Du cours aux exercices (Aide à la révision du cours)

Chapitre III — Structures algébriques

1 Rappels et compléments

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.

1.2 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.

1.3 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.

1.4 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.

2 Groupes

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$^\circ$ 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.*

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 ?
☢	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*.

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.

Table des matières