Sous-groupes normaux, quotients

Sommaire

1 Sous-groupes normaux, groupes simples **1**
- 1.1 Sous-groupes normaux . . . 1
- 1.2 Groupes simples . . . 3
- 1.3 Sous-groupes normaux de $\mathcal{S}_n$ . . . 5
- 1.4 Sous-groupes normaux minimaux d'un groupe fini . . . 7

2 Quotients **8**
- 2.1 Généralités et premiers exemples . . . 9
- 2.2 Les « théorèmes d'isomorphisme » . . . 12
- 2.3 Le théorème de Goursat . . . 14

3 Structure normale **15**
- 3.1 Suites de composition . . . 16
- 3.2 Groupe dérivé et abélianisé . . . 18
- 3.3 Groupes résolubles . . . 20

1 Sous-groupes normaux, groupes simples

Les notions de sous-groupe normal et de groupe simple apparaissent d'elles-mêmes lorsqu'est formulé le problème du quotient. Elle sont ici introduites de façon axiomatique et illustrées par deux exemples classiques : groupes alternés $\mathcal{A}_n$ pour $n \geq 5$, groupe des isométries directes d'un espace euclidien de dimension 3. Le paragraphe **1.4**, optionnel, décrit les sous-groupes normaux minimaux d'un groupe fini.

1.1 Sous-groupes normaux

Le sous-groupe H de G est dit *normal (ou distingué)* dans G si

$$\forall (g,h) \in G \times H, \qquad ghg^{-1} \in H.$$

On note alors :

$$H \triangleleft G.$$

Dire que H est normal dans G, c'est dire que H est une réunion de classes de conjugaison de G, ou encore que H est stable par les automorphismes intérieurs de G. C'est encore dire que les classes à droite et à gauche modulo H coïncident, car

$$\forall (g,h) \in G \times H, \qquad gh = ghg^{-1}g.$$

Exemples

1. *Sous-groupes centraux*
   Tout sous-groupe central de G (c'est-à-dire contenu dans le centre de G) est normal dans G. En particulier, tout sous-groupe d'un groupe abélien est normal.
2. *Intersection d'un sous-groupe et d'un sous-groupe normal*
   Si N est un sous-groupe normal de G et H un sous-groupe de G, $H \cap N$ est un sous-groupe normal de H.
3. *Sous-groupes d'indice* 2
   Le résultat ci-après est suffisamment utile pour mériter le statut de lemme.

   Lemme 1. *Tout sous-groupe d'indice*[1] *2 de G est normal dans G.*

   Preuve. Soient H un tel sous-groupe, $a \in G \setminus H$ de sorte que $G \backslash H = aH$. Soit $g \in G$. On veut établir $gHg^{-1} \subset H$. Si $g \in H$, c'est clair. Sinon, g s'écrit ah avec $h \in H$, et tout revient à vérifier $aHa^{-1} \subset H$. Dans le cas contraire, il existerait h et h' dans H tels que : $aha^{-1} = ah'$, i.e. $ah^{-1} = h'^{-1}$, contradiction.
4. *Sous-groupes caractéristiques*
   Un sous-groupe de G est dit *caractéristique* s'il est stable par tout automorphisme de G. Comme les automorphismes intérieurs sont des automorphismes, tout sous-groupe caractéristique de G est normal.
5. *Le sous-groupe de Klein de $\mathcal{S}_4$*
   Le groupe de Klein $\mathcal{V}$ est la réunion de deux classes de conjugaison de $\mathcal{S}_4$, donc normal dans $\mathcal{S}_4$.
6. *Les sous-groupes de $\mathcal{H}_8$ sont normaux*
   Le groupe $\mathcal{H}_8$ n'est pas abélien, mais tous ses sous-groupes sont normaux ; c'est une conséquence du résultat suivant, dont la vérification est immédiate. [2]

   Lemme 2. *Le treillis des sous-groupes de $\mathcal{H}_8$ est le suivant :*

$$\begin{array}{ccccccc} & & & & \{\pm id\,, \pm I\} & & \\ & & \nearrow & & & \searrow & \\ \{id\,\} \to \{\pm id\,\} & \to & & \{\pm id\,, \pm J\} & & \to & \mathcal{H}_8 \\ & & \searrow & & & \nearrow & \\ & & & & \{\pm id\,, \pm K\} & & \end{array}$$

Exercice 1. ② *Soient N un sous-groupe normal de G et H un sous-groupe caractéristique de N. Montrer que H est normal dans G.*

Exercice 2. ② *Indiquer un groupe fini G et deux sous-groupes H et N de G tels que : $N \subset H$, que N (resp. H) soit normal dans H (resp. G) mais que N ne soit pas normal dans G.*

---

1. Rappelons que l'indice de H dans G est le cardinal de l'ensemble quotient G/H des classes (à droite ou à gauche) modulo H ; il est égal à $\frac{|G|}{|H|}$ si G est fini. Plus de détails dans le paragraphe **2.1**.
2. Les groupes non abéliens dont tous les sous-groupes sont normaux sont dits *hamiltoniens*. Baer a classé les groupes hamiltoniens finis.

L'exercice ci-après généralise l'exemple 3.

Exercice 3. ④ *Soient G un groupe fini, p le plus petit diviseur premier de $|G|$, H un sous-groupe de G d'indice p. Montrer que H est normal dans G. On pourra considérer l'action de G sur G/H par translation.*

1.2 Groupes simples

La notion de sous-groupe normal suggère une définition : un groupe G est dit *simple* s'il est non nul et si ses seuls sous-groupes normaux sont G et le sous-groupe nul. [3]

Exemple *Groupes simples abéliens*

Si p est premier et si G est un groupe fini d'ordre p, le théorème de Lagrange montre que les seuls sous-groupes de G sont $\{e\}$ et G. En particulier, G est simple [4].

Voici une conséquence immédiate mais très utile de la définition.

Lemme 3. *Tout morphisme non nul dont la source est un groupe simple est injectif.*

En d'autres termes, un morphisme dont la source est un groupe simple est trivial ou injectif.

Exercice 4. ③ *Soit G un groupe infini simple. Montrer que G ne possède pas de sous-groupe d'indice fini autre que G. On supposera par l'absurde l'existence d'un tel sous-groupe H et on utilisera l'action par translation de G sur G/H.*

Exercice 5. ④ *Soit m un élément de $\mathbb{N}^*$. Montrer que, si G est un groupe simple possédant une classe de conjugaison de cardinal m, G est isomorphe à un sous-groupe de $\mathcal{S}_m$ [5]. On utilisera l'action par translation de G sur G/H, où H est le commutant d'un élément de la classe de conjugaison de cardinal m.*

Nous allons présenter deux démonstrations de simplicité instructives. La première concerne $\mathcal{A}_5$, qui est le « plus petit groupe simple dont le cardinal n'est pas premier ». [6]

Théorème 1. *Le groupe $\mathcal{A}_5$ est simple.*

Preuve. Nous allons présenter une démonstration très pédestre. Nous allons déterminer les classes de conjugaison de $\mathcal{A}_5$ et montrer que les seules réunions de classes de conjugaison contenant e et dont le cardinal divise 60 sont $\{\mathrm{id}\}$ et $\mathcal{A}_5$. Il en résultera, via le théorème de Lagrange, qu'aucun sous-groupe non trivial de $\mathcal{A}_5$ est réunion finie de classes de conjugaison.

Les classes de conjugaison de $\mathcal{S}_5$ sont données par le type cyclique ; en particulier, $\mathcal{A}_5$ est réunion de quatre classes de conjugaison de $\mathcal{S}_5$: les 20 trois-cycles, les 15 doubles transpositions, les 24 cinq-cycles et l'identité.

3. De même que 1 n'est pas un nombre premier, le groupe nul n'est pas simple.

4. Rappelons qu'un groupe d'ordre. p est cyclique, engendré par n'importe lequel de ses éléments autre que e.

5. À isomorphisme près, il n'y a donc qu'un nombre fini de sous-groupes possédant une classe de conjugaison de cardinal m.

6. Précisément, on peut établir que, parmi les groupes d'ordre non premier inférieur ou égal à 60, $\mathcal{A}_5$ est le seul groupe simple.

Cependant, deux éléments de $\mathcal{S}_5$ conjugués dans $\mathcal{S}_5$ peuvent ne pas rester conjugués dans $\mathcal{A}_5$. Étudions ce phénomène. Soient σ et σ' deux éléments de $\mathcal{A}_5$ tels qu'existe $g \in \mathcal{S}_5 \setminus \mathcal{A}_5$ vérifiant $\sigma' = g \circ \sigma \circ g^{-1}$. Pour h dans $\mathcal{A}_5$, on a

$$\sigma' = h \circ \sigma \circ h^{-1} \Longleftrightarrow (g^{-1} \circ h) \circ \sigma = \sigma \circ (g^{-1} \ \circ h).$$

Puisque l'application $h \longmapsto g^{-1} \circ h$, est une bijection de $\mathcal{S}_5 \setminus \mathcal{A}_5$ sur $\mathcal{A}_5$, on en déduit les points suivants :

- s'il existe une permutation impaire commutant à σ, les classes de conjugaison de σ dans $\mathcal{A}_5$ et $\mathcal{S}_5$ sont égales ;

- sinon, la classe de conjugaison de σ dans $\mathcal{S}_5$ est réunion disjointe de deux classes de conjugaison de $\mathcal{A}_5$ de même cardinal.

