Du cours aux exercices
Chapitre III — Structures algébriques

1 Aide à la révision du cours

1.1 Rappels et compléments

1.1.1 Sur les morphismes

Motivation de cette partie

On effectue quelques rappels sur les morphismes, en insistant sur la raison pour laquelle ils sont si intéressants : ils conservent presque tout, voire tout s'ils sont bijectifs, ce qui est relatif à la structure. Ainsi on peut les utiliser pour ramener l'étude de structures compliquées à celle de structures mieux connues.

Le principe moral des isomorphismes.

✓	Bien vérifier pourquoi $\Leftarrow$ nécessite l'injectivité. Est-ce que cela ne nécessite pas aussi d'être un morphisme ?
★	— Et pourquoi la surjectivité ? — Ayant en tête que deux groupes isomorphes sont « moralement les mêmes » ou « identifiables », comprendre pourquoi il est intuitif de conjecturer que les groupes suivants le sont : S_{n-1} et le groupe des permutations dans S_n fixant n ; $S_k \times S_{n-k}$ et le groupe des permutations dans S_n laissant stable $[\![1,k]\!]$, S_{n-k} et le groupe des permutations dans S_n laissant fixes les éléments de $[\![1,k]\!]$. — En déduire que ce principe moral des isomorphismes permet de rapidement montrer, par l'absurde, que des groupes ne sont pas isomorphes. Par exemple, S_3 et $\mathbb{U}_6$ sont-ils isomorphes ?

Exemple 1.

✓	— Montrer diverses variantes de ce résultat (le sens réciproque, ou : si $(x,y) \in G^2$, alors x et y commutent si et seulement si $f(x)$ et $f(y)$ commutent). Se demander à chaque fois si on peut remplacer la bijectivité par l'injectivité ou surjectivité. — Trouver un énoncé équivalent quand f est surjectif (et non nécessairement injectif). — Montrer de même qu'un isomorphisme préserve les inverses : $x, y \in G$ sont inverses l'un de l'autre si et seulement si $f(x)$ et $f(y)$ sont inverses l'un de l'autre.

Exemple 2.

✓	Proposer d'autres bijections analogues, entre les sous-groupes commutatifs de G et H par exemple, ou entre le centre de G (défini par : $\{g \in G \mid \forall g' \in G, gg' = g'g\}$) et celui de H, etc.

Exemple 3.

✓	— Vérifier que si f est un isomorphisme, alors A est intègre si et seulement si B l'est. — Montrer dans le cas des anneaux des résultats analogues à ceux obtenus plus haut pour les groupes. — Trouver un énoncé équivalent quand f est surjectif (et non nécessairement injectif).
★	Si $f : A \to B$ est injectif avec A intègre, peut-on en déduire que B est intègre ?

Après votre révision de cette partie

1. Faire un récapitulatif des propriétés se préservant par isomorphisme, ou par morphisme surjectif, ou par morphisme injectif. Vous pouvez de vous-mêmes étendre la liste à loisir.
2. **Lecture conseillée.** *Méthodes*, *Comment démontrer un isomorphisme* et *Comment utiliser un isomorphisme*.

3. Dans les *Savoir-faire à vérifier* : faire les 1°, 2° et 4° sur les structures.

1.1.2 Sur les relations d'équivalence

Motivation de cette partie

On montre comment les relations d'équivalence et, surtout, la notion d'ensemble quotient, permet de créer de nouveaux ensembles, en « rendant égales » des quantités qui, *a priori*, ne le sont pas, mais qu'on « aimerait rendre égales ». On illustre cette idée avec la construction d'ensembles connus depuis toujours ($\mathbb{Z}$, $\mathbb{Q}$, et plus tard $\mathbb{C}$).

Définition 1 (Relation d'équivalence, classe d'équivalence, ensemble-quotient)**.**

✓	— Se demander en quoi les trois propriétés d'une relation d'équivalence justifient que les relations d'équivalence « sont comme des égalités » (et c'est d'ailleurs ce qui justifie le choix de la définition). — Bien être au clair sur la nature de tous les objets : à quoi appartient $\mathrm{cl}_R(x)$? Et le représentant d'une classe ? Et un système complet de représentants ? (À chaque fois, en gros, la question est de savoir si cela appartient à $\mathcal{P}(E)$ ou si c'est inclus dans $\mathcal{P}(E)$). — Pour toutes les relations d'équivalence vues cette année et l'année dernière, se demander s'il est possible de décrire l'ensemble quotient E/R aussi explicitement que possible, avec un système complet de représentants. — Vérifier l'équivalence entre toutes les façons de décrire un système complet de représentants.
★	Et pour une relation d'ordre, pourrait-on définir un analogue des classes d'équivalence et des ensembles quotients ?

Notations.

✓	Se demander quels sont les avantages et défauts de chaque notation. À chaque notation introduite en mathématiques, les questions sont les mêmes : confort de rédaction, risque de confusion sur la nature de l'objet ou avec une notation proche, dépendances implicites susceptibles d'être oubliées ou au contraire pas bien graves, etc.

Exemple 4.

★	Que penser de l'application $g : E/R \to F$ définie $\mathrm{cl}_R(x) \mapsto f(x)$ (dont on vérifiera d'abord qu'elle est correctement définie) ? Pourquoi illustre-t-elle bien l'objectif des relations d'équivalence, qui est de « rendre égales » des quantités qui ne le sont *a priori* pas ? On reviendra là-dessus plus tard (théorèmes 8 et 14).

Proposition 2 (Propriétés de base)**.**

✓	Les démontrer, en identifiant où servent les trois propriétés d'une relation d'équivalence.
★	Cette proposition admet-elle une réciproque ? C'est-à-dire, si des parties E_i de E vérifient : $E = \bigsqcup_{i\in I} E_i$, est-ce qu'il existe une relation d'équivalence R sur E telle que : $E/R = \{E_i \mid i \in I\}$?

Théorème 3 (Existence et minimalité du corps des fractions)**.**

✓	— Vérifier ce que je n'ai pas détaillé dans ma démonstration. On s'attachera à comprendre : 1° où sert l'intégrité de A, 2° pourquoi il faut prendre $b \in A \setminus \{0\}$ au lieu de $b \in A$. — Est-ce que la commutativité est essentielle ? — S'inspirer de cette construction pour définir l'anneau $\mathbb{D}$ des décimaux sans même construire $\mathbb{Q}$. Vous aurez ainsi construit le premier *anneau localisé* de votre vie. Émus ?

★	— L'énoncé dit explicitement que A n'est pas inclus dans $\mathrm{Frac}(A)$ mais qu'on s'y ramène en raisonnant par isomorphisme. Essayer de comprendre pourquoi, d'un point de vue logique, c'est inévitable de raisonner ainsi : on ne peut pas fabriquer le corps des fractions de A comme un ensemble contenant directement A. — Si A n'est pas intègre, j'affirme qu'il n'y a pas grand'chose à modifier à la relation d'équivalence pour malgré tout donner un sens à $\frac{a}{s}$ avec $a \in A$ et $s \in S$, où S est l'ensemble des éléments de A qui ne divisent pas 0_A. — Montrer l'*unicité* du corps L, à isomorphisme près, à vérifier la propriété suivante : il existe un morphisme injectif de A dans L, et pour tout corps K contenant A, le corps K contient un sous-corps isomorphe à L.
☢	Proposer une construction qui autorise la division par zéro (mais on perd alors la structure d'anneau, par exemple $0 \cdot x = 0$ n'est plus vrai pour tout x). La structure ainsi obtenue s'appelle une *roue*. Elle n'est pas très intéressante.

Exemple 5.

✓	Se demander si d'autres anneaux de votre cours de 1re année admettent un corps des fractions (cela revient à se demander s'ils sont commutatifs et intègres), et si oui : expliciter ces corps de fractions.
★	Avec cette définition de $\mathbb{Q}$, définir ou démontrer toutes les propriétés que vous connaissez bien. Par exemple, comment définir $\leqslant$ sur $\mathbb{Q}$, en considérant la définition de $\leqslant$ sur $\mathbb{N}$ ou $\mathbb{Z}$ acquise ? Et comment vérifier que l'inégalité reste compatible avec la multiplication par un rationnel positif (ce qu'il convient bien sûr de définir), etc. ?

Exercice 1. (Construction de $\mathbb{Z}$)

✓	— Le faire, et se demander à quelle structure cette construction se généralise. — Qu'est-ce qui motive la définition des lois $\oplus$ et $\otimes$? Notamment, pourquoi le fameux « $-$ par $-$ donne $+$ » ?
★	— Se poser la même question qu'avec $\mathbb{Q}$ pour la définition de $\leqslant$ (en considérant que $\leqslant$ est déjà définie sur $\mathbb{N}$). — Et $\mathbb{N}$? Comment est-il construit ? Cela ne s'invente pas et vous aurez sans doute besoin de vous documenter.

Après votre révision de cette partie

Seule l'idée morale des ensembles quotients est vraiment à retenir. Vous pouvez cependant vous amuser à loisir, en regardant ce que vous obtenez comme ensembles en vous autorisant toutes sortes « d'identifications », y compris les plus délirantes imaginables. Pour avoir des idées, il vaut peut-être mieux attendre les sections suivantes.

1.1.3 Groupes quotients

Motivation de cette partie

On introduit un cas particulier très important de groupe quotient, qui permet le calcul *modulaire*. Vous en connaissez déjà un exemple : le calcul modulo n (qui revient à « poser $n = 0$ » dans $\mathbb{Z}$). Il s'agit de le généraliser, pour pouvoir parler de calculer « modulo H » (qui revient à « poser $h = e_G$ » pour tout $h \in H$). Vous faisiez déjà du calcul modulo n sans parler de groupe quotient et on peut donc se questionner sur l'intérêt de cet excès de formalisme : c'est pour que les théorèmes sur les groupes permettent de simplifier, justement, le calcul modulo n (il y a d'autres motivations).

Définition-Proposition 4 (Relation d'équivalence associée à un sous-groupe)**.**

✓
- — Dans la démonstration, se demander où les différentes propriétés caractérisant un sous-groupe interviennent (j'affirme qu'on en a besoin pour TOUTES les vérifications que c'est une relation d'équivalence).
- — Et si l'on remplace $g_1^{-1}g_2 \in H$ par $g_2^{-1}g_1 \in H$, est-ce que cela change la proposition ? Même question en changeant la place de l'exposant -1.
- — Prendre des exemples (par exemple S_3 et H un sous-groupe de la forme $\{\mathrm{Id}, \tau\}$ avec τ une transposition, ou $\{\mathrm{Id}, (1\,2\,3), (1\,2\,3)^2\}$, etc., mais les exemples ne manquent pas : considérer $\mathbb{U}_n$ et ses sous-groupes par exemple !). Compter le nombre de classes et le cardinal de chacune d'entre elles (dans le cas où le groupe ambiant est fini). Les expliciter dans la mesure du possible. Qu'observez-vous de remarquable ? Vous pourrez vérifier que vous ne vous trompez pas avec le théorème de Lagrange plus loin (théorème 6).
- — Pour s'assurer que la démonstration est bien comprise : si H et K sont deux sous-groupes de G, montrer que la relation définie par : $\forall (g_1, g_2) \in G^2$, $g_1 \sim g_2 \iff \exists (h, k) \in H \times K$, $g_2 = hg_1k$, est une relation d'équivalence, et décrire les classes (on parle de « double classe »).

Remarque.

✓ Décrire les classes dans le cas additif, si je ne l'ai pas fait en cours.

Le principe moral des groupes quotients.

★ Il semble que je mente un peu : l'égalité $g_1 = hg_2$ ne semble pas se simplifier quand on passe aux classes. Si vous avez joué le jeu plus haut, en fabriquant différents ensembles quotients, vous trouverez peut-être des contre-exemples. Dans la suite de ce cours, vous vérifierez cependant que je me place toujours dans un cas de figure où c'est *vrai* que $g_1 = hg_2$ implique $\overline{g_1} = \overline{g_2}$.

Définition-Proposition 5 (Définition de $\mathbb{Z}/n\mathbb{Z}$ et système complet de représentants)**.**

✓
- — Vérifier que $n\mathbb{Z}$ est effectivement un sous-groupe de $\mathbb{Z}$.
- — Et si $n = 0$, que donne l'ensemble quotient $\mathbb{Z}/\{0\}$? Pourquoi n'en parlé-je pas dans cette proposition ?

Notation.
Remarque.

✓ Se demander quel peut être l'intérêt d'avoir ces autres systèmes complets de représentants (indication : l'intérêt peut être dans les *calculs* dans $\mathbb{Z}/n\mathbb{Z}$).

Théorème 6 (Théorème de Lagrange)**.**

✓
- — Comparer ce qu'annonce ce résultat avec ce que vous avez observé sur des exemples concrets.
- — S'assurer qu'on sait le démontrer de A à Z, y compris avec les propositions auxquelles on renvoie. En effet, c'est un résultat hors programme et vous devez savoir le démontrer si besoin.
- — **Lecture conseillée.** *Méthodes*, *Utiliser le théorème de Lagrange.*
- — Est-il possible d'avoir G/H de cardinal fini bien que G ne le soit pas ? Et si G et H sont infinis, peut-on dire quelque chose de général sur le cardinal de G/H ?

Proposition 7 (Groupes quotients remarquables)**.**

✓
- — Vérifier ce que je n'ai pas vérifié, relativement à la structure de groupe (associativité, existence du neutre).
- — Formuler « les relations dans G sont conservées dans G/H » avec un morphisme surjectif $\pi : G \to G/H$ peut paraître inutilement pédant. Pourtant j'affirme que non, la formulation avec le morphisme est vraiment intéressante : pourquoi ?
- — Que donne G/G ? Et $G/\{e_G\}$? Ont-ils une une structure de groupe compatible avec celle de G ?)

★	— Réciproquement, est-ce que, si G/H est un groupe de sorte que $\pi : G \to G/H$ soit un morphisme, alors G est commutatif ou H de la forme $H = \ker(f)$? — Pourquoi cette vérification que la loi est « correctement définie » ? Pour comprendre qu'il peut y avoir un vrai problème : considérer $G = S_3$ et $H = \{\mathrm{Id}, (1\ 2)\}$, et montrer qu'on tombe sur une bizarrerie si l'on veut définir une loi de groupe sur G/H en posant $\bar{\sigma}\bar{\tau} = \overline{\sigma\tau}$ pour tout $(\bar{\sigma}, \bar{\tau}) \in (G/H)^2$. — Soit G un groupe fini. Montrer qu'on peut toujours définir, et de plein de façons différentes, une loi de groupe sur G/H, en partant d'une bijection avec $[\![1, n]\!]$ où $n = \mathrm{card}(G/H)$ (si vous séchez : se poser éventuellement la question après le corollaire 13). Comprendre sous un autre œil, alors, l'exigence de la compatibilité avec le morphisme $\pi : G \to G/H$. — J'utilise le terme « distingué » pour les sous-groupes vérifiant (a) ou (b). Vous pouvez si vous le souhaitez vous documenter sur la notion générale (et hors programme) de *sous-groupe distingué*. On en rencontrera d'autres, mais sans le dire.
☢	Montrer que si R est une relation d'équivalence telle que G/R soit un groupe qui fasse de $\pi : G \to G/R$ un morphisme, alors c'est nécessairement la relation d'équivalence associée à un sous-groupe de G, qui vérifie de plus... ?

Théorème 8 (Théorème de factorisation des morphismes, théorème d'isomorphisme)**.**

✓	— Pourquoi le théorème d'isomorphisme est-il « intuitif » et aurait pu être conjecturé en se souvenant : 1° que f est injectif si et seulement si $\ker(f)$ est trivial, 2° que passer au quotient, c'est rendre triviaux des éléments ? — Réciproquement, si $\bar{f}$ est injectif, est-ce que $H = \ker(f)$? — En utilisant la relation d'équivalence de l'exemple 4, généraliser cet énoncé (ou du moins une partie) à toute application, même s'il n'y a pas de structure sur les ensembles. C'est potentiellement utile même en théorie des groupes, lorsqu'on fait des *actions de groupe* (parce qu'on y manipule des applications surjectives entre des groupes et des ensembles qui n'en sont pas). — Comprendre pourquoi le théorème d'isomorphisme permet de dire : si $f : G \to K$ est un morphisme, alors $G/\ker(f)$ s'identifie à un sous-groupe de K. — Faire le lien avec la première section sur les morphismes, où j'ai mis en valeur l'importance de la bijectivité ou injectivité à plusieurs reprises, mais pas la surjectivité : pouvez-vous utiliser le théorème d'isomorphisme pour avoir un énoncé analogue à ceux des exemples, mais avec f surjective ?
★	— Est-ce que les quotients se « simplifient » comme des vrais quotients ? (C'est-à-dire : est-ce que $(G/K)/(H/K)$ est isomorphe à G/H, lorsque tout cela a un sens ?)

Exemple 6.

✓	— Expliciter les classes de $\mathbb{R}/2\pi\mathbb{Z}$ pour comprendre ce qu'est « concrètement » ce groupe. À comparer avec $\mathbb{Z}/n\mathbb{Z}$. — Pourquoi cet isomorphisme est-il « naturel », au vu de la philosophie des isomorphismes ? Cette question attend à la fois une réponse algébrique et géométrique : à quoi « ressemble » l'axe réel lorsqu'on identifie les points séparés d'un multiple entier de 2π ? — Quel est l'isomorphisme réciproque de celui de cet exemple ? J'affirme qu'en méditant cet isomorphisme réciproque, vous pourrez trouver un intérêt supérieur de $\mathbb{R}/2\pi\mathbb{Z}$ sur $[0,2\pi[$ ou $]-\pi,\pi]$. — Regarder ce qu'enseigne le théorème d'isomorphisme pour d'autres morphismes qui vous viennent à l'esprit. Il y en a des très basiques ($x \mapsto x^2$ par exemple, de $\mathbb{R}^*$ ou $\mathbb{C}^*$ dans lui-même), ne cherchez pas forcément très loin. Il est très important de suivre ce conseil, car c'est *via* l'application de ce théorème que vous allez vous approprier les groupes quotients, s'ils sont trop abstraits pour vous ! En effet, dès que vous l'appliquez à un morphisme, il vous permet d'écrire un isomorphisme entre un groupe quotient et un groupe sans quotient (dans le cas de $x \mapsto x^2$, c'est entre $\mathbb{R}^*/\{-1,1\}$ et $\mathbb{R}_+^*$, par exemple) : en méditant pourquoi l'isomorphisme est « naturel », vous comprendrez mieux ce que représente le groupe quotient.
★	— À quoi sont isomorphes de simple les groupes quotients $(\mathbb{R}/\mathbb{Z})^2$, $\mathbb{R}^2/\mathbb{Z}^2$, $\mathbb{R}^2/(\mathbb{Z}\times\{0\})$, $\mathbb{R}^*/\{-1,1\}$, $\mathbb{R}^*/\mathbb{R}_+^*$, $\mathbb{C}^*/\mathbb{U}$, $\mathbb{C}^*/\mathbb{R}_+^*$, $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$? Dans la mesure du possible, les interpréter algébriquement et géométriquement. — Essayer d'obtenir un ruban de Möbius et une bouteille de Klein avec un ensemble quotient (ce n'est pas un groupe quotient). Pour ce faire : se demander ce qu'on veut identifier (la construction « manuelle » d'un ruban de Möbius donne aussi la construction abstraite), et introduire une relation d'équivalence qui le permet.

Exemple 7.

