Groupes

Dimitri Ara

Introduction historique

Il est toujours délicat d'essayer d'identifier une source unique pour un idée. Néanmoins, il semble raisonnable de faire remonter l'introduction du concept de groupe à Lagrange dans son article *Réflexions sur la résolution algébrique des équations* publié en 1770–1771. Dans cette article, Lagrange s'intéresse au nombre de valeurs que prend une fonction rationnelle quand on permute ses variables. Les groupes y sont vus – dans un langage anachronique – comme des sous-groupes du groupe symétrique. Son but est d'appliquer cette étude à la résolution par radicaux des équations polynômiales.

La théorie est ensuite développée par Ruffini (*Teoria generale della equazioni*, 1799), Abbati (à qui on doit la première démonstration du théorème de... Lagrange), Abel (qui utilise la théorie des groupes pour prouver que l'équation polynômiale générale de degré 5 n'est pas résoluble par radicaux), Galois (dont on reparle ci-dessous) et surtout Cauchy entre 1844 et 1846 (qui démontre entre autres le théorème de Cauchy énoncé par... Galois).

Une application spectaculaire de la théorie des groupes est le célèbre théorème de Galois (dont on célèbre le bicentenaire de la naissance en cette année 2011) : Galois associe à toute équation polynômiale un groupe de permutations de ses racines (qu'on appelle maintenant le groupe de Galois) et donne un critère portant sur ce groupe pour déterminer si l'équation est résoluble par radicaux.

La définition moderne de groupe (c'est-à-dire sans passer par le groupe symétrique) est publiée par Cayley en 1854 dans un article intitulé *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$. Dans ce même article, Cayley prouve que tout groupe se plonge dans un groupe symétrique faisant ainsi le lien avec l'ancienne définition : c'est le théorème de Cayley.

1 Premières définitions

Définition 1.1. Un groupe G est un ensemble muni d'une loi interne

$$\begin{aligned} G \times G &\to G \\ (x, y) &\mapsto xy \end{aligned}$$

vérifiant les axiomes suivants :

1. la loi est associative : pour tous x, y, z dans G, on a $(xy)z = x(yz)$;

2. la loi admet un élément neutre : il existe un élément e de G tel que pour tout x dans G, on ait $xe = x = ex$;
3. tout élément admet un inverse : pour tout x dans G, il existe x' dans G tel que $xx' = e = x'x$.

Remarques 1.2.

1. L'élément neutre est unique. On le notera souvent 1.
2. L'inverse est unique. On notera souvent x^{-1} l'inverse d'un élément x.

Définition 1.3. On dit qu'un groupe G est *abélien* (ou *commutatif*) si la loi de G est commutative, c'est-à-dire si pour tous x, y dans G, on a $xy = yx$.

Remarque 1.4. Si G est un groupe abélien, on notera souvent $+$ sa loi interne, 0 son neutre et $-x$ l'inverse de x. On parle alors de notation additive (par opposition à la notation multiplicative).

Exemples 1.5.

1. Soit E un ensemble. On note S_E l'ensemble des bijections de E dans E. On vérifie immédiatement que S_E muni de la composition des applications est un groupe. L'élément neutre de ce groupe est l'application identité. Pour $n \geq 0$, si $E = \{1, \ldots, n\}$, on note $S_n = S_E$. On appelle S_n le *groupe symétrique* sur n éléments. Ce groupe est abélien si et seulement si $n \geq 2$.
2. Les entiers relatifs $\mathbb{Z}$ munis de l'addition forment un groupe. De même, pour $n \geq 2$, les entiers modulo n munis de l'addition forment un groupe noté $\mathbb{Z}/n\mathbb{Z}$. Ces deux groupes sont abéliens.
3. L'ensemble $\mathbb{Q}$ des nombres rationnels est un groupe pour l'addition et l'ensemble $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ est un groupe pour la multiplication. Plus généralement, si k est un corps, $(k, +)$ et $(k^*, \times)$ sont deux groupes abéliens.
4. Soient k un corps et V un espace vectoriel sur k. L'ensemble des automorphismes linéaires de V muni de la composition forme un groupe noté $\mathrm{GL}(V)$. Pour $n \geq 0$, si $V = k^n$, on note $\mathrm{GL}_n(k) = \mathrm{GL}(k^n)$. On appelle $\mathrm{GL}_n(k)$ le *groupe linéaire*. Ce groupe est abélien si et seulement si $n \geq 1$.
5. Soit $k = \mathbb{R}$. Le sous-ensemble de $\mathrm{GL}_n(\mathbb{R})$ formé des automorphismes préservant le produit scalaire euclidien forme un groupe pour la composition noté $\mathrm{O}_n(\mathbb{R})$. On appelle $\mathrm{O}_n(\mathbb{R})$ le *groupe orthogonal*. Ce groupe est abélien si et seulement si $n \geq 3$. (Plus généralement, si k est un corps de caractéristique différente de 2 et V est un espace vectoriel sur k muni d'une forme quadratique q, on peut considérer le groupe $\mathrm{O}(q)$ des automorphismes linéaires de V préservant q.)
6. Soit $n \geq 3$. Les isométries du polygone régulier à n sommets forment un groupe pour la composition. On appelle ce groupe le *groupe diédral* et on le note D_n. Ce groupe n'est jamais abélien.

