Sous-groupes et groupes quotients

1 Classes modulo un sous-groupe

Soit H un sous-groupe d'un groupe G, et a un élément de G. La *classe à gauche de a modulo H* est le sous-ensemble

$$aH \overset{\text{déf}}{=} \{g \in G \,/\, \exists h \in H,\ g = ah\}\,.$$

On définit de manière analogue la classe à droite de a modulo H, notée Ha.

Pour tout $g \in aH$, il y a clairement unicité de l'élément $h \in H$ vérifiant $g = ah$, ainsi le cardinal de chaque classe à gauche modulo H est égal à celui de H. Par ailleurs, les classes à gauche modulo le sous-groupe H sont les classes d'équivalence pour la relation $\mathscr{R}$ définie par

$$a\mathscr{R}g \overset{\text{déf}}{\iff} a^{-1}g \in H.$$

(Vérifier que cela définit bien une relation d'équivalence !) Les classes à gauche modulo H forment donc une partition de G.

On note G/H l'ensemble des classes à gauche modulo H. Ce n'est pas un groupe en général (voir le paragraphe concernant les sous-groupes normaux). Le cardinal de G/H est appelé *indice de H dans G*, et généralement noté $(G : H)$. L'indice de H dans G est aussi égal au nombre de classes à droite modulo H [...].

1.1 Théorème de Lagrange

Dans le cas où G est un groupe fini, on déduit immédiatement de ce qui précède le résultat suivant, couramment appelé *théorème de Lagrange.*

Théorème 1.1 (Lagrange) *Soit G un groupe fini, et H un sous-groupe de G. Alors l'ordre de H et l'indice de H dans G divisent l'ordre de G. Plus précisément, on a*

$$|G| \;=\; |H|\,(G : H).$$

Pour un élément quelconque g du groupe fini G, l'ordre de g est égal au cardinal du groupe $< g >$ engendré par g. Une conséquence directe du théorème de Lagrange s'énonce donc comme suit.

Corollaire 1.2 *Si G est un groupe fini, l'ordre de tout élément g de G divise l'ordre de G, et on a*

$$\forall\, g \in G, \quad g^{|G|} \;=\; 1.$$

Deux applications du théorème de Lagrange à la théorie des nombres

Deux résultats classiques de l'arithmétique, le petit théorème de Fermat et l'infinité des nombres premiers, peuvent être obtenus *via* le théorème de Lagrange, en considérant le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles modulo un entier n. Rappelons que ce groupe est d'ordre $\varphi(n)$, où φ est la fonction d'Euler : $\varphi(n)$ est le nombre d'entiers entre 1 et n qui sont premiers avec n. L'application directe du corollaire 1.2 à ce groupe donne le théorème d'Euler-Fermat : pour tout entier a premier avec n,

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Écrit dans le cas particulier où n est un nombre premier p (on a alors évidemment $\varphi(p) = p-1$), cet énoncé n'est autre que le petit théorème de Fermat : si p est un nombre premier et a un entier non multiple de p, alors

$$a^{p-1} \equiv 1 \pmod p.$$

Moins classique est l'utilisation du théorème de Lagrange pour prouver que le cardinal de l'ensemble des nombres premiers est infini (preuve tirée de [1]). Il s'agit de montrer qu'étant donné un nombre premier p, on peut toujours trouver un nombre premier $q > p$. Pour cela, considérons un facteur premier q de l'entier $2^p - 1$. On a $2^p \equiv 1 \pmod q$, et puisque p est premier, 2 est d'ordre p dans le groupe $(\mathbb{Z}/q\mathbb{Z})^*$. Ce groupe étant d'ordre $q-1$, le théorème de Lagrange affirme que p divise $q-1$, et donc nécessairement $q \geq p+1$. ❏

1.2 Autres résultats sur l'indice d'un sous-groupe

Théorème 1.3 (Poincarré) *L'intersection d'un nombre fini de sous-groupes d'indice fini dans G est un sous-groupe d'indice fini dans G. Plus précisément, si $H_1, \ldots, H_n$ sont des sous-groupes d'indice fini dans G, alors*

$$\left(G : \bigcap_{j=1}^{n} H_j\right) \leq \prod_{j=1}^{n} (G : H_j).$$

Preuve — Laissée en exercice. Indication : si $H_1, \ldots, H_n$ sont des sous-groupes de G, on vérifie que pour tout $g \in G$, $\left(\bigcap_{j=1}^{n} H_j\right) g = \bigcap_{j=1}^{n} (H_j g)$.