✓	— Se convaincre que la réunion est disjointe. — Observer que le théorème d'isomorphisme démontre en même temps la finitude de $\mathrm{im}(f)$. — Attention aux raisonnements par analogie avec les espaces vectoriels : le théorème du rang est avec une somme de dimensions, ici nous avons un produit de cardinaux. Avez-vous d'autres exemples de formules sur les cardinaux faisant apparaître un produit, et dont l'analogue linéaire fait apparaître une somme ? L'expliquez-vous ?
★	— Réciproquement, est-ce que cette identité impliquerait le théorème de Lagrange ? — Si f est à valeurs dans un groupe fini, est-ce que cela enseigne quelque chose sur le cardinal de G et $\ker(f)$? — Est-ce que les deux démonstrations proposées ici présentent des analogies avec celle du théorème du rang ?
☢	Réciproquement, pouvait-on démontrer le théorème du rang avec un théorème d'isomorphisme ?

Après votre révision de cette partie

Lecture conseillée. *Méthodes*, *Utiliser le théorème de Lagrange*, si ce n'est pas encore fait.

1.1.4 Anneaux quotients

Motivation de cette partie

Même principe que dans la section précédente, mais avec les anneaux. C'est l'occasion de définir les idéaux, qui est la sous-structure réellement intéressante dans un anneau (bien davantage que les sous-anneaux).

Définition 9 (Idéal d'un anneau)**.**

✓	Comparer cette définition à celle d'un sous-espace vectoriel d'un espace vectoriel.
★	Pourquoi se place-t-on dans le cas commutatif ? Éventuellement se poser la question après avoir vu quelques exemples et propositions.

Proposition 10 (Intersection et somme d'idéaux)**.**

✓	Se convaincre que la propriété se généralise effectivement à une intersection quelconque d'idéaux. Et pour la somme ? Quel sens, d'ailleurs, donner à une somme (indexée par un ensemble infini) d'idéaux ? Penser à la situation analogue dans le cas des espaces vectoriels.

Proposition 11 (Exemples d'idéaux, idéaux principaux)**.**

✓	— Est-ce que le noyau d'un morphisme d'anneaux est un sous-anneau de l'anneau de départ ?
★	— Si A n'est plus supposé commutatif, qu'est-ce qui coince dans la démonstration ? — Est-ce que l'image d'un morphisme d'anneaux est un sous-anneau de l'anneau d'arrivée ? — Est-ce que l'idéal engendré par $a_1, \dots, a_n$ vérifie une propriété de minimalité au même titre que le sous-espace vectoriel engendré par une famille de vecteurs ? Est-ce qu'on n'aurait pas pu le définir ainsi ?

Proposition 12 (Anneaux quotients)**.**

✓	— Se convaincre qu'il n'y a pas ambiguïté dans la compréhension de A/I : pourquoi n'y a-t-il pas à hésiter pour savoir si, dans A/I, on « pose » $i = 0_A$ pour tout $i \in I$, ou $i = 1_A$ pour tout $i \in I$? — Vérifier ce que je n'ai pas vérifié, relativement à la structure d'anneau (distributivité, associativité). — Est-ce que la commutativité intervient dans cette définition et démonstration ? — Que donne l'anneau quotient A/A ? Et $A/\{0_A\}$?

★	— Réciproquement, est-ce que, si A/I est un anneau de sorte que $\pi : A \to A/I$ soit un morphisme, alors I de la forme $I = \ker(f)$? — Pourquoi cette vérification que la loi est « correctement définie » ? — Est-ce que, si A est commutatif, alors A/I est commutatif, et si oui pourquoi ? Même question avec l'intégrité et la structure de corps. — Imiter ce qu'on a fait pour les groupes et anneaux, en définissant des espaces vectoriels quotients. C'est intéressant si vous essayez d'en tirer quelques propriétés : dimension d'un espace vectoriel quotient, par exemple ?
☢	Réciproquement, si R est une relation d'équivalence telle que A/R soit un anneau qui fasse de $\pi : A \to A/R$ un morphisme d'anneaux, est-ce que c'est nécessairement la relation d'équivalence associée à un idéal de A ?

Corollaire 13 ($\mathbb{Z}/n\mathbb{Z}$ est un anneau)**.**

✓	— Vous remarquez que j'inclus $n = 1$ à ce corollaire. Que pensez-vous de ce choix ? — J'affirme que cet énoncé est une reformulation de quelque chose que vous savez depuis longtemps. Pourquoi ?

Exemple 8.

✓	— Retrouver de même un critère de divisibilité par 3, 5, 9 et 10 (voire 4, même s'il est moins « efficace »). — Pourquoi cet exemple illustre-t-il l'utilité que les lois sur $\mathbb{Z}/n\mathbb{Z}$ font de $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ un morphisme d'anneaux ?
★	Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer ce qui permet d'avoir un critère de divisibilité par n basé sur l'écriture en base 10 (vous pouvez vous poser la question de l'efficacité du critère séparément).

Exemple 9.

✓	Montrer *vraiment* que $\iota : a \mapsto \bar{a}$ est un morphisme *injectif* de $\mathbb{R}$ dans $\mathbb{C}$. Justifier ensuite, par un autre argument, que ι l'est nécessairement (sans calcul).
★	— Réciproquement, si l'on avait construit $\mathbb{C}$ par un autre moyen, expliquer comment on aurait obtenu un isomorphisme entre $\mathbb{R}[X]/I$ et $\mathbb{C}$. — Varier les plaisirs : que donne concrètement $\mathbb{R}[X]/(X-a)$ avec $a \in \mathbb{R}$? et $\mathbb{R}[X]/(X^2-1)$? et $\mathbb{C}[X]/(X^2+1)$? et $\mathbb{Z}/2\mathbb{Z}[X]/(X^2+1)$? et $\mathbb{Z}/3\mathbb{Z}[X]/(X^2+1)$? etc. La seule limite est votre imagination. (J'affirme que les réponses sont radicalement différentes dans chacun des exemples que je propose.)
☢	— Montrer que $\mathbb{C}$ est le plus petit corps (en un sens à préciser) contenant $\mathbb{R}$ et une racine du polynôme X^2+1. — Aurait-on pu construire $\mathbb{Z}$ et $\mathbb{Q}$ de la même manière, en quotientant par un idéal ?

Exercice 2.

★	— Le faire. Si vous tombez sur une bizarrerie, c'est normal : c'est le but ! On s'efforcera de l'expliquer. — Varier les exemples, en changeant 4 par d'autres entiers naturels non nuls et $2X-1$ par d'autres polynômes (de degré 1 d'abord, et vous pouvez varier les plaisirs ensuite).

Culture scientifique.

★	Montrer que $\mathbb{R}$ est un corps. Le reste est plus difficile à obtenir.

Théorème 14 (Théorème de factorisation des morphismes d'anneaux)**.**

✓	— On remarque que l'énoncé du premier item n'est pas exactement le même que pour les groupes. Pourquoi ? — Reprendre les commentaires du théorème 8.

1.2 Groupes

1.2.1 Partie génératrice, groupe monogène, ordre d'un élément

Motivation de cette partie

Vous voulons ici imiter l'algèbre linéaire, où plusieurs résultats peuvent se démontrer en raisonnant sur une base ou une partie génératrice. Après avoir défini la partie génératrice d'un groupe, nous nous attarderons sur les groupes engendrés par un seul élément (cas ultra-favorable où l'étude d'un seul élément peut s'étendre à tout le groupe), qu'on appelle les groupes monogènes ou cycliques. L'important théorème de Lagrange, et la caractérisation de l'ordre d'un élément, aideront à déterminer si un groupe est cyclique, ou à exploiter cette donnée.

Lemme 15 (Intersection de sous-groupes)**.**

✓	Faire la démonstration.

Définition-Proposition 16 (Partie génératrice d'un groupe, sous-groupe engendré par une partie, ordre d'un élément)**.**

✓	— Si S est vide, que donne $\langle S\rangle$? — Dans la démonstration de (b), vérifier effectivement que le membre de droite de l'égalité à démontrer est un sous-groupe de G. — Se convaincre que G admet *toujours* une partie génératrice. — Est-ce qu'un groupe infini peut avoir une partie génératrice finie ? — Est-ce que dans un groupe fini, tout élément est d'ordre fini ? — Dans $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{U}_n$ (avec n explicite), S_3, S_4, S_5, etc., $\mathrm{GL}_n(K)$, éventuellement d'autres groupes : considérer des éléments explicites et leurs sous-groupes engendrés. Varier le nombre d'éléments dans les parties génératrices. Comparer les cardinaux des sous-groupes obtenus. Qu'observez-vous de remarquable ? — Tout au long du chapitre : se demander pourquoi l'ordre d'un élément nous intéresse particulièrement (il peut y avoir de très nombreuses réponses à cette question).
★	— Pour motiver cette définition de $\langle S\rangle$: montrer que s'il existe un plus petit élément de $\{H \in \mathscr{S}(G) \mid S \subseteq H\}$ pour la relation d'ordre $\subseteq$, alors ce doit être $\bigcap_{\substack{H\in\mathscr{S}(G)\\ S\subseteq H}} H$. — Peut-on de même définir l'idéal d'un anneau engendré par une partie ? (À comparer avec les idéaux $\sum_{i=1}^{n} a_i A$, et se demander quel avantage aurait une définition des idéaux engendrés par une partie qui serait calquée sur la définition d'un sous-groupe engendré.) Ou un sous-corps engendré par une partie ?

Remarque.

✓	— À quoi cette description explicite ressemble-t-elle, dans un autre contexte que celui de ce chapitre ? — Et en notation multiplicative, toujours dans le cas commutatif, quelle est la description ?

Remarque.
Remarque.

Définition 17 (Groupe monogène, groupe cyclique)**.**

✓	Tout au long du chapitre : se demander pourquoi ces groupes nous intéressent particulièrement.

Remarque.
Remarque.

✓	Et pour $n = 1$ et $n = 2$, est-ce que S_1 et S_2 sont cycliques ?

Exemple 10. ♡

✓	Et est-ce que les sous-groupes de $\mathbb{U}_n$ sont tous cycliques ? Éventuellement reprendre cette étude plus tard.
★	On a proposé $e^{\frac{2i\pi}{n}}$ comme générateur. Pouvez-vous en proposer d'autres ? Lesquels ? Combien y a-t-il de possibilités ?

Proposition 18 (Les groupes $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ sont monogènes)**.**

✓	Considérer d'autres groupes vus en 1re année et dire s'ils sont monogènes : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}^*$, $\mathbb{U}$, $\mathrm{GL}_p(K)$.

Lemme 19 (Les sous-groupes de $\mathbb{Z}$)**.**

✓	— Bien comprendre la philosophie de la démonstration (pourquoi avoir traité le cas $H = \{0\}$ à part ? pourquoi prendre $n = \min(H \cap (\mathbb{N} \setminus \{0\}))$? pourquoi faire une division euclidienne ?). Toutes les étapes ont une raison d'être et on pouvait y être amené par une analyse-synthèse intelligente. On reverra de tels raisonnements. — Que vient faire ce lemme ici ? Dans la progression du cours, pourquoi est-il *naturel* de s'intéresser aux sous-groupes de $\mathbb{Z}$ en vue d'étudier les groupes monogènes en général, et l'ordre d'un élément ? Se poser éventuellement la question en finissant la section.
★	— Utiliser ce lemme pour répondre à cette question : un groupe peut-il être isomorphe à ses sous-groupes stricts ? — En essayant d'imiter cette démonstration dans d'autres groupes (Soit $(G, +)$ un groupe commutatif. Est-ce que ses sous-groupes sont tous de la forme $\langle g \rangle = g\mathbb{Z}$ avec $g \in G$?), et en échouant éventuellement, comprendre la propriété spécifique à $\mathbb{Z}$ qui est la clé de ce résultat. Que connaissez-vous comme autres ensembles vérifiant la même propriété ? Essayer d'imiter la démonstration *dans ce cas précis*.

Proposition 20 (Caractérisation de l'ordre d'un élément)**.**

✓	— J'ai supposé que g est d'ordre fini d'emblée. Et s'il existe un entier naturel non nul k tel que $g^k = 1_G$, peut-on en déduire que g est d'ordre fini ? — Se convaincre de l'item (b) dont je n'ai pas détaillé la démonstration. Pourquoi le fait d'être le plus petit élément pour la relation de divisibilité est infiniment plus intéressante que l'être pour la relation d'ordre $\leqslant$? — Déduire de cette proposition un moyen de démontrer qu'un groupe N'EST PAS cyclique.
★	— Démontrer autrement l'item (a), sans le théorème d'isomorphisme. Vous aurez besoin d'une division euclidienne. — Proposer une autre démonstration de l'item (c). Voyez-vous pourquoi j'ai décidé de procéder plutôt ainsi ? — Se demander quand il est plus pertinent, dans un exercice, d'utiliser la définition de l'ordre de g comme cardinal de $\langle g \rangle$, ou sa caractérisation comme plus petite puissance de g qui donne 1_G (au sens de la relation de divisibilité). Se poser à nouveau la question après chaque utilisation de l'ordre en exercice ou dans le cours.

Exemple 11.

✓	Vérifier que $\sigma^p = \mathrm{id}$ si σ est un p-cycle, si je ne l'ai pas vérifié en détail en cours.
★	— J'ai montré que $\sigma^k \neq \mathrm{id}$ pour tout $k < p$ si σ est un p-cycle. Mais peut-on être plus précis ? Quelle est la décomposition en cycles à supports disjoints de σ^k en fonction de p et de k ? — Calculer σ^k pour tout $k < 6$. Peut-on prédire *a priori* la décomposition en cycles à supports disjoints de σ^k ? — Peut-on donner l'ordre d'une permutation quelconque en fonction de la longueur des cycles de sa décomposition à supports disjoints ?

☢	Conjecturer l'ordre de grandeur de l'ordre maximal d'un élément de S_n. Vous aurez probablement besoin d'une estimation du ppcm de n entiers consécutifs (voir le devoir maison n° 3).

Exemple 12. ♡

✓	Généraliser à $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$ avec les m_i premiers entre eux (deux à deux ou dans leur ensemble).
★	— Réfléchir à ce qui put mener à multiplier tout élément de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ par le ppcm de m et n. Cela peut se trouver par analyse, grâce aux propositions précédentes : si un entier ℓ vérifie $\ell(a \bmod m, b \bmod n)$ pour tout $(a \bmod m, b \bmod n)$, que peut-on dire de ℓ ? — Et si m et n sont premiers entre eux, que dire ?

Proposition 21 (Compatibilité des morphismes avec les parties génératrices et l'ordre des éléments)**.**

✓	— Compléter le principe moral des isomorphismes avec les résultats de cette proposition. — Reformuler l'égalité $\langle f(S)\rangle = f(\langle S\rangle)$ en termes simples, et la rapprocher d'un résultat proche en algèbre linéaire. — Pour chaque raisonnement « abstrait » dans la démonstration : essayer d'obtenir le même résultat par un raisonnement concret (nécessitant une manipulation explicite des éléments de S et de G, des calculs, etc.).
★	Réciproquement, si f transforme une partie génératrice de G en une partie génératrice de H, est-ce que f est surjectif ?

Théorème 22 (Théorème de Lagrange : le cas particulier au programme)**.**

✓	— **Lecture conseillée.** *Méthodes*, *Utiliser le théorème de Lagrange* (si cela n'a pas été fait auparavant). — Pourquoi ce théorème paraît remarquable si on le reformule en termes de « racines de l'unité » ?
★	Dans le cas où H est un sous-groupe de G distingué : noter que ce théorème permet d'expliciter un entier non nul k (plus petit en général que le cardinal du groupe) tel que : $\forall g \in G$, $g^k \in H$. Pourquoi ?

Exercice 3.

★	— Faire les deux démonstrations, et se demander pourquoi la première démonstration nécessite la commutativité. — S'amuser en regardant ce que donne φ_g pour des éléments concrets g d'un groupe concret G (prendre $\mathbb{Z}/n\mathbb{Z}$ par exemple) : effectuer la décomposition en cycles à supports disjoints et calculer la signature.

Exemple 13. ♡

✓	On montre davantage que le simple fait que G soit cyclique : quoi donc ?
★	— Montrer de même que si G est commutatif et de cardinal p^2, avec p premier, alors soit G est cyclique, soit G est engendré par deux éléments d'ordre p. — Montrer le même résultat en utilisant le morphisme injectif de G dans S_G de l'exercice ci-dessus : à quoi ressemble nécessairement un sous-groupe de cardinal p dans S_p ?

Exemple 14.

✓	— Pour déterminer l'ordre de $\bar{3}$, pourquoi ai-je choisi de d'abord calculer 3 à la puissance 6, 10 et 15 ? Pourquoi ne pas avoir commencé par 2, 3 et 5 ? — Une fois le chapitre IV achevé : pourquoi sait-on que $(\mathbb{Z}/31\mathbb{Z})^\times$ est d'ordre 30 ? — Est-ce que notre exemple permet, *a posteriori*, de démontrer que $(\mathbb{Z}/31\mathbb{Z})^\times$ est effectivement d'ordre 30 ? — S'entraîner avec d'autres groupes multiplicatifs $(\mathbb{Z}/n\mathbb{Z})^\times$, avec n de taille raisonnable : déterminer les ordres de tous ses éléments, ainsi que ses générateurs lorsqu'il en existe. Établir une conjecture concernant les valeurs de n qui donnent un groupe cyclique. Pour économiser les calculs, ne perdez pas de vue qu'il y a des systèmes complets de représentants plus intelligents, parfois, que $[\![0, n-1]\!]$. — Puisque $\bar{3}$ engendre $(\mathbb{Z}/31\mathbb{Z})^\times$, cela veut dire que $\bar{2}$ est une puissance de $\bar{3}$. Laquelle ? (Vous pouvez la conjecturer, au vu de l'ordre de $\bar{2}$).
★	On a montré que $\bar{3}^{15} = -\bar{1}$: pourquoi était-ce prévisible ? Pourquoi a-t-on $\bar{x}^{15} = \pm\bar{1}$ pour tout $\bar{x}$ dans $(\mathbb{Z}/31\mathbb{Z})^\times$? Attention, il y a un argument non trivial à invoquer : la primalité de 31 intervient.

Proposition 23 (Tout groupe monogène est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$)**.**

✓	Démontrer l'isomorphisme proposé sans passer par le théorème de factorisation, qui est hors programme (cela revient à démontrer « à la main » que l'application $k \bmod n \mapsto g^k$ est correctement définie et injective).

Remarque.

✓	Pourquoi fais-je cette remarque ? À quoi peut-elle nous servir ? Y réfléchir éventuellement plus tard, après avoir étudié les propriétés du groupe $\mathbb{Z}/n\mathbb{Z}$ dans la section suivante.

Remarque.
Remarque.

✓	Trouver des cardinaux pour lesquels il n'y a pas unicité à isomorphisme près. Il n'y a pas besoin de chercher des cardinaux élevés.