Remarque 1.6. Les groupes S_E, $\mathrm{GL}(V)$, $\mathrm{O}(q)$ et D_n sont des exemples de groupes d'automorphismes d'une certaine structure (un ensemble, un espace vectoriel, un espace vectoriel quadratique et une forme géométrique). Considérer les automorphismes d'une structure est un moyen très général de créer de nouveaux groupes.

Définition 1.7. Soient G et H deux groupes. Un *morphisme* (ou *homomorphisme*) de groupes de G vers H est une application $f : G \to H$ telle que pour tous x, y dans G, on ait $f(xy) = f(x)f(y)$.

Remarques 1.8.

1. On a automatiquement $f(1) = 1$ (et si ce n'était pas automatique on le demanderait, comme dans la définition d'un morphisme de monoïdes).
2. On a automatiquement $f(x) = x^{-1}$.

Définition 1.9. Un morphisme de groupes $f : G \to H$ est un *isomorphisme* de groupes s'il existe un morphisme de groupes $g : H \to G$ tel que $g \circ f = \mathrm{id}_G$ et $f \circ g = \mathrm{id}_H$. On dit que deux groupes sont *isomorphes* s'il existe un isomorphisme entre eux.

Proposition 1.10. *Un morphisme de groupes est un isomorphisme si et seulement s'il est bijectif.*

Démonstration. Il est clair qu'un morphisme de groupes est une bijection. Réciproquement, une bijection f admet un unique inverse f^{-1} et il s'agit de montrer que si f est un morphisme de groupes alors f^{-1} est un morphisme de groupes. La démonstration est laissée en exercice. (Un résultat similaire a été démontré en algèbre linéaire.) □

Exemples 1.11.

1. Soit G un groupe. L'identité $\mathrm{id}_G : x \mapsto x$ est évidemment un isomorphisme de groupes.
2. L'application de $\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ qui envoie un entier sur sa classe modulo n est un morphisme de groupes.
3. L'inclusion de $\mathbb{Z}$ dans $\mathbb{Q}$ est un morphisme de groupes.
4. L'exponentiel est un morphisme de groupes de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$.
5. Soient k un corps et a un élément de k. La multiplication par a est un morphisme de groupes de $(k, +)$ dans lui-même. C'est un isomorphisme si et seulement si a est non nul.
6. Soient k un corps et V un espace vectoriel sur k de dimension finie. Le déterminant est un morphisme de groupes de $\mathrm{GL}(V)$ vers k^*.
7. Soit $n \geq 0$. Il existe un unique morphisme de groupes $S_n \to \{\pm 1\}$ qui envoie les transpositions (voir TD pour une définition) sur -1. Ce morphisme s'appelle la *signature*.
8. Soit $n \geq 2$. Notons U_n l'ensemble des racines n-ième de l'unité dans $\mathbb{C}$. Il est immédiat que celles-ci forment un groupe pour la multiplication. L'application de $\mathbb{Z}/n\mathbb{Z}$ vers U_n qui envoie la classe de k sur ζ_n^k, où $\zeta_n = \exp^{2i\pi/n}$, est bien définie et est un isomorphisme de groupes.

Remarque 1.12. Si G est un groupe, les automorphismes de G forment un groupe (selon la remarque 1.6).

