11. (📄) Si d_1 et d_2 sont les deux ordres en jeu : montrer que d_1 divise d_2 et inversement en calculant le produit des deux éléments de l'énoncé par d_1 et d_2 respectivement. Ne pas oublier que par définition, n et k divisent leur pgcd. À noter qu'il est aussi possible d'écrire explicitement l'un en fonction de l'autre grâce à un important théorème d'arithmétique.

Commentaires. Lorsqu'il apparaît un pgcd dans un contexte non arithmétique, une relation de Bézout permet souvent de l'exploiter dans des identités algébriques (même si ce n'est pas la seule façon de faire ici, mais elle est très naturelle parce qu'elle permet justement de relier les deux quantités en présence : k et son pgcd avec n).
Comme l'ordre est défini comme le plus petit élément d'un certain ensemble (au sens de la relation de divisibilité), les égalités sur l'ordre s'obtiennent souvent par double divisibilité. Observation faite fréquemment (avec des bornes supérieures, des normes infinies, et plus tard avec les pgcds, ppcms, intérieurs et adhérences de parties, etc.).

★ **Exercice 12.** Plusieurs approches sont possibles. Dans le contexte de ce chapitre : remarquer qu'il s'agit d'une égalité entre cardinaux. Grâce au cours, vous savez en effet que $\varphi(d)$ est le cardinal d'un certain ensemble ; est-ce que la somme du membre de droite ne pourrait pas s'interpréter comme le cardinal d'une réunion disjointe de tels ensembles ?

Lorsque vous saurez que φ est multiplicative : vous pourrez raisonner par récurrence sur n par exemple, pour démontrer autrement cette identité (mais vous en perdez la compréhension conceptuelle).

Commentaires. En attendant d'avoir des formules explicites au chapitre IV, on pourra s'amuser à calculer $\varphi(n)$, où n a « peu de diviseurs », par récurrence *via* cette identité.
Cette égalité peut s'interpréter avec le produit de convolution introduit dans l'exercice 37 du chapitre II et que l'on revoit implicitement au chapitre IV, dans les exercices 59 à 64.
Cette identité permet de démontrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique (et plus généralement tout sous-groupe fini du groupe multiplicatif d'un corps) : voir l'exercice 34 du chapitre IV. Elle apparaît aussi dans l'exercice 64 de ce même chapitre pour montrer qu'un nombre entier n a « en moyenne » $\frac{3n}{\pi^2} \approx 0{,}304n$ entiers inférieurs qui lui sont premiers. Bref, un résultat loin d'être artificiel !

Exercice 13. Il s'agit de démontrer qu'il existe un élément d'ordre n, où n est le cardinal de G. Utiliser l'exercice 4 pour montrer que si d est l'exposant du groupe, alors $X^d - 1$ admet n racines. Conclure grâce à un argument de degré.

Commentaires. La théorie des groupes dans K^* (où K est un corps) devient très riche du fait que l'ordre d'un élément a deux significations : il y a l'interprétation évidente en termes de groupes (par définition), mais aussi en termes de racines. En effet, $x^d = 1$ si et seulement $X^d - 1$ admet x pour racine.
En jouant sur ces deux interprétations de l'ordre, ainsi que sur le théorème de Lagrange, on peut obtenir de nombreux jolis résultats, ou caractériser très simplement un ensemble comme étant l'ensemble des racines d'un polynôme bien choisi. Cette stratégie reviendra au chapitre d'arithmétique, lorsq'on verra de $\mathbb{Z}/p\mathbb{Z}$ est un corps si p est premier.

Exercice 14.

1. Comparer une propriété évidente qui devrait être conservée par une bijection.
2. Si deux groupes sont isomorphes, ils ont autant d'éléments d'ordre divisant 2. Montrer que ce n'est pas le cas ici, par une détermination *explicite* de ces éléments dans $(K, +)$ et $(K^*, \times)$. Attention, $x^2 = 1$ n'a pas toujours deux solutions (songez à $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z}(X)$), et vous aurez à faire une distinction de cas.

Commentaires. On se souvient qu'un isomorphisme doit conserver tout ce qui est relatif à la structure, et c'est ainsi qu'il *faut* le comprendre pour avoir du recul : commutativité, intégrité (en cas d'anneaux), ordre des éléments, etc. Une fois qu'on a testé les propriétés les plus facilement vérifiables (en vue de démontrer que deux structures ne sont pas isomorphes), compter le nombre d'éléments d'ordre 2, 3, etc., est souvent le plus accessible.

★ **Exercice 15.** (📄)

1. L'hypothèse de l'énoncé signifie que tout élément est son propre inverse. Exploiter le fait que l'inverse d'un produit soit le produit des inverses en sens contraire.
2. Analyse : s'il y a un tel isomorphisme de $(\mathbb{Z}/2\mathbb{Z})^s$ dans G, alors G devrait admettre une partie génératrice à s éléments (par analogie avec les isomorphismes de K^n dans E en algèbre linéaire, qui transforment bases en bases, familles génératrices en familles génératrices, etc.). Synthèse : introduire une partie génératrice « bien choisie » (elle n'est pas quelconque : que représente s ?), et l'utiliser pour fabriquer un isomorphisme. La surjectivité sera par définition d'une partie génératrice, et l'injectivité vraie à condition qu'elle soit « bien choisie ».

Autre approche plus mûre : utiliser les hypothèses pour montrer que la loi de composition externe $\mathbb{Z}/2\mathbb{Z}\times G\to G$ définie par $(\bar{k},g)\mapsto g^k$ est bien définie et munit G d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. À l'aide d'une base, on construit alors un isomorphisme $(\mathbb{Z}/2\mathbb{Z})^s\to G$ où $s=\dim_{\mathbb{Z}/2\mathbb{Z}}(G)$.

Commentaires. Pour donner plus de hauteur à cette idée : en fait, il n'est pas difficile de constater que tout groupe commutatif $(G,+)$ serait un « $\mathbb{Z}$-espace vectoriel » si cela avait un sens, c'est-à-dire si $\mathbb{Z}$ était un corps : on a déjà la stabilité par combinaison linéaire (entière), la distributivité, l'associativité, etc. La multiplication externe par un entier est définie classiquement : $k\cdot g=g+\cdots+g$ (k fois) si $k\geqslant 0$, et $k\cdot g=(-g)+\cdots+(-g)$ ($-k$ fois) sinon. Je l'écris ici additivement pour renforcer l'analogie avec les espaces vectoriels, mais cela vaut aussi en notation multiplicative (même si vous le remarquez moins naturellement).
Pour pouvoir obtenir un *vrai* espace vectoriel (en vue de faire des raisonnements dimensionnels, sur l'indépendance linéaire, etc.), il faut que l'ensemble des scalaires soit un corps, c'est-à-dire : il faut pouvoir remplacer $\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$ (avec p premier) dans la définition de la multiplication externe. On vérifie que ceci n'est correctement défini que si : $\forall g\in G,\ p\cdot g=0_G$, c'est-à-dire : si tout élément de G est d'ordre divisant p (donc si tout élément non trivial est d'ordre p, puisque p est premier). C'est exactement ce que permet l'hypothèse de l'énoncé.
Cette observation permet directement d'en déduire que n'importe quel groupe commutatif fini $(G,\cdot)$ dans lequel : $\forall g\in G,\ g^p=1_G$, avec p premier, est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^k$ avec k entier naturel.
Même sans structure d'espace vectoriel, néanmoins, le raisonnement par analogie peut être fructueux : de la même manière qu'une famille libre (resp. une famille génératrice, une base) d'un espace vectoriel E équivaut à la donnée d'un morphisme injectif (resp. surjectif, bijectif) $K^n\to E$, une partie génératrice d'un groupe commutatif G permet d'écrire un morphisme surjectif $\mathbb{Z}^n\to G$. Si la partie génératrice est bien choisie, ce morphisme induit un isomorphisme par le théorème de factorisation : $\prod_i\mathbb{Z}/d_i\mathbb{Z}\to G$, où les d_i sont les ordres des éléments des générateurs. C'est une idée exploitée dans l'exercice 5.
Ce constat vaut aussi pour les anneaux commutatifs et les corps. Pour les corps, ce sont même des « vrais » espaces vectoriels sur leur sous-corps premier : voir l'exercice 50 pour une application de cette idée.
En fait, dans la littérature, on parle de $\mathbb{Z}$-module, ou plus généralement de A-module, lorsque les axiomes définissant un espace vectoriel sont vérifiés sur un anneau A qui n'est pas un corps. Tout groupe commutatif est un $\mathbb{Z}$-module, et réciproquement.

✓ **Exercice 16.** (🗎)

1. Utiliser le théorème de Lagrange.
2. Les cardinaux sont les mêmes, donc c'est bijectif si et seulement si c'est injectif ou surjectif. On peut montrer l'injectivité par des raisonnements sur les ordres des éléments et de l'arithmétique élémentaire. Autre possibilité : construire une application réciproque. Cela nécessite d'écrire tout (ω_1,ω_2) sous la forme $\omega_1=z^b$ et $\omega_2=z^a$. Comment « extraire » des racines a^{es} et b^{es} ? Ne pas oublier que les racines de l'unité sont explicites.
   La relation de Bézout peut simplifier certaines considérations.
   On peut aussi s'inspirer de la démonstration du lemme chinois au prochain chapitre : noter la grande ressemblance dans les énoncés.

Commentaires. Lorsqu'il apparaît un pgcd dans un contexte non arithmétique (il apparaît ici implicitement, puisque des éléments sont premiers entre eux), une relation de Bézout permet souvent de l'exploiter dans des identités algébriques.
Le théorème de Lagrange est le lien le plus direct entre une hypothèse sur le cardinal du groupe et une conclusion sur la puissance d'un élément. Cela tombe bien, les éléments de $\mathbb{U}_n$ sont définis par une condition sur leurs puissances.