Théorème 1.4 (Formule des indices) *Soit H un sous-groupe d'un groupe G, et K un sous-groupe de H. Si deux quelconques des indices $(G : H)$, $(H : K)$, $(G : K)$ sont finis, alors le troisième l'est aussi, et on a*

$$(G : K) = (G : H)(H : K).$$

Preuve — Laissée en exercice. Indication : vérifier que si $(g_i)_{i \in I}$ est un système de représentants des classes à gauche distinctes modulo H dans G, et si $(h_j)_{j \in J}$ est un système de représentants des classes à gauche distinctes modulo K dans H, alors $(g_i h_j)_{(i,j) \in I \times J}$ est un système de représentants des classes à gauche distinctes modulo K dans G.

2 Sous-groupes normaux

Soit H un sous-groupe d'un groupe G ; notons π la surjection canonique de G sur G/H, qui à tout $g \in G$ associe la classe à gauche gH de g modulo H. Le théorème suivant précise à quelle condition il est possible de munir G/H d'une loi de groupe telle que π soit un homomorphisme. Sa preuve est laissée en exercice.

Théorème 2.1 *Les propriétés suivantes sont équivalentes.*

1. *Le sous-groupe H est stable par les automorphismes intérieurs*[1], *autrement dit $\forall g \in G$, $gHg^{-1} \subset H$.*
2. *Pour tout $g \in G$, les classes à droite et à gauche de g modulo H coïncident, i.e. $\forall g \in G$, $gH = Hg$.*
3. *On peut munir G/H d'une loi de groupe telle que π soit un homomorphisme.*
4. *Il existe un groupe G' et un homomorphisme $\varphi : G \longrightarrow G'$ dont le noyau est H.*

Un sous-groupe H vérifiant ces propriétés sera appelé *sous-groupe normal*, ou *sous-groupe distingué* de G. On note dans ce cas $H \lhd G$.

Exercice 2.1 *énumérer tous les sous-groupes de $\mathbf{S}_3$, et indiquer lesquels sont des sous-groupes normaux de $\mathbf{S}_3$.*

Si H et K sont deux sous-groupes de G, avec $K \subset H$, il est immédiat que $K \lhd G \Longrightarrow K \lhd H$. En revanche, K peut être normal dans H sans être normal dans G. (Trouver un contre-exemple !)

Une intersection quelconque de sous-groupes normaux de G est encore un sous-groupe normal de G. Comme G est lui-même un sous-groupe normal de G, cette remarque permet de définir le sous-groupe normal engendré par une partie A de G comme l'intersection de tous les sous-groupes normaux de G qui contiennent A.

Dans le cas où G est abélien, il est immédiat que tout sous-groupe de G est normal. Mais un groupe peut n'avoir que des sous-groupes normaux sans être abélien, comme le montre l'étude du *groupe des quaternions* $\mathbb{H}_8$. Ce groupe est constitué de 8 éléments notés $\pm 1, \pm i, \pm j, \pm k$, et sa loi interne est définie par la règle des signes, et par les formules

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

On vérifie que tous les sous-groupes de $\mathbb{H}_8$ sont normaux [...], cependant $\mathbb{H}_8$ n'est pas abélien.

Exercice 2.2 *Montrer que si H est un sous-groupe d'indice 2 dans G, alors $H \lhd G$.*

2.1 Groupe quotient

Si H est un sous-groupe normal de G, la loi de groupe dont on peut munir G/H et qui fait de π un homomorphisme est évidemment unique, et on parle alors du *groupe quotient* G/H.