Définition 1.13. Soit G un groupe. Un sous-groupe H de G est un sous-ensemble de G vérifiant les propriétés suivantes :

1. si x et y sont dans H, alors xy est dans H ;
2. 1 appartient à H ;
3. si x appartient à H, alors x^{-1} appartient à H.

Proposition 1.14. *Si H est un sous-groupe de G, alors il existe une unique structure de groupe sur H faisant de l'inclusion de H dans G un morphisme de groupes.*

Démonstration. Notons $i : H \to G$ l'application d'inclusion. Si i est un morphisme, pour x, y dans H, on a $i(xy) = i(x)i(y)$. On est donc conduit à poser $xy = i^{-1}(i(x)i(y))$. En terme moins pédant, cette loi n'est autre que la restriction à H de la loi de G. On vérifie par ailleurs immédiatement que cette loi fait de H un groupe. □

Remarque 1.15. La formulation de la proposition précédente peut sembler pédante. Elle a le mérite d'insister sur l'importance de la notion de morphisme.

Proposition 1.16. *Soit $f : G \to H$ un morphisme de groupes.*

1. *Si G' est un sous-groupe de G, alors $f(G)$ est un sous-groupe de H.*
2. *Si H' est un sous-groupe de H, alors $f^{-1}(H')$ est un sous-groupe de G.*

Démonstration. La démonstration est laissée en exercice. (Un résultat similaire a été démontré en algèbre linéaire.) □

Définition 1.17. Soit $f : G \to H$ un morphisme de groupes.

1. On appelle *image* de f le sous-groupe $f(G)$ de H. On le note $\operatorname{Im} f$.
2. On appelle *noyau* de f le sous-groupe $f^{-1}(\{1\})$ de G. On le note $\operatorname{Ker} f$.

Proposition 1.18. *Un morphisme de groupes f est injectif si et seulement si son noyau est trivial (*i.e. *réduit à* 1*).*

Démonstration. La démonstration est laissée en exercice. (Un résultat similaire a été démontré en algèbre linéaire.) □

Exemples 1.19.

1. Les inclusions
$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$
forment une chaîne de sous-groupes.
2. Les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ (ensemble des multiples de n) pour $n \geq 0$ (voir TD pour une démonstration).
3. Soit k un corps et V un espace vectoriel sur k de dimension finie. Le noyau du déterminant $\mathrm{GL}(V) \to k^*$ est un sous-groupe du groupe linéaire appelé *groupe spécial linéaire* et noté $\mathrm{SL}(V)$.
4. Le noyau de la signature $S_n \to \{\pm 1\}$ est un sous-groupe du groupe symétrique appelé *groupe alterné* et noté A_n.
5. Les n rotations appartenant à D_n forment un sous-groupe de D_n isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Si $\mathcal{D}$ est une droite passant par un sommet du polygone régulier à n sommets et par son centre, alors $\{1, \tau\}$, où τ est la symétrie d'axe $\mathcal{D}$, est un sous-groupe de D_n isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
6. Soit G un groupe. On note $Z(G)$ l'ensemble des éléments g de G qui commutent à tout autre élément g' de G. Cet ensemble est un sous-groupe de G qu'on appelle le *centre* de G.

Proposition 1.20. *Soient G et H deux groupes. Il existe une unique structure de groupe sur le produit cartésien $G \times H$ faisant des projections $p_G : G \times H \to G$ et $p_H : G \times H \to H$ des morphismes de groupes.*

Démonstration. Soient (g, h) et (g', h') dans $G \times H$. Si p_G est un morphisme de groupes, on a
$$p_G((g, h)(g', h')) = p_G(g, h)p_G(g', h') = gg'.$$
De même si p_H est un morphisme de groupes, on a
$$p_G((g, h)(g', h')) = hh'.$$
D'où nécessairement $(g, h)(g', h') = (gg', hh')$. Par ailleurs, on vérifie immédiatement qu'on définit ainsi une structure de groupe. □

Définition 1.21. Si G et H sont deux groupes, on notera $G \times H$ le produit cartésien muni de cette unique structure de groupe.

Exemples 1.22.

1. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ s'appelle le *groupe de Klein*.
2. Si G est un groupe, on peut itérer la construction et définir un groupe G^n pour $n \geq 0$.
3. On peut montrer que tout groupe abélien de type fini, *i.e.* engendré par un nombre fini d'éléments (voir la section suivante) est un produit fini de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$.