Soient i, j, k trois éléments distincts de $\{1, \ldots, 5\}$, ℓ et m les deux autres éléments de cet ensemble. La transposition (ℓm) commute à (ijk). Il s'ensuit que les 3-cycles forment une classe de conjugaison de $\mathcal{A}_5$.

Soient i, j, k, ℓ quatre éléments distincts de $\{1, \ldots, 5\}$. La transposition (ij) commute à $((ij)\ (k\ell))$. Il s'ensuit que les doubles transpositions forment une classe de conjugaison de $\mathcal{A}_5$. [7]

En revanche, si σ est un 5-cycle de $\mathcal{S}_5$, le commutant $C(\sigma)$ de σ dans $\mathcal{S}_5$ se réduit aux puissances de σ et est donc contenu dans $\mathcal{A}_5$. En effet, si u commute à σ, on a, pour k dans $\{0, \ldots, 4\}$:

$$u \circ \sigma^k = \sigma^k \circ u \quad \text{d'où} \quad u(k+1) = \sigma^k \circ u(1).$$

Ces relations montrent qu'un élément u de $C(\sigma)$ est déterminé par $u(1)$; il en résulte que $|C(\sigma)| \leq 5$. Comme $C(\sigma)$ contient les puissances de σ, on én déduit bien que $C(\sigma)$ est le sous-groupe engendré par σ. Par conséquent, les 5-cycles se divisent en deux classes de conjugaison, chacune de cardinal 12.

Finalement, il y a cinq classes de conjugaison dans $\mathcal{A}_5$, dont les cardinaux sont 20, 15, 12, 12 et 1. On en déduit que l'assertion formulée dans le premier paragraphe de la démonstration est vraie.

Exercice 6. ③ *Déterminer les sous-groupe normaux de $\mathcal{S}_4$ (même méthode que dans la preuve du théorème).*

Exercice 7. ⑤ *Dénombrer les classes de conjugaison de $GL(\mathbb{F}_2)$ et en déduire que ce groupe est simple.*

Si $(g, h) \in G^2$, on note $[g, h]$ et on appelle *commutateur* de (g, h) l'élément

$$[g, h] = ghg^{-1}h^{-1}$$

de G. Le résultat suivant est immédiat mais utile dans beaucoup de démonstrations de simplicité.

Lemme 4. *Si N est un sous-groupe normal de G et si $(g, n) \in G \times N$, alors $[g, n]$ est dans N.*

Voici une application.

7. Ce que l'on savait a priori puisque 2 ne divise pas 15.

Théorème 2. *Le groupe $SO_3(\mathbb{R})$ est simple.*

Preuve. Soient G un sous-groupe normal non nul de $SO_3(\mathbb{R})$ et $g \in G \setminus \{I_3\}$.

Étape 1. Deux éléments a et b de $SO_3(\mathbb{R})$ sont conjugués dans ce groupe si et seulement s'ils ont même trace.

Car tout élément de $SO_3(\mathbb{R})$ est orthogonalement semblable à une matrice :

$$R(\alpha) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

la matrice de passage pouvant être choisie dans $SO_3(\mathbb{R})$ (remplacer si besoin est le dernier vecteur de la base de réduction par son opposé).

Étape 2. Si pour $a \in SO_3(\mathbb{R})$, $f(a) = \mathrm{Tr}([g,a])$, l'image de f est un segment $[r,3]$ avec $r < 3$.

Puisque $SO_3(\mathbb{R})$ est une partie compacte et connexe de $\mathcal{M}_3(\mathbb{R})$, la continuité de f montre que l'image de cette application est un compact connexe de $\mathbb{R}$, donc un segment. Vu que $3 = \mathrm{Tr}(I_3)$ est le maximum de Tr sur $SO_3(\mathbb{R})$, ce segment est de la forme $[r,3]$ où $r \leq 3$. L'égalité $r = 3$ impliquerait, puisque I_3 est le seul élément de trace 3 de $SO_3(\mathbb{R})$, que g est central dans $SO_3(\mathbb{R})$, donc que $g = I_3$. Contradiction.

Étape 3. Conclusion. Écrivons $r = \cos(\alpha)$ avec $0 < \alpha \leq \pi$. Les éléments $[g,a]$ pour $a \in SO_3(\mathbb{R})$ étant dans G, l'étape 1 montre que G contient toutes les $R(\beta)$ avec $\beta \in [0,\alpha]$. Prenant les puissances de ces éléments, G contient toutes les $R(\beta)$ avec $\beta \in \mathbb{R}$. Puisque toute matrice de $SO_3(\mathbb{R})$ est conjuguée à une $R(\beta)$, la normalité de G entraîne :

$$G = SO_3(\mathbb{R}).$$

1.3 Sous-groupes normaux de $\mathcal{S}_n$

Commençons par la généralisation ci-après du théorème 1, obtenue par Galois.

Théorème 3. *Si $n \geq 5$, le groupe $\mathcal{A}_n$ est simple.*

Preuve. Soit G un sous-groupe normal de $\mathcal{A}_n$ non réduit à $\{id\}$. On montre que $G = \mathcal{A}_n$ en se ramenant au cas $n = 5$.

Étape 1. Il suffit de montrer que G contient un élément non nul dont le support est de cardinal est majoré par 5.

Supposons en effet ce point acquis, notons h un élément non nul dont le support est de cardinal inférieur ou égal à 5, X une partie de cardinal 5 de $\{1,\ldots,n\}$ contenant le support de h, G_X le sous-groupe de G constitué des permutations à support contenu dans X,

$$\tilde{G}_X = \{g_{|X}, g \in G_X\}.$$

Il est clair que $\tilde{G}_X$ est un sous-groupe normal de $\mathcal{A}(X)$, donc est égal à $\mathcal{A}(X)$. Il s'ensuit que $\tilde{G}_X$ contient un 3-cycle, donc que G contient un 3-cycle ; les 3-cycles

étant conjugués dans $\mathcal{A}_n$(même argument que dans la preuve du théorème 1), et G normal dans $\mathcal{A}_n$, $G = \mathcal{A}_n$.

Étape 2. Construction d'un élément non nul de G dont le support est de cardinal inférieur ou égal à 5.

Fixons désormais g dans $G \setminus \{e\}$. Nous allons montrer que $\mathcal{A}_n$ contient un élément σ tel que $[g, \sigma]$ soit non nul et ait un support de cardinal majoré par 5. On note que le support de $[g, \sigma]$ est contenu dans la réunion des supports de $g\sigma g^{-1}$ et σ. Si σ est un 3-cycle de support S, $g\sigma g^{-1}$ est un 3-cycle de support $g(S)$. Si de plus S et $g(S)$ ne sont pas disjoints, le cardinal du support de $[g, \sigma]$ est au plus 5. Il suffit donc de construire un 3-cycle σ tel que :

$$g \circ \sigma \neq \sigma \circ g \quad \text{et} \quad S \cap g(S) \neq \emptyset.$$

Soient a un élément de $\{1, \ldots, n\}$ tel que $g(a) \neq a$, $b = g(a)$, c un élément de $\{1, \ldots, n\} \setminus \{a, b\}$. Posons

$$\sigma = (a, b, c).$$

Il est facile de vérifier que σ convient.

Exercice 8. ③ *Soit $m \geq 5$ un entier impair. Montrer que, pour $n \geq m$, le sous-groupe de $\mathcal{S}_n$ engendré par les m-cycles est égal à $\mathcal{A}_n$.*

Remarques

1. *Le groupe de Klein dans $\mathcal{S}_4$*
   Si $n = 4$, le groupe de Klein $\mathcal{V}$ est un sous-groupe normal de $\mathcal{A}_4$. En notant que les classes de conjugaison de $\mathcal{A}_4$ sont $\{id\}$, l'ensemble des 3 doubles transpositions, et deux classes constituées chacune de quatre 3-cycles, le raisonnement utilisé pour établir le théorème 1 montre que $\mathcal{V}$ est le seul sous-groupe normal non trivial de $\mathcal{A}_4$.
2. *Sur les groupes simples*
   Il existe 18 familles infinies dénombrables de groupes simples : les deux premières sont celle dess groupes de cardinal premier et celle des groupes alternés $\mathcal{A}_n$ pour $n \geq 5$. Viennent ensuite les groupes $PSL_n(\mathbb{K})$ sauf pour $n = 2$ et $\mathbb{K} = \mathbb{F}_2$ ou $\mathbb{F}_3$, ainsi que d'autres familles issues de la géométrie sur les corps finis, étudiées par Jordan. Vers 1955, Chevalley a découvert d'autres séries de ce type. D'autre part, on connaît 26 groupes finis simples ne se rattachant à aucune des familles précédentes, dits *sporadiques*. Les cinq premiers ont été découverts par Mathieu en 1861 et 1873. Le plus grand d'entre eux (le « Monstre ») a un cardinal d'environ 8.10^{53}. [8]

Le théorème 1 permet de décrire les sous-groupes normaux de $\mathcal{S}_n$.