Exercice 17. (Groupe quasi-cyclique de Prüfer)

1. S'il existe $g\in G$ qui engendre G, il doit également appartenir à l'un des $\mathbb{U}_{p^n}$. Conclure à une impossibilité.
2. Soit H un sous-groupe strict. D'abord montrer que si H admet des éléments d'ordre arbitrairement élevé, alors $H=G$ (pour cela, vous aurez peut-être besoin de remarquer que si $\mathbb{U}_{p^k}\subseteq\mathbb{U}_{p^\ell}$ pour tout $k\leqslant\ell$). Dans le cas contraire : introduire p^k l'ordre maximal d'un élément de H, et montrer $H=\mathbb{U}_{p^k}$. Une inclusion est triviale par définition de p^k et l'autre découle de l'observation entre parenthèses dans la phrase précédente.

Commentaires. Nous avons là un exemple explicite de groupe infini dont tous les sous-groupes stricts sont finis. C'est aussi un contre-exemple à une autre conjecture tentante : il est un groupe *non* monogène dont tous les sous-groupes stricts sont monogènes. Un autre contre-exemple serait le groupe quaternionique $\mathbb{H}_8=\{\pm1,\pm i,\pm j,\pm k\}$.

★ **Exercice 18.** Si $\mathbb{Q}$ admet une partie génératrice finie, on a une égalité du type : $\mathbb{Q}=\sum_i a_i\mathbb{Z}$ avec $a_i\in\mathbb{Q}$. Se ramener à des sous-groupes de $\mathbb{Z}$ pour simplifier le membre de droite et en déduire une égalité absurde.

Commentaires. La description des sous-groupes peut être délicate lorsqu'on étudie un groupe infini (on le verra aussi lorsqu'on étudie les sous-groupes de $\mathbb{R}$). Pour le moment, puisque vous connaissez principalement les sous-groupes de $\mathbb{Z}$ (et ceux de $\mathbb{Z}/n\mathbb{Z}$, mais là je ne parle que des groupes infinis) : essayer de s'y ramener dans la mesure du possible. Ce n'est bien sûr pas toujours possible, mais comme $\mathbb{Q}$ est une extension naturelle de $\mathbb{Z}$ on est en droit d'y penser dans cet exercice.

★ **Exercice 19.** Comme $\mathbb{Z}/a\mathbb{Z}$ est cyclique, un morphisme f est caractérisé par son image d'un générateur, ici $\bar{1}$. Raisonner sur l'ordre de $f(\bar{1})$ (il y a deux façons de le faire, à combiner) pour dénombrer le nombre de possibilités pour $f(\bar{1})$ et donc pour f (penser à vérifier que réciproquement, cela définit bien un morphisme de $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$).

Commentaires. Exemple d'utilisation des parties génératrices pour simplifier une étude. Ici : pour définir un morphisme uniquement par son image d'une partie génératrice (comme vous le faites en algèbre linéaire).
Pour un morphisme $f : G \to H$, l'ordre d'un élément (ou de son image par f) s'étudie à la fois en tenant compte du groupe de départ et d'arrivée. En effet, le cardinal de G influe sur l'ordre de g, qui lui-même influe sur l'ordre de $f(g)$, qui lui-même dépend du cardinal de H : ainsi l'ordre de $f(g)$ dépend à la fois du cardinal de G et de H.
Le théorème d'isomorphisme et l'identité $\mathrm{card}(G) = \mathrm{card}(\ker(f))\mathrm{card}(\mathrm{im}(f))$ abondent en ce sens et montrent aussi que cette observation pourrait être faite pour le noyau de f : il est intimement lié à $\mathrm{card}(\ker(f))$, mais aussi à $\mathrm{card}(\mathrm{im}(f))$ qui est un diviseur de $\mathrm{card}(H)$. Bien prendre en compte le départ et l'arrivée !

Exercice 20. (📄)

1. Comme $\mathbb{Z}$ est monogène, un morphisme est caractérisé par son image d'un générateur, ici 1.
2. En utilisant le fait que $\mathbb{Q}$ soit stable par division par 2, mais pas $\mathbb{Z}$, montrer qu'il n'y a pas beaucoup de tels morphismes.
3. Comme $\mathbb{Z}/n\mathbb{Z}$ est cyclique, un morphisme est caractérisé par son image d'un générateur, ici $\bar{1}$. Raisonner sur l'ordre de $f(\bar{1})$, et penser à vérifier que réciproquement, cela définit bien un morphisme.
4. Même principe. On peut aussi se ramener au cas précédent en songeant que $\mathbb{U}_n$ et $\mathbb{Z}/n\mathbb{Z}$ sont intimement liés.

Commentaires. Exemple d'utilisation des parties génératrices pour simplifier une étude. Ici : pour définir un morphisme uniquement par son image d'une partie génératrice (comme vous le faites en algèbre linéaire).
On a vu en cours diverses propriétés conservées par les isomorphismes, ou préservées au moins partiellement, par les morphismes. La deuxième question en illustre une autre (dont en vérité j'ai déjà parlé informellement en disant que les morphismes préservent les solutions des équations), à savoir : ils préservent les éléments « à division », c'est-à-dire les éléments $g \in G$ tels que pour tout $n \in \mathbb{N} \setminus \{0\}$, il existe $h \in G$ tel que : $g = h^n$ (ou, en notation additive : $g = nh$).
On remarque, dans les deux dernières questions, que les morphismes $G \to C^*$ déterminés (avec $G \in \{\mathbb{Z}/n\mathbb{Z}, \mathbb{U}_n\}$) sont naturellement associés, de manière bijective, à un élément de G. Ce phénomène s'observe pour tous les groupes commutatifs finis G : il y a un isomorphisme entre G entre l'ensemble des morphismes de G dans $\mathbb{C}^*$, appelés *caractères* de G, où ce dernier groupe est muni de la multiplication. Cet isomorphisme est utilisé pour étudier un groupe G *via* de l'analyse de Fourier avec les fonctions $G \to \mathbb{C}^*$, ce qui revient essentiellement au même puisqu'il y a un isomorphisme.
Quand on veut généraliser ce dernier paragraphe au cas non commutatif, on utilise ce qu'on appelle des *représentations* de groupes.

✓ **Exercice 21.** Utiliser une fonction célèbre pour le premier isomorphisme. Pour le second : on peut toujours diviser par 2 dans $\mathbb{Q}$. Par isomorphisme, qu'est-ce que cela impliquerait comme opération toujours licite dans $\mathbb{Q}_+^*$?

Commentaires. On se souvient qu'un isomorphisme doit conserver tout ce qui est relatif à la structure, et c'est ainsi qu'il *faut* le comprendre pour avoir du recul : commutativité, intégrité (en cas d'anneaux), ordre des éléments, etc. Une fois qu'on a testé les propriétés les plus facilement vérifiables (en vue de démontrer que deux structures ne sont pas isomorphes), compter le nombre d'éléments d'ordre 2, 3, etc., est souvent le plus accessible.
On a vu en cours diverses propriétés conservées par les isomorphismes, ou préservées au moins partiellement, par les morphismes. Selon votre façon de raisonner pour résoudre cet exercice, vous avez pu en illustrer une autre (dont j'ai déjà parlé informellement en disant que les morphismes préservent les solutions des équations), à savoir : ils préservent les éléments « à division », c'est-à-dire les éléments $g \in G$ tels que pour tout $n \in \mathbb{N} \setminus \{0\}$, il existe $h \in G$ tel que : $g = h^n$ (ou, en notation additive : $g = nh$).

★ **Exercice 22.** Utiliser le fait que pour tout $h \in G$, l'application $h \mapsto gh$ soit une permutation de G, et faire un changement d'indice dans la somme. Conclure avec h bien choisi (cela dépend aussi d'une certaine hypothèse sur f).

Commentaires. Les permutations des groupes finis impliquent des relations riches vérifiées par les sommes et produits indexés par ces groupes. Ce fut déjà observé dans le cours (démonstration de la version *au programme* du théorème de Lagrange), et c'est d'autant plus riche lorsqu'il y a un morphisme en jeu. Cette idée est aussi mise en application dans le décompte de solutions de l'exercice 52 du chapitre IV.

Exercice 23. Noter que : 1° il y a des inclusions toujours vraies, 2° il y a des relations entre les cardinaux des noyaux et des images.

Commentaires. Remarquer l'analogie avec un exercice classique d'algèbre linéaire. Ce même exercice d'algèbre linéaire dit que les égalités entre images, entre noyaux, équivaut à $E = \ker(f) \oplus \mathrm{im}(f)$. En regardant comment se traite cet exercice classique, on pourra se demander si l'on peut obtenir un résultat analogue à cette décomposition en somme directe, dans le cas des groupes.

✓ **Exercice 24.** Si $f : G \to G'$ est un isomorphisme, et si $\varphi \in \mathrm{Aut}(G)$, se demander comment on peut « naturellement » fabriquer une application de G' dans lui-même à l'aide de f et φ. Vérifier ensuite que c'est un automorphisme. En déduire l'isomorphisme demandé.

Commentaires. On illustre encore une fois en quoi des groupes isomorphes ont tout en commun : leurs groupes d'automorphismes sont aussi « les mêmes ». On pourrait plus généralement montrer qu'il y a une bijection entre les morphismes dont le groupe de départ (resp. d'arrivée) est G et ceux dont le groupe de départ (resp. d'arrivée) est G' : comment ?

Exercice 25. (📄) Montrer que son noyau est trivial par un argument de divisibilité sur les cardinaux.