4. Si m et n sont deux entiers premiers entre eux, alors l'application

$$\begin{aligned}\mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\\ \overline{k} &\mapsto (\overline{k}, \overline{k})\end{aligned}$$

qui envoie la classe de k modulo mn sur le couple constitué de la classe de k modulo m et de la classe de k modulo n, est bien définie et est un isomorphisme de groupes (et même d'anneaux). On appelle ce résultat (et ses généralisations, voir le chapitre sur les anneaux) le *lemme chinois*.

2 Parties génératrices, ordres et groupes cycliques

Proposition 2.1. *Soient G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupes de G. Alors l'intersection $\bigcap_{i\in I} H_i$ est un sous-groupe de G.*

Démonstration. La démonstration est laissée en exercice. (Un résultat similaire a été démontré en algèbre linéaire.) □

Définition 2.2. Soit A une partie d'un groupe G. On appelle *sous-groupe engendré* par A le plus petit sous-groupe de G contenant A. Un tel sous-groupe existe par la proposition précédente : il suffit de considérer l'intersection de tous les sous-groupes contenant A. On note $<A>$ ce sous-groupe.

Proposition 2.3. *Soit A un sous-ensemble d'un groupe G. Alors*

$$<A> = \{g_1 g_2 \dots g_n;\ n \geq 0,\ \forall i\ g_i \in A \text{ ou } g_i^{-1} \in A\}.$$

Démonstration. Posons $H = \{g_1 g_2 \dots g_n;\ n \geq 0,\ \forall i\ g_i \in A \text{ ou } g_i^{-1} \in A\}$. Il s'agit de montrer que H est un sous-groupe et que tout sous-groupe contenant A contient H. La démonstration est laissée en exercice. (Un résultat similaire a été démontré en algèbre linéaire.) □

Définition 2.4. On dit qu'une partie A d'un groupe G est une *partie génératrice* de G (ou que A *engendre* G) si on a $G = <A>$.

Exemples 2.5.

1. L'élément 1 (*i.e.* la partie $\{1\}$) engendre $\mathbb{Z}$. De même, la classe de 1 engendre $\mathbb{Z}/n\mathbb{Z}$.
2. Le groupe symétrique est engendré par les transpositions (voir TD pour une démonstration et d'autres générateurs).
3. Le groupe D_n est engendré par une rotation d'ordre n et une symétrie axiale.
4. Soit k un corps. Le groupe $\mathrm{GL}_n(k)$ est engendré par les transvections et les dilatations, *i.e.* les matrices respectivement semblables à

$$\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1\ 1 \\ & & & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & & \lambda \end{pmatrix}, \quad \lambda \in k^*.$$

5. Le groupe $\mathrm{O}_n(\mathbb{R})$ est engendré par les réflexions (*i.e.* les symétrie orthogonales par rapport à un hyperplan). (Plus généralement si k est un corps de caractéristique différente de 2, V un espace vectoriel sur k de dimension finie et q est une forme quadratique sur V non dégénérée, alors $\mathrm{O}(q)$ est engendré par les réflexions.)

Définition 2.6. Soit G un groupe. On appelle *ordre* de G son cardinal vu comme un élément de $\mathbb{N} \cup \{\infty\}$. On le notera $|G|$. Si g est un élément de G, on appelle *ordre* de g l'ordre du sous-groupe de G engendré par g.

Proposition 2.7. *Soit g un élément d'un groupe G. L'ordre de g est le plus petit entier $n \geq 1$ tel que $g^n = 1$ s'il existe, et est infini sinon.*

Démonstration. Supposons qu'il n'existe pas de n tel que $g^n = 1$. Alors les g^k pour k dans $\mathbb{Z}$ sont distincts. Sinon, on aurait $g^l = g^k$ pour $l > k$ et donc $g^{l-k} = 1$ avec $l-k \geq 1$. L'ordre de g est donc infini.