Corollaire 1. *Si $n \geq 5$, $\mathcal{A}_n$ est le seul sous-groupe normal non trivial de $\mathcal{S}_n$.*

8. La découverte de groupes sporadiques s'est poursuivie jusqu'à la fin des années 1970. La classification des groupes simples finis affirme que tout groupe fini simple est soit membre de l'une des 18 familles, soit un des 26 groupes sporadiques ; elle est considérée comme complète par les spécialistes.

Preuve. Soit G un sous-groupe normal de $\mathcal{S}_n$. Alors $G \cap \mathcal{A}_n$ est un sous-groupe normal de $\mathcal{A}_n$, donc égal à $\mathcal{A}_n$ ou nul. Dans le premier cas, G est égal à $\mathcal{A}_n$ ou $\mathcal{S}_n$. Dans le second, G est de cardinal au plus 2 donc central grâce au lemme ci-après. Or, le centre de $\mathcal{S}_n$ est trivial.

Lemme 5. *Tout sous-groupe normal d'ordre 2 d'un groupe G est central.*

Preuve. Si x est l'élément non nul d'un tel sous-groupe N, alors pour tout $g \in G$, gxg^{-1} est un élément non nul de G, donc égal à x.

Exercice 9. ③ *Soient G un groupe fini, p le plus petit diviseur premier de $|G|$, N un sous-groupe normal d'ordre p de G. Montrer que N est central dans G.*

1.4 Sous-groupes normaux minimaux d'un groupe fini

On décrit ici les sous-groupes normaux minimaux d'un groupe fini en termes de groupes simples ; la démonstration utilise la description « interne » d'un produit direct ci-après.

Lemme 6. *Soient A et B deux sous-groupes normaux du groupe G, d'intersection réduite au neutre. Alors le sous-groupe de G engendré par A et B est $AB = \{ab,\ a \in A \text{ et } b \in B\}$, isomorphe à $A \times B$ par :*

$$\begin{array}{ccc} A \times B & \to & AB \\ (a,b) & \mapsto & ab \end{array}.$$

Ce sous-groupe est normal dans G.

Preuve. Le seul point important à vérifier est la relation :

$$\forall (a,b) \in A \times B, \qquad ab = ba.$$

Or, $aba^{-1}b^{-1}$ est dans A car il s'écrit $a\left(ba^{-1}b^{-1}\right)$ et $A \lhd G$. Le même argument montre que $aba^{-1}b^{-1}$ est dans B. Donc $aba^{-1}b^{-1} \in A \cap B = \{e\}$ et $ab = ba$.

La suite de la démonstration, immédiate, est laissée au lecteur.

Théorème 4. *Soient G un groupe fini non nul, N un sous-groupe normal de G différent de $\{e\}$, minimal pour l'inclusion. Il existe un groupe simple P et s dans $\mathbb{N}^*$ tel que N soit isomorphe à P^s.*

Preuve. On raisonne par récurrence sur $|G|$. Le cas $|G| = 2$ est évident. On suppose donc le résultat prouvé si $|G| < k$ ($k \geq 3$) et on considère un groupe fini G de cardinal k. Si G est simple, il n'y a rien à prouver.

Supposons donc que G n'est pas simple et prenons N comme dans l'énoncé ; $N \neq G$ et on peut appliquer à N l'hypothèse de récurrence. Si P est un sous-groupe normal de N distinct de $\{e\}$ et minimal dans l'ensemble des sous-groupes de G vérifiant ces conditions, alors, P est isomorphe à un groupe Q^s où Q est un groupe simple et $s \in \mathbb{N}^*$. On va démontrer que N est lui-même isomorphe à P^r pour un certain $r \in \mathbb{N}^*$, ce qui fournira l'isomorphisme de N et Q^{rs}, puis le résultat.

Étape 1 : N est engendré par les conjugués de P dans G, lesquels sont normaux dans N.

Puisque $N \triangleleft G$, les conjugués de P dans G sont contenus dans N. Le sous-groupe qu'ils engendrent est normal dans G donc égal à N par minimalité. Et, puisque $N \triangleleft G$ et $P \triangleleft N$, on vérifie simplement que les conjugués de P dans G sont normaux dans N.

Étape 2 : Soit $(P_1, \dots, P_r)$ une famille de conjugués de P dans G engendrant N et minimale pour cette propriété ; alors N est isomorphe à $P_1 \times \cdots \times P_r$ donc à P^r.

Grâce au lemme 6, on montre par récurrence sur $i \in \{1, \dots, r\}$, que le sous-groupe de G engendré par $P_1, P_2, \dots, P_i$ n'est autre que $H = P_1 P_2 \dots P_i$, qui est isomorphe à $P_1 \times P_2 \times \cdots \times P_i$. Le point clef est que P_i n'est pas contenu dans $P_1 \dots P_{i-1}$, donc que l'intersection de P_i et $P_1 P_2 \dots P_{i-1}$ est triviale, vu que ces deux groupes sont normaux dans N et que P_i est minimal.

La dernière partie de l'argument prouve le fait suivant.

Corollaire 2. *Si $N_1, \dots, N_r$ sont des sous-groupes normaux, minimaux, non nuls d'un groupe G, il existe $I \subset \{1, \dots, r\}$ tel que le sous-groupe engendré par les N_i pour $i \in \{1, \dots, r\}$ soit produit direct des N_i pour $i \in I$.*

La preuve du théorème 4 contient en germe celle d'un résultat plus général, décrit dans l'exercice suivant.

Exercice 10. ⑤ *Un groupe est dit caractéristiquement simple si et seulement s'il n'a pas de sous-groupes caractéristiques non triviaux.*

a) Soient S un groupe simple, $m \in \mathbb{N}^*$. Montrer que S^m est caractéristiquement simple.

Dans les questions b) à d), G est un groupe fini caractéristiquement simple, H un sous-groupe normal non nul de G minimal pour l'inclusion.

b) Montrer que G est engendré par $\bigcup_{\varphi \in Aut(G)} \varphi(H)$.

c) On note H_i pour $1 \leq i \leq m$ les images distinctes de H par des automorphismes de G. Montrer que G est isomorphe à $H_1 \times \cdots \times H_m$.

d) Montrer que H est simple. Puisque G est isomorphe à H^m, on en déduit, avec a), une description des groupes caractéristiquement simples finis.

e) Quels sont les groupes abéliens finis caractéristiquement simples ? Donner un exemple de groupe abélien infini caractéristiquement simple.

f) Ici, G est un groupe fini, N un sous-groupe normal non nul de G minimal pour l'inclusion. Montrer que N est caractéristiquement simple. Compte-tenu des résultats des questions c) et d), on a bien généralisé le théorème 4.

2 Quotients

On met ici en place la notion fondamentale de groupe quotient, qui justifie a posteriori celle de sous-groupe normal. La donnée d'un sous-groupe normal N du groupe G permet de construire une image de G, le groupe quotient G/N, ce que l'on peut voir comme un « dévissage » de G. Dans le paragraphe **2.1**, on construit les quotients et on en établit les propriétés les plus simples. Le paragraphe **2.2** est dévolu aux classiques « théorèmes d'isomorphismes ». La section

2.3, beaucoup moins fondamentale, montre comment la notion de quotient permet de décrire les sous-groupes d'un produit direct.

2.1 Généralités et premiers exemples

Rappel : ensemble quotient G/H, indice

Soient G un groupe, H un sous-groupe de G. Généralisant la relation de congruence modulo n sur le groupe $\mathbb{Z}$, on peut définir sur G la relation de congruence à droite modulo H en décrétant que deux éléments g et g' de G sont équivalents s'il existe h dans H tel que : $g' = gh$. On vérifie aussitôt que cette relation est d'équivalence ; la classe gH de g, notée $\overline{g}$, est équipotente à H (bijectivité des translations dans un groupe). Cette construction, effectuée pour la première fois par Lagrange à propos de sous-groupes de $\mathcal{S}_n$, a pour première conséquence le *théorème de Lagrange* ci-après.

Théorème 5. *Si G est fini, l'ordre de H divise celui de G. Le quotient des ordres est celui de l'ensemble quotient G/H.*

Si G/H est fini, son cardinal est appelé *indice de H dans G*.

Exercice 11. ④ *Soient H et K deux sous-groupes d'indice fini du groupe G. Montrer que $H \cap K$ est d'indice fini dans G, et que :*

$$|G/H \cap K| \leq |G/H||G/K|.$$

Quand peut-on définir la loi de groupe naturelle sur G/H ?

Il est tentant d'aller plus loin et de munir l'ensemble quotient G/H des classes de la relation précédente d'une structure de groupe. On souhaite évidemment poser :

$$\forall (g, g') \in G^2, \qquad \overline{g_1 g_2} = \overline{g_1}\,\overline{g_2},$$

afin que la surjection canonique $g \to \overline{g}$ de G sur G/H devienne un morphisme.