Commentaires. On a déjà formulé que le théorème de Lagrange est le lien le plus direct entre une hypothèse sur le cardinal du groupe et une conclusion sur la puissance d'un élément. Ici, il est doublement pertinent puisqu'il permet d'avoir des conditions sur le cardinal du noyau ou de l'image du morphisme.
On en déduit notamment que tout élément de G admet une et une seule racine k^{e}. Situation remarquable. On s'évertuera à expliciter la racine k^{e} en question, ce qui revient à expliciter la bijection réciproque.

Exercice 26. (Automorphismes de $\mathbb{Z}/n\mathbb{Z}$) (📄) Un automorphisme f de $\mathbb{Z}/n\mathbb{Z}$ est caractérisé par son image d'un générateur de $\mathbb{Z}/n\mathbb{Z}$. En utilisant le fait qu'un isomorphisme préserve tout ce qui est relatif à la structure, justifier que $f(\bar{1})$ doit être la classe d'un élément premier avec n (dans quel contexte ces éléments apparaissent-ils, lorsqu'on étudie $(\mathbb{Z}/n\mathbb{Z}, +)$?). En déduire l'isomorphisme demandé (bien vérifier l'injectivité et la surjectivité).

Commentaires. Exemple d'utilisation des parties génératrices pour simplifier une étude. Ici : pour définir un morphisme uniquement par son image d'une partie génératrice (comme vous le faites en algèbre linéaire). Comme d'habitude, le fait que les isomorphismes (et donc automorphismes) préservent tout est la meilleure façon de comprendre comment ils sont construits.

Groupe symétrique

★ **Exercice 27.** Dénombrer le nombre de possibilités pour le support du p-cycle, puis sur l'ordre des éléments dans l'écriture du p-cycle. Attention au fait qu'un simple décalage des éléments donne le même p-cycle : éviter les doublons.

Reformulation en termes d'action de groupe du même argument : utiliser le fait que p-cycles soient tous conjugués pour construire une application surjective de S_n dans l'ensemble des p-cycles, et compter le nombre d'antécédents de chaque p-cycle par cette application. Conclure avec le principe des bergers.

Commentaires. On pourra prolonger cet exercice en se demandant combien il y a de permutations dont le nombre et la longueur des cycles, dans la décomposition en cycles à supports disjoints, sont prescrits.

★ **Exercice 28.** Si $\sigma = (a_1 \ \cdots \ a_n)$, se convaincre qu'obtenir la décomposition de σ^k en cycles à supports disjoints revient à déterminer $\left\{\sigma^{k\ell}(a_i) \mid \ell \in \mathbb{N}\right\}$ pour tout i (plus précisément, la longueur du cycle contenant a_i est donnée par le cardinal de cet ensemble et le nombre de cycles est donné par le nombre d'ensembles distincts de cette forme obtenus quand on fait varier i de 1 à n). Or il existe une application surjective naturelle de $\langle\sigma^k\rangle$ dans $\left\{\sigma^{k\ell}(a_i) \mid \ell \in \mathbb{N}\right\}$: utiliser le principe des bergers. Pour avoir le cardinal de $\langle\sigma^k\rangle$, noter que $\langle\sigma^k\rangle = \langle\sigma^d\rangle$ simplifie la description de ses éléments.

Autre approche plus terre-à-terre : avec les notations ci-dessus, exprimer explicitement $\sigma^{k\ell}(a_i)$ pour tous i, k et ℓ, et remarquer que compter les éléments obtenus en prenant l'image par σ^k de a_i (et en réitérant) revient à déterminer le plus petit ℓ non nul tel que $k\ell \equiv 0 \bmod n$: expliciter ℓ en interprétant cela en termes de divisibilité.

Commentaires. La première approche proposée ci-dessus est l'étude déguisée d'une action de groupes : on compte le nombre de classes d'équivalence de la relation $i \sim j \iff \exists \ell \in \mathbb{Z},\ j = \sigma^{k\ell}(i)$, qui correspondent aux orbites de l'action de groupe $\langle\sigma^k\rangle \to S_n$ donnée par $\tau \mapsto (i \mapsto \tau(i))$.
Cette relation entre k et $d = \text{pgcd}(n, k)$ est fréquente en théorie des groupes (on l'a aussi vue dans l'exercice 11). Remarquer plus généralement que si g est d'ordre n, alors g^k est d'ordre $\frac{n}{d}$ (et non $\frac{n}{k}$, qui n'aurait pas de sens si k ne divise pas n), et aussi que $\langle g^k\rangle = \langle g^{n/d}\rangle$, etc. Tout cela pourrait d'ailleurs se déduire de l'étude de $\langle\bar{k}\rangle$ dans $\mathbb{Z}/n\mathbb{Z}$, puisque c'est l'unique groupe cyclique de cardinal n (à isomorphisme près) et que $\langle g\rangle$ en est un.

Exercice 29. Comment expliciterait-on la bijection réciproque si l'on était dans $\mathbb{R}$? S'en inspirer ici. Expliciter la décomposition en cycles à supports disjoints, en remarquant que tous les cycles se ressemblent (c'est pour voir comment ces cycles « bouclent » que l'hypothèse $n \equiv 2 \bmod 3$ intervient). Partant de là, on sait aisément en obtenir la signature.

Commentaires. On pourra se demander plus généralement quelle est la signature de $\bar{x} \mapsto \bar{k}\bar{x}$ dans $\mathbb{Z}/n\mathbb{Z}$, lorsque k et n sont premiers entre eux (pourquoi ?). Les cycles sont construits de façon très régulière.
La question de la signature se pose pour d'autres automorphismes. Dans le cas des isomorphismes sur des $\mathbb{Z}/p\mathbb{Z}$-espaces vectoriels de dimension finie, on peut effectuer les voir comme des permutations d'un ensemble fini. On peut alors exprimer leur signature à l'aide du déterminant : un joli théorème dû à Frobenius et Zolotarev.

☢ **Exercice 30.** Si H est un sous-groupe de cardinal $\frac{n!}{2}$, montrer que tout 3-cycle σ est dans H en raisonnant par

l'absurde : si $\sigma \notin H$, montrer que l'on a : $\sigma H = S_n \setminus H$ (raisonner sur les cardinaux). En déduire que $\sigma^2 \in H$, et obtenir une contradiction. Conclure en se souvenant que les 3-cycles engendrent A_n.

Commentaires. (G/H) Si G est un groupe, alors un sous-groupe H d'indice 2 (c'est-à-dire tel que G/H soit de cardinal 2) est toujours « distingué », c'est-à-dire concrètement que G/H hérite de la structure de groupe de G comme on l'a vu dans le cas commutatif ou lorsque H est le noyau d'un morphisme.
Cela peut servir ici à plier l'exercice rapidement (et plus naturellement, à mon goût) : si G/H est un groupe, il est forcément commutatif puisqu'il est de cardinal 2, donc par l'exercice 33 on a $D(S_n) = A_n \subseteq H$ (groupe dérivé). On conclut avec les cardinaux.
Autre raisonnement : les groupes de cardinal 2 sont tous isomorphes entre eux, puisqu'ils sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$ d'après le cours. Donc il existe un isomorphisme entre S_n/H et $\{-1,1\}$, qui provient d'un morphisme surjectif $S_n \to \{-1,1\}$ de noyau H par le théorème de factorisation des morphismes. Or le morphisme de signature est l'unique morphisme surjectif de S_n dans $\{-1,1\}$, donc le morphisme précédent est ε, et son noyau est $H = \ker(\varepsilon) = A_n$. Voyez comment la structure quotient est efficace !

Exercice 31. (Commutant d'un p-cycle) Montrer qu'une permutation appartient à $C(\sigma)$ si et seulement si elle est de la forme : $\tau = \sigma^k \sigma'$, avec $k \in [\![0, p-1]\!]$ et $\sigma' \in S_n$ une permutation dont le support ne rencontre pas celui de σ (éventuellement utiliser le principe de conjugaison). En déduire que σ' induit une permutation d'un ensemble à $n-p$ éléments. Cela permet de faire le lien avec $\mathbb{Z}/p\mathbb{Z} \times S_{n-p}$.

Commentaires. Une relation de commutation entre deux permutations doit faire penser au principe de conjugaison, vu que $\sigma\tau = \tau\sigma$ si et seulement si $\sigma = \tau\sigma\tau^{-1}$ (et $\tau = \sigma^{-1}\tau\sigma$). Comme toute permutation est un produit de cycles, on peut utiliser notre connaissance des conjugués de cycles pour exploiter ce genre d'égalité. C'est ainsi que l'on a déterminé le centre de S_n en cours.

★ **Exercice 32. (Parties génératrices de S_n)**

1. On a donné, dans le cours, un exemple de partie génératrice de S_n qui y ressemble beaucoup. Montrer que les permutations de cette partie génératrice peuvent s'exprimer à l'aide de transpositions de la forme $(i\ i+1)$. Le principe de conjugaison vous y aidera.
2. Même principe.
3. On essaie de se ramener au cas précédent. Remarquer que quitte à conjuguer τ et σ par une permutation convenable, on peut supposer $\tau = (1\ k+1)$ avec $k \in [\![1, n-1]\!]$ et $\sigma = (1\ 2\ \cdots\ n)$. Pour montrer qu'on peut se ramener à la transposition $(1\ 2)$: montrer que $\left\{\sigma^\ell \tau \sigma^{-\ell} \mid \ell \in \mathbb{Z}\right\} = \{(i\ i+k) \mid i \in [\![1, n-k]\!]\} \cup \{(i\ i-k) \mid i \in [\![k+1, n]\!]\}$. En peu de mots, on obtient toutes les transpositions échangeant des éléments distants de k. Écrire $(1\ 2)$ à l'aide de telles transpositions (c'est ici que la primalité de n intervient : remarquer que k est premier avec n qu'il existe ℓ tel que : $k\ell \equiv 1 \bmod n$; écrire alors $(1\ 2)$ à l'aide de $(1\ k+1)$, $(k+1\ 2k+1)$, etc., $((\ell-1)k+1\ \ell k+1)$.
   Moins laborieux mais plus astucieux : introduire la relation d'équivalence sur $[\![1, n]\!]$ définie par : $i \sim j \iff (i\ j) \in \langle \sigma, \tau \rangle$ (vérifier que c'en est une). Montrer que toutes les classes ont le même nombre d'éléments grâce au principe de conjugaison et au fait que σ et ses puissances permettent d'envoyer tout élément de $[\![1, n]\!]$ sur un autre élément de $[\![1, n]\!]$. En déduire qu'il n'y a qu'une seule classe en utilisant la primalité de n, et donc que toutes les transpositions sont dans $\langle \sigma, \tau \rangle$.