[1]Les automorphismes intérieurs de G sont les automorphismes i_g, $g \in G$, définis par $\forall h \in G,\ i_g(h) \overset{\text{déf}}{=} ghg^{-1}$.

Théorème 2.2 (Propriété universelle du groupe quotient) *Soit H un sous-groupe normal de G, et $\pi\ :\ G \longrightarrow G/H$ la surjection canonique. Si $\varphi\ :\ G \longrightarrow G'$ est un morphisme de groupes tel que $H \subset \operatorname{Ker}\varphi$, alors il existe un unique morphisme $\psi\ :\ G/H \longrightarrow G'$ tel que $\varphi = \psi \circ \pi$.*

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/H \arrow[d, "\psi"] \\ & G' \end{tikzcd}$$

La démonstration de ce résultat classique est laissée en exercice. On peut vérifier de plus que si φ est surjective, ψ l'est aussi. Et si on a l'égalité entre H et $\operatorname{Ker}\varphi$, ψ est injective. Dans ce cas, ψ est donc un isomorphisme entre G/H et $\operatorname{Im}\varphi$, d'où le théorème qui suit.

Théorème 2.3 (Premier théorème d'isomorphisme) *Soit $\varphi\ :\ G \longrightarrow G'$ un morphisme de groupes. Le groupe image $\operatorname{Im}\varphi$ est isomorphe au groupe quotient $G/\operatorname{Ker}\varphi$.*

Ainsi, à un isomorphisme près, les images homomorphes d'un groupe G sont les groupes quotients de G.

Il faut penser à utiliser ce premier théorème d'isomorphisme chaque fois qu'il s'agit de montrer qu'un groupe quotient est isomorphe à un autre groupe. Les trois exercices qui suivent donnent des exemples d'application de ce théorème.

Exercice 2.3 (Produit de groupes quotients) *Soient $G_1, \ldots, G_k$ des groupes, et $G_1 \times \cdots \times G_k$ leur produit direct. Pour chaque $j \in \{1, \ldots, k\}$, on se donne un sous-groupe N_j distingué dans G_j.*

Prouver que $N_1 \times \cdots \times N_k \lhd G_1 \times \cdots \times G_k$, et que

$$(G_1 \times \cdots \times G_k)/(N_1 \times \cdots \times N_k)\ \simeq\ (G_1/N_1) \times \cdots \times (G_k/N_k).$$

Exercice 2.4 (Second théorème d'isomorphisme) *Soit H un sous-groupe distingué d'un groupe G. Montrer que pour tout sous-groupe K de G,*

- *$HK \stackrel{\text{déf}}{=} \{hk\ /\ h \in H,\ k \in K\}$ est un sous-groupe de G,*
- *$H \lhd HK$,*
- *$H \cap K \lhd K$,*
- *les groupes quotients $(HK)/H$ et $K/(H \cap K)$ sont isomorphes.*

Exercice 2.5 (Troisième théorème d'isomorphisme) *Soient H et K deux sous-groupes normaux d'un groupe G, tels que $H \subset K$. Montrer que K/H est un sous-groupe normal de G/H, et que le groupe quotient $\frac{G/H}{K/H}$ est isomorphe à G/K.*

2.2 Centre d'un groupe G

Le *centre* d'un groupe G est le sous-groupe, souvent noté $Z(G)$, formé des éléments de G qui commutent avec tous les autres. Autrement dit,

$$Z(G)\ \stackrel{\text{déf}}{=}\ \{h \in G\ /\ \forall g \in G,\ gh = hg\}\,.$$

Les éléments de $Z(G)$ sont les h tels que l'automorphisme intérieur

$$i_h \,:\, g \longmapsto hgh^{-1}$$

coïncide avec l'identité sur G. Ainsi, $Z(G)$ est aussi le noyau du morphisme de G dans le groupe $\mathrm{Aut}(G)$ des automorphismes de G, qui à h fait correspondre i_h. Le centre de G est donc toujours un sous-groupe distingué de G. En fait, $Z(G)$ est même un sous-groupe *caractéristique* de G, ce qui signifie qu'il est stable par *tous* les automorphismes de G (pas seulement les automorphismes intérieurs !).