Après votre révision de cette partie

Dans les *Savoir-faire à vérifier*, faire les 1°, 3°, 4° et 6° de *L'étude spécifique des groupes.*

1.2.2 Le sous-groupe cyclique de référence : $\mathbb{Z}/n\mathbb{Z}$

Motivation de cette partie

Puisque tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, cela veut dire : quiconque connaît par cœur le groupe $\mathbb{Z}/n\mathbb{Z}$ comprend tous les groupes cycliques. C'est l'objectif de cette section, avoir une connaissance exhaustive de tous les groupes cycliques à l'aide de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 24 (Les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les éléments premiers avec n)**.**

✓	Démontrer cette proposition de manière effective, c'est-à-dire : montrer que si k et n sont premiers entre eux, alors tout $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ s'écrit : $\bar{x} = u \cdot \bar{k}$, avec $u \in \mathbb{Z}$ *construit effectivement* (au sens où : la démonstration fournit un moyen d'expliciter u si besoin).
★	— Au vu de la formulation de la proposition, il semble que pour tout représentant de la classe $\bar{k}$, le pgcd avec n soit le même. Pourquoi ? — Au vu de ce qu'on veut montrer, j'affirme que passer par le théorème de Bézout est une idée loin d'être saugrenue : comment pourrait-on réécrire : $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists u \in \mathbb{Z}$, $\bar{x} = u \cdot \bar{k}$, qui équivaut au fait que $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$, de sorte à faire apparaître une relation de Bézout sans forcer ?

Exercice 4.

★	Montrer que le résultat de cet exercice, et la proposition précédente, sont équivalents, en étudiant savamment l'endomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ défini par $\bar{x} \mapsto \bar{k}\bar{x}$.

Exemple 15.

✓	— Démontrer que $\bar{2}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si 2 est impair, sans recourir à la proposition précédente. Le cas particulier que j'ai disposé dans un tableau permet en effet de comprendre ce qu'il se passe, de manière très explicite : comment écrire la classe d'un entier impair comme un multiple de $\bar{2}$? Et celle d'un entier pair ? — Plus généralement, si n est un nombre premier, à quelle condition nécessaire et suffisante la classe d'un entier k engendre $\mathbb{Z}/n\mathbb{Z}$?

Définition-Proposition 25 (Indicatrice d'Euler)**.**

✓	— Dans la démonstration, on omet une subtilité : pourquoi compter les classes des générateurs de $\mathbb{Z}/n\mathbb{Z}$ revient à compter les éléments premiers avec n dans $[\![1, n]\!]$ spécifiquement ? (Et non dans $\mathbb{Z}$, ou une autre partie de $\mathbb{Z}$.) — Comparer le résultat de cette proposition, avec ce qu'on a démontré pour les groupes de cardinal p avec p premier. Que vaut $\varphi(p)$ dans ce cas ?

Exemple 16. ♡

✓	Plus généralement en s'inspirant de cet exemple, si G est un groupe cyclique dont on note g un générateur : donner une condition nécessaire et suffisante simple pour qu'un élément quelconque soit un générateur de G.
★	Décrire de même les éléments d'ordre d, pour d divisant n. Se reposer éventuellement la question après avoir lu le reste de la section.

Proposition 26 (Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, d'un groupe cyclique)**.**

✓	— Vérifier VRAIMENT que $U_d = \left\langle \frac{n}{d} \right\rangle$ est de cardinal d. — Démontrer l'égalité : $H = \pi(\pi^{-1}(H))$, et vérifier que c'est faux si π n'est pas surjectif. — Est-ce que l'égalité $H = \pi^{-1}(\pi(H))$ est vraie ? Sans hypothèse de surjectivité ?
★	— Déduire de cette proposition un moyen, par contraposée, de montrer qu'un groupe n'est PAS cyclique. L'appliquer à $(\mathbb{Z}/2\mathbb{Z})^2$ par exemple, ou plus généralement à $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ avec m et n non premiers entre eux. — Réciproquement, si tout sous-groupe strict d'un groupe G est cyclique, est-ce que G est cyclique ? — Peut-on généraliser le raisonnement de la démonstration ? Peut-on toujours établir une correspondance entre les sous-groupes d'un groupe quotient G/H, et les sous-groupes de G ?
☢	Trouver une autre démonstration que tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques, et uniques pour chaque cardinal d divisant n, sans utiliser les sous-groupes de $\mathbb{Z}$.

Remarque.

★	Comment peut-on décrire le groupe engendré par $\langle \bar{k} \rangle$, si k ne divise pas n ?

Corollaire 27 (Nombre d'éléments d'ordre d dans un groupe cyclique)**.**

✓	— S'assurer d'avoir bien compris le raisonnement. En particulier : pourquoi a-t-on impérativement besoin de mentionner qu'il existe un unique sous-groupe de cardinal d ? — Reprendre l'exemple 14, dont on a vu qu'il est cyclique : donner l'ordre de tous ses éléments, compter le nombre d'éléments de chaque ordre pour vérifier la cohérence de ce corollaire, et expliciter le sous-groupe de chaque cardinal possible.
★	On a donné une condition nécessaire et suffisante simple, en termes de pgcd, pour qu'un élément d'un groupe cyclique de cardinal n soit d'ordre n. Caractériser de même les éléments d'ordre d, pour d divisant n (attention à ne pas aller trop vite). Vous pouvez y arriver soit en imitant la démonstration de la proposition 24, soit en notant que vous cherchez les générateurs de $\left\langle g^{\frac{n}{d}} \right\rangle$ (où g est un générateur de votre groupe cyclique de cardinal n), et que ces générateurs peuvent être obtenus *via* un isomorphisme avec $\mathbb{Z}/d\mathbb{Z}$. Les deux façons de faire sont instructives.

Après votre révision de cette partie

1. Appliquer les résultats de cette section à $\langle g \rangle$, où g est un élément quelconque d'un groupe G, pour voir ce qu'il nous enseigne sur les puissances de g (ordre de g^k, par exemple ?).
2. On a justifié l'étude de $\mathbb{Z}/n\mathbb{Z}$ par le fait que tout groupe cyclique de cardinal n soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Mais il est aussi vrai que tout groupe cyclique de cardinal n est isomorphe à $\mathbb{U}_n$, donc on aurait très bien pu étudier $\mathbb{U}_n$ à la place de $\mathbb{Z}/n\mathbb{Z}$. J'affirme qu'il y a au moins une proposition qui aurait été plus facile à démontrer ainsi : laquelle, et pourquoi ?
3. Dans les *Savoir-faire à vérifier*, étudier *Utiliser la structure des groupes cycliques*.

1.2.3 Approfondissements sur le groupe symétrique

Motivation de cette partie

Tout groupe pouvant s'identifier à un sous-groupe du groupe des permutations (théorème de Cayley), l'algébriste maîtrisant le groupe symétrique peut *en théorie* résoudre tout problème de théorie des groupes. Sans avoir autant d'ambition, nous allons approfondir notre connaissance de S_n : parties génératrices, centre... C'est le premier groupe, aussi, où nous pouvons commenter le principe de conjugaison, permettant de changer d'élément étudié (idéalement : en se ramenant à un élément plus simple) tout en ayant un contrôle sur ses propriétés.

Proposition 28 (Les cycles, les transpositions engendrent S_n)**.**

✓	Revoir, dans le cours de 1re année, comme il fut démontré que toute permutation est produit de transpositions. Se convaincre de l'écriture d'un cycle en produit de transpositions.
★	Quel est le cardinal de chaque partie génératrice de cette proposition ?
☢	Si la décomposition en cycles à supports disjoints ne fut pas démontrée en 1re année : le faire à présent. Vous pouvez vous simplifier la vie en introduisant une relation d'équivalence $\sim$ dont les classes sont exactement les éléments dans une même orbite : $\forall (x,y) \in [\![1,n]\!]^2,\ x \sim y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$.

Le principe de conjugaison : un principe fondamental.

★	— Hormis X l'ensemble des points fixes d'une permutation, que peut-on considérer comme ensemble X intéressant qui soit relié à une permutation σ ? Et quel est l'ensemble correspondant pour $\tau\sigma\tau^{-1}$? — Réfléchir à des illustrations du principe de conjugaison en algèbre linéaire : si M est une matrice, quelles sont les caractéristiques géométriques de PMP^{-1}, pour P inversible, qui se déduisent des caractères de M en prenant l'image par $X \mapsto PX$? Inutile de chercher au-delà des propriétés vues dans le cours de 1re année. — Est-ce que le principe de conjugaison est instructif dans le groupe $\mathbb{Z}/n\mathbb{Z}$?

Théorème 29 (Le conjugué d'un p-cycle est un p-cycle)**.**

★	— Est-ce que des permutations différentes donnent des conjugués différents ? Si $\tau \neq \tau'$, a-t-on $\tau\sigma\tau^{-1} \neq \tau'\sigma\tau^{-1}$? — Comment construire *explicitement* une bijection de $[\![1,n]\!] \setminus \{a_1,\dots,a_p\}$ dans $[\![1,n]\!] \setminus \{b_1,\dots,b_p\}$?

Exemple 17. ♡

✓	— Est-ce que le 1 joue un rôle particulier ? Aurait-on pu avoir le même résultat avec les transpositions de la forme $(2\ i)$, par exemple ? — Plus généralement, comment s'écrit un p-cycle à l'aide de transpositions de la forme $(1\ i)$?
☢	On a exhibé une partie génératrice de S_n avec $n-1$ transpositions seulement. Peut-on en trouver une à $n-2$ transpositions ou moins ?

Exemple 18. ♡

✓	S'inspirer de cet exemple pour décrire l'ensemble des permutations commutant avec un p-cycle fixé.
★	— S'inspirer de cet exemple pour décrire l'ensemble des permutations commutant avec une permutation fixée. — Partant de $\sigma\tau = \tau\sigma$, avec σ dans le centre de S_n, on pouvait aussi bien écrire : $\sigma\tau\sigma^{-1} = \tau$, que : $\tau\sigma\tau^{-1} = \sigma$. Comment pourquoi j'ai privilégié un choix plutôt que l'autre. (On peut aboutir dans les deux cas, mais l'approche que je n'ai pas choisie est plus tortueuse.) — Observer que ce principe de conjugaison permet, faute de mieux, d'écrire une égalité du type : $\sigma\tau = \tau^k\sigma^\ell$ dans certains cas (ce qui est mieux que rien si σ et τ ne commutent pas). Par exemple : comment utiliser le principe de conjugaison pour montrer que si $\sigma = (1\ 2\ 3)$ et $\tau = (1\ 2)$, alors : $\tau\sigma = \sigma^{-1}\tau$? Comment généraliser cela ? — S'inspirer de cette stratégie pour déterminer le centre d'autres groupes. Par exemple : déterminer le centre de $\mathrm{GL}_n(K)$ grâce au principe de conjugaison.

Corollaire 30 (Unicité du morphisme non trivial $S_n \to \{-1,1\}$)**.**

✓	Quelle est la signature d'un p-cycle ? Important et à connaître par cœur.
☢	— Si l'existence a été admise en 1re année : s'y atteler à présent. Ce n'est pas simple du tout : il ne suffit pas de poser que $\varepsilon(\sigma) = (-1)^k$ si σ s'écrit comme produit de k transpositions, parce que ce nombre k n'est pas uniquement défini. Par exemple, l'identité s'écrit aussi bien $\mathrm{id} = (1\ 2)(1\ 2)$ que $\mathrm{id} = (1\ 2)(3\ 4)(3\ 4)(1\ 2)$. Il faut soit justifier que ce problème est un faux problème, soit proposer une autre définition de ε (mais dans ce cas, c'est plutôt la vérification que c'est un morphisme qui risque d'être compliquée). — Adapter la démonstration pour compter le nombre de morphismes de S_n dans un groupe commutatif quelconque. Il faut d'abord démontrer que l'image d'un tel morphisme admet au plus deux éléments, ce qui nécessite une compréhension fine du noyau : le groupe alterné (voir ci-après) et ses générateurs devraient vous servir.

Définition 31 (Groupe alterné A_n)**.** 🔍

✓	Si σ est un p-cycle, donner une condition nécessaire et suffisante simple sur p pour que σ appartienne à A_n.

Exemple 19.

✓	Faire la même chose avec A_3 et A_5 (pour A_5, il y a beaucoup plus d'éléments : se contenter de donner le type des permutations, ainsi que leur nombre pour chaque type).
★	Pouviez-vous dénombrer l'ensemble des 3-cycles et des doubles-transpositions de A_4 autrement que par un recensement exhaustif ? Le faire dans A_n pour n quelconque.

Proposition 32 (Générateurs de A_n)**.** 🔍

✓	— Au vu de ce qu'on affirme d'emblée dans la démonstration, il semble qu'une autre partie génératrice aurait pu être trivialement proposée. Laquelle ? Pourquoi les 3-cycles sont-ils plus intéressants ? — Se convaincre que les 3-cycles sont effectivement dans A_n. — Trouver un moyen de se convaincre que l'identité $(i\ j)(k\ \ell) = (k\ j\ i)(k\ \ell\ i)$ (ou la variante proposée en cours) ne tombe pas du ciel.
☢	— Aurait-on pu montrer que toute double-transposition est produit de 3-cycles, en le montrant uniquement pour une double-transposition bien choisie puis en invoquant le principe de conjugaison ? — On a montré que tous les p-cycles sont conjugués dans S_n. Le sont-ils dans A_n ? (Avec p bien choisi pour que les p-cycles soient bien dans A_n.)

Après votre révision de cette partie

Traiter les *Savoir-faire* non encore traités.

2 Savoir-faire à vérifier

Les principaux acquis à vérifier sont :

Généralités sur les structures.

✓ 1. Montrer qu'un ensemble est un groupe, est un anneau. ☐

✓ 2. Montrer qu'une application est un morphisme. ☐

✓ 3. Déterminer des automorphismes de corps en dimension finie. (📄) ☐

★ 4. Déterminer si deux structures sont isomorphes. Le cas échéant, exploiter la donnée d'un isomorphisme. ☐

☢ 5. Reconnaître une structure même quand l'énoncé ne l'explicite pas, et l'exploiter pour démontrer un résultat. (📄) ☐

Étude spécifique des groupes.

✓ 1. Déterminer l'ordre d'un élément dans un groupe fini explicite. (📄) ☐

✓ 2. Décomposer une permutation en cycles à supports disjoints. ☐

✓ 3. Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances. (📄) ☐

★ 4. Utiliser le théorème de Lagrange pour l'étude de sous-groupes et parties génératrices. (📄) ☐

★ 5. Utiliser la structure des groupes cycliques. ☐

★ 6. Déterminer les morphismes d'un groupe dans un autre. ☐

☢ 7. Penser au principe de conjugaison, en particulier dans S_n, pour simplifier une étude. ☐

☢ 8. Utiliser une action de groupe pour le dénombrement, trouver des parties génératrices, etc. (📄) ☐

L'icône « (📄) » signifie que les documents *Méthodes* donnent des compléments sur ces savoir-faire.
L'indication « **(G/H)** », dans le corrigé d'un savoir-faire, indique des approfondissements sur la structure d'ensemble quotient, hors programme mais susceptibles d'intéresser le féru d'algèbre.

Généralités sur les structures

✓ Montrer qu'un ensemble est un groupe, un anneau, un corps.

Exemples.

1. Soit $\mathbb{H}_8 = \{\mathrm{I}_2, -\mathrm{I}_2, I, -I, J, -J, K, -K\}$, avec : $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Montrer que $\mathbb{H}_8$ est un groupe pour le produit matriciel.
2. On pose : $j = e^{\frac{2i\pi}{3}}$. Soient $r : z \mapsto jz$ et $s : z \mapsto \bar{z}$. Montrer que $\mathrm{D}_3 = \left\{r^k \circ s^\ell \mid (k,\ell) \in \mathbb{Z}^2\right\}$ est un groupe pour $\circ$ (c'est le groupe diédral d'ordre 3, ou d'ordre 6 selon les auteurs).
3. Soient $r : z \mapsto iz$ et $s : z \mapsto \bar{z}$. Montrer que $\mathrm{D}_4 = \left\{r^k \circ s^\ell \mid (k,\ell) \in \mathbb{Z}^2\right\}$ est un groupe pour $\circ$ (c'est le groupe diédral d'ordre 4, ou d'ordre 8 selon les auteurs).
4. Soient $f, g : A \to B$ deux morphismes d'anneaux. Montrer que : $\{x \in A \mid f(x) = g(x)\}$ est un anneau.
5. Soit $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid (a,b) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\}),\ p \not| b\right\}$. Montrer que $\mathbb{Z}_{(p)}$ est un anneau. Est-ce un corps ?
6. Soit $\mathbb{Q}[j] = \{a + bj \mid (a,b) \in \mathbb{Q}^2\}$. Montrer que c'est un corps.
7. Soit $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right] = \left\{P\left(e^{\frac{2i\pi}{n}}\right) \mid P \in \mathbb{Q}[X]\right\}$. Montrer que c'est un corps.
8. Soit $\mathbb{Q}[\pi] = \{P(\pi) \mid P \in \mathbb{Q}[X]\}$. Montrer que c'est un anneau, mais que ce n'est pas un corps.

✓ Montrer qu'une application est un morphisme.

Exemples.

1. Soient G un groupe et $g \in G$. Montrer que $h \mapsto ghg^{-1}$ est un automorphisme du groupe G.
2. Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que l'application $f : \mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n^2\mathbb{Z})^\times$ définie par $(\bar{m}, \bar{r}) \mapsto (1+n)^m r^n \bmod n^2$ est correctement définie et est un morphisme de groupes.

✓ Déterminer des automorphismes de corps en dimension finie.

Exemples. Soit K un corps.

1. Soit $\mathbb{Q}[j] = \{a + bj \mid (a,b) \in \mathbb{Q}^2\}$. Déterminer les automorphismes de $\mathbb{Q}[j]$.
2. Soit $K\left(X + \frac{1}{X}\right) = \left\{R\left(X + \frac{1}{X}\right) \mid R \in \mathbb{R}(X)\right\}$. Déterminer les automorphismes de corps de $K(X)$ dont la restriction à $K\left(X + \frac{1}{X}\right)$ est l'identité.

★ Déterminer si deux structures sont isomorphes. Le cas échéant, exploiter un isomorphisme.

Exemples. Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions, dont la table de multiplication découle entièrement des identités suivantes : $i^2 = j^2 = k^2 = ijk = -1$, et : $ij = k$, $jk = i$, $ki = j$. Soit T le sous-groupe de $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ constitué des matrices triangulaires supérieures n'ayant que des 1 sur la diagonale. On reprend les définitions de D_3 et D_4 données plus haut.

1. Déterminer si les groupes suivants sont isomorphes :

(a)	$\mathbb{R}^*$ et $\{-1,1\} \times \mathbb{R}_+^*$	(b)	$\mathbb{C}^*$ et $\mathbb{R}_+^* \times \mathbb{U}$	(c)	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$
(d)	$(\mathbb{Z}/2\mathbb{Z})^3$ et $\mathbb{H}_8$	(e)	$\mathbb{Z}/8\mathbb{Z}$ et $\mathbb{H}_8$	(f)	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
(g)	D_4 et $\mathbb{H}_8$	(h)	T et $\mathbb{H}_8$	(i)	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{H}_8$
(j)	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et S_3	(k)	D_3 et S_3	(l)	$\{\sigma \in S_n \mid \sigma(n) = n\}$ et S_{n-1}

2. Déterminer si $\mathbb{Q}[j] = \{a + bj \mid (a,b) \in \mathbb{Q}^2\}$ et $\mathbb{Q}[i] = \{a + bi \mid (a,b) \in \mathbb{Q}^2\}$ sont des anneaux isomorphes.