Commentaires. Bien noter que, dans cet exercice comme dans le cours, on ne montre pas qu'une partie X engendre S_n en écrivant toute permutation de S_n comme produit d'éléments de X : on se contente de montrer que toute permutation d'une partie génératrice *connue* de S_n est produit d'éléments de X. Cela diminue grandement la complexité de l'étude : on se ramène à étudier des transpositions. Cela vaudrait dans d'autres groupes que S_n.

★ **Exercice 33. (Groupe dérivé de S_n)**

1. Calculer la signature d'un élément de la forme $\sigma\tau\sigma^{-1}\tau^{-1}$, puis utiliser le fait que l'image d'un morphisme se déduit de l'image des éléments d'une partie génératrice.
2. Utiliser le fait qu'un 3-cycle et son carré soient conjugués.
3. Se souvenir que les 3-cycles engendrent A_n.
4. Montrer que le noyau d'un tel morphisme contient A_n. Par un raisonnement sur le cardinal, en déduire le raisonnement voulu.

Commentaires. Cet exercice, noyé au milieu de tant d'autres, contient pourtant un résultat historiquement important : c'est l'un des arguments majeurs de Galois pour démontrer que les équations polynomiales de degré au moins cinq ne sont pas résolubles par radicaux (un autre argument majeur est que A_n est « simple » pour tout $n \geqslant 5$, mais je ne définirai pas ce que cela veut dire). **(G/H)** Le sous-groupe dérivé d'un groupe (défini de la même manière que dans S_n) permet de « rendre commutatif » ce groupe par passage au quotient. C'est-à-dire : si G est un groupe, de sous-groupe dérivé $D(G)$, alors $G/D(G)$ est un groupe pour la structure héritée de G (exercice) et il est toujours commutatif. En effet, par définition du sous-groupe dérivé, on a toujours $\bar{g}\bar{h}\bar{g}^{-1}\bar{h}^{-1} = \bar{1}$ (modulo $D(G)$), donc : $\bar{g}\bar{h} = \bar{h}\bar{g}$.

C'est même le plus petit sous-groupe de G dont le quotient est un groupe commutatif (donc, formulé autrement : $G/D(G)$ est le plus *grand* groupe quotient qui rende G commutatif) : si G/H est un groupe commutatif, alors $D(G) \subseteq H$. C'est ainsi qu'on aurait pu traiter la première question : puisque S_n/A_n est isomorphe à $\{-1,1\}$ (théorème d'isomorphisme appliqué à la signature), il est commutatif, donc $D(S_n) \subseteq A_n$. Cette caractérisation du sous-groupe dérivé permet de simplifier l'étude des morphismes à valeurs dans un groupe commutatif (comme dans la dernière question) : si $f : G \to A$ est un morphisme de groupes, avec A commutatif, alors $G/\ker(f)$ est commutatif puisqu'il est isomorphe à un sous-groupe de A (théorème d'isomorphisme), donc $D(G) \subseteq \ker(f)$ d'après ce qu'on vient de raconter. Cela montre, par le théorème de factorisation des morphismes, que $f : G \to A$ induit un morphisme $G/D(G) \to A$. Si $D(G)$ est « gros », alors $G/D(G)$ devient « petit » et il devient facile d'expliciter ce dernier morphisme. Exploiter cette idée pour traiter la dernière question *via* les groupes quotients.

Exercice 34. Quelle est la façon la plus naturelle de passer d'une permutation impaire à une permutation paire ? Exploiter cette idée pour fabriquer une application $S_n \to A_{n+2}$, dont on vérifiera que c'est un morphisme injectif.

Commentaires. Il est difficile de montrer qu'il n'existe pas de morphisme injectif de S_n dans A_{n+1} (la question serait naturelle). Cela passe par une étude fine des sous-groupes de A_{n+1}, pour montrer qu'il n'admet pas de sous-groupe de cardinal $n!$.

Exercice 35. (🖹) Se souvenir que S_3 est engendré par les transpositions : un automorphisme f de S_3 est donc entièrement déterminé par l'image de (1 2), (1 3) et (2 3). En raisonnant sur l'ordre, puis sur le fait que (1 2) = (2 3)(1 3)(2 3), etc., montrer que f coïncide sur les transpositions avec un automorphisme de la forme $\tau \mapsto \sigma\tau\sigma^{-1}$ où $\sigma \in S_3$, et donc lui est égal. Vous aurez alors la forme de tous les éléments de $\mathrm{Aut}(S_3)$ et verrez qu'ils sont naturellement associés à une permutation de S_3. Il reste à vérifier que cela définit un isomorphisme.

Commentaires. Exemple d'utilisation des parties génératrices pour simplifier une étude. Ici : pour définir un morphisme uniquement par son image d'une partie génératrice (comme vous le faites en algèbre linéaire). Mieux : les isomorphismes (et donc les automorphismes) doivent préserver tout ce qui est relatif à la structure : ordres, commutation, etc. Toutes ces contraintes sont à prendre en compte au moment de déterminer les images possibles d'une partie génératrice par un automorphisme.

Initiation aux actions de groupe (sans le dire)

Exercice 36. (Théorème de Cayley) Montrer que φ_g est une bijection, puis que $g \mapsto \varphi_g$ est un morphisme, est un calcul direct. L'injectivité : si $\varphi_g = \mathrm{Id}_G$, évaluer cette égalité en un élément de G convenable.

Commentaires. Ce théorème permet de comprendre pourquoi les groupes de permutation sont les groupes les plus complexes à étudier : ils contiennent pour ainsi dire tous les groupes qui existent. Il a aussi une importance historique, puisqu'il permet de comprendre que les deux premières définitions d'un groupe (comme ensemble de permutations, ou comme on les a définis en 1re année) sont finalement les mêmes : les éléments d'un groupe SONT des permutations. Ce que finalement, l'on remarque bien en observant la table de Cayley d'un groupe : chaque ligne (ou chaque colonne) est une permutation des éléments du groupe.

Ainsi, au moins en théorie, on pourrait démontrer tout théorème sur les éléments g d'un groupe G en travaillant avec sa permutation φ_g naturellement associée, en la décomposant en cycles, etc. C'est ainsi qu'on peut démontrer le cas particulier du théorème de Lagrange dans le cours (l'ordre d'un élément divise le cardinal du groupe). Mais cette idée fait rarement recette, justement à cause de la trop grande complexité conceptuelle des permutations.

Exercice 37. (Les actions de groupe donnent des générateurs)

1. Vérification bêtement calculatoire. Ne pas oublier de vérifier que φ_M laisse stable $\mathcal{H}$. La vérification de l'identité $\varphi_M \circ \varphi_N = \varphi_{MN}$ permet à peu de frais de vérifier en même temps que φ_M admet toujours une bijection réciproque, et est donc bien dans $S_{\mathcal{H}}$.
2. Ramener l'égalité $\varphi_M(i) = i$ à une égalité entre deux nombres complexes mis sous forme algébrique, et identifier parties réelles et parties imaginaires. Cela donnera une relation entre les coefficients de M. Se souvenir ensuite que $\det(M) = 1$ pour comprendre l'origine des cosinus et sinus.
3. Simplifier $\varphi_T(i)$ en utilisant le fait que T soit triangulaire et de déterminant 1.
4. Utiliser la question 3 pour obtenir une égalité du type : $\varphi_M(i) = \varphi_T(i)$, avec $T \in \mathrm{T}_2(\mathbb{R})$, et conclure avec la question 2.

Commentaires. Ce qu'on a fait dans cet exercice peut être généralisé. Si l'on veut obtenir un système de générateurs d'un groupe G, à l'aide d'un morphisme naturel $g \mapsto \varphi_g$ de G dans un groupe de permutations S_X : 1° on trouve un sous-ensemble $H \subseteq G$ et $x \in X$ tels que $\{\varphi_g(x) \mid g \in H\} = X$, 2° on prend $g \in G$ quelconque, et on remarque que $\varphi_g(x) \in X$, donc par le point précédent il existe $h \in H$ tel que : $\varphi_g(x) = \varphi_h(x)$, 3° la propriété de morphisme permet d'écrire $\varphi_{h^{-1}g}(x) = x$, ce qui permet souvent d'expliciter $h^{-1}g$ puis d'écrire $g = h(h^{-1}g)$: ainsi g est produit d'éléments de H et de $K = \left\{g' \in G \mid \varphi_{g'}(x) = x\right\}$, donc $H \cup K$ engendre G. Cette stratégie peut être affaiblie (par exemple on n'est pas obligé d'obtenir X tout entier à l'étape 1°), mais dans les grandes lignes elle est toujours la même.