Exercice 2.6 *Montrer que tous les sous-groupes de $Z(G)$ sont des sous-groupes normaux de G.*

Exercice 2.7 *Montrer que si $G/Z(G)$ est un groupe monogène, alors G est abélien.*

2.3 Notion de groupe simple

Lorsqu'un groupe G possède un sous-groupe normal H non trivial (*i.e.* $H \neq G$ et $H \neq \{1\}$), on peut tenter de ramener l'étude de G à celle des groupes "plus petits" H et G/H. (Remarquer que si G est un groupe fini, ces deux groupes sont nécessairement d'ordre strictement inférieur à celui de G.) Au contraire, si G n'admet aucun sous-groupe normal non trivial, un tel "dévissage" n'est pas possible ; on dit alors que G est *un groupe simple.*

Depuis le début de l'étude de la théorie des groupes au XIX[e] siècle, les mathématiciens ont cherché à décrire tous les groupes simples finis. Les spécialistes considèrent que ce gigantesque travail de classification fut achevé en 1980. Les groupes simples finis se rangent ainsi en 17 familles infinies (dont deux, élémentaires, sont présentées dans la suite) auxquelles il faut ajouter 26 groupes dits *sporadiques.*

Groupes simples abéliens

L'exemple le plus élémentaire de groupes simples finis est fourni par la famille des groupes simples finis abéliens, qui ne sont autres que les groupes cycliques d'ordre premier. En effet, le théorème de Lagrange implique qu'un tel groupe n'admet pas d'autre sous-groupe que $\{1\}$ et lui-même. *A fortiori*, il n'admet pas de sous-groupe normal autre que ces deux sous-groupes triviaux, et il est donc simple. Réciproquement, remarquons que si un groupe abélien fini est simple, alors il ne peut admettre de sous-groupe non trivial, donc il est monogène d'ordre premier [...].

Groupes alternés

Présentons maintenant une seconde famille de groupes simples finis : les groupes alternés $\mathbf{A}_n$, pour $n \geq 5$. Rappelons que pour $n \geq 2$, le groupe symétrique $\mathbf{S}_n$ (groupe des permutations de l'ensemble $\{1, \ldots, n\}$) est muni d'un morphisme surjectif à valeurs dans le groupe multiplicatif $\{-1, 1\}$. Ce morphisme est traditionnellement noté ε, et appelé *signature.* Si τ est une transposition, $\varepsilon(\tau) = -1$, et plus généralement si σ est un cycle de longueur k on a $\varepsilon(\sigma) = (-1)^{(k+1)}$. Le noyau de ε est constitué des permutations dites *paires*, c'est-à-dire celles qui se décomposent en un nombre pair de transpositions ; c'est évidemment un sous-groupe normal de $\mathbf{S}_n$, appelé *groupe alterné d'ordre n*, et noté $\mathbf{A}_n$. Il est d'indice 2 dans $\mathbf{S}_n$ [...], et donc d'ordre $n!/2$.

Théorème 2.4 *Pour $n \geq 5$, le groupe alterné $\mathbf{A}_n$ est simple.*

Pour prouver la simplicité de $\mathbf{A}_n$ ($n \geq 5$)

1 *Vérifier que le produit de deux transpositions peut toujours s'écrire comme un produit de 3-cycles. En déduire que les 3-cycles engendrent $\mathbf{A}_n$.*

Soit H un sous-groupe normal de $\mathbf{A}_n$, non réduit à $\{\mathrm{Id}\}$. On veut donc montrer que $H = \mathbf{A}_n$.