3. Soient A un cors, B un anneau, et $f : A \to B$ un morphisme d'anneaux. On suppose que f est un isomorphisme. Montrer que B est un corps.
4. Soit $k \in \mathbb{N} \setminus \{0,1,2,3\}$. On admet que $\left((\mathbb{Z}/2^k\mathbb{Z})^\times, \times\right)$ est isomorphe à $\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}, +\right)$. Donner le nombre de solutions à l'équation : $x^4 \equiv 1 \bmod 2^k$, d'inconnue $x \in \mathbb{Z}$.
5. On admet le résultat difficile suivant : soit G un groupe commutatif fini. Il existe une unique suite d'entiers naturels $d_1, \dots, d_r$ tels que $d_1 | d_2 | \cdots | d_r$, et tels que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$. Déduire de ce résultat que pour tout groupe commutatif G fini, si l'on note d le plus grand ordre d'un élément de G, alors : $\forall g \in G,\ g^d = 1_G$.

☢ Reconnaître une structure même quand l'énoncé ne l'explicite pas, et l'exploiter pour démontrer un résultat.

Exemples.

1. Compter le nombre d'entiers au cube modulo 73. On admet que 73 est un nombre premier. *Vous aurez besoin d'un résultat hors programme.*
2. Démontrer que si n est un entier naturel premier avec 10, il existe un nombre de la forme $11\cdots1$ (constitué uniquement du chiffre 1) qui soit un multiple de n.
3. Soit $p \in \mathbb{N}$ un entier qui n'est pas le cube d'un entier naturel. Montrer que $\sqrt{2}$ ne peut pas être obtenu comme une combinaison linéaire de puissances de $\sqrt[3]{p}$.

Étude spécifique des groupes

✓ Déterminer l'ordre d'un élément dans un groupe fini explicite.

Exemples.

1. Donner l'ordre de tous les éléments de $((\mathbb{Z}/15\mathbb{Z})^\times, \cdot)$ (on admet que ce groupe est de cardinal 8 et qu'il contient les classes des éléments premiers avec 15).
2. Donner l'ordre de $\sigma = (6\ 2)(3\ 5\ 4)(1\ 10\ 8\ 9\ 7)$ dans S_{10}.
3. Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que $1+n$ est d'ordre n dans $((\mathbb{Z}/n^2\mathbb{Z})^\times, \cdot)$.

✓ Décomposer une permutation en cycles à supports disjoints.

Exemples.

1. Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 1 & 7 & 4 & 3 & 6 & 9 & 5 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 6 & 4 & 7 & 8 & 5 & 9 & 3 \end{pmatrix}$ en cycles à supports disjoints, et donner leurs signatures.
2. Soit $\sigma = (1\ 2\ 3\ 4\ 5\ 6) \in S_6$. Décomposer en cycles à supports disjoints σ^k pour tout $k \in [\![2,5]\!]$.

✓ Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances.

Exemples.

1. Calculer 13^{100000} modulo 101. On admet que 101 est un nombre premier.
2. Calculer $2^{5^{4^3}}$ modulo 105.

★ Utiliser le théorème de Lagrange pour l'étude de sous-groupes et de parties génératrices.

Exemple. Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions, dont la table de multiplication découle entièrement des identités suivantes : $i^2 = j^2 = k^2 = ijk = -1$, et : $ij = k$, $jk = i$, $ki = j$. Décrire tous les sous-groupes de $\mathbb{H}_8$ et donner le cardinal minimal d'une partie génératrice.

★ Utiliser la structure des groupes cycliques.

Exemples.

1. Soit q un entier naturel impair. Déterminer l'ordre de $\overline{2q-1}$ et $\overline{2q+1}$ dans $((\mathbb{Z}/4q\mathbb{Z})^\times, \cdot)$, puis déterminer si c'est un groupe cyclique ou non.
2. On admet que $((\mathbb{Z}/101\mathbb{Z})^\times, \cdot)$ est cyclique et de cardinal 100. Donner le nombre de solutions de l'équation : $\bar{x}^{50} = \bar{1}$, puis de : $\bar{x}^{12} = \bar{1}$ et enfin de : $\bar{x}^7 = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/101\mathbb{Z}$.

★ Déterminer les morphismes d'un groupe dans un autre.

Exemples. Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions, dont la table de Cayley découle entièrement des identités suivantes : $i^2 = j^2 = k^2 = ijk = -1$, et : $ij = k$, $jk = i$, $ki = j$. Soit $n \in \mathbb{N} \setminus \{0\}$.

1. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{U}_n$ dans $\mathbb{C}^*$.
2. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{U}_n$ dans $\mathbb{R}^*$.
3. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{U}_{n^2}$ dans $\mathbb{U}_n$ et de $\mathbb{U}_n$ dans $\mathbb{U}_{n^2}$.
4. Déterminer les morphismes de groupes de $\mathbb{H}_8$ dans $\mathbb{C}^*$.
5. Soit $n \in \mathbb{N} \setminus \{0\}$. Déterminer les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{H}_8$ et de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$.

☢ Penser au principe de conjugaison, en particulier dans S_n, pour simplifier une étude.

Exemples.

1. On pose : $V_4 = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \mathrm{Id}\}$. On admet que V_4 est un sous-groupe de S_4 (vous pouvez le vérifier si vous le souhaitez). Montrer que V_4 est commutatif.
2. Déterminer l'ensemble des matrices inversibles d'ordre 2 qui commutent avec toute matrice inversible. *On pourra s'intéresser au conjugué d'une matrice de symétrie.*

☢ Utiliser une action de groupe pour le dénombrement, trouver des parties génératrices, etc.

Exemples.

1. Soient $n \in \mathbb{N} \setminus \{0\}$ et $k \in [\![1, n]\!]$, et soit $I(k, n)$ l'ensemble des applications injectives de $[\![1, k]\!]$ dans $[\![1, n]\!]$. Définir un morphisme convenable $\sigma \mapsto \varphi_\sigma$, défini de S_n dans $S_{I(k,n)}$, tel que l'étude d'une orbite $\{\varphi_\sigma(\iota) \mid \sigma \in S_n\}$ avec $\iota \in I(k, n)$ bien choisi, permette de redémontrer l'égalité bien connue :
$$\mathrm{card}(I(k, n)) = A_n^k = \frac{n!}{(n-k)!}.$$
2. On munit $\mathbb{C}$ de sa structure de $\mathbb{R}$-espace vectoriel. Soient $\mathrm{Is}(\mathbb{C}) = \{f \in \mathrm{GL}(\mathbb{C}) \mid \forall z \in \mathbb{C},\ |f(z)| = |z|\}$, et : $\mathrm{D}_n = \{f \in \mathrm{Is}(\mathbb{C}) \mid f(\mathbb{U}_n) \subseteq \mathbb{U}_n\}$. On vérifierait aisément que D_n est un sous-groupe de $\mathrm{GL}(\mathbb{C})$. Soient $r : z \mapsto e^{\frac{2i\pi}{n}} z \in \mathrm{D}_n$ et $s : z \mapsto \bar{z} \in \mathrm{D}_n$. Expliciter $\{f(1) \mid f \in \langle r \rangle\}$ et $\{f \in \mathrm{D}_n \mid f(1) = 1\}$. En déduire que D_n est engendré par r et s.

Généralités sur les structures

✓ Montrer qu'un ensemble est un groupe, un anneau, un corps. □

Réponse.

1. On montre que $\mathbb{H}_8$ est un sous-groupe de $(\mathrm{GL}_2(\mathbb{C}), \times)$. L'inclusion est claire (on a $I \cdot (-I) = \mathrm{I}_2$ et de même avec J et K, ce qui prouve l'inversibilité de toutes les matrices en présence), la stabilité par produit vient des identités suivantes, qui procèdent d'un calcul matriciel sans mystère :

$$(\pm I)^2 = (\pm J)^2 = (\pm K)^2 = -\mathrm{I}_2, \quad IJ = K,\ JK = I,\ KI = J, \quad JI = -K,\ KJ = -I,\ IK = -J.$$

On obtient les autres produits *via* une multiplication par $-\mathrm{I}_2$. La stabilité par inversion découle des premières identités ci-dessus, qui impliquent : $I^{-1} = -I \in \mathbb{H}_8$, etc. Ainsi $\mathbb{H}_8$ est un sous-ensemble non vide de $\mathrm{GL}_2(\mathbb{C})$, stable par produit et inverse, donc c'est un sous-groupe de $(\mathrm{GL}_2(\mathbb{C}), \times)$.

2. Montrons que c'est un sous-groupe de $\mathrm{GL}(\mathbb{C})$. Les applications r et s sont $\mathbb{R}$-linéaires, et bijectives car elles admettent respectivement pour bijections réciproques $z \mapsto j^{-1}z$ et s, donc $r^k \circ s^\ell \in \mathrm{GL}(\mathbb{C})$ pour tout $(k, \ell) \in \mathbb{Z}^2$. Ainsi D_3 est bien un sous-ensemble de $\mathrm{GL}(\mathbb{C})$.
Montrons la stabilité par produit. Soit $(k, k', \ell, \ell') \in \mathbb{Z}^4$. On a :

$$\left(r^k \circ s^\ell\right) \circ \left(r^{k'} \circ s^{\ell'}\right) = r^k \circ s^\ell \circ r^{k'} \circ s^{\ell'}.$$

Le problème est ce s^ℓ qui n'est « pas à la bonne place ». Néanmoins, si $\ell = 0$, on obtient $r^{k+k'} \circ s^{\ell'} \in \mathrm{D}_3$. Supposons à présent $\ell \neq 0$. Comme $s^2 = \mathrm{Id}$, il suffit en vérité de considérer $\ell = 1$. On remarque alors que l'on a pour tout $z \in \mathbb{C}$: $s \circ r^{k'}(z) = s\left(j^{k'} z\right) = \bar{j}^{k'} \bar{z} = j^{-k'} \bar{z} = r^{-k'} \circ s(z)$, donc : $s \circ r^{k'} = r^{-k'} \circ s$ (formule très commode pour inverser l'ordre dans le produit, bien que ce ne soit pas commutatif : on la retrouve dans S_3), puis :

$$\left(r^k \circ s^\ell\right) \circ \left(r^{k'} \circ s^{\ell'}\right) = r^k \circ r^{-k'} \circ s^{1+\ell'} = r^{k-k'} \circ s^{\ell+\ell'} \in \mathrm{D}_3,$$

d'où la stabilité par produit. Pour la stabilité par inverse, on écrit : $(r^k \circ s^\ell)^{-1} = s^{-\ell} r^{-k}$, et le même raisonnement que ci-dessus permet d'en déduire que si $\ell = 1$ alors : $\left(r^k \circ s\right)^{-1} = r^k \circ s \in \mathrm{D}_3$, le cas $\ell = 0$ étant trivial.
Ainsi D_3 est un sous-ensemble de $\mathrm{GL}(\mathbb{C})$ non vide, stable par produit et inverse, donc c'est un sous-groupe de $(\mathrm{GL}(\mathbb{C}), \circ)$.
Remarque. On peut démontrer que D_3 est l'ensemble des isométries du plan complexe qui laissent stable le triangle dont les sommets ont pour affixes 1, j et j^2 (c'est même parfois la définition de D_3).
Remarque. Pour la stabilité par inverse, il y a une autre façon de procéder, une fois qu'on a classifié les isométries du plan complexe. Les éléments de D_3 sont en effet des isométries (c'est clairement le cas pour r et s, et la stabilité par produit et inverse de $\mathrm{O}(\mathbb{C})$ donne le résultat pour $r^k \circ s^\ell$). Il suffit alors de remarquer que si ℓ est impair, alors $r^k \circ s^\ell$ est de déterminant -1 car s l'est (et r est de déterminant 1), donc c'est une isométrie indirecte du plan : c'est une symétrie. On en déduit : $(r^k \circ s^\ell)^{-1} = r^k \circ s^\ell \in \mathrm{D}_3$.

3. Ce sont exactement les mêmes calculs que ci-dessus.

4. Soit $C = \{x \in A \mid f(x) = g(x)\}$. Montrons que C est un sous-anneau de B. Il est contenu dans B car f et g sont à valeurs dans B, et non vide car $f(0_A) = g(0_A) = 0_B$, donc $0_A \in C$. Montrons qu'il est stable par somme et inversion pour $+$, le cas du produit étant en tout point analogue. Soit $(a_1, a_2) \in C^2$. On a : $f(a_1) = g(a_1)$, et : $f(a_2) = g(a_2)$, donc :

$$f(a_1 - a_2) = f(a_1) - f(a_2) = g(a_1) - g(a_2) = g(a_1 - a_2),$$

donc : $a_1 - a_2 \in C$, ce qui démontre la stabilité par somme.
Ainsi C est un sous-anneau de B, ce qui démontre le résultat voulu.

5. Montrons que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$. Il est clairement inclus dans cet anneau, et non vide parce que $0 = \frac{0}{1} \in \mathbb{Z}_{(p)}$. Il est stable par somme et inverse pour $+$, car pour tous $(a, b) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ et $(a', b') \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ tels que p ne divise pas b et b', on a :
$$\frac{a}{b} - \frac{a'}{b'} = \frac{ab' - a'b}{bb'},$$
et p ne divise pas bb' (sinon, par le lemme d'Euclide, il diviserait b ou b'). Donc : $\frac{a}{b} - \frac{a'}{b'} \in \mathbb{Z}_{(p)}$. Raisonnement analogue pour la stabilité par produit, donc $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$.
Il n'est pas un corps, puisque $p \in \mathbb{Z}_{(p)}$ et $\frac{1}{p} \notin \mathbb{Z}_{(p)}$. En effet, si $\frac{1}{p}$ s'écrit : $\frac{1}{p} = \frac{a}{b}$, avec a et b entiers tels que p ne divise pas b, alors on a : $b = pa$, et donc p divise b : c'est contraire à l'hypothèse sur b.

6. Montrons que $\mathbb{Q}[j]$ est un sous-corps de $\mathbb{C}$. Il est clairement inclus dans $\mathbb{C}$, non vide et stable par somme. Montrons la stabilité par produit. Soit $(a, b, c, d) \in \mathbb{Q}^4$. Comme $j^2 = -1 - j$, on a :
$$(a + bj)(c + dj) = ac + (ad + bc)j + bdj^2 = ac - bd + (ad + bc - bd)j \in \mathbb{Q}[j],$$
et il reste à montrer que tout élément non nul est inversible. Soit $(a, b) \in \mathbb{Q}^2$ tel que : $a + bj \neq 0$. Pour construire son inverse, il est raisonnable de penser que son inverse dans $\mathbb{C}$ est aussi son inverse dans $\mathbb{Q}[j]$. On va mettre $\frac{1}{a+bj}$ sous forme algébrique pour vérifier qu'il est bien dans $\mathbb{Q}[j]$. C'est l'idée de ce qui suit. On a : $(a + bj)(a + b\bar{j}) = |a + bj|^2 \in \mathbb{Q}^*$, donc :
$$\frac{a + b\bar{j}}{|a + bj|^2} \cdot (a + bj) = (a + bj) \cdot \frac{a + b\bar{j}}{|a + bj|^2} = 1,$$
et on a : $\frac{a+b\bar{j}}{|a+bj|^2} = \frac{a}{|a+bj|^2} + \frac{b}{|a+bj|^2}(-1 - j) \in \mathbb{Q}[j]$ (on a en effet : $\bar{j} = -1 - j$ d'après les relations coefficients-racines avec le polynôme $X^2 + X + 1$). Donc $a + bj$ est inversible dans $\mathbb{Q}[j]$, ce qu'il fallait démontrer.
On a montré que $\mathbb{Q}[j]$ est un sous-corps de $\mathbb{C}$.

7. L'ensemble $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est un sous-anneau de $\mathbb{C}$, puisque c'est l'image de l'anneau $\mathbb{Q}[X]$ par le morphisme d'évaluation $P \mapsto P\left(e^{\frac{2i\pi}{n}}\right)$ (qui est un morphisme d'anneaux de $\mathbb{Q}[X]$ dans $\mathbb{C}$). Montrons que c'est un corps. Nous proposons deux arguments différents.
Premier argument. Soit $z \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ un élément non nul. Alors l'application $x \mapsto xz$ est un endomorphisme du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ (parce qu'il est stable par produit), injectif parce que $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est intègre en tant que sous-anneau de $\mathbb{C}$ qui l'est. Or $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est de dimension finie. En effet, en effectuant la division euclidienne d'un polynôme $\mathbb{Q}[X]$ par $X^n - 1$, on peut montrer que pour tout $P \in \mathbb{Q}[X]$, il existe $R \in \mathbb{Q}_{n-1}[X]$ tel que : $P\left(e^{\frac{2i\pi}{n}}\right) = R\left(e^{\frac{2i\pi}{n}}\right)$. Cela implique concrètement que $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ admet pour partie génératrice *finie* la famille $\left(e^{\frac{2i\pi k}{n}}\right)_{0 \leqslant k \leqslant n-1}$, donc c'est un $\mathbb{Q}$-espace vectoriel de dimension finie.
Un endomorphisme injectif d'un espace vectoriel de dimension finie est aussi surjectif, donc $1 \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ admet un antécédent par $x \mapsto xz$: il existe $x \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ tel que : $xz = 1$, ce qui démontre l'inversibilité de z. Ceci vaut pour tout $z \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ non nul, donc $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ est un corps.
Deuxième argument (nécessite le polynôme minimal, chapitre IV). Comme $e^{\frac{2i\pi}{n}}$ est annulé par $X^n - 1 \in \mathbb{Q}[X]$, il admet un polynôme minimal sur $\mathbb{Q}$ qu'on note Φ_n. Soit $z = P\left(e^{\frac{2i\pi}{n}}\right) \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ non nul. Comme $P\left(e^{\frac{2i\pi}{n}}\right) \neq 0$, le polynôme Φ_n ne divise pas P, et donc ils sont premiers entre eux (en effet, un diviseur unitaire commun à Φ_n et P est en particulier un diviseur de Φ_n, donc est égal à 1 ou Φ_n ; le second cas est exclu puisque le cas échéant, Φ_n diviserait P). Par le théorème de Bezout, il existe $(U, V) \in \mathbb{Q}[X]^2$ tel que : $UP + V\Phi_n = 1$. En évaluant cette égalité en $e^{\frac{2i\pi}{n}}$, on obtient : $U\left(e^{\frac{2i\pi}{n}}\right) P\left(e^{\frac{2i\pi}{n}}\right) = 1$ (en effet $\Phi_n\left(e^{\frac{2i\pi}{n}}\right) = 0$ par définition d'un polynôme minimal, qui est aussi annulateur). Donc : $U\left(e^{\frac{2i\pi}{n}}\right) z = zU\left(e^{\frac{2i\pi}{n}}\right) = 1$, avec $U\left(e^{\frac{2i\pi}{n}}\right) \in \mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$, ce qui prouve que z est inversible dans $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$: c'est ce qu'on voulait démontrer.

Remarque. Ces deux arguments se généralisent à tout anneau de la forme $\mathbb{Q}[z]$ avec z annulé par un polynôme non nul à coefficients rationnels.

8. La démonstration que c'est un sous-anneau de $\mathbb{C}$ est la même que pour $\mathbb{Q}\left[e^{\frac{2i\pi}{n}}\right]$ traité ci-dessus. Justifions que ce n'est pas un corps. Si tel était le cas, on aurait $\frac{1}{\pi} \in \mathbb{Q}[\pi]$, donc il existerait $P \in \mathbb{Q}[X]$ tel que : $\frac{1}{\pi} = P(\pi)$, avec P non nul sinon cette égalité impliquerait $\frac{1}{\pi} = 0$. Le polynôme non nul $XP-1$ admettrait donc π comme racine, ce qui est impossible puisque π n'est annulé par aucun polynôme à coefficients rationnels : il est transcendant (théorème de Lindemann). Par l'absurde, on a montré : $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$, donc π n'est pas inversible dans $\mathbb{Q}[\pi]$. Ce n'est pas un corps.