Pour que cette définition soit cohérente, il faut et il suffit que la classe de $g_1 g_2$ ne dépende que des classes de g_1 et g_2. Écrivons donc $g_1 = g_1' h_1$, $g_2 = g_2' h_2$ avec $(h_1, h_2) \in H^2$. Alors :

$$g_1 g_2 = g_1' h_1 g_2' h_2 = g_1' g_2' {g_2'}^{-1} h_1 g_2' h_2.$$

Ainsi, $g_1 g_2$ et $g_1' g_2'$ sont équivalents, si et seulement si ${g_2'}^{-1} h_1 g_2'$ est dans H. Ceci est réalisé pour tout g_2' dans G et tout h_1 dans H si et seulement si H est normal dans G, d'où la proposition suivante.

Proposition 1. *Si $H \triangleleft G$, on définit, en posant :*

$$\forall (g_1, g_2) \in G_1 \times G_2, \qquad \overline{g_1}\,\overline{g_2} = \overline{g_1 g_2},$$

une structure de groupe sur G/H. La surjection canonique $g \to \overline{g}$ est un morphisme de G sur G/H de noyau H.

Le groupe obtenu est appelé *quotient de G par H*.

Exemples

1. *Quotients d'un groupe monogène*
   Si G est monogène engendré par x, tout quotient de G est monogène engendré par la classe de x.
2. *Identification de $\mathcal{S}_n/\mathcal{A}_n$*
   Le groupe alterné A_n est un sous-groupe normal de $\mathcal{S}_n$. Le quotient $\mathcal{S}_n/\mathcal{A}_n$ est d'ordre 2, donc cyclique.
3. *Le groupe $\mathcal{A}_4$ n'a pas de sous-groupe d'ordre 6*
   Le titre de cet item montre que le théorème de Lagrange n'admet pas de réciproque naïve. Soient $G = \mathcal{A}_4$, H un éventuel sous-groupe d'ordre 6 de G. Alors H est d'indice 2 dans G, donc normal et le quotient G/H est d'ordre 2. La surjection canonique étant un morphisme, il vient
   $$\forall g \in G, \qquad g^2 \in H.$$
   Mais comme tout 3-cycle γ de $\mathcal{A}_4$ est le carré du 3-cycle γ^2, H contient tous les 3-cycles, donc est égal à G : contradiction.
4. *Quotient d'un groupe par son centre*
   Si G est non abélien, $G/Z(G)$ n'est pas monogène (sinon G serait engendré par $Z(G) \cup \{x\}$ où $\bar{x}$ est un générateur de $G/Z(G)$ et G serait abélien). En particulier, si l'indice de $Z(G)$ dans G est fini, il ne peut être premier et est donc supérieur ou égal à 4.
5. *Notion d'extension*
   Si G est un groupe et N un sous-groupe normal de G, on dit que G est *une extension de G/N par N* ; cela n'implique évidemment pas que G soit isomorphe à $G/N \times N$, comme on le voit en considérant $G = \mathcal{S}_3$ et $N = \mathcal{A}_3$, ni même que G contienne un sous-groupe isomorphe à G/N, comme on le voit en prenant $G = \mathcal{H}_8$ et $N = \{I, -I\}$ [9]. La théorie des extensions de groupes étudie comment reconstituer G à partir de N et de G/N.

Exercice 12. ③ *Donner un exemple de couple (G, H) où G est un groupe abélien, H un sous-groupe propre de G et où G, H et G/H sont isomorphes.*

Exercice 13. ③ *Démontrer sans utiliser la notion de quotient que, si G est un groupe fini non abélien, $|G| \geq 4|Z(G)|$.*

Exercice 14. ③ *Soient p un nombre premier, n dans $\mathbb{N}^*$, G un groupe admettant un quotient isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$. Montrer que toute partie génératrice de G est de cardinal supérieur ou égal à n.*

L'exercice suivant peut être résolu à partir du théorème de structure des groupes abéliens finis.

Exercice 15. ⑤ *Soient G un groupe abélien fini, H un sous-groupe de G. Montrer que G est isomorphe à $G/H \times H$.*

9. Pour ce dernier exemple, remarquer que tout élément de G/N est d'ordre 2 alors que les sous-groupes d'ordre 4 de G sont cycliques.

Exercice 16. ④ *a) On suppose $G/Z(G)$ engendré par $\{\overline{a_i}\ ;\ 1 \leq i \leq r\}$. Montrer que $\bigcap_{i=1}^{r} \langle \overline{a_i} \rangle$ est nul.*

b) Monter que, si p et q sont deux nombres premiers, le groupe $G/Z(G)$ ne peut être engendré par une famille de deux éléments d'ordres respectifs p et pq.

Soit φ un morphisme de groupes de source G. On vérifie que $\mathrm{Ker}(\varphi)$ est un sous-groupe normal de G. L'image d'un élément g de G par φ ne dépend que de la classe de g dans $G/\mathrm{Ker}(\varphi)$, ce qui permet de définir une application $\tilde{\varphi}$ de $G/\mathrm{Ker}(\varphi)$ dans $\mathrm{Im}(\varphi)$ en posant :

$$\forall g \in G, \qquad \tilde{\varphi}(\overline{g}) = \varphi(g).$$

Cette application est trivialement un isomorphisme de $G/\mathrm{Ker}(\varphi)$ sur $\mathrm{Im}(\varphi)$, ce que résume le résultat ci-après, immédiat mais suffisamment important pour mériter le nom de théorème.

Théorème 6. *Si φ est un morphisme de groupes de source G, φ induit par passage au quotient un isomorphisme de $G/Ker(\varphi)$ sur $Im(\varphi)$.*

Le théorème 6 montre que les noyaux (resp. les images) des morphismes de source G sont exactement les sous-groupes normaux (resp. les quotients) de G. On retiendra ce principe fondamental :

$$\textit{quotient} = \textit{image}\,;\ \textit{sous-groupe normal} = \textit{noyau}.$$

Voici quelques illustrations immédiates du théorème 6.

Exemples

1. *Le quotient $\mathcal{S}_n/\mathcal{A}_n$*
   Le morphisme signature montre que, si $n \geq 2$, le groupe $\mathcal{S}_n/\mathcal{A}_n$ est isomorphe au groupe cyclique çà deux éléments. [10]
2. *Le quotient $GL_n(\mathbb{K})SL_n(\mathbb{K})$*
   Soient $\mathbb{K}$ un corps et n un élément de $\mathbb{N}^*$. Le morphisme déterminant donne, par passage au quotient, un isomorphisme de $\mathrm{GL}_n(\mathbb{K})/\mathrm{SL}_n(\mathbb{K})$ sur $\mathbb{K}^*$.
3. *Les quotients $\mathbb{R}/\mathbb{Z}$ et $\mathbb{C}/\mathbb{Z}$*
   Les groupes $(\mathbb{C}/\mathbb{Z}, +)$ et $(\mathbb{C}^*, \times)$ sont isomorphes (par l'exponentielle complexe $z \longmapsto \exp(2i\pi z)$.). De même, $(\mathbb{R}/\mathbb{Z}, +)$ et $(\mathbb{U}, \times)$ sont isomorphes (via l'exponentielle imaginaire $x \longmapsto \exp(2i\pi x)$).
4. *Le quotient $\mathcal{B}_n(\mathbb{K})/\mathcal{U}_n(\mathbb{K})$*
   Si E est un espace vectoriel de dimension finie, les sous-groupes de Borel de $\mathrm{GL}(E)$ sont les stabilisateurs des drapeaux. Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$. On appelle sous-groupe de Borel standard de $\mathrm{GL}_n(\mathbb{K})$ et on note $\mathcal{B}_n(\mathbb{K})$ le stabilisateur du drapeau canonique de $\mathbb{K}^n$, c'est-à-dire le groupe des matrices triangulaires supérieures inversibles.

   En associant à M dans $\mathcal{B}_n(\mathbb{K})$ le n-uplet de ses éléments diagonaux, on voit que $\mathcal{U}_n(\mathbb{K})$ est un sous-groupe normal de $\mathcal{B}_n(\mathbb{K})$ et que $\mathcal{B}_n(\mathbb{K})/\mathcal{U}n(\mathbb{K})$ est isomorphe au groupe multiplicatif $(\mathbb{K}^*)^n$.

10. Il n'y a d'ailleurs pas le choix, car tout groupe d'ordre 2 est cyclique.

5. *Quotient d'un produit par un de ses facteurs*
   Si H et K sont deux groupes et $G = H \times K$, on peut identifier H (resp. K) au premier (resp. second) facteur de G. La projection sur ce premier facteur est un morphisme de noyau K, d'où $H \lhd G$ et un isomorphisme de G/H sur K.
6. *Identification de $\mathcal{S}_4/\mathcal{V}$*
   Le quotient $\mathcal{S}_4/\mathcal{V}$ est d'ordre 6 et n'est pas abélien (car les classes modulo $\mathcal{V}$ de $(1,2)$ et $(1,2,3,4)$ ne commutent pas). Il est donc isomorphe à $\mathcal{S}_3$.

   Une manière plus instructive de démontrer ce résultat est de construire une action de $\mathcal{S}_4$ sur un ensemble de cardinal 3 telle que le noyau du morphisme associé soit $\mathcal{V}$. Faisons donc agir $\mathcal{S}_4$ par conjugaison sur l'ensemble des doubles transpositions. L'action est transitive, le noyau contient $\mathcal{V}$ puisque deux doubles transpositions commutent. Le résultat suit par comparaison des cardinaux.

