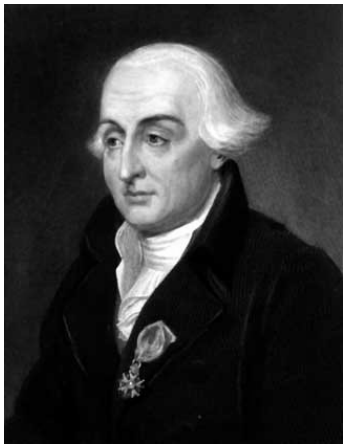
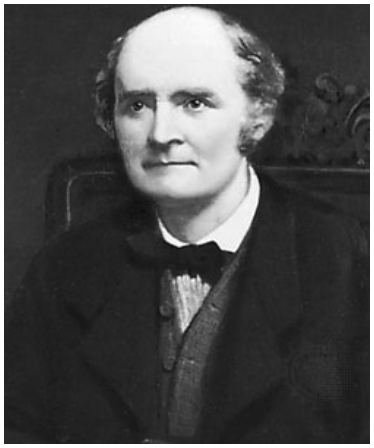
Chapitre III — Structures algébriques



Joseph-Louis Lagrange
(1736–1813)

Évariste Galois
(1811–1832)



Arthur Cayley
(1821–1895)

Révisions attendues

1. L'intégralité du cours de 1re année sur les structures.
2. L'intégralité des résultats sur le groupe symétrique.

Vos révisions sont insuffisantes si vous ne parvenez pas à faire ces exercices :

Exercice 1.

1. On définit une relation binaire R sur $\mathbb{R}^*$ par : $\forall (x,y) \in (\mathbb{R}^*)^2$, $xRy \iff xy > 0$. Montrer que R est une relation d'équivalence et décrire ses classes.
2. Soit $f : E \to F$ une application. On définit une relation binaire R sur E par : $\forall (x,y) \in E^2$, $xRy \iff f(x) = f(y)$. Montrer que R est une relation d'équivalence et décrire ses classes.
3. Montrer que sur $\mathrm{M}_n(K)$, les relations « être équivalente à » et « être semblable à » définissent des relations d'équivalence. Décrire les classes pour la première relation.

Exercice 2. Déterminer les entiers $x \in \mathbb{Z}$ tels que : $3x \equiv 1 \bmod 7$. Même question avec : $3x \equiv 1 \bmod 51$, $5x \equiv 0 \bmod 30$, et : $5x \equiv 0 \bmod 19$.

Exercice 3. Soit $p \in \mathbb{N} \setminus \{0\}$. Montrer que $\left\{ e^{\frac{2ik\pi}{p^n}} \mid (k,n) \in \mathbb{Z} \times \mathbb{N} \right\}$ est un sous-groupe de $\mathbb{C}^*$.

Exercice 4. Soit G un groupe tel que : $\forall x \in G$, $x^2 = 1_G$. Montrer que G est commutatif.

Exercice 5.

1. Soient G un groupe et $g \in G$. Montrer que $\iota_g : h \mapsto ghg^{-1}$ est un automorphisme du groupe G.
2. Montrer que $g \mapsto \iota_g$ définit un morphisme de groupes de G dans S_G, et déterminer son noyau.

Exercice 6. Montrer que $\left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ isomorphe à $\mathbb{Z}$.

Exercice 7.

1. Déterminer les morphismes de corps de $\mathbb{R}$ dans lui-même.
2. Montrer qu'un morphisme de corps est toujours injectif.

Exercice 8.

1. Montrer que $F = \mathrm{Vect}_{\mathbb{C}} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right)$ est un corps isomorphe à $\mathbb{C}$.
2. Montrer que $\mathbb{Q}(\sqrt{3}) = \left\{ a + b\sqrt{3} \mid (a,b) \in \mathbb{Q}^2 \right\}$ est un corps. Est-il isomorphe à $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2 \right\}$?

Exercice 9.

1. Décomposer en cycles à supports disjoints $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 6 & 7 & 4 & 3 & 1 & 9 & 8 \end{pmatrix}$.
2. Calculer σ^{-1}.
3. Décrire l'ensemble $\left\{ \sigma^k \mid k \in \mathbb{Z} \right\}$, et donner le plus petit entier naturel k non nul tel que : $\sigma^k = \mathrm{id}$.

Exercice 10. Montrer que $\{(12)(34), (13)(24), (14)(23), \mathrm{id}\}$ est un sous-groupe de S_4 et qu'il est commutatif.