✓ Montrer qu'une application est un morphisme. □

Réponse.

1. Notons f_g l'application de l'énoncé. Elle est bien à valeurs dans G car G est stable par produit. Pour tout $(h_1, h_2) \in G^2$, on a :

$$f_g(h_1)f_g(h_2) = gh_1g^{-1}gh_2g^{-1} = g(h_1h_2)g^{-1} = f_g(h_1h_2),$$

donc f_g est un morphisme de groupes de G dans G. C'est un automorphisme, puisqu'un calcul direct montre que $f_{g^{-1}}$ est son application réciproque. Nous ne le détaillons que pour la composition dans un sens, l'autre étant analogue (inverser les rôles de g et g^{-1}) :

$$\forall h \in G, \quad f_g \circ f_{g^{-1}}(h) = f_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h.$$

Donc f_g est un morphisme bijectif de G dans G : c'est un automorphisme de G.

Remarque. Les automorphismes de cette forme sont appelés les *automorphismes intérieurs*.

2. Tout d'abord, $(1+n)^n \equiv 1 \bmod n^2$ (utiliser la formule du binôme de Newton), donc d'une part $1+n \in (\mathbb{Z}/n^2\mathbb{Z})^\times$ (son inverse étant $(1+n)^{n-1}$), et d'autre part l'application de $\mathbb{Z}$ dans $(\mathbb{Z}/n^2\mathbb{Z})^\times$, définie par $m \mapsto (1+n)^m \bmod n^2$, induit un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $(\mathbb{Z}/n^2\mathbb{Z})^\times$ défini par $\bar{m} \mapsto (1+n)^m \bmod n^2$ (théorème de factorisation des morphismes). Ensuite, pour que $f : (\bar{m}, \bar{r}) \mapsto (1+n)^m r^n \bmod n^2$ soit correctement définie, encore faut-il que le résultat ne dépende pas du choix du représentant dans la classe de r. Considérons donc $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ et $(r_1, r_2) \in ((\mathbb{Z}/n\mathbb{Z})^\times)^2$ tel que : $\overline{r_1} = \overline{r_2}$. Montrons : $r_1^n \equiv r_2^n \bmod n^2$. Comme : $\overline{r_1} = \overline{r_2}$, il existe $k \in \mathbb{Z}$ tel que : $r_1 = r_2 + kn$. Alors : $r_1^n = (r_2+kn)^n = \sum_{i=0}^{n} \binom{n}{i} r_2^{n-i}(kn)^i \equiv r_2^n + \binom{n}{1} r_2^{n-1}(kn) \equiv r_2^n + r_2^{n-1}kn^2 \equiv r_2^n \bmod n^2$. Ainsi $r^n \bmod n^2$ ne dépend pas du choix du représentant de $\bar{r} \in (\mathbb{Z}/n\mathbb{Z})^\times$ et cela suffit à démontrer que f est bien définie. Montrons à présent que c'est un morphisme de groupes. Attention à ne pas s'emmêler les pinceaux : la loi de $\mathbb{Z}/n\mathbb{Z}$ est $+$ et celle de $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\times$. On doit donc démontrer :

$$\forall ((\overline{m_1}, \overline{r_1}), (\overline{m_2}, \overline{r_2})) \in \left(\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times\right)^2, \quad f(\overline{m_1} + \overline{m_2}, \overline{r_1} \times \overline{r_2}) = f(\overline{m_1}, \overline{r_1}) \times f(\overline{m_2}, \overline{r_2}).$$

Soit $((\overline{m_1}, \overline{r_1}), (\overline{m_2}, \overline{r_2})) \in (\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^\times)^2$. On a :

$$f(\overline{m_1}, \overline{r_1}) \times f(\overline{m_2}, \overline{r_2}) \equiv (1+n)^{m_1} r_1^n \times (1+n)^{m_2} r_2^n = (1+n)^{m_1+m_2}(r_1r_2)^n = f(\overline{m_1} + \overline{m_2}, \overline{r_1} \times \overline{r_2}),$$

ce qui prouve que f est un morphisme.

✓ Déterminer des automorphismes de corps en dimension finie. □

Réponse.

1. Soit f un automorphisme de corps de $\mathbb{Q}[j]$. Pour tout $(a, b) \in \mathbb{Q}^2$, on a : $f(a+bj) = f(a) + f(b)f(j)$. Or, partant de $f(1) = 1$, il est classique de démontrer que $f(x) = x$ pour tout $x \in \mathbb{Q}$ (en le montrant d'abord pour $x \in \mathbb{N}$ par récurrence grâce à l'identité $f(n \cdot 1) = nf(1)$, puis pour $x \in \mathbb{Z}$ grâce à l'identité $f(x) = -f(-x)$, pour $x = \frac{p}{q} \in \mathbb{Q}$ grâce à l'identité $f(p) = qf\left(\frac{p}{q}\right)$; je préfère néanmoins le démontrer

en montrant que $\{x \in \mathbb{Q}[j] \mid f(x) = x\}$ est un corps et qu'il doit donc contenir le sous-corps premier de $\mathbb{Q}[j]$, qui est $\mathbb{Q}$). Donc : $\forall (a,b) \in \mathbb{Q}^2$, $f(a+bj) = a + bf(j)$. Il reste à déterminer $f(j)$.
Or : $j^2 + j + 1 = 0$. En prenant l'image par f dans cette égalité, et en utilisant le fait que ce soit un morphisme de corps, on a : $f(j)^2 + f(j) + 1 = 0$, donc $f(j)$ est racine de $X^2 + X + 1$. On en déduit que $f(j) = j$ ou $f(j) = j^2$, ce qu'on résume en disant qu'il existe $k \in \{1,2\}$ tel que : $f(j) = j^k$. Par conséquent, si f est un automorphisme de corps, alors : $\forall (a,b) \in \mathbb{Q}^2$, $f(a+bj) = a + bj^k$ (par ailleurs j^2 est bien dans $\mathbb{Q}[j]$, puisque : $j^2 = -1 - j$).
Réciproquement, pour tout $j \in \{1,2\}$, montrons que l'application définie par $a + bj \mapsto a + bj^k$ (elle est correctement définie car tout élément de $\mathbb{Q}[j]$ s'écrit sous la forme $a + bj$ de manière unique) est un automorphisme de corps. Le cas $k = 1$ est évident puisqu'on reconnaît là l'application identité. Supposons donc $k = 2$. Soit $(a,b,c,d) \in \mathbb{Q}^4$. On a $f(1) = 1$, et :

$$\begin{aligned} f(a+bj)f(c+dj) = (a+bj^2)(c+dj^2) &= ac + (ad+bc)j^2 + bdj^4 \\ &= ac + (ad+bc)j^2 + bdj \\ &= ac + (ad+bc)(-1-j) + bdj, \\ &= ac - ad - bc + (bd - ad - bc)j, \end{aligned}$$

tandis que :

$$\begin{aligned} f((a+bj)(c+dj)) = f\left(ac + (ad+bc)j + bdj^2\right) &= f\left(ac - bd + (ad+bc-bd)j\right) \\ &= ac - bd + (ad+bc-bd)j^2 \\ &= ac - bd + (ad+bc-bd)(-1-j) \\ &= ac - bd - ad - bc + bd - (ad+bc-bd)j \\ &= ac - ad - bc + (bd - ad - bc)j \\ &= f((a+bj)(c+dj)), \end{aligned}$$

donc f est bien un morphisme de corps. Il est injectif comme tout morphisme de corps, et surjectif parce que 1 et j sont dans son image : on a $1 = f(1)$ et $j = -j^2 - 1 = f(-j-1)$. Comme 1 et j engendrent $\mathbb{Q}[j]$, par $\mathbb{Q}$-linéarité f est surjectif. On a donc démontré que c'est un morphisme de corps de $\mathbb{Q}[j]$ dans lui-même et bijectif : c'est donc un automorphisme de corps.
Conclusion. Les automorphismes de $\mathbb{Q}[j]$ sont exactement les applications de la forme $a+bj \mapsto a+bj^k$ avec $k \in \{1,2\}$. Il y en a donc deux.
Remarque. Le caractère bijectif peut aussi se démontrer en notant que f est un endomorphisme du $\mathbb{Q}$-espaces vectoriel $\mathbb{Q}[j]$, qui est injectif comme tout morphisme de corps ; comme $\mathbb{Q}[j]$ est de dimension finie (égale à 2) sur $\mathbb{Q}$, on en déduit que f est bijectif.
Remarque. La vérification que f est un morphisme est beaucoup, beaucoup moins calculatoire si l'on remarque que l'on a : $\mathbb{Q}[j] = \{P(j) \mid P \in \mathbb{Q}[X]\}$ (il suffit alors d'écrire : $f(P_1(j))f(P_2(j)) = P_1(j^k)P_2(j^k) = (P_1P_2)(j^k) = f(P_1P_2(j))$ pour avoir le résultat ! c'est tout !). En revanche, dans ce cas-là il faut vérifier que la définition de f ne dépend pas de l'écriture d'un élément $z \in \mathbb{Q}[j]$ sous la forme $z = P(j)$ avec $P \in \mathbb{Q}[X]$: si P_1 et P_2 vérifient : $z = P_1(j) = P_2(j)$, il faut vérifier que $f(P_1(j)) = f(P_2(j))$. Cette vérification nécessite la notion de polynôme minimal de j sur $\mathbb{Q}$ (qui vaut $X^2 + X + 1$) pour être efficace : on dit que si $P_1(j) = P_2(j)$, alors $P_1 - P_2$ annule j et est donc divisible par le polynôme minimal de j sur $\mathbb{Q}$, qui vaut $X^2 + X + 1$. Il existe donc $Q \in \mathbb{Q}[X]$ tel que : $P_1 = P_2 + (X^2 + X + 1)Q$, et en évaluant cette égalité en j^k (qui est racine de $X^2 + X + 1$ pour $k \in \{1,2\}$) on a : $P_1(j^k) = P_2(j^k)$, ce qu'il fallait démontrer.
L'avantage, aussi, de procéder comme décrit dans cette remarque, est que cela permet de traiter simultanément $k = 1$ et $k = 2$.

2. Soit f un automorphisme de corps de $K(X)$ qui fixe $K\left(X + \frac{1}{X}\right)$. Déterminons f, en commençant par déterminer $f(X)$. Comme souvent, on cherche une relation vérifiée par X sur $K\left(X + \frac{1}{X}\right)$ afin d'en déduire une relation vérifiée par $f(X)$. Or on a :

$$X^2 - X\left(X + \frac{1}{X}\right) + 1 = 0$$

(je me suis inspiré des relations coefficients-racines pour trouver cette expression : j'ai fabriqué un polynôme à *coefficients* dans $K\left(X+\frac{1}{X}\right)$ dont les racines sont X et $\frac{1}{X}$), et comme f est un morphisme de corps qui fixe $K\left(X+\frac{1}{X}\right)$ on en déduit : $f(X)^2 - f(X)\left(X+\frac{1}{X}\right)+1=0$, ce qui équivaut à : $(f(X)-X)\left(f(X)-\frac{1}{X}\right)=0$ (car X et $\frac{1}{X}$ sont racines du polynôme $Y^2-\left(X+\frac{1}{X}\right)Y+1 \in K\left(X+\frac{1}{X}\right)[Y]$). Comme $K(X)$ est intègre, on en déduit : $f(X)=X$, ou : $f(X)=\frac{1}{X}$. On étend alors f à tout élément de $K(X)$ par somme et produit. On en déduit que si f est un automorphisme de $K(X)$ qui fixe $K\left(X+\frac{1}{X}\right)$, alors il est de la forme :

$$R \mapsto R(X), \quad \text{ou :} \quad R \mapsto R\left(\frac{1}{X}\right).$$

Réciproquement, il est facile de démontrer que ces deux applications sont des automorphismes de $K(X)$ fixant $K\left(X+\frac{1}{X}\right)$.

★ Déterminer si deux structures sont isomorphes. Le cas échéant, exploiter un isomorphisme. □

Réponse.

1. (a) Intuitivement, $\mathbb{R}^*$ et $\{-1,1\}\times\mathbb{R}_+^*$ sont isomorphes puisque tout réel non nul est caractérisé par la donnée de son signe (qu'on représente par 1 ou -1) et de sa valeur absolue. Ceci conduit à considérer l'application $x \mapsto \left(\frac{x}{|x|},|x|\right)$, qui est un morphisme par multiplicativité de la valeur absolue et bijective puisqu'elle admet pour réciproque $(\varepsilon,r)\mapsto \varepsilon r$. La réponse est donc **positive**.
   (b) Intuitivement, $\mathbb{C}^*$ et $\mathbb{R}_+^*\times\mathbb{U}$ sont isomorphes puisque tout complexe non nul est caractérisé par la donnée de son module (qui est dans $\mathbb{R}_+^*$) et de son argument (ou, cela revient au même, un élément de $\mathbb{U}$, qui apparaît en facteur du module dans la forme exponentielle). Ceci conduit à considérer l'application $z\mapsto\left(|z|,\frac{z}{|z|}\right)$, qui est un morphisme par multiplicativité du module et bijective puisqu'elle admet pour réciproque $(r,\omega)\mapsto r\omega$. La réponse est donc **positive**.
   (c) Tous les éléments sont d'ordre 1 ou 2 dans $(\mathbb{Z}/2\mathbb{Z})^3$, tandis que $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ admet un élément d'ordre 4 (en l'occurrence : (0 mod 2,1 mod 4), comme on le vérifie facilement). Donc les groupes ne sont pas isomorphes : la réponse est **négative**.
   (d) Le premier groupe est commutatif et pas le second (on a $ij=k$ et $ji=-k\neq k$) : la réponse est **négative**.
   (e) Même argument : la réponse est **négative**.
   (f) Il s'avère que ces deux groupes sont isomorphes. Le plus rapide, pour le démontrer, est d'utiliser convenablement le théorème chinois (chapitre IV). Le groupe $\mathbb{Z}/6\mathbb{Z}$ est en effet isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, et il n'est pas difficile de se convaincre que cela implique un isomorphisme entre $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Encore par le théorème chinois, ce dernier groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. La réponse est donc **positive**.

   Remarque. Un isomorphisme explicite est donné par $(a \bmod 4, b \bmod 6) \mapsto (b \bmod 2, 4b-3a \bmod 12)$. On le trouve en explicitant l'isomorphisme réciproque de $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$.
   (g) Le groupe D_4 admet deux éléments d'ordre 4, à savoir r et $r^3=r^{-1}$ (on vérifiera que r^ks est toujours d'ordre 2), tandis que $\mathbb{H}_8$ en admet beaucoup plus : $\pm i$, $\pm j$, $\pm k$. Les groupes ne sont donc pas isomorphes. La réponse est **négative**.
   (h) Soit $M=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\in T$. On a : $M^2=\begin{pmatrix}1&0&ac\\0&1&0\\0&0&1\end{pmatrix}$ (on a $2\cdot a=2\cdot b=2\cdot c=0$ vu qu'on raisonne dans $\mathbb{Z}/2\mathbb{Z}$). On en déduit que M est d'ordre divisant 2 si et seulement si : $ac=0$, sans condition sur $b\in\mathbb{Z}/2\mathbb{Z}$. Cela fournit six éléments d'ordre divisant 2, or $\mathbb{H}_8$ n'en a que deux, à savoir 1 et -1. Ils ne sont donc pas isomorphes et la réponse est **négative**.

   Remarque. En fait, D_4 et T sont isomorphes, et comme nous avons démontré que D_4 n'est pas isomorphe à $\mathbb{H}_8$, il en est de même de T. Pour comprendre en quoi D_4 et T sont isomorphes, il

faut comprendre à quoi correspondent la rotation r et la symétrie s dans T : un élément d'ordre 4 est $R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ par exemple, tandis qu'un élément d'ordre 2 (qui n'est pas dans le groupe engendré par R) est $S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. On vérifie alors que l'application $f : \mathrm{D}_4 \to \mathrm{T}$ définie par $r^k s^\ell \mapsto R^k S^\ell$ est bien définie, est un morphisme (cela ne va pas de soi du tout, et il faudra sans doute démontrer : $SRS = R^{-1}$), et est injectif : comme les deux groupes ont même cardinal, cela suffit à démontrer qu'ils sont isomorphes.

(i) Le premier groupe est commutatif et pas le second : la réponse est **négative**.

(j) Le premier groupe est commutatif et pas le second (on a $(1\ 2)(1\ 2\ 3) = (2\ 3)$ et $(1\ 2\ 3)(1\ 2) = (1\ 3) \neq (2\ 3)$) : la réponse est **négative**.

(k) Puisque D_3 est engendré par $r : z \mapsto jz$ et $s : z \mapsto \bar{z}$ qui, géométriquement, permutent les trois sommets du triangle régulier dont les sommets sont d'affixes 1, j et $j^2 = \bar{j}$, il ressemble de près au groupe S_3 qui consiste en la permutation de trois éléments (où r serait un 3-cycle et s une transposition). Montrons qu'ils sont isomorphes, en considérant l'application $f : \mathrm{D}_3 \to S_3$ qui envoie $r^k \circ s^\ell$ sur $(1\ 2\ 3)^k(2\ 3)^\ell$ pour tout $(k, \ell) \in \mathbb{Z}^2$ (en vérité, prendre $k \in \{0,1,2\}$ et $\ell \in \{0,1\}$ suffirait). Vérifions que c'est bien un morphisme. Soit $(k, \ell, k', \ell') \in \mathbb{Z}^4$. Comparons $f\left(r^k \circ s^\ell\right) \circ f\left(r^{k'} \circ s^{\ell'}\right)$ et $f\left(\left(r^k \circ s^\ell\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right)$. Si $\ell = 0$, alors on a directement :

$$f\left(r^k\right) \circ f\left(r^{k'} \circ s^{\ell'}\right) = (1\ 2\ 3)^k \circ (1\ 2\ 3)^{k'}(1\ 2)^{\ell'} = (1\ 2\ 3)^{k+k'}(1\ 2)^{\ell'} = f\left(r^{k+k'} \circ s^{\ell'}\right) = f\left(r^k \circ r^{k'} \circ s^{\ell'}\right),$$

et si $\ell = 1$ nous allons utiliser le principe de conjugaison pour mettre cette composition sous la bonne forme (comme $s^2 = \mathrm{Id}$, prendre $\ell \in \{0,1\}$ suffit). On a :

$$\begin{aligned} f\left(r^k \circ s\right) \circ f\left(r^{k'} \circ s^{\ell'}\right) &= (1\ 2\ 3)^k(1\ 2) \circ (1\ 2\ 3)^{k'}(1\ 2)^{\ell'} \\ &= (1\ 2\ 3)^k(1\ 2)(1\ 2\ 3)^{k'}(1\ 2)(1\ 2)^{\ell'+1} \\ &= (1\ 2\ 3)^k(2\ 1\ 3)^{k'}(1\ 2)^{\ell'+1} \\ &= (1\ 2\ 3)^k(1\ 2\ 3)^{-k'}(1\ 2)^{\ell'+1} \\ &= (1\ 2\ 3)^{k-k'}(1\ 2)^{\ell'+\ell}. \end{aligned}$$

Pour calculer $f\left(\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right)$, simplifions d'abord la composition $\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)$. Là encore, nous allons utiliser le principe de conjugaison (qui est un principe général et ne vaut pas que dans S_n, même si c'est là qu'on l'a illustré majoritairement). Pour tout $z \in \mathbb{C}$, on a :

$$s \circ r^{k'}(z) = s\left(j^{k'} z\right) = \bar{j}^{k'} \bar{z} = j^{-k'} \bar{z} = r^{-k'} \circ s(z),$$

donc :

$$f\left(\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right) = f\left(r^k \circ r^{-k'} \circ s^{1+\ell'}\right) = f\left(r^{k-k'} \circ s^{\ell+\ell'}\right) = (1\ 2\ 3)^{k-k'}(1\ 2)^{\ell'+\ell}.$$

On a donc bien : $f\left(r^k \circ s\right) \circ f\left(r^{k'} \circ s^{\ell'}\right) = f\left(\left(r^k \circ s\right) \circ \left(r^{k'} \circ s^{\ell'}\right)\right)$, ce qui prouve que f est un morphisme. Comme D_3 et S_3 sont tous les deux de cardinal 6 (pour D_3 on ne l'a pas démontré, mais sa description explicite, ainsi que les relations $r^3 = \mathrm{Id}$ et $s^2 = \mathrm{Id}$, permettent de s'en assurer rapidement), il suffit de montrer qu'il est injectif pour avoir le résultat. Soit $(k, \ell) \in \mathbb{Z}^2$ tel que : $f(r^k \circ s^\ell) = \mathrm{Id}$. Cela signifie : $(1\ 2\ 3)^k(1\ 2)^\ell = \mathrm{Id}$, donc : $(1\ 2\ 3)^k = (1\ 2)^\ell$. L'unicité de la décomposition en cycles à supports disjoints ne permet cette égalité que si chaque membre de l'égalité vaut Id, ce qui correspond à $k \equiv 0 \bmod 3$ et $\ell \equiv 0 \bmod 2$. Pour de telles conditions sur k et ℓ, on a aussi : $s^\ell = \mathrm{Id}$, et : $\forall z \in \mathbb{C}$, $r^k(z) = j^k z = z$, donc : $r^k = \mathrm{Id}$. Donc : $r^k \circ s^\ell = \mathrm{Id}$. Notre calcul montre donc que : $\ker(f) = \{\mathrm{Id}\}$, et f est alors un morphisme injectif entre deux groupes de même cardinal : c'est un isomorphisme.