Sinon, soit m le plus $n \geq 1$ tel que $g^n = 1$. Le même argument que ci-dessus montre que les g^k pour $0 \leq k < m$ sont distincts. Soit k quelconque. Faisons la division euclidien de k par m. On a $k = qm + r$ avec $0 \leq r < m$. D'où

$$g^k = g^{qm+r} = g^{qm} g^r = (g^m)^q g^r = g^r.$$

L'ordre de g est donc m, ce qui achève la démonstration. □

Définition 2.8. Un groupe est dit *monogène* s'il est engendré par un unique élément. Un groupe est dit *cyclique* s'il est monogène et fini.

Proposition 2.9. *Les seuls groupes monogènes sont $\mathbb{Z}$ et les $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 1$.*

Démonstration. Considérons un groupe G engendré par un générateur g.

Si l'ordre de g est infini, on définit un morphisme $\mathbb{Z} \to G$ en envoyant n sur g^n. L'image de ce morphisme est un sous-groupe contenant le générateur et le morphisme est donc surjectif. Soit n dans le noyau. Puisque g est d'ordre infini, on a $n \leq 0$. Mais $-n$ est également dans le noyau. D'où $n \geq 0$ et $n = 0$. Le morphisme est donc un isomorphisme.

Supposons g d'ordre fini m. On définit un morphisme $\mathbb{Z}/m\mathbb{Z} \to G$ en envoyant la classe de k sur g^k. Ce morphisme est bien défini puisque $g^{km} = 1$ pour tout entier k. Ce morphisme est surjectif pour la même raison que ci-dessus. Mais puisque $\mathbb{Z}/m\mathbb{Z}$ et G ont même ordre, ce morphisme est un isomorphisme. □

3 Groupes quotients

3.1 Congruences et sous-groupes distingués

3.1. Si E est un ensemble et $\sim$ est une relation d'équivalence sur E, on notera $E/\sim$ l'ensemble des classes d'équivalence pour la relation $\sim$. On dispose d'une application canonique $E \to E/\sim$ qui envoie élément x de E sur sa classe $\overline{x}$.

Si maintenant G est un groupe et $\sim$ est une relation d'équivalence sur G, en général, la multiplication de G n'induit pas une loi interne sur $G/\sim$.

Définition 3.2. Soit G un groupe et $\sim$ une relation d'équivalence sur G. On dit que $\sim$ est une congruence si pour tous x, x', y, y' dans G, si $x \sim x'$ et $y \sim y'$, alors $xy \sim x'y'$.

Remarque 3.3. Dire que $\sim$ est un congruence signifie précisément que la multiplication

$$G \times G \to G$$

de G induit une application

$$G/\sim \times G/\sim \to G/\sim.$$

Proposition 3.4. *Soit G un groupe et $\sim$ une relation d'équivalence sur G. Il existe une unique structure de groupe sur $G/\sim$ faisant de l'application $G \to G/\sim$ un morphisme de groupes. De plus, cette structure est donnée par la loi interne définie ci-dessus.*

Démonstration. L'unicité résulte immédiatement de la surjectivité de l'application canonique : tout élément de $G/\sim$ s'écrit $\overline{x}$ pour x dans G et on a nécessairement $\overline{x}\,\overline{y} = \overline{xy}$. Par ailleurs, on vérifie facilement qu'on définit ainsi une structure de groupe. □

Remarque 3.5. On vérifie facilement que si on part d'une relation d'équivalence quelconque, une telle structure existe si et seulement si cette relation est une congruence.

Proposition 3.6. *Si G est un groupe et $\sim$ est une congruence sur G, alors la classe de* 1 *(pour la relation $\sim$) est un sous-groupe de G.*

Démonstration. En effet, c'est le noyau de l'application canonique $G \to G/\sim$. □

Notation 3.7. Si H est un sous-groupe d'un groupe G et x un élément de G, on notera xH (respectivement Hx) l'ensemble des xy (respectivement yx) avec y dans H.

Proposition 3.8. *Soient G un groupe et $\sim$ une congruence sur G. Notons H le sous-groupe $\overline{1}$. Alors la classe d'un élément x de G est*

$$\overline{x} = xH = Hx.$$

Démonstration. Pour y dans G, on a $y \sim x$ si et seulement si $x^{-1}y \sim 1$ si et seulement si $x^{-1}y$ appartient à H si et seulement si y appartient à xH.