1 Rappels et compléments

Sauf mention explicite du contraire, dans tout ce chapitre la lettre G désigne un groupe dont la loi de composition interne est notée $\cdot$. Son élément neutre est noté 1_G ou e_G. Pour tout $x \in G$ et tout $k \in \mathbb{N}$, l'élément x^k de G désigne $x \cdots x$ (k fois).

La loi du groupe sera occasionnellement notée additivement ($+$). En ce cas, on préférera écrire 0_G l'élément neutre, et $kx = x + \cdots + x$ plutôt que x^k.

La lettre A désignera un anneau unitaire dont les lois sont implicitement $+$ et $\times$. L'élément neutre pour la multiplication est noté génériquement 1_A.

1.1 Sur les morphismes

Le principe moral des isomorphismes.

Exemple 1. Les isomorphismes préservent la commutativité.

Exemple 2. Les isomorphismes préservent le nombre de sous-groupes de cardinal donné. → prop. 26

Exemple 3. Morphisme injectif à valeurs dans un anneau intègre.

> Un isomorphisme conserve TOUT ce qui est relatif à la structure.

1.2 Sur les relations d'équivalence

Définition 1 (Relation d'équivalence, classe d'équivalence, ensemble quotient, système complet de représentants)**.**

Notations.

Exemple 4. Relation d'équivalence mesurant le défaut d'injectivité d'une application.

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

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

Exemple 5. Construction de $\mathbb{Q}$ et $K[X]$.

Exercice 11. (Construction de $\mathbb{Z}$) Cet exercice fournit une construction rigoureuse de $\mathbb{Z}$. Soit R la relation sur $\mathbb{N}^2$ définie par : $\forall (a,b) \in \mathbb{N}^2,\ \forall (c,d) \in \mathbb{N}^2,\ (a,b)\ R\ (c,d) \iff a+d = c+b$.

1. Montrer que R est une relation d'équivalence. Il y a une subtilité dans la propriété de transitivité : l'objectif de l'exercice étant de *construire* $\mathbb{Z}$, vous ne pouvez pas utiliser la soustraction *a priori*.

On pose : $\mathbb{Z} = \mathbb{N}^2/R$, et :

$$\forall (\overline{(a,b)}, \overline{(c,d)}) \in \mathbb{Z}^2, \quad \overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a+c, b+d)}, \quad \overline{(a,b)} \otimes \overline{(c,d)} = \overline{(ac+bd, ad+bc)}.$$

2. Montrer que les lois $\oplus$ et $\otimes$ sont correctement définies (c'est-à-dire : si $\overline{(a',b')} = \overline{(a,b)}$, a-t-on bien $\overline{(a,b)} \oplus \overline{(c,d)} = \overline{(a',b')} \oplus \overline{(c,d)}$? de même pour $\otimes$) et que $(\mathbb{Z}, \oplus, \otimes)$ est un anneau.
3. Montrer que l'application $(\mathbb{N}, +, \times) \to (\mathbb{Z}, \oplus, \otimes)$, définie par $n \mapsto \overline{(n,0)}$ est un morphisme *injectif* de semi-anneaux (c'est la même définition que pour un morphisme d'anneaux ; le terme « semi » est nécessaire parce que $(\mathbb{N}, +)$ n'est pas un groupe).

Comme un morphisme injectif induit un isomorphisme sur son image, et qu'un isomorphisme conserve tout ce qui est relatif à la structure, on peut abusivement identifier $\mathbb{N}$ *et* $\iota(\mathbb{N})$*, de sorte que par cette identification on a :* $\mathbb{N} \subseteq \mathbb{Z}$*. Pour cette même raison, il n'y a pas de risque de confusion en notant* $\oplus = +$ *et* $\otimes = \times$*.*

4. Montrer que pour tout $\overline{(a,b)} \in \mathbb{Z}$, il existe un unique $c \in \mathbb{N}$ tel que $\overline{(a,b)} = \overline{(c,0)} = c$ (la dernière égalité vient de l'identification entre $\mathbb{N}$ et $\iota(\mathbb{N})$) ou $\overline{(a,b)} = \overline{(0,c)}$.

On pose : $\forall c \in \mathbb{N}$, $-c = \overline{(0,c)}$*. Cette question démontre que tout entier relatif est de la forme* c *ou* $-c$ *avec* $c \in \mathbb{N}$*. On pose aussi :* $a - b = a + (-b) = \overline{(a,0)} + \overline{(0,b)} = \overline{(a,b)}$*. On a défini rigoureusement tout ce que vous connaissiez sur* $\mathbb{Z}$*.*

1.3 Groupes quotients

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

Remarque. Cas additif.