La propriété de factorisation décrite dans l'énoncé ci-après est la *propriété universelle du quotient.*

Proposition 2. *Soient N un sous-groupe normal de G, π la surjection canonique de G sur G/N. Si φ est un morphisme de G dans un groupe H, les deux conditions suivantes sont équivalentes.*

(i) Il existe un morphisme ψ de G/N dans H tel que :

$$\varphi = \psi \circ \pi.$$

(ii) On a

$$N \subset Ker(\varphi).$$

Preuve. L'implication $(i) \Rightarrow (ii)$ est évidente. Supposons (ii). Alors deux éléments g et g' de G tels que $\pi(g) = \pi(g')$ vérifient $g^{-1}g' \in N$, donc

$$\varphi(g) = \varphi(g').$$

Il est donc légitime de définir une application ψ de G/N dans H en posant

$$\forall g \in G, \qquad \psi(\pi(g)) = \varphi(g).$$

Il est immédiat de vérifier que ψ est un morphisme.

Exercice 17. ③ *Montrer que la proposition 2 caractérise le coupe $(G/N, \pi)$ à isomorphisme près.*

2.2 Les « théorèmes d'isomorphisme »

Commençons par identifier les sous-groupes d'un quotient.

Proposition 3. *Soient G un groupe, N un sous-groupe normal de G. Alors les sous-groupes de G/N sont les H/N pour H sous-groupe de G contenant N.*

Plus précisément, l'application $H \mapsto H/N$ ainsi définie est une bijection croissante pour l'inclusion de l'ensemble des sous-groupes de G contenant N dans celui des sous-groupes de G/N.

Exemple *Sous-groupes d'un groupe cyclique*

Si n est un entier ≥ 2, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec d diviseur de n. En particulier, chacun de ces sous-goupes est cyclique et leur treillis est isomorphe au treillis des diviseurs de n dans $\mathbb{N}^*$.

Exercice 18. ④ *Dénombrer les sous-groupes de $GL_n(\mathbb{F}_q)$ contenant $SL_n(\mathbb{F}_q)$.*

Exercice 19. ③ *On sait que tout sous-groupe fermé de $(\mathbb{R}, +)$ est égal à $\mathbb{R}$ ou monogène. En déduire, en utilisant l'exponentielle imaginaire, les sous-groupes fermés de $(\mathbb{U}, \times)$.*

La proposition 3 est un des trois « théorèmes d'isomorphisme » généraux de la théorie des groupes attribués à Emmy Noether. Les deux autres sont les propositions 4 et 5 ci-dessous.

Proposition 4. *Soient G un groupe, N et H deux sous-groupes de G avec $N \subset H$ et $N \lhd G$. Alors H/N est normal dans G/N si et seulement si H est normal dans G. Dans ce cas, le quotient de G/N par H/N est isomorphe à G/H.*

Preuve. La première assertion est immédiate. Pour la deuxième, il suffit d'appliquer le théorème au morphisme φ qui à la classe de $g \in G$ modulo N associe la classe de g modulo H, qui est bien défini, surjectif et de noyau H/N.

On déduit de ce théorème la description des quotients simples de G.

Corollaire 3. *Soit N un sous-groupe normal de G autre que G. Dire que G/N est simple, c'est dire que N est maximal pour l'inclusion dans l'ensemble des sous-groupes normaux de G.*

L'exercice suivant peut être traité par des techniques de réduction des matrices.

Exercice 20. ⑤ *a) Montrer que deux éléments non centraux de $G = SL_2(\mathbb{C})$ sont conjugués dans G si et seulement s'ils ont même trace.*

b) Déterminer le centre de G.

c) Démontrer que le seul sous-groupe de G contenant strictement le centre de G est G. En déduire, si $PSL_2(\mathbb{C})$ est le quotient de G par son centre, que $PSL_2(\mathbb{C})$ est simple.

Il résulte du corollaire 3 qu'un groupe fini non nul admet toujours un quotient simple non nul. Cette propriété ne s'étend pas aux groupes infinis.

Exercice 21. ③ *Soient p un nombre premier et*

$$C_p = \bigcup_{n=1}^{+\infty} \mathbb{U}_{p^n}.$$

Il est clair que C_p est un sous-groupe de $(\mathbb{C}^*, \times)$ [11] *Décrire les sous-groupes de C_p et montrer que C_p n'a pas de quotient simple non nul.*

11. Dit *groupe quasi-cyclique de Prüfer*.

Proposition 5. *Soient G un groupe, N et H deux sous-groupes de G, tels que $N \triangleleft G$. Alors l'ensemble $NH = \{nh\ ;\ (n,h) \in N \times H\}$ est un sous-groupe de G et les groupes NH/N et $H/N \cap H$ sont isomorphes.*

Preuve. Le premier point vient de l'égalité :

$$\forall (n,h) \in N \times H, \qquad nhn'h' = nhn'h^{-1}hh'$$

et du caractère normal de N dans G. Pour le second, on considère le morphisme qui associe à l'élément h de H sa classe modulo N, dont l'image est NH/N et le noyau $H \cap N$.

Exercice 22. ③ *Le groupe G est dit métacyclique s'il admet un sous-groupe normal cyclique N tel que G/N soit cyclique.*

a) Montrer qu'un groupe abélien est métacyclique si et seulement s'il est cyclique ou produit de deux groupe cycliques.

b) Montrer que tout sous-groupe et tout quotient d'un groupe métacyclique sont métacycliques.

c) Si G est métacyclique, montrer que G contient un élément d'ordre supérieur ou égal à $\sqrt{|G|}$.

d) Pour quels entiers $n \geq 2$ le groupe $\mathcal{S}_n$ est-il métacyclique ?

e) Quel est le cardinal minimal d'un groupe non métacyclique ?

Exercice 23. ④ *Soient G un groupe fini. On suppose que l'ensemble des sous-groupes d'indice 2 n'est pas vide. On note $H_1, \ldots, H_r$ les sous-groupes d'indice 2 de G et $H = \bigcap_{i=1}^{r} H_i$.*

a) Vérifier que H est normal dans G et que G/H est un groupe d'exposant 2 ; ce quotient est donc abélien et naturellement muni d'une structure de $\mathbb{F}_2$-espace vectoriel.

b) Montrer que l'ensemble des sous-groupes d'indice 2 de G est naturellement en bijection avec l'ensemble des sous-groupes d'indice 2 de G/H.

c) Conclure que le nombre de sous-groupe d'indice 2 de G est de la forme $2^m - 1$ avec m dans $\mathbb{N}$.

d) Soit p un diviseur premier de $|G|$. Supposons que tous les diviseurs premiers de G soient normaux dans G[12] *Montrer que le nombre de sous-groupes d'indice p de G est de la forme p_1^m avec m dans $\mathbb{N}$.*

2.3 Le théorème de Goursat

Nous allons illustrer la notion de quotient par une application marginale mais intéressante : une méthode permettant de déterminer les sous-groupes d'un produit direct. On fixe donc deux groupes G_1 et G_2, on note p_1 (resp. p_2) la projection canonique de $G_1 \times G_2$ sur G_1 (resp. G_2).

Soient H un sous-groupe de $G_1 \times G_2$, $H_1 = p_1(H)$ et $H_2 = p_2(H)$, K_1 (resp. K_2) l'ensemble des x_1 de H_1 tels que (x_1, e) appartienne à H (resp. des x_2 de H_2 tels que (e, x_2) appartienne à H. On vérifie que K_1 est un sous-groupe normal

12. C'est le cas si p est le plus petit diviseur premier de $|G|$.

de H_1, K_2 un sous-groupe normal de H_2. D'autre part, si x est un élément de G_1, y et y' des éléments de G_2, tels que (x, y) appartienne à H, on a

$$(x, y') \in H \iff y^{-1}y' \in K_2.$$

On peut donc attacher à H un morphisme de H_1 dans H_2/K_2 associant à l'élément x de H_1 la classe commune modulo K_2 des éléments y de H_2 tels que (x, y) appartienne à H. Le noyau de ce morphisme est par définition K_1, ce qui permet d'obtenir, par passage au quotient, un morphisme φ de H_1/K_1 dans H_2/K_2 tel que

$$\forall (x, y) \in H_1 \times H_2, \quad \varphi(\overline{x}_{K_1}) = \overline{y}_{K_2} \iff (x, y) \in H.$$

Inversant les rôles de H_1 et H_2, on obtient un morphisme ψ de H_2/K_2 dans H_1/K_1 tel que

$$\forall (x, y) \in H_1 \times H_2, \quad \psi(\overline{y}_{K_2}) = \overline{x}_{K_1} \iff (x, y) \in H.$$

Il s'ensuit que φ et ψ sont deux isomorphismes réciproques.

Récapitulons. On appelle *section d'un groupe* G tout quotient H/K où H est un sous-groupe de G, K un sous-groupe normal de H. On vient de montrer que tout sous-groupe de $G_1 \times G_2$ détermine une section de G_1, une section de G_2 et un isomorphisme entre ces deux sections.