De même, $y \sim x$ si et seulement si $1 \sim xy^{-1}$ si et seulement si $1 \sim yx^{-1}$ si et seulement si y appartient à Hx. □

3.9. Soit G un groupe. On définit une application

$$\{\text{congruences sur } G\} \to \{\text{sous-groupes de } G\}$$

en envoyant une congruence $\sim$ sur la classe de 1 pour la relation $\sim$. La proposition précédente montre que cette application est injective.

Définition 3.10. Soit G un groupe. On appelle sous-groupe *distingué* (*normal* en anglais) de G un sous-groupe dans l'image de l'application ci-dessus.

3.11. Un sous-groupe H est donc distingué si la relation $\sim_H$, définie par $x \sim_H y$ si et seulement si xy^{-1} appartient à H, est une congruence. Par définition, l'application ci-dessus induit une bijection des congruences sur G vers les sous-groupes distingués de G. L'inverse de cette bijection associe à un sous-groupe distingué H la congruence $\sim_H$.

Définition 3.12. Si H est un sous-groupe distingué d'un groupe G, on notera G/H le groupe $G/\sim_H$. On appelle G/H le *quotient* de G par H.

Les éléments de G/H sont donc les xH où x parcourt G. La multiplication est donnée par $(xH)(yH) = xyH$, le neutre est H et l'inverse de xH est $x^{-1}H$.

Remarque 3.13. La définition de sous-groupe distingué donnée ci-dessus n'est pas la définition usuelle. La proposition 3.27 établira l'équivalence avec des définitions plus standard.

3.2 Classes à gauche et à droite

Définition 3.14. Soit H un sous-groupe (non nécessairement distingué) d'un groupe G. On définit deux relations $\sim_H$ et $\sim^H$ sur G de la manière suivante :

1. $x \sim_H y$ si et seulement si $x^{-1}y$ appartient à H ;
2. $x \sim^H y$ si et seulement si xy^{-1} appartient à H.

Proposition 3.15. *Soit H un sous-groupe d'un groupe G. Alors les relations $\sim_H$ et $\sim^H$ sont des relations d'équivalence.*

Démonstration. Traitons le cas de $\sim_H$.

Soit x dans G. On a $x \sim_H x$ puisque 1 appartient à H.

Si $x \sim_H y$, alors $x^{-1}y$ appartient à H et donc son inverse $y^{-1}x$ également. D'où $y \sim_H x$.

Enfin, si $x \sim_H y$ et $y \sim_H z$, alors $x^{-1}y$ et $y^{-1}z$ appartiennent à H et il en est donc de même de leur produit $x^{-1}z$. D'où $x \sim_H z$. □

Définition 3.16. Soit H un sous-groupe d'un groupe G. On note G/H l'*ensemble* $G/\sim_H$. Attention, ce n'est pas un groupe si H n'est pas distingué ! De même, on note $H\backslash G$ l'*ensemble* $G/\sim^H$.

Proposition 3.17. *Soit H un sous-groupe d'un groupe G. Alors les relations $\sim_H$ et $\sim^H$ sont des relations d'équivalence.*

Démonstration. Par symétrie, il suffit de traiter le cas de $\sim_H$.

Soit x dans G. On a $x \sim_H x$ puisque 1 appartient à H.

Si $x \sim_H y$, alors $x^{-1}y$ appartient à H et donc son inverse $y^{-1}x$ également. D'où $y \sim_H x$.

Enfin, si $x \sim_H y$ et $y \sim_H z$, alors $x^{-1}y$ et $y^{-1}z$ appartiennent à H et il en est donc de même de leur produit $x^{-1}z$. D'où $x \sim_H z$. □

Proposition 3.18. *Soit H un sous-groupe d'un groupe G. La classe d'un élément x pour la relation $\sim_H$ (respectivement pour la relation $\sim^H$) est xH (respectivement Hx).*

Démonstration. Traitons le cas de $\sim_H$. Soit x dans G. On a $x \sim y$ si et seulement si $x^{-1}y$ appartient à H si et seulement si y appartient à xH. □

Remarque 3.19. On appelle les xH (respectivement les Hx) les classes à gauche (respectivement à droite) de H dans G. Ainsi, G/H est l'ensemble des classes à gauche et $H\backslash G$ l'ensemble des classes à droite. Notons aussi que si H est distingué, alors l'ensemble sous-jacent du groupe quotient G/H défini dans la section précédente est bien l'ensemble G/H des classes à gauche.