Le principe moral des groupes quotients.

Passer de G à G/H, c'est « rendre triviaux » les éléments de H.

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

Notation.

Remarque. D'autres systèmes complets de représentants sont possibles.

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

Démonstration (idée). Écrire : $G = \bigsqcup_{i=1}^{r} \mathfrak{cl}_{\sim}(x_i)$, où les x_i forment un système complet de représentants pour la relation d'équivalence associée au sous-groupe H. Montrer : $\forall i \in [\![1,r]\!]$, $\mathfrak{cl}_{\sim}(x_i) = x_i H$, et conclure en comparant les cardinaux. □

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

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

Exemple 6. Isomorphisme entre $\mathbb{U}$ et $\mathbb{R}/2\pi\mathbb{Z}$.

Exemple 7. Un analogue du théorème du rang pour les morphismes de groupes. ♡

Démonstration alternative. Écrire : $G = \bigsqcup_{y \in \mathrm{im}(f)} f^{-1}(\{y\})$ et comparer les cardinaux, en remarquant que pour un MORPHISME, toutes les fibres $f^{-1}(\{y\})$ ont le même cardinal. □

1.4 Anneaux quotients

Définition 9 (Idéal d'un anneau)**.**

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

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

Proposition 12 (Anneaux quotients)**.**

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

Exemple 8. Critère de divisibilité par 11.

Exemple 9. Construction de $\mathbb{C}$.

Exercice 12. Décrire les éléments de l'anneau quotient $A = \mathbb{Z}/4\mathbb{Z}[X]/(2X-1)$.

Culture scientifique. Construction de $\mathbb{R}$.

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

2 Groupes

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

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

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

Remarque. Cas où G est commutatif.
Remarque. Description de $\langle x \rangle$ dans le cas additif.
Remarque. Élément d'ordre 1.

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

Remarque. Reformulation équivalente en termes d'ordre.
Remarque. Un groupe monogène est nécessairement commutatif.

Exemple 10. Le groupe $\mathbb{U}_n$ est cyclique.

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

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

↗ IV th. 16

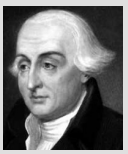
Démonstration (idée). Si $H \neq \{0\}$ est un sous-groupe, effectuer la division euclidienne de $x \in H$ par le plus petit entier strictement positif n de H. Montrer que le reste appartient à H, et conclure par minimalité de n. □

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

Exemple 11. Ordre de $\sigma = (12)(345) \in S_5$.

Exemple 12. Si m et n sont deux entiers naturels non nuls et non premiers entre eux, alors $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est pas cyclique.

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



1736-1813

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

Exercice 13. Nous proposons deux démonstrations de ce résultat, toutes les deux très instructives, l'une n'étant valable que si G est commutatif.

1. Soit $g \in G$. Montrer que l'application $\varphi_g : x \mapsto gx$ est une bijection de G dans G.

2. Première démonstration. On suppose G commutatif. Justifier : $\prod_{x\in G} x = \prod_{x\in G} \varphi_g(x)$, et conclure.
3. Deuxième démonstration, sans hypothèse de commutativité.
   (a) Montrer que l'application $g \mapsto \varphi_g$ est un morphisme injectif de G dans S_G, et que g et φ_g ont même ordre pour tout $g \in G$.
   (b) Soit $g \in G$. Soit d l'ordre de g. Dans la décomposition de φ_g en cycles à supports disjoints, montrer que tous les cycles sont de longueur d.
   (c) Montrer que l'ensemble des points fixes de φ_g est $\emptyset$ si $g \neq 1_G$ et G si $g = 1_G$.
   (d) À quoi doit être égale la somme des longueurs des cycles apparaissant dans la décomposition à supports disjoints d'une permutation ? Conclure.

Exemple 13. Les groupes de cardinal premier sont cycliques. ♡

Exemple 14. Ordres de $\bar{2}$ et $\bar{3}$ dans $(\mathbb{Z}/31\mathbb{Z})^\times$.

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

Remarque. Caractérisation de l'ordre en termes d'isomorphisme.
Remarque. L'application $k \bmod n \mapsto g^k$ est correctement définie.
Remarque. Unicité à isomorphisme près des groupes de cardinal premier.

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

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

Exercice 14. Déduire de cette proposition une condition nécessaire et suffisante pour être un élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ (l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour la multiplication).

Exemple 15. Condition nécessaire et suffisante pour que $\bar{2}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$.