Réciproquement, soient H_1 (resp. H_2) un sous-groupe de G_1 (resp. G_2), K_1 un sous-groupe normal de H_1 (resp. H_2), φ un isomorphisme de H_1/K_1 sur H_2/K_2. Alors

$$H = \left\{(x, y) \in G_1 \times G_2,\ \varphi(\overline{x}_{K_1}) = \overline{y}_{K_2}\right\}$$

est un sous-groupe de G. On a exhibé une bijection entre les sous-groupes de $G_1 \times G_2$ et les graphes d'isomorphismes entre une section de G_1 et une section de G_2.

Ces considérations établissent le théorème suivant. [13]

Théorème 7. *Soient G_1 et G_2 deux groupes. L'ensemble des sous-groupes de $G_1 \times G_2$ est en bijection avec l'ensemble des graphes d'isomorphismes entre une section de G_1 et une section de G_2.*

Exercice 24. ④ *Donner une condition nécessaire et suffisante pour que les sous-groupes de $G_1 \times G_2$ soient de la forme $H_1 \times H_2$ où H_1 est un sous-groupe de G_1, H_2 un sous-groupe de G_2.*

3 Structure normale

Le paragraphe **3.1** est consacré aux suites de composition. Ces suites formalisent l'idée de « dévissage » d'un groupe fini en groupes plus petits. On atteint un dévissage ultime lorsque les quotients mis en jeux sont simples, ce qui conduit au théorème de Jordan-Hölder. Dans le paragraphe **3.2**, on introduit un nouveau sous-groupe normal d'un groupe G, le *dérivé* de G ; le quotient

13. Découvert par Goursat en 1889 lors de l'étude de groupes issus de la géométrie, notamment des sous-groupes finis de $\mathrm{SO}_4(\mathbb{R})$.

de G par son dérivé, ou *abélianisé* de G, donne un moyen (parmi d'autres) de comprendre à quel point G diffère d'un groupe commutatif. On termine par la notion de groupe résoluble, naturelle dès que celle de groupe dérivé est dégagée, et fondamentale en théorie de Galois classique. [14]

3.1 Suites de composition

Soit $(G_i)_{0\leq i\leq n}$ une suite croissante (pour l'inclusion) de sous-groupes de G telle que : $G_0 = \{e\}$, $G_n = G$.

1. On dit que $(G_i)_{0\leq i\leq n}$ est une *suite de composition* de G si, pour tout $i \in \{0, \ldots, n-1\}$, $G_i \triangleleft G_{i+1}$.

   Les groupes G_{i+1}/G_i sont appelés *quotients de la suite* $(G_i)_{0\leq i\leq n}$.
2. La suite de composition $(G_i)_{0\leq i\leq n}$ de G est une *suite normale* de G si, pour tout $i \in \{0, \ldots, n-1\}$, $G_i \triangleleft G$.
3. La suite de composition $(G_i)_{0\leq i\leq n}$ de G est une *suite de Jordan-Hölder* de G si les quotients G_i/G_{i+1} sont simples. D'après le corollaire 3, ceci revient à demander que G_i soit, pour tout i, un sous-groupe normal de G_{i+1} distinct de G_i et maximal au sens de l'inclusion.

Un raisonnement par récurrence immédiat établit la proposition suivante.

Proposition 6. *Tout groupe fini admet une suite de Jordan-Hölder.*

Un groupe admettant une suite de Jordan-Hölder est dit *de longueur finie*.

Exemples

1. *Suites de Jordan-Hölder de $\mathcal{S}_n$ pour $n \geq 5$*
   Pour $n \geq 5$, la description de sous-groupes normaux de $\mathcal{S}_n$ montre que la seule suite de Jordan-Hölder de $\mathcal{S}_n$ est :
   $$\{id\} \subset \mathcal{A}_n \subset \mathcal{S}_n.$$
2. *Suites de Jordan-Hölder de $\mathcal{S}_4$*
   Les suites de Jordan-Hölder de $\mathcal{S}_4$ sont les :
   $$\{id\} \subset \{\tau\} \subset V \subset \mathcal{A}_4 \subset \mathcal{S}_4$$
   où τ est une double transposition.
3. *Groupe de longueur infinie*
   Soit G un groupe monogène infini. Les sous-groupes maximaux de G sont les sous-groupes d'indice premier et les quotients sont monogènes infinis. On en déduit que G n'est pas de longueur finie.

Exercice 25. ③ *Quels sont les groupes abéliens de longueur finie ?*

Exercice 26. ③ *Soient $n \in \mathbb{N}^*$, p un nombre premier. Donner le nombre de suites de Jordan-Hölder des groupes additifs $\mathbb{Z}/p^n\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^n$.*

14. Appelée dans les ouvrages anciens « théorie des équations ».

Deux suites de composition $(G_i)_{1\leq i\leq m}$, $(H_i)_{1\leq i\leq n}$ du groupe G sont dites *équivalentes* si $m = n$ et s'il existe σ dans $\mathcal{S}_n$ telle que , pour tout $i \in \{1, \ldots, n\}$, les quotients G_{i+1}/G_i et $H_{\sigma(i+1)}/H_{\sigma(i)}$ sont isomorphes. On a alors le *théorème de Jordan-Hölder.* [15]

Théorème 8. *Deux suites de Jordan-Hölder d'un groupe fini sont équivalentes.*

La démonstration se fait par récurrence sur le cardinal à l'aide du lemme suivant.

Lemme 7. *Si H et K sont deux sous-groupes normaux distincts du groupe G, distincts de G et maximaux pour l'inclusion, alors $HK = KH = G$ et G/H (resp. G/K) est isomorphe à $K/H \cap K$ (resp. $K/H \cap K$).*

Preuve. L'égalité $HK = KH = G$ vient de la maximalité, le reste du « troisième théorème d'isomorphisme ».

Preuve du théorème 8. Le résultat est trivial pour les groupes simples. Supposons-le acquis pour les groupes de cardinal strictement plus petit que $|G|$, et considérons $(H_i)_{0\leq i\leq m}$, $(K_j)_{0\leq j\leq n}$ deux suites de Jordan-Hölder de G.

Montrons que les deux suites $(H_i)_{0\leq i\leq m}$, $(K_j)_{0\leq j\leq n}$ sont équivalentes. Si $H_{m-1} = K_{n-1}$, l'hypothèse de récurrence permet de conclure. Sinon, le lemme 6 montre que les quotients G/H_{m-1} et $K_{n-1}/H_{m-1} \cap K_{n-1}$ (resp. G/K_{n-1} et $H_{m-1}/H_{m-1} \cap K_{n-1}$) sont isomorphes. Soit $(L_k)_{0\leq k\leq p}$ une suite de Jordan-Hölder de $H_{m-1} \cap K_{n-1}$. Alors $(L_0, \ldots, L_p, H_{m-1})$ est une suite de Jordan-Hölder de H_{m-1}, donc équivalente, par hypothèse de récurrence, à $(H_i)_{0\leq i\leq m-1}$. De même, $(K_j)_{0\leq j\leq n-1}$ est équivalente à $(L_0, \ldots, L_p, K_{n-1})$. Comme G/H_{m-1} (resp. G/K_{n-1}) est isomorphe à K_{n-1}/L_p (resp. H_{m-1}/L_p), on obtient la propriété désirée.

Remarques

1. *Interprétation galoisienne*

   Le théorème de Jordan-Hölder donne un premier renseignement sur la « structure normale » d'un groupe fini. Combiné à la correspondance de Galois, il montre que les diverse manières de dévisser une extension galoisienne finie en sous-extensions normales « minimales » font apparaître les mêmes quotients. [16]

2. *Longueur d'un groupe fini*

   Le théorème de Jordan-Hölder permet de définir la longueur d'un groupe fini comme la longueur commune de ses suites de Jordan-Hölder. Il subsiste pour les groupes de longueur finie, au prix d'une preuve légèrement plus compliquée, ce qui autorise finalement à définir la longueur d'un groupe de longueur finie [17]

15. Jordan a démontré l'égalité à permutation près des cardinaux des quotients de Jordan-Hölder. L'énoncé complet est dû à Hölder.

16. C'est cette application qui a conduit Jordan, puis Hölder, à étudier les suites de composition. Le résultat entraîne que deux méthode de résolution par radicaux d'une équations résolubles font apparaître « les mêmes calculs ».

17. C'est la même situation qui prévaut en algèbre linéaire, où l'on définit le fait qu'un espace vectoriel est de dimension finie *avant* de définir la dimension.

3. *Unicité de la décomposition en facteurs premiers*

   En appliquant le théorème de Jordan-Hölder au groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ et en tenant compte du fait que les groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier, on retrouve l'unicité de la factorisation première de n.

Exercice 27. ② *Soient r et s dans $\mathbb{N}^*$, $H_1, \ldots, H_r$, $K_1, \ldots, K_s$ des groupes simples. On suppose que $H_1 \times \cdots \times H_r$ et $K_1 \times \cdots \times K_s$ sont isomorphes. Que peut-on dire ?*

Exercice 28. ③ *Quelle est la longueur d'un groupe abélien fini ?*

3.2 Groupe dérivé et abélianisé

Si G est un groupe, le sous-groupe de G engendré par les commutateurs d'éléments de G est appelé *groupe dérivé* de G, et noté $D(G)$ [18].