2 *Dire pourquoi il suffit de montrer que H contient un 3-cycle.*

À partir d'un élément σ de H, $\sigma \neq \mathrm{Id}$, on cherche donc à construire un 3-cycle dans H.

3 *Montrer que si α est un 3-cycle quelconque, $\alpha^{-1}\sigma\alpha\sigma^{-1}$ est un élément de H.*

Prenons i non fixe par σ, posons $\sigma(i) = j$, et soit $k \in \{1, \dots, n\} \setminus \{i, j, \sigma^{-1}(i)\}$. On définit le 3-cycle $\alpha \stackrel{\text{déf}}{=} (i, j, k)$.

4 *Vérifier que $\tilde{\sigma} \stackrel{\text{déf}}{=} \alpha^{-1}\sigma\alpha\sigma^{-1}$ n'est pas l'identité, mais a au moins $n - 5$ points fixes. En déduire que cet élément de H est un 3-cycle, un 5-cycle, ou un produit de deux transpositions de supports disjoints.*

Dans les deux derniers cas, on recommence avec $\tilde{\sigma}$ au lieu de σ : si $\tilde{\sigma}$ est un 5-cycle (i, j, k, l, m), on considère $\tilde{\alpha} \stackrel{\text{déf}}{=} (i, j, k)$, et si $\tilde{\sigma} = (i, j)(k, l)$, on pose $\tilde{\alpha} \stackrel{\text{déf}}{=} (i, j, m)$ où $m \in \{1, \dots, n\} \setminus \{i, j, k, l\}$.

5 *Dans chaque cas, vérifier que $\tilde{\alpha}^{-1}\tilde{\sigma}\tilde{\alpha}\tilde{\sigma}^{-1}$ est un 3-cycle élément de H. Conclure.*

Et pour $n \leq 4$?

Il est immédiat que les groupes alternés $\mathbf{A}_2$ et $\mathbf{A}_3$ sont eux aussi des groupes simples : le premier est réduit à l'identité, et le second est d'ordre 3. Ces deux groupes alternés rentrent donc en fait dans la première famille de groupes simples : les groupes simples abéliens.

Le groupe alterné $\mathbf{A}_4$ est d'ordre 12. Outre l'identité, il contient 8 cycles d'ordre 3 et 3 permutations d'ordre 2 qui sont chacune le produit de deux transpositions de supports disjoints : $(1, 2)(3, 4)$, $(1, 3)(2, 4)$ et $(1, 4)(2, 3)$. Ces dernières constituent avec l'identité un sous-groupe d'ordre 4 de $\mathbf{A}_4$, qui est *distingué* dans $\mathbf{A}_4$. En effet, l'ensemble des produits de 2 transpositions à supports disjoints est stable par les automorphismes intérieurs [...]. $\mathbf{A}_4$ est donc le seul groupe alterné non simple.

2.4 Sous-groupe dérivé, groupe résoluble

On appelle *sous-groupe dérivé* du groupe G le sous-groupe noté $D(G)$ engendré par les *commutateurs* de G, c'est-à-dire par les éléments de la forme $aba^{-1}b^{-1}$ lorsque a et b décrivent G. Tout comme le centre de G, il est très facile de voir que $D(G)$ est toujours un sous-groupe caractéristique de G, en particulier c'est un sous-groupe normal de G.

Exercice 2.8 *Montrer que le groupe quotient $G/D(G)$ est toujours abélien. Vérifier aussi que $D(G)$ est le plus petit sous-groupe normal de G tel que $G/D(G)$ soit abélien.*

On définit naturellement la suite décroissante des groupe dérivés successifs $D^k(G)$, $k \geq 0$ par $D^0(G) \stackrel{\text{déf}}{=} G$, et $D^{k+1}(G) \stackrel{\text{déf}}{=} D(D^k(G))$. Le groupe G est dit *résoluble* s'il existe un entier k tel que $D^k(G) = \{1\}$.