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

Exemple 16. Racines primitives n^{es} de l'unité. ♡

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

Démonstration (idée). Se ramener aux sous-groupes de $\mathbb{Z}$ en prenant l'image réciproque par le morphisme naturel $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. □

← ex. 2

Remarque. Trois représentations possibles de l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d.

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

2.3 Approfondissements sur le groupe symétrique

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

Le principe de conjugaison : un principe fondamental.

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

Démonstration (idée). Montrer : $\tau(a_1 \cdots a_p)\tau^{-1} = (\tau(a_1) \cdots \tau(a_p))$, en calculant l'image d'un $x \in [\![1, n]\!]$ par chacun des membres de l'égalité. Faire une distinction de cas, selon que x appartienne au support du p-cycle du membre de droite ou non. □

Exemple 17. Parties génératrices plus petites de S_n. ♡

Exemple 18. Centre de S_n. ♡

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

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

Exemple 19. Description explicite de A_4.

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

— Fin du chapitre III —

Compléments et approfondissements

1. On a utilisé le théorème de Lagrange pour montrer que l'ordre d'un élément divise le cardinal de son groupe. Il y a néanmoins de très nombreuses façons de l'utiliser. Il y en a quatre, dont deux déjà illustrées dans ce cours : 1° pour simplifier le calcul de puissances (profitant de l'égalité $x^{\mathrm{card}(G)} = 1_G$ valable pour tout $x \in G$), 2° pour déterminer l'ordre d'un élément par élimination, 3° pour déterminer une famille génératrice d'un groupe fini (card $(\langle S \rangle)$ est divisible par les ordres de tous ses éléments ; si l'on a assez de diviseurs, on peut en déduire $\langle S \rangle = G$), 4° il contraint l'image de certains éléments par un morphisme (si $f : G \to G'$ est un morphisme et $x \in G$ d'ordre d, alors $f(x)$ est d'ordre divisant d et $\mathrm{card}(G')$: cela élimine plusieurs possibilités). Dans le cours comme dans les exercices, on s'efforcera de reconnaître chacune des quatre applications et de les utiliser à propos.
2. On peut approfondir la connaissance de S_n : systèmes de générateurs, morphismes de S_n dans d'autres groupes, etc. À cet égard, le principe de conjugaison est à avoir parfaitement à l'esprit. On commencera par identifier les manières de l'utiliser dans ce cours.

   Pour se l'approprier, l'étudiant patient pourra dresser dans son temps libre la liste de tous les sous-groupes de S_n pour $n \in [\![2,4]\!]$ et identifiera pour chacun d'entre eux une partie génératrice, et quels sous-groupes s'obtiennent les uns à partir des autres par conjugaison.

   Le groupe S_n est une source féconde de problèmes combinatoires : quel est l'ordre maximal d'un élément de S_n ? (Cela passe notamment par une compréhension fine des cycles et de leurs puissances.) Combien y a-t-il de cycles de longueur donnée ? De permutations dont la décomposition fait intervenir un nombre donné de cycles de longueurs données ? etc.
3. Un groupe est réellement intéressant lorsqu'il *agit* sur un ensemble (comme le groupe des permutations qui agit sur $[\![1,n]\!]$, ou le groupe linéaire sur K^n, etc.). Bien qu'il me semble trop ambitieux de traiter la théorie des *actions de groupe* en classes préparatoires, il est instructif d'en voir quelques cas particuliers en exercices : pour la combinatoire et le dénombrement de solutions, ou pour obtenir aisément des parties génératrices de certains groupes. Le cas particulier de l'action par conjugaison $g \mapsto (h \mapsto ghg^{-1})$ permet d'étudier la commutation dans un groupe (existence d'un centre non trivial, etc.).
4. Les notions de *caractéristique* ou de *sous-anneau premier* d'un anneau permettent de mieux comprendre comment ils sont construits (à partir de $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$, avec adjonction d'éléments). Elles fournissent par ailleurs un beau panaché « algèbre linéaire + théorie des corps », puisqu'on peut toujours munir un corps d'une structure d'espace vectoriel sur son sous-corps premier. Une application classique de cette stratégie est la démonstration que les corps finis ont nécessairement un cardinal de la forme p^k avec p premier et $k \in \mathbb{N} \setminus \{0\}$.

Les compléments et approfondissements sur l'arithmétique de $\mathbb{Z}/n\mathbb{Z}$, l'usage des groupes cycliques, la détermination des idéaux d'un anneau et les extensions de corps seront dans le chapitre IV. Les groupes d'isométries seront étudiés au chapitre XII.

Table des matières