La réponse est donc **positive**.

Remarque. On a démontré en passant cette formule très commode qui permet d'inverser l'ordre dans le produit : $(1\ 2)(1\ 2\ 3)^{k'} = (1\ 2\ 3)^{-k'}(1\ 2)$. Formule analogue avec r et s.

(l) Intuitivement, une permutation de S_{n-1} et une permutation de S_n fixant n est la même chose. Les deux groupes devraient être isomorphes. On le démontre très simplement grâce à l'isomorphisme $\sigma \mapsto \sigma_{|[\![1,n-1]\!]}$, qui est correctement défini et va de $\{\sigma \in S_n \mid \sigma(n) = n\}$ dans S_{n-1}.

2. Intuitivement, deux anneaux isomorphes devraient avoir autant de solutions à toute équation polynomiale (en première approximation c'est un peu faux, sauf si les équations polynomiales sont à coefficients entiers voire rationnels, grâce au fait qu'un morphisme vérifie $f(1) = 1$). Mais le second a une solution de $X^2 + 1$ mais pas le premier : cela mène à la conjecture qu'ils ne sont pas isomorphes. Démontrons-le : supposons l'existence d'un isomorphisme d'anneaux $f : \mathbb{Q}[i] \to \mathbb{Q}[j]$. On a : $(f(i))^2 + 1 = f(i^2) + f(1) = f(i^2 + 1) = f(0) = 0$, donc $f(i) \in \mathbb{Q}[j]$ est racine de $X^2 + 1$. On a donc : $f(i) = \pm i$, or i et $-i$ n'appartiennent pas à $\mathbb{Q}[j]$. En effet, si $i \in \mathbb{Q}[j]$, alors il existe $(a, b) \in \mathbb{Q}^2$ tel que : $i = a + bj$, et en utilisant les parties imaginaires : $1 = b\frac{\sqrt{3}}{2}$, puis : $b = \frac{2}{\sqrt{3}} = \frac{2}{3}\sqrt{3} \notin \mathbb{Q}$: absurde.
On en déduit que $\mathbb{Q}[i]$ et $\mathbb{Q}[j]$ **ne** sont **pas** isomorphes.

3. Soit $a \in B \setminus \{0_B\}$: montrons qu'il existe $b \in B$ tel que $ab = 1_B$. Nous allons « transporter » a dans A grâce à l'isomorphisme, pour y trouver un inverse : comme $f^{-1}(a) \in A$ et $f^{-1}(a) \neq 0_A$ (dans le cas contraire, on aurait : $a = f\left(f^{-1}(a)\right) = f\left(0_A\right) = 0_B$, ce qui est faux), et comme A est un corps, il existe un élément $y \in A$ tel que : $f^{-1}(a)y = 1_A$. En prenant l'image par f, qui est un morphisme, on obtient : $af(y) = f(1_A) = 1_B$. Ainsi $f(y)$ est l'inverse de a, et tout élément non nul de B est inversible.
On montrerait de même que $ab = ba$ pour tout $(a, b) \in A^2$ en utilisant le fait que $f(a)f(b) = f(b)f(a)$, donc A est un anneau commutatif dont tout élément non nul est inversible : c'est un corps.

4. On remarque qu'une solution $\bar{x}$ est inversible modulo 2^k, d'inverse $\bar{x}^3$. C'est pourquoi nous allons nous contenter de raisonner dans $(\mathbb{Z}/2^k\mathbb{Z})^\times$.
Soit $\varphi : (\mathbb{Z}/2^k\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ un isomorphisme de groupes, qui existe par hypothèse de l'énoncé. Soit $\bar{x} \in (\mathbb{Z}/2^k\mathbb{Z})^\times$. Posons : $(a \bmod 2, b \bmod 2^{k-2}) = \varphi(\bar{x})$. Alors : $x^4 \equiv 1 \bmod 2^k \iff 4\varphi(\bar{x}) = \varphi(\bar{1}) \iff (4a \bmod 2, 4b \bmod 2^{k-2}) = (0 \bmod 2, 0 \bmod 2^{k-2})$. La condition $4a \equiv 0 \bmod 2$ est toujours vérifiée, car 4 est pair. Donc : $x^4 \equiv 1 \bmod 2^k \iff 4b \equiv 0 \bmod 2^{k-2} \iff \exists \ell \in \mathbb{Z}$, $4b = 2^{k-2}\ell \iff \exists \ell \in \mathbb{Z}$, $b = 2^{k-4}\ell$. Modulo 2^{k-2}, cela fait 4 valeurs de b possibles : 0, 2^{k-4}, 2^{k-3}, $3 \cdot 2^{k-4}$. Donc : $x^4 \bmod 1 \bmod 2^k \iff \varphi(\bar{x}) \in \mathbb{Z}/2\mathbb{Z} \times \left\{\ell 2^{k-4} \mid \ell \in [\![0,3]\!]\right\} \iff \bar{x} \in \varphi^{-1}\left(\mathbb{Z}/2\mathbb{Z} \times \left\{\ell 2^{k-4} \mid \ell \in [\![0,3]\!]\right\}\right)$. Comme φ^{-1} est bijective, ce dernier ensemble a huit éléments : on en déduit que l'équation : $x^4 \equiv 1 \bmod 2^k$ admet huit solutions $\bar{x}$ dans $(\mathbb{Z}/2^k\mathbb{Z})^\times$.

5. Puisque tout groupe commutatif fini est isomorphe à un groupe de la forme $G' = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, où $d_1|d_2|\cdots|d_r$, et qu'un isomorphisme conserve les ordres, il suffit de démontrer le résultat voulu pour un groupe de cette forme (attention, désormais la loi est notée additivement dans G' : il faut donc que démontrer $dx = 0$ pour tout $x \in G'$).
Soit d l'ordre maximal d'un élément de G' : montrons d'abord que $d = d_r$. Si $(x_1, \ldots, x_r) \in G'$, alors : $\forall i \in [\![1, r]\!]$, $d_i x_i = 0$, et donc, comme d_i divise d_r pour tout $i \in [\![1, r]\!]$, on en déduit : $\forall i \in [\![1, r]\!]$, $d_r x_i = 0$, ce qui signifie que $d_r(x_1, \ldots, x_r) = (0, \ldots, 0)$. Par conséquent l'ordre de $(x_1, \ldots, x_r)$ divise d_r : ceci montre que l'ordre de tout élément de G' est inférieur ou égal à d_r, donc d également, puisqu'il est supposé être le plus grand : on a $d \leqslant d_r$.
Mais il existe un élément qui est exactement d'ordre d_r : en effet, $\forall k \in [\![1, d_r - 1]\!]$, $k(0, \ldots, 0, 1) = (0, \ldots, 0, k) \neq (0, \ldots, 0)$, et : $d_r(0, \ldots, 0, 1) = (0, \ldots, 0)$. Ainsi d_r est le plus petit entier naturel non nul à annuler $(0, \ldots, 0, 1)$, donc c'est l'ordre de $(0, \ldots, 0, 1)$. Puisqu'il existe un élément d'ordre d_r, et que d est supposément le plus grand, on a $d_r \leqslant d$.
Ayant démontré que $d \leqslant d_r$ et $d_r \leqslant d$, on a en vérité $d = d_r$. Il est alors clair, d'après le premier paragraphe, que $d(x_1, \ldots, x_r) = (0, \ldots, 0)$ pour tout $(x_1, \ldots, x_r) \in G'$, d'où le résultat.

☢ Reconnaître une structure même quand l'énoncé ne l'explicite pas, et l'exploiter pour démontrer un résultat. □

Réponse.

1. On nous demande de dénombrer : $\{\bar{y} \in \mathbb{Z}/73\mathbb{Z} \mid \exists \bar{x} \in \mathbb{Z}/73\mathbb{Z},\ \bar{y} = \bar{x}^3\}$. C'est presque l'image du morphisme $\bar{x} \mapsto \bar{x}^3$ de $(\mathbb{Z}/73\mathbb{Z})^\times$ dans lui-même (il faut simplement enlever $\bar{0}$ qui est trivialement un cube). On peut dénombrer son image grâce au théorème d'isomorphisme, qui implique l'égalité entre

cardinaux : $\text{card}((\mathbb{Z}/73\mathbb{Z})^\times) = \text{card}(\ker(f))\text{card}(\text{im}(f))$. Or, comme souvent, déterminer un noyau est plus facile que déterminer une image. Ici : $\ker(f) = \{\bar{x} \in (\mathbb{Z}/73\mathbb{Z})^\times \mid \bar{x}^3 = \bar{1}\}$ peut difficilement se trouver par une résolution explicite. Il est plus avisé de remarquer que $\ker(f)$ est l'ensemble des éléments de $(\mathbb{Z}/73\mathbb{Z})^\times$ dont l'ordre divise 3 ; or 73 est premier, donc $(\mathbb{Z}/73\mathbb{Z})^\times$ est cyclique (résultat hors programme à savoir redémontrer), donc la structure des sous-groupes des groupes cycliques implique qu'il y a exactement 3 éléments d'ordre divisant 3. On en déduit : $\text{card}(\ker(f)) = 3$, puis : $\text{card}(\text{im}(f)) = \frac{\text{card}((\mathbb{Z}/73\mathbb{Z})^\times)}{3} = \frac{72}{3} = 24$. En conclusion :

$$\text{card}\left(\{\bar{y} \in \mathbb{Z}/73\mathbb{Z} \mid \exists \bar{x} \in \mathbb{Z}/73\mathbb{Z},\ \bar{y} = \bar{x}^3\}\right) = \text{card}\left(\text{im}(f) \cup \{\bar{0}\}\right) = 25.$$

2. On demande de montrer qu'il existe $k \in \mathbb{N} \setminus \{0\}$ tel que : $\sum_{i=0}^{k-1} 10^i \equiv 0 \bmod n$. Si l'on note $\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ l'application $\bar{x} \mapsto \overline{10x} + \bar{1}$, il est équivalent d'écrire qu'on veut l'existence de $k \in \mathbb{N} \setminus \{0\}$ tel que : $\sigma^k(\bar{0}) = \bar{0}$. Or σ est une permutation de $\mathbb{Z}/n\mathbb{Z}$ (en effet, puisque 10 est premier avec n, il est inversible modulo n, et la bijection réciproque de σ est alors $\bar{y} \mapsto \overline{10}^{-1}(\bar{y} - \bar{1})$), donc par le théorème de Lagrange il existe $k \in \mathbb{N} \setminus \{0\}$ tel que : $\sigma^k = \text{Id}$: il suffit de prendre $k = \text{card}(S_n) = n!$, même si l'on pourrait prendre largement plus petit. Pour ce choix de k, on a alors : $\sigma^k(\bar{0}) = \text{Id}(\bar{0}) = \bar{0}$, d'où le résultat : n divise $\sum_{i=0}^{k-1} 10^i = 11\cdots1$.

3. Cela revient à montrer que l'inclusion : $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{p}]$, est fausse, où $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2\right\}$, et : $\mathbb{Q}[\sqrt[3]{p}] = \left\{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid (a,b,c) \in \mathbb{Q}^3\right\}$. L'élève en exercice vérifiera que ce sont des corps, et qu'ils sont munis naturellement d'une structure de $\mathbb{Q}$-espace vectoriel, et on a facilement :

$$\dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = 2, \quad \dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{p}]) = 3.$$

Si l'inclusion $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{Q}[\sqrt[3]{p}]$ était vraie, alors $\mathbb{Q}[\sqrt[3]{p}]$ serait également muni d'une structure de $\mathbb{Q}[\sqrt{2}]$-espace vectoriel, où la multiplication externe serait définie par le produit dans $\mathbb{Q}[\sqrt[3]{p}]$. Alors, en notant $(\vec{e}_1, \ldots, \vec{e}_n)$ une $\mathbb{Q}[\sqrt{2}]$-base de $\mathbb{Q}[\sqrt[3]{p}]$, on vérifie que $(\vec{e}_1, \ldots, \vec{e}_n) \cup \left(\sqrt{2}\vec{e}_1, \ldots, \sqrt{2}\vec{e}_n\right)$ serait une $\mathbb{Q}$-base de $\mathbb{Q}[\sqrt[3]{p}]$ (vérification à faire ! ce n'est pas trivial). On aurait donc : $3 = \dim_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{p}]) = 2n$, ce qui est impossible puisque 2 ne divise pas 3. Par l'absurde, on a donc : $\mathbb{Q}[\sqrt{2}] \not\subseteq \mathbb{Q}[\sqrt[3]{p}]$, et donc $\sqrt{2} \notin \mathbb{Q}[\sqrt[3]{p}]$ (en effet, la stabilité par produit et somme d'un corps impliquerait l'inclusion qu'on vient de contredire), ce qui démontre le résultat voulu.

Étude spécifique des groupes

✓ Déterminer l'ordre d'un élément dans un groupe fini explicite. □

Réponse.

1. Explicitons le groupe $(\mathbb{Z}/15\mathbb{Z})^\times$. On a : $(\mathbb{Z}/15\mathbb{Z})^\times = \{\pm1, \pm2, \pm4, \pm7\}$.
Tout d'abord, 1 est bien sûr d'ordre 1 et -1 d'ordre 2. On a : $2^4 = 16 \equiv 1 \bmod 15$, donc 2 est d'ordre divisant 4, mais n'est pas d'ordre 1 ou 2 puisque : $2^2 = 4 \not\equiv 1 \bmod 5$. Donc 2 est d'ordre 4 et il en est de même de -2 comme on le vérifie aisément. Comme $4 = 2^2$, on en déduit aisément que 4 est d'ordre 2 (ce qu'un calcul direct montrerait), ainsi que -4. Il reste 7 et -7. Pour ces éléments, utilisons le théorème de Lagrange : comme $(\mathbb{Z}/15\mathbb{Z})^\times$ est de cardinal 8, l'ordre de 7 divise 8, et est donc égal à 1, 2, 4 ou 8. Or : $7^2 = 49 \equiv 4 \not\equiv 1 \bmod 15$, donc 7 n'est pas d'ordre 1 ou 2. Enfin : $7^4 \equiv 4^2 \equiv 1 \bmod 15$, donc 4 est la plus petite puissance à convenir et 7 est d'ordre 4. De même pour -7.
En conclusion, voici les différents ordres :

élément	1	-1	2	-2	4	-4	7	-7
ordre	1	2	4	4	2	2	4	4

On note que $(\mathbb{Z}/15\mathbb{Z})^\times$ n'est pas cyclique (aucun élément d'ordre 8, ou autre argument : il y a trois éléments d'ordre 2, à savoir 4, -4 et -1, alors qu'un groupe cyclique admet $\varphi(2) = 1$ éléments d'ordre 2, lorsque 2 divise son cardinal).

2. Comme $(6\ 2)^2 = \mathrm{Id}$, $(3\ 5\ 4)^3 = \mathrm{Id}$, et : $(1\ 10\ 8\ 9\ 7)^5 = \mathrm{Id}$, le fait que ces trois cycles commutent implique : $\sigma^{2\cdot3\cdot5} = \left((6\ 2)^2\right)^{3\cdot5}\left((3\ 5\ 4)^3\right)^{2\cdot5}\left((1\ 10\ 8\ 9\ 7)^5\right)^{2\cdot3} = \mathrm{Id}$. Donc l'ordre de σ divise $2\cdot3\cdot5$: il appartient donc à {1,2,3,5,6,10,15,30}. Mais $\sigma^k \neq \mathrm{Id}$ pour tout k dans cet ensemble, excepté 30. Donc σ est d'ordre 30.
3. Pour tout $k \in \mathbb{N}$, on a : $(1+n)^k = \sum_{j=0}^{k} \binom{k}{j} n^j \equiv 1 + kn \bmod n^2$. On en déduit que $(1+n)^k \equiv 1 \bmod n^2$ si et seulement si $kn \equiv 0 \bmod n^2$, si et seulement si n divise k. Donc n est le plus petit entier naturel au sens de la relation de divisibilité tel que $(1+n)^k \equiv 1 \bmod n^2$: on en déduit que $1+n$ est d'ordre n dans $\left((\mathbb{Z}/n^2\mathbb{Z})^\times, \cdot\right)$.

✓ Décomposer une permutation en cycles à supports disjoints. ☐

Réponse.

1. On a : $\sigma = (1\ 8\ 9\ 5\ 4\ 7\ 6\ 3)$, et : $\tau = (1\ 2)(3\ 6\ 8\ 9)(5\ 7)$. On en déduit : $\varepsilon(\sigma) = (-1)^7 = -1$, et : $\varepsilon(\tau) = (-1)\cdot(-1)^3\cdot(-1) = -1$.
2. On trouve, en utilisant le fait que $\sigma^6 = \mathrm{Id}$ pour les dernières puissances :

$$\sigma^2 = (1\ 3\ 5)(2\ 4\ 6), \quad \sigma^3 = (1\ 4)(2\ 5)(3\ 6), \quad \sigma^4 = \sigma^{-2} = (1\ 5\ 3)(2\ 6\ 4), \quad \sigma^5 = \sigma^{-1} = (1\ 6\ 5\ 4\ 3\ 2).$$

Peut-on trouver un lien entre le nombre de cycles, leur longueur, et l'exposant ?

✓ Utiliser le théorème de Fermat, d'Euler ou de Lagrange pour simplifier des puissances. ☐

Réponse.