Exemples

1. *Groupes à dérivé nul*
   Le groupe $D(G)$ est nul si et seulement si G est abélien.
2. *Un argument général pour fabriquer des commutateurs*
   Si un élément x de G est conjugué à son carré, x est un commutateur de G comme on le voit en remarquant que
   $$x^2 = gxg^{-1} \Longleftrightarrow x = gxg^{-1}x^{-1}.$$
3. *Dérivé de $\mathcal{S}_n$*
   Si $n \geq 2$,
   $$D(\mathcal{S}_n) = \mathcal{A}_n.$$
   Le cas $n = 2$ est évident. Si $n \geq 3$, il suffit, comme l'inclusion de $D(\mathcal{S}_n)$ dans $\mathcal{A}_n$ est évidente et puisque les 3-cycles engendrent $\mathcal{A}_n$, de montrer que chaque 3-cycle est dans $D(\mathcal{S}_n)$. On utilise le point précédent. Si σ est un 3-cycle, il en est de même de σ^2. Les permutations σ et σ^2 sont donc conjugués dans $\mathcal{S}_n$, d'où le résultat.
4. *Dérivé de $\mathcal{A}_n$ pour $n \geq 5$*
   Si $n \geq 5$, les 3-cycles sont conjugués non seulement dans $\mathcal{S}_n$ mais aussi dans $\mathcal{A}_n$. En reprenant l'argument précédent, on en déduit, pour $n \geq 5$, l'égalité :
   $$D(\mathcal{A}_n) = \mathcal{A}_n.$$
5. *Dérivé d'un groupe simple non abélien*
   Soit G un groupe simple non abélien. [19] Comme $D(G) \triangleleft G$,
   $$D(G) = \{e\}.$$
6. *Groupe dérivé d'un groupe diédral*
   Le calcul des commutateurs montre que
   $$D(\mathcal{D}_n = \{r_{\omega^2}, \omega \in U_n\}\ ;$$
   ce groupe est de cardinal n si n est impair, de cardinal $n/2$ si n est pair.

18. En général, $D(G)$ contient strictement l'ensemble des commutateurs de G.
19. C'est-à-dire (cf **1.2**) que G n'est pas fini de cardinal premier.

7. *Dérivé de $\mathcal{H}_8$*
   Le calcul des commutateurs montre que
   $$D(\mathcal{H}_8) = \{\pm I\}.$$

8. *Dérivé d'un groupe linéaire*
   Soit $\mathbb{K}$ un corps. Il est classique que
   $$D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K}),$$
   sauf si $n = 2$ et $\mathbb{K} = \mathbb{F}_2$. Si la caractéristique de $\mathbb{K}$ n'est pas 2, une preuve très simple consiste à noter que toute matrice de transvection est conjuguée à son carré et à utiliser le point 1 ci-dessus.

Exercice 29. ① *Si G est un groupe simple, que dire de $D(G)$?*

Exercice 30. ② *Soit $\mathbb{K}$ un corps. Déterminer le dérivé de $Aff_1(\mathbb{K})$.*

Exercice 31. ④ *Soient $\mathbb{K}$ un corps. Pour $n \in \mathbb{N}^*$, soit $\mathcal{U}_n(\mathbb{K})$ le sous-groupe de $GL_n(\mathbb{K})$ constitué des matrices triangulaires supérieures dont les termes diagonaux valent 1. Calculer le dérivé du groupe $\mathcal{U}_3(\mathbb{K})$, puis celui de $\mathcal{U}_n(\mathbb{K})$ si $n \geq 3$.*

Exercice 32. ② *Le groupe G est dit parfait s'il n'a pas de quotient abélien non nul.*

a) Vérifier qu'un groupe simple de cardinal non premier est parfait.

b) Montrer que G est parfait si et seulement si $G = D(G)$.

c) Montrer que tout quotient d'un groupe parfait est parfait.

L'image d'un commutateur par un morphisme est un commutateur : si φ est un morphisme de G dans un groupe,
$$\varphi\left([g,h]\right) = \left[\varphi(g), \varphi(h)\right].$$

On en déduit les points suivants :

- $D(G)$ est un sous-groupe caractéristique de G ; en particulier $D(G)$ est normal dans G ;

- si N est un sous-groupe normal de G, $D(G/N)$ est le sous-groupe de G/N engendré par les images dans G/N des commutateurs de G ; en particulier $D(G/N)$ est nul si et seulement si $D(G) \subset N$.

Par définition même, $G/D(G)$ est abélien. En fait, la proposition suivante établit que $G/D(G)$ est le plus grand quotient abélien de G. On l'appelle *abélianisé* de G.

Proposition 7. *(i) Si H est un sous-groupe de G contenant $D(G)$, alors H est normal dans G, et G/H est un quotient de $G/D(G)$ (donc est abélien).*

(ii) Si K est un sous-groupe normal de G tel que G/K soit abélien, alors $D(G) \subset K$, de sorte que G/K est un quotient de $G/D(G)$.

Preuve. Pour i), on note que si $g \in G$ et $h \in H$, $ghg^{-1}h^{-1}$ est dans $D(G)$, donc dans H. Comme $h \in H$, $ghg^{-1} \in H$ et H est normal dans G. La suite est évidente, car

$$G/H \simeq (G/D(G))/(H/D(G))$$

En ce qui concerne ii), il suffit d'observer que l'hypothèse entraîne que l'image dans G/K de tout commutateur est nulle, c'est-à-dire que tout commutateur est dans K.

Exemples

1. *Abélianisé de $\mathcal{S}_n$*
   Soit $n \geq 2$ un entier. L'abélianisé de $\mathcal{S}_n$ est cyclique de cardinal 2.
2. *Dérivé et abélianisé de $\mathcal{A}_4$*
   Puisque le seul sous-groupe normal de $\mathcal{A}_4$ est $\mathcal{V}$ et que le quotient $\mathcal{A}_4/\mathcal{V}$ est d'ordre 3 donc abélien, on a :
   $$D(\mathcal{A}_4) = \mathcal{V},$$
   ce qui entraîne que l'abélianisé de $\mathcal{A}_4$ est cyclique de cardinal 3.
3. *Abélianisé d'un groupe simple*
   L'abélianisé d'un groupe simple non abélien est nul.
4. *Abélianisé d'un groupe diédral*
   L'abélianisé de $\mathcal{D}_n$ est de cardinal 2 si n est pair, de cardinal 4 si n est pair (et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ car engendré par les classes de r et c où r est la rotation d'angle $2\pi/n$, c la conjugaison complexe).
5. *Abélianisé d'un groupe linéaire*
   Soient $\mathbb{K}$ un corps, n dans $\mathbb{N}^*$. En considérant le morphisme déterminant, on voit que l'abélianisé de $GL_n(\mathbb{K})$ est isomorphe à $\mathbb{K}^*$.

Exercice 33. ① *À quelle condition l'abélianisé de G est-il isomorphe à G ?*

Exercice 34. ③ *Soient G un groupe, m et n deux éléments de $\mathbb{N}^*$ premiers entre eux. On suppose que G est engendré par ses éléments d'ordre m et aussi par ses éléments d'ordre n. En considérant $G/D(G)$, montrer que $D(G) = G$. Application à $\mathcal{A}_n$ si $n \geq 5$.*

Exercice 35. ③ *Soient G un groupe fini et p un nombre premier. Montrer que G possède un sous-groupe normal d'indice p si et seulement si p divise $|G/D(G)|$.*

3.3 Groupes résolubles

On définit par récurrence les *groupes dérivés successifs* $D^n(G)$ où $n \in \mathbb{N}$ par

$$D^0(G) = G \quad \text{et} \quad D^{n+1}(G) = D\left(D^n(G)\right) \quad \text{pour } n \in \mathbb{N}.$$

Les $D^n(G)$ sont des sous-groupes caractéristiques de G, en particulier normaux.

Le groupe G est dit *résoluble* s'il existe $n \in \mathbb{N}$ tel que $D^n(G)$ soit nul. Le plus petit n vérifiant cette égalité est alors appelé *classe de résolubilité* de G.

Il est immédiat que G est abélien si et seulement si $D(G)$ est nul. Les groupes abéliens sont donc résolubles. La résolubilité est une généralisation naturelle de la commutativité équivalente à la nullité de certains commutateurs itérés.

Exercice 36. ① *Expliciter en terme de relations la propriété* $D^2(G) = \{e\}$.

Le résultat suivant est évident mais utile.

Lemme 8. *i) Tout sous-groupe d'un groupe résoluble est résoluble.*

ii) Toute image homomorphe (ou tout quotient) d'un groupe résoluble est résoluble.

iii) Tout produit direct d'un nombre fini de groupes résolubles est résoluble.

Preuve. i) Si H est un sous-groupe de G, on a

$$\forall n \in \mathbb{N}, \qquad D^n(H) \subset D^n(G).$$

ii) Il suffit de noter que, si φ est un morphisme de G dans un groupe, alors

$$D^n(\varphi(G)) = \varphi(D^n(G)).$$

iii) Si G et H sont deux groupes et n un élément de $\mathbb{N}^*$,

$$D^n(G \times H) = D^n(G) \times D^n(H).$$

La propriété essentielle des groupes résolubles est la *stabilité par extension*.