Exercice 2.9 *Montrer que le groupe G est résoluble si et seulement si il existe une suite finie $(G_i)_{0 \leq i \leq r}$ de sous-groupes de G qui vérifient*
- $G_0 = G$, $G_r = \{1\}$,
- *pour tout* $i \in \{1, \ldots, r\}$, $G_{i+1} \lhd G_i$, *et le quotient* G_i/G_{i+1} *est abélien.*

Tout groupe abélien est résoluble, puisque son groupe dérivé est déjà réduit à l'élément neutre. Au contraire, un groupe simple non abélien n'est jamais résoluble [...]. En particulier, les groupes alternés $\mathbf{A}_n$ pour $n \geq 5$ ne sont pas résolubles.

Exercice 2.10 *Étude de la (non) résolubilité des groupes symétriques.*

1. *Montrer que si G est un groupe résoluble, tout sous-groupe de G est résoluble. Montrer aussi que le quotient de G par un sous-groupe distingué est résoluble.*
2. *Inversement, soit H un sous-groupe normal d'un groupe G, avec H et G/H résolubles. Montrer que G est résoluble.*
3. *Montrer que $\mathbf{S}_3$ est résoluble, mais que $\mathbf{S}_n$ n'est pas résoluble pour $n \geq 5$.*
4. *Vérifier que $D(\mathbf{A}_4)$ est un groupe d'ordre 4. En déduire que $\mathbf{S}_4$ est résoluble.*

Vers la théorie de Galois

Le terme *résoluble* provient de la théorie de Galois, dans laquelle on associe à tout polynôme $P \in \mathbb{K}[X]$ ($\mathbb{K}$ est un sous-corps de $\mathbb{C}$) un groupe appelé *groupe de Galois du polynôme* P : si P a pour racines $x_1, \ldots, x_n$, le groupe de Galois de P est l'ensemble des automorphismes du corps $\mathbb{K}(x_1, \ldots, x_n)$ qui laissent invariants les éléments du corps $\mathbb{K}$. On montre que si l'équation $P(x) = 0$ est résoluble par radicaux, alors le groupe de Galois de P est résoluble. Par ailleurs, on trouve des polynômes de degré 5 dans $\mathbb{Q}[X]$ dont le groupe de Galois est isomorphe à $\mathbf{S}_5$, qui n'est pas résoluble. (Par exemple $P = X^5 - 10X + 5$.) On en déduit l'existence d'équations polynomiales de degré 5 non résolubles par radicaux. Pour plus de détails sur la théorie de Galois, consulter par exemple [2] ou [3].

L'exercice qui suit donne une démonstration directe du fait que $\mathbf{A}_n$ (donc $\mathbf{S}_n$) n'est pas résoluble dès que $n \geq 5$, sans passer par la simplicité.

Exercice 2.11 *Soit n un entier supérieur ou égal à 5.*

1. *Montrer que les 3-cycles engendrent $\mathbf{A}_n$, et que si γ_1 et γ_2 sont deux 3-cycles, on peut toujours trouver $\sigma \in \mathbf{A}_n$ tel que $\gamma_1 = \sigma\gamma_2\sigma^{-1}$.*
2. *Soit γ un 3-cycle. Vérifier que γ peut s'écrire comme le produit de deux 3-cycles σ et τ.*
3. *En déduire que γ est un commutateur de $\mathbf{A}_n$, puis que $D(\mathbf{A}_n) = \mathbf{A}_n$*

Références

[1] M. Aigner, G.M. Ziegler. *Proofs from THE BOOK.* Springer, 1998.

[2] J.P. Escofier. *Théorie de Galois, cours et exercices corrigés.* Dunod, 1997.

[3] I. GOZARD. *Théorie de Galois.* Ellipses, 1997.

[4] Alain BOUVIER, Denis RICHARD. *Groupes – observation, théorie, pratique.* Hermann, 1994.

[5] Josette CALAIS. *Éléments de Théorie des Groupes.* Puf, 1998.

[6] Daniel PERRIN. *Cours d'Algèbre.* Ellipses, 1996.