Remarque 3.20. La multiplication par x dans G induit une bijection de H vers xH. En particulier, les classes à gauche ont toutes même cardinal.

Theorem 3.21 (Lagrange)**.** *Soit G un groupe fini et H un sous-groupe de G. Alors*

$$|G| = |G/H||H|.$$

En particulier, l'ordre de H divise l'ordre de G.

Démonstration. La relation $\sim_H$ induit une partition de G en G/H parties qui sont toutes de cardinal $|H|$ d'après la remarque précédente. D'où le résultat. □

Remarque 3.22. La même démonstration démontre la formule analogue pour $H\backslash G$. D'où G/H et $H\backslash G$ ont même cardinal.

Corollaire 3.23. *Soit G un groupe. L'ordre d'un élément de G divise l'ordre de G.*

Démonstration. Il suffit d'appliquer le résultat précédent au sous-groupe engendré par l'élément en question. □

Définition 3.24. Soit H un sous-groupe d'un groupe G. On dit que H est d'*indice fini* si G/H est fini. Dans ce cas, on appelle $|G/H|$ l'indice de H dans G.

Remarque 3.25. Si G est fini, tout sous-groupe H est d'indice fini et cet indice vaut $|G|/|H|$ par le théorème de Lagrange.

3.3 Retour aux sous-groupes distingués

Proposition 3.26. *Un sous-groupe H d'un sous-groupe G est distingué si et seulement si les relations $\sim_H$ et $\sim^H$ coïncident.*

Démonstration. La proposition 3.8 montre que si H est un sous-groupe distingué, les classes à gauche et à droite coïncident et les deux relations sont donc égales.

Réciproquement, supposons $\sim_H = \sim^H$. Il s'agit de montrer que $\sim_H$ est une congruence. Montrons si $x \sim_H x'$ alors pour tout y de G, on a $xy \sim_H x'y$. Ces deux propriétés sont en fait équivalentes : on a $xy \sim_H x'y$ si et seulement si $xy \sim^H x'y$ si et seulement si $x \sim^H x'$ si et seulement si $x \sim_H x'$.

On montre de même que si $y \sim_H y'$ alors pour tout x' de G, on a $x'y \sim_H x'y'$. D'où pour x, x', y, y' dans G, si $x \sim_H x'$ et $y \sim_H y'$, alors $xy \sim_H xy' \sim_H x'y'$, et $\sim_H$ est donc bien une congruence. □

Proposition 3.27. *Soit H un sous-groupe d'un groupe G. Les propriétés suivantes sont équivalentes :*

1. *H est un sous-groupe distingué ;*
2. *pour tout x dans G, $xH = Hx$;*
3. *pour tout x dans G, $xHx^{-1} = H$;*
4. *pour tout x dans G, $xHx^{-1} \subset H$.*

Démonstration. L'équivalence entre 1 et 2 est une reformulation de la proposition précédente. L'équivalence entre 2 et 3 est évidente et 3 implique 4 de manière triviale. Montrons que 4 entraîne 3. Soit x dans G. En appliquant l'hypothèse à x^{-1}, on a $x^{-1}Hx \subset H$ et donc $H \subset xHx^{-1}$, d'où le résultat. □

Remarque 3.28. Si x est un élément de G, on définit un automorphisme de G en envoyant y sur xyx^{-1}. On appelle cette automorphisme la *conjugaison* par x. L'équivalence entre 1 et 4 peut donc se reformuler en disant qu'un sous-groupe est distingué si et seulement s'il est stable par conjugaison.

Exemples 3.29.

1. Soit G un groupe. Alors les sous-groupes $\{1\}$ et G sont distingués dans G.
2. Tout sous-groupe d'un sous-groupe abélien est distingué.
3. Soit G un groupe. Le centre $Z(G)$ est un sous-groupe distingué de G.
4. Le sous-groupe de D_n formé des rotations est distingué. Cela résulte par exemple du fait que les rotations sont les isométries directes de D_n et que le fait d'être direct est stable par conjugaison. Par contre, les sous-groupes engendrés par une symétrie axiale ne sont pas distingués.
5. Le sous-groupe engendré par un 3-cycle de S_3 est distingué. En effet, le calcul montre immédiatement que le conjugué d'un 3-cycle est un 3-cycle. Or les deux 3-cycles sont dans ce sous-groupe. Par contre, les sous-groupes engendrés par une transposition ne sont pas distingués. (En fait, S_3 est isomorphe à D_3 et cet exemple est un cas particulier du précédent.)