1. Par le petit théorème de Fermat, on a : $13^{100} \equiv 1 \bmod 101$. Donc, en élevant cette égalité à la puissance 1000, on a : $13^{10^5} \equiv 1^{10^3} \equiv 1 \bmod 101$.
2. La réponse anticipe légèrement sur le chapitre IV. Tout d'abord, 2 est premier avec $105 = 3\times5\times7$, donc il appartient à $(\mathbb{Z}/105\mathbb{Z})^\times$. De plus : $\varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 2\cdot4\cdot6 = 48$, donc par le théorème d'Euler : $2^{48} \equiv 1 \bmod 105$. Pour simplifier $2^{5^{4^3}}$, nous allons exprimer 5^{4^3} à l'aide d'un multiple de 48 (pour exploiter le fait que $2^{48} \equiv 1 \bmod 105$) et du reste dans la division euclidienne de 5^{4^3} par 48 (pour se ramener à un exposant aussi petit que possible), ce qui revient à calculer 5^{4^3} modulo 48. Or 5 est premier avec $48 = 2^4\times3$, donc il appartient à $(\mathbb{Z}/48\mathbb{Z})^\times$. De plus : $\varphi(48) = 8\cdot2 = 16$, donc par le théorème d'Euler : $5^{16} \equiv 1 \bmod 48$. En élevant cette égalité à la puissance 4, on en déduit : $5^{4^3} \equiv 1 \bmod 48$. Il existe donc $k \in \mathbb{Z}$ tel que : $5^{4^3} = 48k + 1$. Donc : $2^{5^{4^3}} = \left(2^{48}\right)^k \cdot 2 \equiv 2 \bmod 105$, d'où le résultat.

★ Utiliser le théorème de Lagrange pour l'étude de sous-groupes et de parties génératrices. ☐

Réponse. On montre aisément que 1 est d'ordre 1, -1 d'ordre 2, et $\pm i$, $\pm j$, $\pm k$ d'ordre 4 (et il n'y a pas d'autre élément). Cela fournit déjà les sous-groupes :

$$\{1\}, \quad \langle -1\rangle = \{-1,1\}, \quad \langle \pm i\rangle = \{i,-1,-i,1\}, \quad \langle \pm j\rangle = \{j,-1,-j,1\}, \quad \langle \pm k\rangle = \{k,-1,-k,1\}.$$

Montrons qu'il n'y a pas d'autre sous-groupe strict : soit G un sous-groupe de $\mathbb{H}_8$. Par le théorème de Lagrange, son cardinal divise 8, donc il est égal à 1, 2, 4 ou 8. Les cas 1 et 8 sont triviaux (on a $G = \{1\}$ ou $G = \mathbb{H}_8$). S'il est de cardinal 2, alors il contient un élément non trivial qui doit être d'ordre 2, et c'est donc -1. On en déduit : $-1 \in G$, puis : $\langle -1\rangle \subseteq G$. En comparant les cardinaux : $G = \langle -1\rangle$.

Si G est de cardinal 4, alors ses éléments sont d'ordre 1 ou 2 ou 4. Mais ils ne peuvent pas tous être d'ordre 1 ou 2 (vu qu'il n'y a que 1 et -1 à avoir ces ordres : c'est insuffisant), donc il doit contenir un élément d'ordre 4, disons i par exemple. On a alors : $\langle i\rangle \subseteq G$, puis en comparant les cardinaux : $G = \langle i\rangle$. De même si G contient j ou k plutôt que i.

On a traité toutes les possibilités de cardinaux, donc la liste des sous-groupes est complète.

On en déduit aussi que $\{i,j\}$ est une partie génératrice de $\mathbb{H}_8$. En effet, $\langle i,j\rangle$ contient au moins 5 éléments (parmi ceux de $\langle i\rangle$ et $\langle j\rangle$, à savoir : i, 1, -1, $-i$, j), et comme son cardinal divise 8 on a : $\langle i,j\rangle = \mathbb{H}_8$. On ne peut pas trouver de partie génératrice à un seul élément d'après la description ci-dessus, donc $\{i,j\}$ est une partie génératrice de cardinal minimal.

Remarque. Le groupe $\mathbb{H}_8$ n'est pas cyclique bien que tous ses sous-groupes stricts le soient.

★ Utiliser la structure des groupes cycliques. □

Réponse.

1. On a : $(\overline{2q-1})^2 = \overline{4q\cdot q} - \overline{4q} + \bar{1} = \bar{1}$, donc $\overline{2q-1}$ est d'ordre divisant 2. Voyons si l'ordre peut être égal à 1 : c'est le cas si et seulement si $\overline{2q-1} = \bar{1}$, si et seulement si : $2q \equiv 2 \bmod 4q$, si et seulement si : $q \equiv 1 \bmod 2q$. Cela ne peut arriver que si $q = 1$. Si $q = 1$ alors $\overline{2q-1}$ est d'ordre 1, et sinon il est d'ordre 2.

   Un calcul analogue montre que $\overline{2q+1}$ est toujours d'ordre 2 (y compris si $q = 1$). Voyons comment en déduire si $(\mathbb{Z}/4q\mathbb{Z})^\times$ est cyclique ou non : si $q = 1$ c'est le cas parce que $(\mathbb{Z}/4\mathbb{Z})^\times = \{-1,1\}$ est engendré par -1, et si $q > 1$ alors il n'est pas cyclique. En effet, s'il était cyclique, alors il admettrait un unique sous-groupe de cardinal 2 ; or $\langle 2q-1\rangle \neq \langle 2q+1\rangle$ (car $\overline{2q-1} \neq \overline{2q+1}$ pour $q \geqslant 1$), donc cela fournit deux sous-groupes de $(\mathbb{Z}/4q\mathbb{Z})^\times$ de cardinal 2. Par l'absurde, $(\mathbb{Z}/4q\mathbb{Z})^\times$ n'est pas cyclique. (Autre argument : il devrait y avoir $\varphi(2) = 1$ élément d'ordre 2, et là nous en avons fourni deux.)

   En conclusion, $(\mathbb{Z}/4q\mathbb{Z})^\times$ est cyclique si et seulement si : $q = 1$.

2. On nous demande respectivement le nombre d'éléments de $(\mathbb{Z}/101\mathbb{Z})^\times$ d'ordre divisant 50, d'ordre divisant 12 et d'ordre divisant 7 (notons bien qu'une solution de ces équations doit être inversible modulo 101). Pour le dernier cas, l'affaire est vite entendue : comme l'ordre d'un élément de $(\mathbb{Z}/101\mathbb{Z})^\times$ doit diviser le cardinal du groupe, à savoir 100, et qu'on ne peut diviser 7 et 100 qu'à condition de diviser pgcd(7,100) = 1, l'unique élément d'ordre divisant 7 est $\bar{x} = \bar{1}$. Ainsi l'équation $\bar{x}^7 = \bar{1}$ admet une unique solution dans $\mathbb{Z}/101\mathbb{Z}$.

   Passons aux éléments d'ordre divisant 50 : d'après la propriété du cours sur les sous-groupes d'un groupe cyclique, ces éléments sont exactement les éléments de l'unique sous-groupe de cardinal 50 de $(\mathbb{Z}/101\mathbb{Z})^\times$.

   Autre point de vue, si l'on n'utilise pas ce résultat de cours (hors programme) : si $\varphi : ((\mathbb{Z}/101\mathbb{Z})^\times, \cdot) \to (\mathbb{Z}/100\mathbb{Z}, +)$ est un isomorphisme (qui existe puisque $(\mathbb{Z}/101\mathbb{Z})^\times$ est cyclique de cardinal 100), alors : $\bar{x}^{50} = \bar{1} \iff 50\varphi(\bar{x}) = \varphi(\bar{1}) = \tilde{0}$ (attention, ce $\tilde{0}$ représente 0 modulo 100), si et seulement si 100 divise $50\varphi(\bar{x})$, si et seulement si 2 divise $\varphi(\bar{x})$ (ou, plus rigoureusement, un représentant dans $\mathbb{Z}$ de $\varphi(\bar{x})$, mais je les confonds abusivement pour alléger les notations), si et seulement si : $\varphi(\bar{x}) \in \left\{\tilde{2}\tilde{k} \mid \tilde{k} \in \mathbb{Z}/100\mathbb{Z}\right\} = \langle\tilde{2}\rangle$. Or $\langle\tilde{2}\rangle$ admet $\frac{100}{2} = 50$ éléments (soit en invoquant le cours sur la forme des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, soit par une description explicite), donc $\varphi(\bar{x})$ peut prendre 50 valeurs différents. En prenant l'image par φ^{-1}, cela fournit 50 valeurs possibles pour les solutions $\bar{x} \in (\mathbb{Z}/101\mathbb{Z})^\times$ de $\bar{x}^{50} = \bar{1}$.

   Autre résolution avec un point de vue polynomial : comme 101 est un nombre premier, d'après le théorème de Fermat on a : $\forall \bar{x} \in \mathbb{Z}/101\mathbb{Z} \setminus \{\bar{0}\}$, $\bar{x}^{100} = \bar{1}$, donc $X^{100} - \bar{1}$ admet 100 racines dans $\mathbb{Z}/101\mathbb{Z}$, et comme $\mathbb{Z}/101\mathbb{Z}$ est un corps il ne peut en admettre plus : ainsi $X^{100} - \bar{1}$ est scindé et à racines simples sur $\mathbb{Z}/101\mathbb{Z}$. Or : $X^{100} - \bar{1} = (X^{50} - \bar{1})(X^{50} + \bar{1})$, donc l'unicité de la décomposition en facteurs irréductibles implique que $X^{50} - \bar{1}$ est scindé à racines simples aussi, et admet exactement 50 racines. Il existe donc exactement 50 solutions de : $\bar{x}^{50} = \bar{1}$.

   Passons aux éléments d'ordre 12. Comme 12 ne divise pas 100, ce qu'on a fait ci-dessus pour 50 ne s'adapte pas directement. Néanmoins on se ramène à un diviseur de 100 en remarquant que si $\bar{x} \in (\mathbb{Z}/101\mathbb{Z})^\times$, alors : $\bar{x}^{12} = \bar{1} \iff \bar{x}^4 = \bar{1}$. Il y a plusieurs façons d'y parvenir, la plus directe étant : si $\bar{x}^{12} = \bar{1}$, alors l'ordre de x divise 12. Mais l'ordre de x divise aussi le cardinal de $(\mathbb{Z}/101\mathbb{Z})^\times$, à savoir 100, donc il divise pgcd(12,100) = 4 (comment calculer ce pgcd, d'ailleurs ?). Donc : $\bar{x}^4 = \bar{1}$, la réciproque étant facile (élever au cube). Une autre démonstration de cette équivalence passe par une relation de Bezout : il existe $(u,v) \in \mathbb{Z}^2$ tel que : $4 = 12u + 100v$, et donc : $\bar{x}^4 = \left(\bar{x}^{12}\right)^u \left(\bar{x}^{100}\right)^v = \bar{1}$. Comme 4 divise 100, il est facile de vérifier que le raisonnement effectué pour 50 ci-dessus se transpose sans difficulté à 12, et on trouve $\frac{100}{4} = 25$ solutions de l'équation $\bar{x}^{12} = \bar{1}$.

Conclusion. Les équations $\bar{x}^{50} = \bar{1}$, $\bar{x}^{12} = \bar{1}$ et $\bar{x}^{7} = \bar{1}$, d'inconnue $\bar{x} \in \mathbb{Z}/101\mathbb{Z}$, ont respectivement 50, 4 et 1 solutions.

★ Déterminer les morphismes d'un groupe dans un autre. □

Réponse.

1. Soit $f : \mathbb{U}_n \to \mathbb{C}^*$ un morphisme de groupes. Pour déterminer f, il suffit de déterminer $f\left(e^{\frac{2i\pi}{n}}\right)$, puisque $e^{\frac{2i\pi}{n}}$ engendre $\mathbb{U}_n$. Or $e^{\frac{2i\pi}{n}}$ est d'ordre n, donc $f\left(e^{\frac{2i\pi}{n}}\right)$ est d'ordre divisant n dans $\mathbb{C}^*$. Autrement dit : c'est une racine n^{e} de l'unité. Considérons donc $k \in \mathbb{Z}$ tel que : $f\left(e^{\frac{2i\pi}{n}}\right) = e^{\frac{2i\pi k}{n}}$. Les morphismes f et $g_k : \omega \mapsto \omega^k$ (c'est facile de vérifier que c'en est effectivement un) coïncident sur $e^{\frac{2i\pi}{n}}$ qui engendre $\mathbb{U}_n$, donc : $f = g_k$.
   Conclusion. Les morphismes de $\mathbb{U}_n$ dans $\mathbb{C}^*$ sont exactement les applications de la forme $g_k : \omega \mapsto \omega^k$ avec $k \in \mathbb{Z}$ (on peut même prendre $k \in [\![0, n-1]\!]$). On pourrait démontrer que l'application $\bar{k} \mapsto g_k$ est correctement définie et est un isomorphisme entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{C}^*), \times)$ (on a un isomorphisme analogue en remplaçant $\mathbb{Z}/n\mathbb{Z}$ par n'importe quel groupe commutatif fini, mais la démonstration est subtile).
2. Soit $f : \mathbb{U}_n \to \mathbb{R}^*$ un morphisme de groupes. Pour déterminer f, il suffit de déterminer $f\left(e^{\frac{2i\pi}{n}}\right)$, puisque $e^{\frac{2i\pi}{n}}$ engendre $\mathbb{U}_n$. Or $e^{\frac{2i\pi}{n}}$ est d'ordre n, donc $f\left(e^{\frac{2i\pi}{n}}\right)$ est d'ordre divisant n dans $\mathbb{R}^*$; mais les seuls éléments d'ordre fini dans $\mathbb{R}^*$ sont 1 (qui est d'ordre 1) et -1 (qui est d'ordre 2), donc $f\left(e^{\frac{2i\pi}{n}}\right)$ est d'ordre 1 ou 2 en plus de diviser n. On en déduit que si n est impair, alors $f\left(e^{\frac{2i\pi}{n}}\right)$ ne peut être d'ordre 2 (sinon 2 diviserait n), et donc : $f\left(e^{\frac{2i\pi}{n}}\right) = 1$. Puisque f et $z \mapsto 1$ sont deux morphismes qui coïncident en $e^{\frac{2i\pi}{n}}$, qui engendre $\mathbb{U}_n$, on obtient : $f = 1$.
   Si n est pair, en revanche, il est possible que $f\left(e^{\frac{2i\pi}{n}}\right)$ soit d'ordre 2, et plus précisément que l'on ait : $f\left(e^{\frac{2i\pi}{n}}\right) = -1$. On obtient alors, par propriété de morphisme : $\forall k \in \mathbb{Z}$, $f\left(e^{\frac{2i\pi k}{n}}\right) = (-1)^k$. Réciproquement, cela définit bien un morphisme de $\mathbb{U}_n$ dans $\mathbb{R}^*$.
   Conclusion. Si n est impair, alors le seul morphisme de $\mathbb{U}_n$ dans $\mathbb{R}^*$ est trivial. Si n est pair, il y en a deux : le morphisme trivial, et le morphisme défini par $e^{\frac{2i\pi k}{n}} \mapsto (-1)^k$.
3. En raisonnant comme ci-dessus, on montre que si $f : \mathbb{U}_{n^2} \to \mathbb{U}_n$ est un morphisme de groupes, alors il existe $k \in \mathbb{Z}$ tel que : $f\left(e^{\frac{2i\pi}{n^2}}\right) = e^{\frac{2i\pi k}{n}} = \left(e^{\frac{2i\pi}{n^2}}\right)^{nk}$, donc f et l'application $g_k : \omega \mapsto \omega^{nk}$ (dont on vérifie que c'est bien un morphisme de groupes de $\mathbb{U}_{n^2}$ dans $\mathbb{U}_n$) coïncident sur le générateur $e^{\frac{2i\pi}{n}}$ et on en déduit : $f = g_k$.
   Conclusion. Les morphismes de $\mathbb{U}_{n^2}$ dans $\mathbb{U}_n$ sont exactement ceux de la forme $g_k : \omega \mapsto \omega^{nk}$ avec $k \in \mathbb{Z}$. On pourrait même restreindre k à $[\![0, n-1]\!]$.
   Remarque. Le noyau de g_k est $\mathbb{U}_{nk} \cap \mathbb{U}_{n^2} = \mathbb{U}_{nd}$ avec $d = \mathrm{pgcd}(k, n)$, et son image est $\mathbb{U}_{\frac{n}{d}}$. Exercice. En raisonnant semblablement pour les morphismes de $\mathbb{U}_n$ dans $\mathbb{U}_{n^2}$, on trouve que ces morphismes sont exactement ceux de la forme $h_k : \omega \mapsto \omega^k$ avec $k \in \mathbb{Z}$, qu'on peut restreindre à $k \in [\![0, n-1]\!]$.
4. On va d'une part exploiter les ordres des éléments de $\mathbb{H}_8$, et d'autre part que $\mathbb{H}_8$ n'est pas commutatif alors que $\mathbb{C}^*$ l'est. Soit $f : \mathbb{H}_8 \to \mathbb{C}^*$ un morphisme de groupes. On a : $f(ij) = f(i)f(j) = f(j)f(i) = f(ji)$, car $f(i)$ et $f(j)$ sont dans $\mathbb{C}^*$ et commutent donc. On en déduit : $f(ij(ji)^{-1}) = f(ij)f(ji)^{-1} = 1$. Or : $ij(ji)^{-1} = k \cdot (-k)^{-1} = k^2 = -1$ (pour l'égalité $ji = -k$: multiplier à gauche l'égalité $jk = i$ par j), donc : $f(-1) = 1$. Cela implique alors : $f(i) = f(-i)$, $f(j) = f(-j)$ et $f(k) = f(-k)$. Comme $f(1) = 1$ et $f(-1) = 1$ sont connus, on voit qu'il suffit de déterminer $f(i)$, $f(j)$ et $f(k)$ pour expliciter entièrement f. Mieux : comme $ij = k$, on a $f(i)f(j) = f(k)$, donc il suffit d'expliciter $f(i)$ et $f(j)$. On a : $f(i)^2 = f(i^2) = f(-1) = 1$, donc : $f(i) \in \mathbb{U}_2 = \{-1,1\}$, et il existe $\varepsilon_1 \in \{-1,1\}$ tel que : $f(i) = \varepsilon_1$. Par le même argument, il existe $\varepsilon_2 \in \{-1,1\}$ tel que : $f(j) = \varepsilon_2$. Ainsi, si f est un morphisme de $\mathbb{H}_8$ dans $\mathbb{C}^*$, il est défini par : $f(\pm 1) = 1$, $f(\pm i) = \varepsilon_1$, $f(\pm j) = \varepsilon_2$, et : $f(\pm k) = f(\pm i)f(\pm j) = \varepsilon_2\varepsilon_2$, avec $(\varepsilon_1, \varepsilon_2) \in \{-1,1\}^2$. Réciproquement, on vérifie que toute application ainsi définie est bien un morphisme.

Conclusion. Il y a quatre morphismes de $\mathbb{H}_8$ dans $\mathbb{C}^*$. On pourrait démontrer que l'application $(\varepsilon_1, \varepsilon_2) \mapsto f_{\varepsilon_1,\varepsilon_2}$ (où $f_{\varepsilon_1,\varepsilon_2}$ est ce que l'on a défini plus haut en fonction de ε_1 et ε_2) est un isomorphisme entre $(\{-1,1\}^2, \times)$ et $(\mathrm{Hom}(\mathbb{H}_8, \mathbb{C}^*), \times)$.