Exercice 38. (Les actions de groupe permettent le dénombrement)

1. Montrer que si $\sigma \in G$ alors la restriction $\sigma_{|[\![n-k,n]\!]}$ induit une bijection (dans... ?). Conclure. Pour O : noter que σ préserve les cardinaux pour en déduire que O est inclus dans $\mathcal{P}_k(E)$. Étudier la réciproque.
2. Noter que $f : \sigma \mapsto \sigma([\![1,k]\!])$ définit une application surjective de S_n sur O (par définition de O), et que chaque fibre $f^{-1}(\{Y\})$, pour $Y \in O$, a le même cardinal (c'est là que G intervient). Conclure avec le principe des bergers.
3. La première question permet de montrer qu'un élément de G définit par restriction des permutations d'ensembles à k et $n-k$ éléments. Cela conduit à définir une application $G \to S_k \times S_{n-k}$. Vérifier qu'elle est bijective en utilisant le fait que les éléments en présence soient des bijections.

Commentaires. Une action de groupe, c'est-à-dire la donnée d'un morphisme $g \mapsto \varphi_g$ de G dans S_X avec X un ensemble, permet le dénombrement (soit de G, soit de X, soit de $O(x)$ défini ci-dessous) grâce aux idées suivantes :

— pour tout $x \in X$, le principe des bergers appliqué au morphisme surjectif $G \to O(x) = \{\varphi_g(x) \mid g \in G\}$ donne : $\text{card}(G) = \text{card}(O(x)) \cdot \text{card}(\{g \in G \mid \varphi_g(x) = x\})$;

— on vérifie que la relation sur X définie par : $y \sim x \iff y \in O(x)$, est une relation d'équivalence, ce qui permet d'écrire : $X = \bigsqcup_x O(x)$, et on en déduit une expression de $\text{card}(X)$ à l'aide des cardinaux des $O(x)$.

La deuxième formule n'est pas utilisée dans cet exercice, mais dans les exercices 39 et 40. Elle est très commode dans les p-groupes. Il existe une autre formule de dénombrement, appelée *formule de Bursnide*, que j'ai choisi de ne pas intégrer à ces feuilles d'exercices, mais qui est très utilisée lorsqu'on manipule des actions de groupe (pour compter un nombre de classes d'équivalence).
Pour que ces formules soient exploitables, en vue de dénombrer un ensemble X, encore faut-il trouver un groupe G qui agit dessus simplement. Comme l'image d'une partie à k éléments de $[\![1,n]\!]$ par une permutation reste une partie à k éléments (et qu'on les obtient toutes en changeant de permutation), le choix de passer par S_n est relativement naturel.

On remarque que les ensembles $\{\varphi_g(x) \mid g \in G\}$ et $\{g \in G \mid \varphi_g(x) = x\}$ apparaissent même hors des contextes de dénombrement (exercice 37). Ils sont le point de départ de toute étude d'une action !

Exercice 39. (Le centre d'un p-groupe est non trivial)

1. Vérification sans grande subtilité.
2. Au vu de la description de $O(x)$, on peut construire assez facilement une application surjective $G \to O(x)$. Remarquer que le nombre d'antécédents de chaque élément de $O(x)$ est le même et s'exprime à l'aide de $Z(G)$. Conclure avec le principe des bergers.
3. Écrire G comme réunion de classes pour la relation d'équivalence de l'exercice. Regrouper les orbites de cardinal 1, et remarquer qu'il y en a autant que d'éléments dans $Z(G)$. Montrer que les autres orbites sont de cardinal multiple de p grâce à la question précédente. On en déduit le résultat car $\text{card}(G) \equiv 0 \bmod p$.
4. Montrer que S_x est un sous-groupe de G, ce qui ne laisse que peu de possibilités pour son cardinal grâce au théorème de Lagrange. De plus des éléments sont trivialement dans G. Tous les éléments de $Z(G)$ sont aussi dans G. Cela suffit à en déduire que S_x est assez gros pour être égal à G, et utiliser $x \notin Z(G)$ pour conclure.

Commentaires. On le sait grâce au théorème de Lagrange et on l'illustre encore ici : le cardinal d'un groupe conditionne BEAUCOUP sa structure. On a vu dans le cours qu'il n'y a qu'un seul groupe de cardinal premier à isomorphisme près (c'est $\mathbb{Z}/p\mathbb{Z}$), et il est en particulier cyclique (donc commutatif). Cet exercice montre que ceux de cardinal p^2 avec p premier sont aussi commutatifs. Conjointement à l'exercice 10, cela démontre qu'il n'y en a que deux de cardinal p^2. Et ils sont très simples ! En maîtrisant $(\mathbb{Z}/p\mathbb{Z})^2$ et $\mathbb{Z}/p^2\mathbb{Z}$, vous maîtrisez tous les groupes de cardinal 4, 9, 25, etc. Avoir cette classification en tête est très utile.
(G/H) Conséquence très utile de cet exercice : le fait que le centre d'un p-groupe soit non trivial permet, pour démontrer des résultats sur les p-groupes, de raisonner par récurrence sur l'exposant k : dans l'hérédité, on se ramène à des groupes de cardinal inférieur en considérant $Z(G)$ et $G/Z(G)$. C'est par exemple ainsi qu'on peut démontrer qu'un p-groupe admet des sous-groupes de tout cardinal possible (c'est-à-dire divisant le cardinal de G), à condition de savoir que les sous-groupes de $G/Z(G)$ sont en bijection avec ceux de G contenant $Z(G)$.

Si l'on en reste cantonné au programme des classes préparatoires, où l'on ne sait pas que $G/Z(G)$ hérite de la structure de groupe de G, alors cette étape peut parfois être remplacée par une utilisation tortueuse de la relation : $G = \bigcup_{i=1}^{r} g_i Z(G)$, avec $g_1, \dots, g_r$ un système complet de représentants de la relation d'équivalence associée à $Z(G)$ (c'est un contournement artificiel, alourdissant l'utilisation de la loi de groupe sur les classes).

Exercice 40. (Lemme de Cauchy)

1. Remarquer qu'un élément de X est la donnée $p-1$ éléments pouvant être choisis arbitrairement, la valeur du dernier étant imposée par les choix précédents.
2. Pas de subtilité. Ne pas oublier de vérifier que φ_γ est à valeurs dans X. La vérification de l'identité $\varphi_\gamma \circ \varphi_\gamma = \varphi_{\gamma\gamma'}$ permet à peu de frais de vérifier en même temps que φ_γ admet toujours une bijection réciproque, et est donc bien dans S_X.
3. Il est facile de vérifier qu'il y a au plus p éléments, vu que $\langle\sigma\rangle$ en a au plus p. Pour savoir s'il y en a 1 ou p : vérifier que dès que l'égalité $\varphi_\gamma(x) = x$ se produit pour un $\gamma \in \langle\sigma\rangle$ différent de l'identité, alors elle se produit pour tout γ et x a une description triviale. Conclure que dans le cas contraire, les $\varphi_\gamma(x)$ sont tous distincts.
4. Vous devriez déjà avoir explicité de tels x dans la question précédente. Ne pas oublier la définition de X !
5. Comme : $x \sim y \iff y \in O(x)$ définit une relation d'équivalence sur X, on peut l'écrire comme réunion de ses classes. Comparer les cardinaux, et réduire modulo p. Constater qu'il y a exactement $\mathrm{card}(F)$ classes de cardinal 1. Conclure en simplifiant le cardinal de X modulo p, et en se souvenant du lien entre F et l'objectif de l'exercice.

Commentaires. Une action de groupe, c'est-à-dire la donnée d'un morphisme $g \mapsto \varphi_g$ de G dans S_X avec X un ensemble, permet le dénombrement (soit de G, soit de X, soit de $O(x)$ défini ci-dessous) grâce aux idées suivantes :

— pour tout $x \in X$, le principe des bergers appliqué au morphisme surjectif $G \to O(x) = \{\varphi_g(x) \mid g \in G\}$ donne : $\mathrm{card}(G) = \mathrm{card}(O(x)) \cdot \mathrm{card}(\{g \in G \mid \varphi_g(x) = x\})$;

— on vérifie que la relation sur X définie par : $y \sim x \iff y \in O(x)$, est une relation d'équivalence, ce qui permet d'écrire : $X = \bigsqcup_x O(x)$, et on en déduit une expression de $\mathrm{card}(X)$ à l'aide des cardinaux des $O(x)$.

La deuxième formule est commode dans les p-groupes, comme on l'illustre ici, parce que les relations de divisibilité entre puissances de nombres premiers sont très contraignantes.
Il existe une autre formule de dénombrement, appelée *formule de Bursnide*, que j'ai choisi de ne pas intégrer à ces feuilles d'exercices, mais qui est très utilisée lorsqu'on manipule des actions de groupe (pour compter un nombre de classes d'équivalence).

On remarque, avec cet exercice et tous les autres, que les ensembles $\{\varphi_g(x) \mid g \in G\}$ et $\{g \in G \mid \varphi_g(x) = x\}$ sont le point de départ de toute étude d'une action !

Anneaux et corps

✓ **Exercice 41.**

1. Il n'y a rien de subtil, en appliquant la définition d'un morphisme, d'un idéal et d'une image réciproque.
2. La surjectivité sert pour la propriété d'absorption (multiplication externe par un élément $b \in B$ qu'on peut écrire $b = f(a)$ avec $a \in A$). Pour un contre-exemple : songer à un morphisme à valeurs dans un anneau qui a « très peu d'idéaux » (l'exercice 42 vous met sur la voie). Sa correspondance peut être très simple.

Commentaires. En appliquant convenablement la première question, vous devriez retrouver le fait que $\ker(f)$ soit un idéal.
Puisque les idéaux de $\mathbb{Z}$ et $K[X]$ sont toujours connus (voir chapitre IV), et qu'il est facile de produire des morphismes sur ces deux anneaux et à valeurs dans à peu près n'importe quel autre anneau, cet exercice est souvent exploitable pour en déduire les idéaux d'anneaux non usuels.