Théorème 9. *Soient G un groupe, N un sous-groupe normal de G. Les deux assertions suivantes sont équivalentes :*

i) le groupe G est résoluble ;

ii) les groupes N et G/N sont résolubles.

Preuve. Le lemme 8 fournit *i)* $\Rightarrow$ *ii)*. Pour la réciproque, supposons

$$D^r(N) = \{e\} \quad \text{et} \quad D^s(G/N) = \{e\},$$

avec $(r, s) \in \mathbb{N}^2$. On a alors successivement

$$D^s(G) \subset N, \qquad D^{r+s}(G) \subset D^r(N), \qquad D^{r+s}(G) = \{e\}.$$

Exemples

1. *Les groupes $\mathcal{A}_4$ et $\mathcal{S}_4$*
   Puisque $\mathcal{V}$ et $\mathcal{A}_4/\mathcal{V}$ sont abéliens, $\mathcal{A}_4$ est résoluble. Il s'ensuit que $\mathcal{S}_4$ l'est également.

   En fait : $D(\mathcal{S}_4) = \mathcal{A}_4$, $D(\mathcal{A}_4) = \mathcal{V}$ de sorte que $D^3(\mathcal{S}_4) = \{0\}$.
2. *Les groupes diédraux*
   Le groupe diédral $\mathcal{D}_n$ admet un sous-groupe normal isomorphe à $\mathbb{Z}/n\mathbb{Z}$, le quotient étant cyclique d'ordre 2. Il est donc résoluble.
3. *Les groupes $\mathcal{S}_n$, $n \geq 5$*
   Si $n \geq 5$, $\mathcal{S}_n$ n'est pas résoluble. Ceci découle de la première assertion du lemme 8 et de la simplicité de $\mathcal{A}_5$ (ou du lemme 8 et du calcul de $D(\mathcal{A}_n)$).

4. *Sous-groupe de Borel standard d'un groupe linéaire matriciel*
   Le sous-groupe $\mathcal{B}_n(\mathbb{K})$ de $\mathrm{GL}_n(\mathbb{K})$ constitué des matrices triangulaires supérieures est résoluble [20].
5. *Groupe affine en dimension* 1
   Le groupe affine $\mathrm{Aff}_1(\mathbb{K})$ des bijections affines de $\mathbb{K}$ sur lui-même est résoluble. En effet, le sous-groupe T des translations est normal, isomorphe à $(\mathbb{K}, +)$ donc abélien, et $\mathrm{Aff}_1(\mathbb{K})/T$ est isomorphe à $(\mathbb{K}^*, \times)$ donc abélien.

Exercice 37. ① *Justifier l'assertion de la seconde phrase de l'exemple 1.*

Exercice 38. ③ *Justifier le résultat de l'exemple* 4 *ci-dessus.*

Exercice 39. ③ *Soient H et K deux sous-groupes normaux du groupe G tels que G/H et G/K soient résolubles. Montrer que $G/(H \cap K)$ est résoluble.*

Exercice 40. ③ *À quelle condition le groupe des isométries affines de l'espace euclidien $\mathbb{R}^n$ est-il résoluble ?*

Exercice 41. ④ *Un groupe G est dit localement fini si tout sous-groupe de type fini de G est fini.*

a) Vérifier qu'un groupe localement fini est de torsion.

b) Montrer que, si N est un sous-groupe normal de G et si N et G/N sont localement finis alors G est localement fini.

c) Montrer que tout groupe de torsion résoluble est localement fini.

On va identifier les groupes simples et résolubles. On utilise à cet effet le lemme suivant.

Lemme 9. *Soit G un groupe non nul. Les deux assertions suivantes sont équivalentes.*

i) Les sous-groupes de G sont G et $\{e\}$.

ii) Le groupe G est de cardinal premier (donc cyclique).

Preuve. L'implication *ii)* $\Rightarrow$ *i)* est conséquence immédiate du théorème de Lagrange. Pour la réciproque, on suppose que G vérifie *i)*, et on prend x dans $G \setminus \{e\}$. Nécessairement, G est égal au sous-groupe engendré par x, donc est monogène. Mais $(\mathbb{Z}, +)$ contient des sous-groupes propres (les $n\mathbb{Z}$ pour $n \geq 2$). Par ailleurs, si l'entier $q \geq 2$ n'est pas premier, $(\mathbb{Z}/q\mathbb{Z}, +)$ admet également des sous-groupes propres (exactement un par diviseur strict de q). Le résultat suit.

Corollaire 4. *Les seuls groupes simples et résolubles sont les groupes d'ordre premier, c'est-à-dire les $(\mathbb{Z}/p\mathbb{Z}, +)$ où p est premier.*

Preuve. Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est simple et abélien, donc résoluble. Soit réciproquement G un groupe simple et résoluble. Puisque $D(G)$ est normal dans G, la simplicité de G fait que $D(G)$ est égal à G ou $\{e\}$. Si $D(G)$ était égal à G , il en serait de même de tous les $D^n(G)$ pour $n \in \mathbb{N}$, et G ne pourrait être résoluble. Ainsi, $D(G) = \{e\}$ et G est abélien. Mais la simplicité de G fait que G n'a aucun sous-groupe propre non trivial. Le lemme précédent dit que G est de cardinal premier.

20. De manière remarquable, on a une forme de réciproque : si $\mathbb{K}$ est algébriquement clos, tout sous-groupe résoluble et Zariski-connexe de $\mathrm{GL}(E)$ est contenu dans un sous-groupe de Borel de E, i.e. est cotrigonalisable (théorème de Lie-Kolchin).

Exercice 42. ② *Quels sont les groupes résolubles possédant une suite de Jordan-Hölder ?*

Le théorème ci-après caractérise les groupes résolubles en termes de suite de composition, ou de suite normales ; il décrit en particulier les groupes finis résolubles par leurs quotients de Jordan-Hölder.

Théorème 10. *Soit G un groupe. Les conditions suivantes sont équivalentes :*

i) le groupe G est résoluble,

ii) le groupe G admet une suite normale à quotients abéliens,

iii) le groupe G admet une suite de composition à quotients abéliens.

Si de plus G est fini, on peut remplacer dans iii) « abéliens » par « cycliques d'ordres premiers ».

Preuve. Pour *i) ⇒ ii)* on note que si $n \in \mathbb{N}^*$ est tel que $D^n(G) = \{e\}$ alors $(D^i(G))_{0 \leq i \leq n}$ est une suite normale à quotients abéliens.

L'implication *ii) ⇒ iii)* est évidente.

En ce qui concerne *iii) ⇒ i)*, on considère une suite normale à quotients abéliens de G, que l'on note $(G_i)_{0 \leq i \leq n}$. Alors, G_1 et G_2/G_1 sont abéliens, donc G_2 est résoluble. Répétant cet argument, on obtient la résolubilité de G.

Enfin, dans le cas où G est fini, les quotients de Jordan-Hölder de G sont simples et résolubles, donc cycliques d'ordres premiers.

Exercice 43. ① *Si G est infini, peut-on remplacer dans ii) « abéliens » par « cycliques » ?*

Exercice 44. ③ *Soit G un groupe fini. On écrit $|G| = \prod_{i=1}^{r} p_i^{\alpha_i}$ où les p_i (resp. les α_i) sont des nombres premiers deux à deux distincts (resp. des éléments de $\mathbb{N}^*$). Que dire de la longueur de G si G est résoluble ? Réciproque ?*

Exercice 45. ② *Un très difficile théorème de Feith et Thomson (1963 ; article de 254 pages) assure que tout groupe fini simple non abélien est d'ordre pair. En déduire que tout groupe d'ordre impair est résoluble.*

Exercice 46. ③ *Soit G un groupe résoluble fini, N un sous-groupe normal de G autre que G et maximal pour l'inclusion dans l'ensemble des sous-groupes normaux de G. Montrer que $|G/N|$ est premier, donc que N est un sous-groupe maximal de G. Donner un contre-exemple à cette propriété si G n'est pas résoluble.*

Exercice 47. ④ *Montrer que tout groupe fini contient un unique sous-groupe normal N tel que G/N soit résoluble et maximal pour l'inclusion.*

Nous terminons ce chapitre par la structure des sous-groupes normaux minimaux d'un groupe résoluble fini. Rappelons qu'un groupe fini est dit *élémentaire abélien* s'il est isomorphe à $((\mathbb{Z}/p\mathbb{Z})^n, +)$ pour un certain nombre premier p et un certain entier naturel n.

Théorème 11. *Si G est un groupe résoluble fini et N un sous-groupe normal minimal de G, N est élémentaire abélien.*

Preuve 1. On applique le théorème 4 du paragraphe **1.4**, le premier point du lemme 8 et le lemme 9.

Preuve 2. Cette démonstration est directe. En tant que sous-groupe caractéristique d'un sous-groupe normal de G, $D(N)$ est normal dans G, donc égal à N ou à $\{e\}$. Puisque N est résoluble, $D(N)$ est nul et N abélien. Il existe dans N un élément dont l'ordre est un nombre premier p. Comme G est abélien, $\{x \in N, x^p = e\}$ est un sous-groupe de G. Ce sous-groupe est clairement caractéristique dans N, donc normal dans G, donc égal à N, ce qui montre que N est élémentaire abélien.