Remarque. Pour abréger la rédaction, on peut remarquer qu'une partie génératrice de $\mathbb{H}_8$ est $\{-1, i, j\}$ par exemple.

Remarque (G/H). Plus généralement, si $f : G \to A$ est un morphisme à valeurs dans un groupe A commutatif, on a toujours $f(ghg^{-1}h^{-1}) = 1_A$, et donc $ghg^{-1}h^{-1} \in \ker(f)$. Par conséquent, si l'on note $D(G)$ le sous-groupe engendré par les éléments de la forme $ghg^{-1}h^{-1}$ (c'est le *sous-groupe dérivé* de G), alors f induit un morphisme de $G/D(G)$ dans A par le théorème de factorisation des morphismes. Il peut être plus facile à expliciter parce que $G/D(G)$ est toujours commutatif (exercice), et plus petit que G. Par exemple, dans le cadre de cet exercice, on a implicitement démontré que $D(\mathbb{H}_8) = \{-1,1\}$, et comme $\mathbb{H}_8/\{-1,1\} = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (pourquoi ?), déterminer les morphismes $f : \mathbb{H}_8 \to \mathbb{C}^*$ se ramène à déterminer les morphismes $(\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{C}^*$. Les morphismes d'un tel groupe commutatif dans $\mathbb{C}^*$ s'obtiennent toujours assez facilement, en envoyant les générateurs « naturels » du groupe de départ sur n'importe quelles racines de l'unité dans $\mathbb{C}^*$ compatibles avec leurs ordres.

5. En imitant le raisonnement de la question précédente, on trouve qu'un morphisme $f : \mathbb{H}_8 \to \mathbb{Z}/n\mathbb{Z}$ vérifie : $f(-1) = \bar{0}$, puis qu'il suffit de déterminer $f(i)$ et $f(j)$ pour caractériser f. Or : $2 \cdot f(i) = f(i^2) = f(-1) = \bar{0}$, donc $f(i)$ est d'ordre divisant 2 dans $(\mathbb{Z}/n\mathbb{Z}, +)$. De même pour $f(j)$. On doit faire une distinction de cas pour poursuivre.

   Si n est impair, alors 2 ne divise pas le cardinal de $\mathbb{Z}/n\mathbb{Z}$ et donc, par la contraposée du théorème de Lagrange, $f(i)$ ne peut pas être d'ordre 2. Le seul élément d'ordre 1 dans $(\mathbb{Z}/n\mathbb{Z}, +)$ est $\bar{0}$, donc : $f(i) = f(j) = \bar{0}$, et par suite f est identiquement nulle.

   Si n est pair, alors 2 divise $\mathbb{Z}/n\mathbb{Z}$, or $\mathbb{Z}/n\mathbb{Z}$ est cyclique et on sait qu'il admet exactement un élément d'ordre 2 (à savoir $\overline{\frac{n}{2}}$). Comme $f(i)$ est d'ordre divisant 2, on a $f(i) = \bar{0}$ ou $f(i) = \overline{\frac{n}{2}}$, ce qu'on résume en disant qu'il existe $\varepsilon_1 \in \{\bar{0}, \bar{1}\}$ tel que : $f(i) = \overline{\varepsilon_1 \frac{n}{2}}$. De même, il existe $\varepsilon_2 \in \{\bar{0}, \bar{1}\}$ tel que : $f(j) = \overline{\varepsilon_2 \frac{n}{2}}$. Ainsi, si f est un morphisme de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$, avec n pair, il est défini par : $f(\pm 1) = \bar{0}$, $f(\pm i) = \overline{\varepsilon_1 \frac{n}{2}}$, $f(\pm j) = \overline{\varepsilon_2 \frac{n}{2}}$, et : $f(\pm k) = f(\pm i) + f(\pm j) = \overline{(\varepsilon_1 + \varepsilon_2)\frac{n}{2}}$, avec $(\varepsilon_1, \varepsilon_2) \in \{\bar{0}, \bar{1}\}^2$. Réciproquement, on vérifie que toute application ainsi définie est bien un morphisme.

   Conclusion. Si n est impair, alors le seul morphisme de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$ est le morphisme trivial. Si n est pair, alors il y a quatre morphismes de $\mathbb{H}_8$ dans $\mathbb{Z}/n\mathbb{Z}$.

☢ Penser au principe de conjugaison, en particulier dans S_n, pour simplifier une étude. □

Réponse.

1. On doit montrer que pour toutes doubles-transpositions σ et τ de S_4, on a : $\tau\sigma = \sigma\tau$, ce qui équivaut à : $\tau\sigma\tau^{-1} = \sigma$. Or, par le principe de conjugaison, si $\sigma = (a\ b)(c\ d)$ alors : $\tau\sigma\tau^{-1} = (\tau(a)\ \tau(b))(\tau(c)\ \tau(d))$. C'est égal à σ si et seulement si, par unicité de la décomposition en cycles à supports disjoints, on a une des deux conditions suivantes :
   — on a $\{\tau(a), \tau(b)\} = \{a, b\}$ et $\{\tau(c), \tau(d)\} = \{c, d\}$;
   — on a $\{\tau(a), \tau(b)\} = \{c, d\}$ et $\{\tau(c), \tau(d)\} = \{a, b\}$.

   On remarque que toutes les doubles-transpositions de S_4 (et l'identité) vérifient l'une ou l'autre condition : en effet, si une double-transposition τ ne vérifie pas l'une de ces deux conditions, on doit avoir par exemple $\{\tau(a), \tau(b)\} = \{a, c\}$ (quitte à inverser les rôles de a et b, ou de c et d, on peut nécessairement se ramener à ce cas), et dans ce cas $\tau(a) = c$ car une double-transposition de S_4 ne peut pas avoir de point fixe, et $\tau(b) = a$. Mais on doit aussi avoir : $\tau(c) = \tau^2(a) = a$ (en effet $\tau^2 = \mathrm{Id}$ car les transpositions sont d'ordre 2), donc $\tau(b) = \tau(c)$: cela contredit l'injectivité de τ.

   En résumé : toute double-transposition τ vérifie les conditions ci-dessus, donc $\tau\sigma\tau^{-1} = \tau$ est toujours vrai, et donc $\tau\sigma = \sigma\tau$ aussi. Ceci vaut pour tout $(\sigma, \tau) \in (V_4)^2$, donc c'est un groupe commutatif.

   Remarque. Un groupe dont tous les éléments sont d'ordre 1 ou 2 est toujours commutatif. C'est un exercice de travaux dirigés.

2. Soit M une matrice inversible d'ordre 2 telle que : $\forall A \in \mathrm{GL}_2(K)$, $AM = MA$. On a en particulier : $\forall A \in \mathrm{GL}_2(K)$, $A = MAM^{-1}$. Or, si D est une droite quelconque de K^2, et si A est la matrice de la symétrie

par rapport à D et parallèlement à n'importe quel supplémentaire de D, alors on vérifie aisément que MAM^{-1} est toujours une matrice de symétrie (car $(MAM^{-1})^2 = MA^2M^{-1} = M\mathrm{I}_2M^{-1} = \mathrm{I}_2$), par rapport à $M(D)$ (peu importe parallèlement à quoi : nous ne nous en servirons pas) puisque : $\forall X \in \mathrm{M}_{2,1}(K)$, $MAM^{-1}X = X \iff A(M^{-1}X) = M^{-1}X \iff M^{-1}X \in D \iff X \in M(D)$. L'égalité $A = MAM^{-1}$ implique donc que A serait une symétrie à la fois par rapport à D et $M(D)$, donc : $M(D) = D$.

Ceci vaut pour toute droite D de K^2, et c'est un résultat classique que cela implique : $\exists \lambda \in K^*$, $M = \lambda \mathrm{I}_2$. Pour le démontrer dans ce cas particulier : si $(\vec{e}_1, \vec{e}_2)$ est la base canonique de K^2, prendre successivement $D = K\vec{e}_1$, $D = K\vec{e}_2$ et $D = K(\vec{e}_1 + \vec{e}_2)$, et traduire l'égalité $M(D) = D$, implique l'existence de α, β et λ dans K tels que : $M\vec{e}_1 = \alpha\vec{e}_1$, $M\vec{e}_2 = \beta\vec{e}_2$, $M(\vec{e}_1 + \vec{e}_2) = \lambda(\vec{e}_1 + \vec{e}_2)$. On a donc : $\lambda(\vec{e}_1 + \vec{e}_2) = M(\vec{e}_1 + \vec{e}_2) = M\vec{e}_1 + M\vec{e}_2 = \alpha\vec{e}_1 + \beta\vec{e}_2$. Par indépendance linéaire de $\vec{e}_1$ et $\vec{e}_2$, cela implique : $\alpha = \beta = \lambda$. Donc : $M\vec{e}_1 = \lambda\vec{e}_1$, et : $M\vec{e}_2 = \lambda\vec{e}_2$. On en déduit : $M = \lambda \mathrm{I}_2$.

Réciproquement, toute matrice de cette forme commute avec les matrices de $\mathrm{GL}_2(K)$.

☢ Utiliser une action de groupe pour le dénombrement, trouver des parties génératrices, etc. □

Réponse.

1. On fait agir S_n sur $I(k,n)$ *via* le morphisme de S_n dans $S_{I(k,n)}$ défini par :

$$\sigma \mapsto (\varphi_\sigma : \iota \mapsto \sigma \circ \iota)\,.$$

La composée d'une injection et d'une bijection est une injection, donc φ_σ est effectivement à valeurs dans $I(k,n)$ pour tout $\sigma \in S_n$. Soit $\iota_0 : [\![1,k]\!] \to [\![1,n]\!]$ l'injection naturelle définie par $x \mapsto x$. On va étudier, comme souvent pour une action :

$$\mathcal{O} = \{\varphi_\sigma(\iota_0) \mid \sigma \in S_n\}\,, \quad \text{et :} \quad S_{\iota_0} = \{\sigma \in S_n \mid \varphi_\sigma(\iota_0) = \iota_0\}\,.$$

Nous allons montrer qu'en composant ι_0 par toutes les permutations de S_n, on obtient toutes les injections de $[\![1,k]\!]$ dans $[\![1,n]\!]$. Soit $\iota : [\![1,k]\!] \to [\![1,n]\!]$; montrons l'existence de $\sigma \in S_n$ telle que $\iota = \sigma \circ \iota_0 = \varphi_\sigma(\iota_0)$. Pour cela, on note que si σ existe, alors $\sigma^{-1} \circ \iota = \iota_0$. Puisque ι_0 est « presque » l'identité, σ^{-1} est « presque » l'application réciproque de ι ; une telle chose n'existe pas, puisque ι n'est pas bijective, mais néanmoins ι induit une bijection sur son image et nous allons y utiliser son application réciproque pour construire σ.

En effet, $\iota : [\![1,k]\!] \to [\![1,n]\!]$ induit une bijection de $[\![1,k]\!]$ dans $\iota([\![1,k]\!])$; notons $j : \iota([\![1,k]\!]) \to [\![1,k]\!]$ son application réciproque, qu'on complète arbitrairement en une application bijective $\tilde{j} : [\![1,n]\!] \to [\![1,n]\!]$ (par exemple en envoyant le plus petit élément de $[\![1,n]\!] \setminus \iota([\![1,k]\!])$ sur le plus petit élément de $[\![1,n]\!] \setminus [\![1,k]\!]$, puis de même avec le deuxième plus petit élément, etc. Ce procédé donne nécessairement une application injective de $[\![1,n]\!]$ dans lui-même, donc une bijection). En sa qualité d'application réciproque, on a :

$$\forall m \in [\![1,k]\!],\ \tilde{j} \circ \iota(m) = j \circ \iota(m) = m = \iota_0(m),$$

donc : $\tilde{j} \circ \iota = \iota_0$; il suffit alors de poser $\sigma = \tilde{j}^{-1}$ pour avoir : $\iota = \varphi_\sigma(\iota_0)$. On a montré :

$$\mathcal{O} = \{\varphi_\sigma(\iota_0) \mid \sigma \in S_n\} = I(k,n).$$

Passons au second ensemble : $S_{\iota_0} = \{\sigma \in S_n \mid \varphi_\sigma(\iota_0) = \iota_0\} = \{\sigma \in S_n \mid \forall m \in [\![1,k]\!],\ \sigma(m) = m\}$. On se convainc aisément que cet ensemble est un groupe isomorphe à $S_{[\![k+1,n]\!]}$, *via* l'application $\sigma \mapsto \sigma_{|[\![k+1,n]\!]}$. En particulier : $\mathrm{card}\,(S_{\iota_0}) = (n-k)!$.

On peut conclure en répondant à la question posée. Le cardinal cherché est : $\mathrm{card}(I(k,n)) = \mathrm{card}\,(\mathcal{O})$. On déduit de cette description une application naturelle surjective :

$$\left\{ \begin{array}{ccc} S_n & \to & I(k,n) = \mathcal{O} \\ \sigma & \mapsto & \varphi_\sigma(\iota_0) \end{array} \right.$$

et nous allons calculer le nombre d'antécédents de chaque élément de $I(k,n)$. Soit $\iota \in I(k,n)$, dont on note σ un antécédent. Alors :

$$\forall \sigma' \in S_n, \quad \varphi_{\sigma'}(\iota_0) = \varphi_\sigma(\iota_0) \iff \sigma' \circ \iota_0 = \sigma \circ \iota_0 \iff \sigma^{-1} \circ \sigma' \circ \iota_0 = \iota_0 \iff \sigma^{-1} \circ \sigma' \in S_{\iota_0} \iff \sigma' \in \sigma S_{\iota_0}.$$

Autrement dit : l'ensemble des antécédents de ι est σS_{ι_0}, et il y en a donc $\mathrm{card}(S_{\iota_0})$. Cela vaut pour tout ι. Donc, par le principe des bergers :

$$\mathrm{card}(S_n) = \mathrm{card}(S_{\iota_0})\mathrm{card}(I(k,n)),$$

et donc :

$$\mathrm{card}(I(k,n)) = \frac{\mathrm{card}(S_n)}{\mathrm{card}(S_{\iota_0})} = \frac{n!}{(n-k)!},$$

d'où le résultat.

2. On a : $\mathcal{O} = \{f(1) \mid f \in \langle r\rangle\} = \left\{r^k(1) \mid k \in \mathbb{Z}\right\} = \left\{e^{\frac{2i\pi k}{n}} \mid k \in \mathbb{Z}\right\} = \mathbb{U}_n$. Déterminons à présent : $S = \{f \in \mathrm{D}_n \mid f(1) = 1\}$. Si l'on interprète géométriquement S : il s'agit des transformations permutant les sommets d'un polygone régulier à n côtés (traduction de la condition $f(\mathbb{U}_n) \subseteq \mathbb{U}_n$) sans déplacer le sommet d'affixe 1 (traduction de l'égalité $f(1) = 1$). Il semble que seules l'identité et la réflexion par rapport à l'axe des abscisses conviennent. Montrons-le. Soit $f \in S$. Pour déterminer une application $\mathbb{R}$-linéaire, il suffit de l'expliciter sur une $\mathbb{R}$-base, disons la base $(1, i)$ de $\mathbb{C}$. On a $f(1) = 1$ par définition de S, et comme $f \in \mathrm{Is}(\mathbb{C})$ on a : $|f(i)| = |i| = 1$, donc il existe $\theta \in \mathbb{R}$ tel que : $f(i) = e^{i\theta}$. Au vu de notre conjecture formulée ci-dessus, on aimerait montrer : $f(i) = \pm i$, c'est-à-dire : $\theta \equiv \frac{\pi}{2} \bmod \pi$. Or on a d'une part : $|f(i) + f(1)|^2 = |f(i+1)|^2 = |i+1|^2 = 2$, et d'autre part : $|f(i) + f(1)|^2 = \left|e^{i\theta} + 1\right|^2 = 2^2\left(\cos\left(\frac{\theta}{2}\right)\right)^2$, donc : $\left(\cos\left(\frac{\theta}{2}\right)\right)^2 = \frac{1}{2}$, puis : $\frac{\theta}{2} \equiv \frac{\pi}{4} \bmod \frac{\pi}{2}$ (je formule de manière succincte le fait que les quatre angles à convenir modulo 2π soient $\frac{\pi}{4}$, $\frac{3\pi}{4}$, et leurs opposés). On en déduit : $\theta \equiv \frac{\pi}{2} \bmod \pi$, ce que je voulais démontrer. Donc : $f(i) = i$, ou : $f(i) = -i$. Dans le premier cas, f coïncide avec l'endomorphisme $\mathrm{Id}_{\mathbb{C}}$ sur la $\mathbb{R}$-base $(1, i)$, donc : $f = \mathrm{Id}_{\mathbb{C}}$. Dans le second cas, f coïncide avec l'endomorphisme $s : z \mapsto \bar{z}$, donc : $f = s$. Réciproquement, on vérifie aisément que ces deux endomorphismes sont dans S, donc : $S = \{\mathrm{Id}_{\mathbb{C}}, s\} = \langle s\rangle$.

On nous demande d'en déduire que D_n est engendré par r et s. Soit $f \in \mathrm{D}_n$. Comme $1 \in \mathbb{U}_n$, on a par définition de D_n l'appartenance suivante : $f(1) \in \mathbb{U}_n$. Or : $\mathbb{U}_n = \mathcal{O}$, donc il existe $k \in \mathbb{Z}$ tel que : $f(1) = r^k(1)$. Ainsi : $r^{-k} \circ f(1) = 1$, donc : $r^{-k} \circ f \in S = \langle s\rangle$, donc il existe $\ell \in \mathbb{Z}$ tel que : $r^{-k} \circ f = s^\ell$. On conclut : $f = r^k \circ s^\ell \in \langle r, s\rangle$, donc : $\mathrm{D}_n \subseteq \langle r, s\rangle$. L'inclusion réciproque est immédiate car r et s sont dans D_n, donc : $\mathrm{D}_n = \langle r, s\rangle$. Ce qu'il fallait démontrer.

Remarque. L'idée de calculer $|f(i) + f(1)|^2$ sera plus naturelle lorsqu'on définira les isométries au chapitre XII, et qu'on montrera notamment qu'une application $\mathbb{R}$-linéaire qui conserve les longueurs doit aussi conserver les angles droits (c'est ce que je fais implicitement pour montrer que, ayant : $1 \perp i$, on doit avoir : $1 = f(1) \perp f(i)$, et donc $f(i) = \pm i$). On le démontrera en passant par une identité de polarisation : c'est implicitement ce que je fais ici, puisque $(z_1, z_2) \mapsto \mathrm{Re}(\overline{z_1}z_2) = \frac{1}{2}\left(|z_1 + z_2|^2 - |z_1|^2 - |z_2|^2\right)$ est l'écriture intrinsèque du produit scalaire usuel du plan complexe.

3 Feuilles d'exercices

3.1 Indications et commentaires

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 $\text{card}(H \cap K)$ 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 **??** du chapitre II et que l'on revoit implicitement au chapitre IV, dans les exercices **??** à **??**.
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 **??** du chapitre IV. Elle apparaît aussi dans l'exercice **??** 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 $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

★ **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 $\text{card}(G) = \text{card}(\ker(f))\text{card}(\text{im}(f))$ abondent en ce sens et montrent aussi que cette observation pourrait être faite pour le noyau de f : il est intimement lié à $\text{card}(\ker(f))$, mais aussi à $\text{card}(\text{im}(f))$ qui est un diviseur de $\text{card}(H)$. 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 **??** 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 $K = \{g' \in G \mid \varphi_{g'}(x) = x\}$, 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 **??** 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.

3.2 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

Table des matières