★ **Exercice 42.**

1. Sens direct : montrer que si I est un idéal non réduit à 0_A, alors $1_A \in I$ (utiliser la propriété d'absorption). Sens réciproque : si $a \neq 0_A$, regarder l'idéal aA, qui doit être égal à $\{0_A\}$ ou A par hypothèse.
2. Si $a \in A \setminus \{0_A\}$: considérer les idéaux de la forme $a^n A$ quand $n \in \mathbb{N} \setminus \{0\}$ varie.
3. Faire le lien entre le noyau d'un morphisme de corps et les questions précédentes.

Commentaires. Exercice très instructif, dont une conséquence philosophique est que les corps ne sont pas adaptés à l'arithmétique (le chapitre IV nous enseigne en effet que généraliser l'arithmétique des entiers à d'autres anneaux passe naturellement par les idéaux). Finalement, il y a du bon à ne pas être inversible !

Exercice 43.

1. Pour montrer que $\sqrt{I}$ est un sous-groupe de A : utiliser la formule du binôme de Newton avec un exposant suffisamment élevé, pour être sûr que toutes les puissances apparaissant dans le développement soient plus grandes que les indices de nilpotence des éléments en jeu. La propriété d'absorption est facile à vérifier. L'égalité s'obtient par double inclusion et ne soulève pas de difficulté, si l'on écrit patiemment la définition des objets.
2. Si $x^k \in I$, noter que $x^\ell \in I$ pour tout $\ell \geqslant k$. En déduire que si $x \in \sqrt{I} \cap \sqrt{J}$, on peut trouver un exposant suffisamment grand pour que $x^k \in I \cap J$. L'inclusion réciproque est facile. Pour la somme : raisonnement analogue sur les exposants. Vous aurez besoin de la formule du binôme de Newton. Voir aussi l'usage de la formule du binôme dans l'exercice 46.

Commentaires. En choisissant convenablement l'idéal I, vous obtiendrez l'ensemble des éléments nilpotents de A, qui est donc un idéal ! Nous vous recommandons également de calculer $\sqrt{n\mathbb{Z}} \subseteq \mathbb{Z}$, puis de faire le lien avec le résultat de l'exercice 45.
(G/H) Même dans le cas d'un idéal quelconque, on peut remarquer bien des analogies entre les raisonnements de cet exercice et ceux effectués avec des éléments nilpotents. C'est normal : $\sqrt{I}$ est l'image réciproque par la projection naturelle $A \to A/I$ des éléments nilpotents de A/I.
L'intérêt algébrique le plus naïf de $\sqrt{\{0_A\}}$ est d'éliminer tous les éléments nilpotents de A (puisque quotienter par l'idéal des éléments nilpotents revient à les rendre nuls, l'anneau quotient $A/\sqrt{\{0_A\}}$ n'a pas d'élément nilpotent hormis zéro). C'est cependant en géométrie algébrique que cette idée est la plus fructueuse.

✓ **Exercice 44.** Noter que I_x est le noyau d'un morphisme d'anneaux bien choisi. Raisonner par l'absurde pour démontrer qu'il n'est pas principal : s'il existe $g \in A$ tel que : $I_x = gA$, produire des fonctions qui s'annulent en x et qui ne peuvent pas être proportionnelles à g.

Commentaires. Le moyen le plus économe de montrer qu'un ensemble est un idéal, est de montrer que c'est le noyau d'un morphisme d'anneaux (en fait, TOUT idéal est le noyau d'un morphisme d'anneaux : pensez à la projection canonique $A \to A/I$).

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

1. Montrer qu'un tel x ne peut pas être premier avec n. Étudier la réciproque.
2. Écrire ce que l'égalité $x^k \equiv 0 \bmod n$ implique en termes de divisibilité, surtout au niveau des facteurs premiers de n (l'intérêt ? utiliser le lemme d'Euclide). C'est encore plus clair si on utilise le lemme chinois (chapitre IV). Songer à vérifier la réciproque.

Commentaires. Se poser la question de la forme des éléments nilpotents est pertinent, à chaque anneau que vous rencontrez (même si l'explicitation n'est pas toujours simple). De même pour les diviseurs de zéros et les idempotents (c'est-à-dire les éléments tels que $x^2 = x$). Tout cela vous permet de vous approprier l'anneau.
On trouve encore une situation où raisonner sur les diviseurs premiers est plus instructif (sachant que l'unicité de la décomposition en facteurs premiers le permet : montrer qu'un entier divise l'autre revient à comparer leurs valuations p-adiques). Cela permet d'utiliser le lemme d'Euclide. Ou, en termes plus savants : cela permet d'utiliser des propriétés de $\mathbb{Z}/p\mathbb{Z}$ qui ne sont pas valables en général dans $\mathbb{Z}/n\mathbb{Z}$ (inversibilité, intégrité, absence d'éléments nilpotents, cyclicité du sous-groupe multiplicatif, etc.).

★ **Exercice 46.**

1. Facile à vérifier par définition de l'intégrité.
2. Pour $a+b$: utiliser la formule du binôme de Newton. Pour le produit : utiliser la commutativité et un exposant supérieur à l'indice de nilpotence de a et b.
3. Traiter le cas $u = 1_A$ en s'inspirant de la formule $(1-x)^{-1} = \sum_{k=0}^{+\infty} x^k$ pour trouver ce que serait l'inverse de $1_A + v$. Se ramener à ce cas ensuite même pour u inversible quelconque.

Commentaires. Si vous avez aussi traité l'exercice 43, vous avez peut-être remarqué des similitudes entre les raisonnements de ces exercices. C'est normal : en choisissant convenablement l'idéal I dans l'exercice 43, vous obtiendrez l'ensemble des éléments nilpotents de A.
L'indication de la troisième question n'est pas du tout une analogie bancale. Les relations formelles se généralisent souvent à tout anneau (dès que la somme a un sens : c'est pourquoi il faut souvent une hypothèse de nilpotence, ou plus tard une structure topologique), ce qui n'a rien d'étonnant : ces relations sont souvent basées sur des manipulations simples, faisant uniquement intervenir des sommes et produits impliquant x et ses puissances. Aucune raison que cela ne se généralise pas. L'exercice 38 du chapitre IV est basé sur la même observation.

Exercice 47.

1. D'abord montrer que $x^k = 0_A$ pour $k \leqslant 3$ implique $x = 0_A$. Si $x^k = 0_A$ avec $k \geqslant 4$: effectuer la division euclidienne de k par 3 pour baisser l'exposant. Qu'en déduire sur l'indice de nilpotence ?
2. Montrer que $b(1-b)a = 0_A$. En déduire que $(1-b)ab = 0_A$ en utilisant soigneusement l'hypothèse de l'énoncé, puis : $bab = ab$. Un raisonnement analogue permet d'obtenir : $bab = ba$. Conclure.
3. Montrer que a^2 vérifie toujours l'hypothèse de la question précédente.
4. Exprimer $2a$ et $3a$ à l'aide de carrés (penser à la formule du binôme et à l'hypothèse de l'énoncé). Conclure.

Commentaires. Plus généralement, un théorème difficile dû à Jacobson dit qu'un anneau A est commutatif si et seulement s'il existe $n \geqslant 2$ tel que : $\forall x \in A,\ x^n = x$. On a démontré un cas particulier. Sauriez-vous traiter le cas $n = 2$? Il est plus abordable, même sans indications (on parle d'anneau booléen dans ce cas).

Exercice 48. S'inspirer du résultat de l'exercice 46 pour montrer que $A[X]^\times$ est l'ensemble des polynômes dont le coefficient constant est inversible et les autres coefficients nilpotents.

Commentaires. Noter que la description n'est pas la même que pour $K[X]$ avec K un corps. Par exemple $(\bar{2}X + \bar{1})^2 = \bar{1}$ dans $\mathbb{Z}/4\mathbb{Z}[X]$, donc $\bar{2}X + \bar{1}$ est inversible.

Exercice 49. (Anneaux noethériens) Pour $(i) \Rightarrow (ii)$: montrer que si (i) est vrai, alors toute suite croissante $(I_n)_{n\geqslant 0}$ est asymptotiquement égale à $I = \bigcup_{n=0}^{+\infty} I_n$ (on montrera d'abord que c'est bien un idéal, contenant les I_n, puis on lui appliquera (i)). Pour $(ii) \Rightarrow (iii)$: par contraposée. Utiliser l'absence d'élément maximal dans $\mathcal{I}$ pour construire une suite strictement croissante. Pour $(iii) \Rightarrow (i)$: montrer que tout I est de la forme voulue en considérant un élément maximal de $\left\{ J \subseteq I \mid \exists k \in \mathbb{N}\setminus\{0\},\ \exists\, (a_i)_{1\leqslant i\leqslant k} \in A^k,\ J = \sum_{i=1}^{k} a_i A \right\}$, et en montrant qu'il doit être égal à I (par l'absurde et en produisant un nouvel idéal qui contredirait la maximalité).

Commentaires. Une des nombreuses applications des anneaux noethériens est dans la généralisation des raisonnements par l'absurde où l'on raisonne sur un plus petit ou plus grand élément pour obtenir une contradiction, ou consistant en la construction d'une suite strictement décroissante d'entiers naturels (comme le « principe de descente infinie » dû à Fermat).
Exemple concret : on montre l'existence de la décomposition d'un entier naturel non nul en produit de facteurs premiers en raisonnant par l'absurde, et en montrant que le plus petit entier naturel à ne pas se décomposer ainsi est nécessairement composé : les facteurs premiers des deux diviseurs non triviaux ainsi fabriqués permettent d'obtenir une contradiction. On montre de même que dans un anneau noethérien, tout élément non inversible est produit d'éléments irréductibles, en raisonnant par l'absurde et en considérant *l'idéal maximal* de l'ensemble des idéaux aA tels que a ne soit pas produit d'irréductibles. On s'en inspire au chapitre IV pour montrer qu'il y a existence et unicité d'une telle factorisation dans un anneau principal, mais l'existence est déjà vraie dans les anneaux noethériens.

★ **Exercice 50. (Caractéristique d'un anneau)**

1. Le noyau de f_A est un sous-groupe de $\mathbb{Z}$.
2. Utiliser le théorème de factorisation des morphismes.
3. Remarquer que f_A et f_B sont liés *via* la composition par une application injective, donc ils ont même noyau.
4. Montrer que $\mathbb{Z}/n\mathbb{Z}$ doit être intègre également grâce à un isomorphisme, et conclure.
5. On sait que A contient $\mathbb{Z}$ sous cette hypothèse. Comment passer de $\mathbb{Z}$ à $\mathbb{Q}$?

Commentaires. Faire le lien avec le commentaire de l'exercice 41.
Tous les anneaux et corps que vous connaissez ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) sont fabriqués en partant d'anneaux connus, par adjonction d'éléments (on ajoute les opposés de $\mathbb{N}$ pour avoir $\mathbb{Z}$, les inverses des éléments non nuls de $\mathbb{Z}$ pour avoir $\mathbb{Q}$, les limites des suites de Cauchy rationnelles pour avoir $\mathbb{R}$, et enfin une racine carrée de -1 pour avoir $\mathbb{C}$). C'est la manière la plus naturelle de construire progressivement un anneau, ou même de démontrer des résultats sur les éléments d'un anneau (on commence par un sous-anneau aussi petit et simple que possible, puis on étend le raisonnement progressivement à tous les éléments, comme lorsqu'on raisonne par densité). Mais pour un anneau abstrait, à construire ou à étudier, on peut se demander : de quoi part-on ? Quel est le sous-anneau le plus simple qu'il contienne ?
Une façon naïve de procéder : un anneau doit contenir 1_A. Comme il est stable par addition, il doit contenir $n1_A$ pour tout $n \in \mathbb{N}$, et même pour tout $n \in \mathbb{Z}$ grâce à la stabilité par inverse (pour $+$). Ainsi, cette approche naïve nous dit qu'un anneau quelconque devrait contenir tous les entiers relatifs. S'il est un corps, il contient aussi leurs inverses, donc il contient $\mathbb{Q}$.
En résumé : tout anneau contient $\mathbb{Z}$ et tout corps contient $\mathbb{Q}$... Non, pas tout à fait ! Car $n1_A = 0_A$ peut se produire dans un anneau quelconque ! C'est pourquoi il faut traiter à part le cas où cela se produit : d'où l'étude de f_A dans cet exercice. On voit alors que A ne contient que $\mathbb{Z}/n\mathbb{Z}$ et non $\mathbb{Z}$, si n est le plus petit entier non nul tel que $n1_A = 0_A$.
Cet entier est la caractéristique d'un anneau. Comme il nous donne le plus petit sous-anneau contenant A, il donne une idée de la fonction dont il est construit et c'est une donnée essentielle.
En reprenant les commentaires des exercices 5 et 15, on voit que A est « presque » un $\mathbb{Z}/n\mathbb{Z}$-espace vectoriel s'il est de caractéristique n, ce qui permet de s'inspirer de l'algèbre linéaire pour l'étudier. Je dis « presque », parce que $\mathbb{Z}/n\mathbb{Z}$ n'est en général pas un corps. Dans le cas où c'en est un, cela donne des informations riches sur A et notamment son cardinal : voir l'exercice 54.

Exercice 51. (Un morphisme de corps est linéaire) D'abord montrer que $f(x) = x$ pour tout $x \in k$ (en partant de $f(1_K) = 1_K$ par exemple, ou en considérant l'ensemble $\{x \in K \mid f(x) = x\}$ dont on montrera que c'est un corps, de même sous-corps premier que K), et conclure en utilisant adéquatement la définition d'un morphisme de corps.

Commentaires. La seconde indication proposée encourage à reconnaître des structures partout où il y en a, même quand ce n'est pas explicitement indiqué par l'exercice (ici, pour montrer que l'ensemble des points fixes contient le sous-corps premier de K). C'est l'un des aspects qui peuvent faire de vous d'excellents algébristes.

✓ **Exercice 52. (Propriétés invariantes par isomorphisme)**

1. S'inspirer de l'exemple analogue fait en cours (avec des groupes).

2. Calculer $f(x)f(y)$. Pour la réciproque : considérer f^{-1}.
3. Un isomorphisme de corps induit deux isomorphismes de groupes.
4. Les compositions de morphismes restent des morphismes, et les compositions d'applications bijectives restent bijectives. Vérifier que $g \mapsto f \circ g \circ f^{-1}$ définit l'isomorphisme cherché entre $\mathrm{Aut}(K)$ et $\mathrm{Aut}(L)$.
5. Grâce à l'isomorphisme f, on peut écrire un isomorphisme entre $\ker(f_K)$ et $\ker(f_L)$ (notations de l'exercice 50).
6. Immédiat en utilisant la définition d'un morphisme de corps, et le fait que $f(0_K) = 0_L$.
7. Vérifier d'abord que pour tout $(A, B) \in K[X]^2$, on a $f(AB) = f(A)f(B)$. En déduire que l'image par f de la décomposition de P sous forme irréductible donne la décomposition de $f(P)$ sous forme irréductible.

Commentaires. Au fond, si vous avez bien compris la philosophie des isomorphismes, cet exercice ne vous enseigne rien : vous n'avez fait que la mettre en œuvre techniquement. L'avantage de la comprendre, c'est que même si vous rencontrez une nouvelle propriété $\mathcal{P}$ dans un exercice ou problème, alors même si cette propriété est complètement inédite pour vous, vous savez qu'un isomorphisme préserve les éléments qui la vérifient (ou non).
Le résultat des deux dernières questions est très important lorsqu'on veut expliciter des morphismes définis sur un corps L, lorsque le corps L est de la forme $L = K(\alpha) = \{R(\alpha) \mid R \in K(X)\}$ avec $\alpha \in L \setminus K$ une racine d'un polynôme $P \in K[X]$. En effet, dans ce cas, déterminer un morphisme f revient à déterminer $f_{|K}$ et $f(\alpha)$, comme on peut s'en convaincre aisément. D'après cet exercice, une condition suffisante sur $f(\alpha)$ est qu'il soit racine de $f(P)$; en explicitant les racines de $f(P)$, on en déduit les possibilités pour la valeur de $f(\alpha)$, et on détermine f. C'est illustré dans l'exercice 53.

★ **Exercice 53.** (🗎)

1. Montrer que $f_{|\mathbb{Q}}$ est l'identité par un raisonnement analogue à celui de l'exercice 51 ou, sur un rythme plus pédestre : partir de $f(1) = 1$ pour en déduire $f(x) = x$ pour tout $x \in \mathbb{N}$, puis pour tout $x \in \mathbb{Z}$, puis pour tout $x \in \mathbb{Q}$. Pour passer de $\mathbb{Q}$ à $\mathbb{R}$: raisonner par densité, en ne perdant pas de vue que f n'est pas continue *a priori*. Montrer que f est monotone : c'est mieux que rien et cela suffit pour conclure.
2. En considérant $f(x + iy)$ avec $(x, y) \in \mathbb{R}^2$, noter qu'expliciter $f(i)$ suffit à déterminer f. Or un morphisme préserve toutes les relations : connaissant une relation vérifiée par i, on en déduit une relation vérifiée par $f(i)$ (on peut faire le lien avec l'exercice 52, même si ici nous n'avons pas un isomorphisme *a priori*). Cela laisse un nombre très restreint de possibilités pour la définition de f.

Commentaires. La première question encourage à reconnaître des structures partout où il y en a, même quand ce n'est pas explicitement indiqué par l'exercice.
La stratégie de la seconde question est classique : une fois qu'on a compris qu'un morphisme de corps fixe le sous-corps premier (ou un autre corps, $\mathbb{R}$ ici), on étend progressivement son explicitation du sous-corps premier au corps entier par adjonction d'éléments (pour passer de $\mathbb{Q}$ à $\mathbb{Q}[\alpha]$, on doit « ajouter α »), et en considérant l'image de ces éléments par ce morphisme. Pour déterminer $f(\alpha)$, c'est à chaque fois la même idée : utiliser une équation vérifiée par α pour en déduire une équation vérifiée par $f(\alpha)$, ce qui limite le nombre de possibilités. C'est naturel puisqu'un morphisme injectif préserve la structure : il préserve aussi les solutions aux équations.
Lorsqu'on ne peut pas passer du « petit » corps au corps entier par le procédé ci-dessus, par exemple lorsqu'on veut passer de $\mathbb{Q}$ à $\mathbb{R}$ (ce qui ne peut se faire par une suite finie d'adjonctions d'éléments : il n'y a pas de famille finie qui engendre $\mathbb{R}$ sur $\mathbb{Q}$), la densité permet parfois de remplacer les raisonnements sur les parties génératrices, à la condition (suffisante) d'avoir de la *continuité*. Cependant les morphismes de corps ne sont pas toujours continus (et on peut même démontrer que, hormis l'identité et la conjugaison complexe, les automorphismes d'un sous-corps de $\mathbb{C}$ ne sont jamais continus !), ce qui complique les raisonnements par densité. Pas grave : la monotonie peut remplacer la continuité sans certains cas de figure, étant donné qu'une application monotone sur $\mathbb{R}$ admet des limites à gauche et à droite en tout point (ce qui est mieux que rien).
Les automorphismes d'un corps L fixant un sous-corps K forment le *groupe de Galois* de l'extension (L, K) (du moins, on utilise cette terminologie lorsque (L, K) est *galoisienne*, ce que je ne définirai mais qui consiste essentiellement à dire qu'il ne « manque pas d'automorphismes de L fixant K » par rapport à ce qu'on pourrait théoriquement espérer), et le théorème de correspondance de Galois formule, de manière plus explicite et plus impressionnante, qu'en connaissant ce groupe et tous ses sous-groupes, on connaît aussi tous les sous-corps contenant K et contenus dans L ; on les obtient tous en considérant les corps de la forme $\{x \in L \mid \forall \sigma \in G,\ \sigma(x) = x\}$ avec G un sous-groupe du groupe de Galois. Autrement dit : ce sont les points fixes des automorphismes de L fixant K qui permettent de décrire tous les sous-corps. Au fond, on le sait déjà dans certains cas particuliers : cet exercice démontre que le groupe de Galois de $\mathbb{C}/\mathbb{R}$ est $G = \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$, où $\sigma : z \mapsto \bar{z}$ est la conjugaison complexe. Ici, G n'a que deux sous-groupes : le sous-groupe réduit à l'élément neutre et lui-même. En considérant les points fixes dans $\mathbb{C}$ du sous-groupe $\{\mathrm{Id}_{\mathbb{C}}\}$, on obtient trivialement $\mathbb{C}$. En considérant les points fixes de G (ce qui revient à prendre les points fixes de la conjugaison complexe), on obtient $\mathbb{R}$. On obtient ainsi deux corps, et il n'y en a pas d'autre par un argument dimensionnel : si $\mathbb{R} \subseteq K \subseteq \mathbb{C}$, alors K est de dimension 1 ou 2 sur $\mathbb{R}$, donc par un argument dimensionnel il est égal à $\mathbb{R}$ ou $\mathbb{C}$. On a illustré la correspondance de Galois dans ce cas particulier (même si cette correspondance donne beaucoup plus de liens entre les sous-groupes du groupe de Galois et les corps intermédiaires entre K et L).

Exercice 54.

1. Le noyau de f est un sous-groupe de $\mathbb{Z}$. Raisonner sur les cardinaux pour exclure l'injectivité de f, et utiliser le théorème d'isomorphisme pour montrer que $\mathbb{Z}/\ker(f)$ doit être intègre. Conclure (on peut aussi s'en sortir sans

ce théorème, en supposant que p n'est pas premier et en regardant ce qu'impliquerait l'égalité $p = ab$). Faire le lien avec l'exercice 50.

2. La structure d'espace vectoriel est une vérification bête et méchante : presque tout découle de la structure de corps de K. Pour vérifier que c'est correctement défini : vérifier que si $\bar{k} = \bar{\ell}$ alors $f(k)x = f(\ell)x$. Immédiat d'après la question précédente et le théorème de factorisation des morphismes.
3. Montrer que K doit être un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie pour une raison de cardinal. Conclure en écrivant tout élément de K dans une base et en faisant du dénombrement.

Commentaires. Méditer le raisonnement de cet exercice à la lumière des commentaires de l'exercice 50, et éventuellement des autres exercices où l'algèbre linéaire s'invite subtilement.
La réciproque est vraie au sens suivant : pour tout nombre premier p et tout d entier naturel non nul, il existe un corps fini à p^d éléments (et il est unique à isomorphisme près). L'exercice 55 en donne des exemples, même s'il ne donne pas les constructions les plus naturelles et n'est pas généralisable.

Exercice 55. (Quelques exemples de corps finis)

1. Un recensement exhaustif des éléments de $\mathbb{Z}/3\mathbb{Z}$ est facile, et permet de faire la vérification à la main.
2. Si l'on note E et I les deux matrices qui engendrent K : montrer par un calcul que $I^2 \in K$ et $E^2 \in K$, et en déduire par linéarité que K est stable par produit. Pour montrer la commutativité : noter que E et I commutent. Pour montrer que tout élément non nul est inversible : conjecturer un inverse de tout élément $aE+bI$ non nul en remarquant une analogie entre les éléments de K et ceux d'un corps plus connu. Le cardinal est facile à obtenir : on a une base de cardinal 2, et il suffit donc de compter le nombre de coordonnées possibles.
3. Vérification bêtement calculatoire pour la structure d'anneau. Comme l'ensemble est de cardinal 4, faire sa table de multiplication à la main est raisonnable, et cela permet de vérifier l'inversibilité de tous ses éléments.
4. Un corps a toujours 0 et 1 comme éléments. Donner un nom aux deux autres éléments, et compléter la table d'addition et de multiplication du corps en utilisant les propriétés basiques de 0 et 1, puis le fait que dans chaque ligne ou colonne ne figure qu'une et une seule fois chaque élément, sauf pour la ligne ou colonne de 0 (pourquoi ?). Noter que ce corps contient $\mathbb{Z}/2\mathbb{Z}$ (cf. exercice 50). Remarquer qu'on tombe sur la table de multiplication obtenue à la question précédente.

Commentaires. Cet exercice propose une réciproque du résultat de l'exercice 55 dans des cas particuliers. Le chapitre IV fournira plus généralement des corps de cardinal p pour tout p premier, à savoir $\mathbb{Z}/p\mathbb{Z}$. C'est la seule famille de corps finis qui soit au programme.
On pourrait se demander quel est l'intérêt de ces corps finis apparemment artificiels. En fait, c'est la construction de cet exercice qui leur donne une apparence artificielle : ils s'obtiennent plus naturellement à partir de $\mathbb{Z}/p\mathbb{Z}$ par adjonction de racines, comme $\mathbb{C}$ fut obtenu à partir de $\mathbb{R}$ en ajoutant une racine carrée de -1. Par exemple, le corps à quatre éléments s'obtient en ajoutant à $\mathbb{Z}/2\mathbb{Z}$ une racine de X^2+X+1 (tout autre choix de polynôme donnerait un anneau non intègre ou du mauvais cardinal), et le corps à neuf éléments s'obtient en ajoutant à $\mathbb{Z}/3\mathbb{Z}$ une racine de X^2+1, ou de X^2-X+1, ou de X^2+X-1 (peu importe : on obtient des corps isomorphes).
Une fois qu'on a cela en tête, on comprend un intérêt des corps finis : créer des racines qui « manquent » pour poursuivre nos raisonnements. De la même manière que si l'on veut déterminer les suites *réelles* vérifiant $u_{n+2}+u_{n+1}+u_n = 0$, on a besoin de les exprimer en fonction de $j = \exp\left(\frac{2i\pi}{3}\right)$ et $\bar{j}$ (et donc de raisonner dans $\mathbb{C}$), vouloir expliciter les suites de $\mathbb{Z}/2\mathbb{Z}$ vérifiant la même relation nécessite d'avoir des racines de l'équation caractéristique $x^2+x+\bar{1} = \bar{0}$ d'inconnue $x \in \mathbb{Z}/2\mathbb{Z}$. Mais il n'y en a pas ! On se place alors dans un corps plus grand contenant $\mathbb{Z}/2\mathbb{Z}$ (en l'occurrence le corps de la troisième question) pour que cette équation ait des racines et qu'on puisse expliciter notre suite.
Petits prolongements possibles : 1° vérifier que $x \mapsto x^3$ est un automorphisme du corps de la question 2, et décrire ses points fixes : qu'obtient-on ? même question avec $x \mapsto x^2$ dans la question 3 ; on pourra faire le lien avec le théorème de correspondance de Galois brièvement décrit dans les commentaires de l'exercice 53, 2° vérifier que K^* est toujours cyclique, et trouver un ou plusieurs générateurs (comparer avec le résultat de l'exercice 13).

Exercice 56. L'idée est la même que dans l'exercice 22 : utiliser une permutation de la forme $x \mapsto yx$ pour simplifier la somme. Pour le produit : regrouper chaque élément avec son inverse. C'est néanmoins impossible pour les éléments égaux à leurs inverses : les déterminer et les isoler du produit.

Commentaires. Voir les commentaires de l'exercice 22.

Exercice 57. (🖹) Même idée que dans l'exercice 22 ou 56, mais en notant que le théorème de Lagrange permet de simplifier autrement les x^m dans certains cas.

Commentaires. Voir les commentaires de l'exercice 22. J'ajoute qu'on observe encore une fois que le théorème de Lagrange est naturellement présent lorsqu'il s'agit de simplifier des puissances d'éléments grâce à la connaissance du cardinal d'un groupe.

Classement des exercices par thèmes

Action de groupe déguisée	27, 28, 32, 36, 37, 38, 39, 40
Expliciter un morphisme	19, 20, 21, 24, 26, 31, 33, 53
Groupes cycliques	3, 12, 13, 17, 19, 20, 26
Nilpotence	43, 45, 46, 47, 48
Opérer par translation : $g \mapsto gx$	22, 36, 56, 57
Ordre d'un élément : calcul	2, 5, 7, 11
Principe de conjugaison	24, 27, 28, 31, 32, 35, 39
Principe des bergers	5, 6, 9, 23, 27, 28, 32, 38, 39, 40
Quasi-démonstration du cours	3, 16
Raisonnement arithmétique	4, 12, 28, 45
Sommes et produits indexés par un groupe fini	22, 56, 57
Sous-groupes de $(\mathbb{Z}, +)$ et applications	18, 50, 54
Structure d'espace vectoriel sous-jacente	10, 15, 54
Théorème de factorisation, d'isomorphisme	5, 23, 50, 54
Théorème de Lagrange et exponentiations	6, 20, 25, 57
Théorème de Lagrange et sous-groupes	1, 8, 10, 16, 25, 39
Un (iso)morphisme préserve la structure	14, 20, 21, 24, 26, 35, 50, 52, 53
Utilisation d'une partie génératrice	5, 15, 17, 19, 20, 26, 30, 32, 33, 35