Proposition 3.30. *Soit $f : G \to G'$ un morphisme de groupes.*

1. *Si H est un sous-groupe distingué de G, alors $f(H)$ est un sous-groupe distingué de $f(G)$.*
2. *Si H' est un sous-groupe distingué de G', alors $f^{-1}(H')$ est un sous-groupe distingué de G.*

Démonstration. On sait déjà que l'image (respectivement l'image réciproque) d'un sous-groupe est un sous-groupe. Il s'agit donc seulement d'établir le caractère distingué.

1. Si H est un sous-groupe de G stable par conjugaison par un x dans G, alors $f(H)$ est stable par conjugaison par $f(x)$, d'où le résultat.

2. Soit x dans G. On a

$$f(xf^{-1}(H')x^{-1}) = f(x)f(f^{-1}(H))f(x)^{-1} \subset f(x)H'f(x)^{-1} \subset H',$$

et $f^{-1}(H')$ est donc stable par conjugaison par x, d'où le résultat.

□

Remarque 3.31. Attention, si H' est un sous-groupe de H, le sous-groupe $f(H)$ n'est pas distingué dans G en général.

Corollaire 3.32. *Le noyau d'un morphisme de groupes est un sous-groupe distingué.*

Exemples 3.33.

1. Le groupe alternée A_n est un sous-groupe distingué du groupe symétrique S_n.
2. Soit k un corps. Le groupe spécial linéaire $SL_n(k)$ est un sous-groupe distingué du groupe linéaire $GL_n(k)$.

Proposition 3.34. *Soit H un sous-groupe distingué d'un groupe G et $p : G \to G/H$ la projection canonique. L'application p induit une bijection entre les sous-groupes de G contenant H et les sous-groupes de G/H. De plus, cette bijection respecte les sous-groupes distingués.*

Démonstration. On sait déjà que p et p^{-1} respectent les sous-groupes. Par ailleurs, il est évident que p^{-1} envoie tout sous-groupe sur un sous-groupe contenant H. Pour établir la première assertion, il suffit donc de montrer que si L est un sous-groupe de G/H, alors $p(p^{-1}(L)) = L$, et que si K est un sous-groupe de G contenant H, alors $p^{-1}(p(K)) = K$. La première égalité résulte de la surjectivité de p.

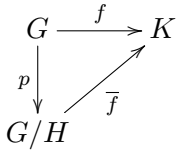
Montrons la deuxième. Si K est un sous-groupe de G, on a

$$p^{-1}(p(K)) = \bigcup_{k \in K} p^{-1}(\{p(k)\}).$$

Or $p^{-1}(\{p(k)\})$ n'est autre que la classe de k, *i.e.* kH. D'où $p^{-1}(p(K)) = KH$. En particulier, si K contient H, on a bien l'égalité recherchée, ce qui établit la première assertion.

La seconde assertion résulte de la proposition précédente. □

Proposition 3.35. *Soit H un sous-groupe distingué d'un groupe G. Pour tout groupe K et tout morphisme $f : G \to K$ qui envoie tout élément de H sur 1, il existe un unique morphisme $\overline{f} : G/H \to K$ tel que le triangle*



soit commutatif.

Démonstration. L'unicité résulte de la surjectivité de p : elle impose $\overline{f}(xH) = f(x)$. Montrons que cette application est bien définie. Si $x^{-1}y$ appartient à H, alors $f(x^{-1}y) = 1$ par hypothèse et on a bien $f(x) = f(y)$. Il est immédiat que $\overline{f}$ est bien un morphisme de groupes. □

Remarque 3.36. Cette propriété caractérise en fait G/H (muni de la projection canonique) à unique isomorphisme près. On parle de *propriété universelle* du groupe quotient.

Exemple 3.37. Voir l'exercice sur l'abélianisé d'un groupe en TD.

Proposition 3.38. *Soit $f : G \to G'$ un morphisme de groupes. Alors l'unique morphisme $\overline{f} : G/\operatorname{Ker} f \to G'$ (voir proposition précédente) est une injection. En particulier, f induit un isomorphisme $G/\operatorname{Ker} f \to \operatorname{Im} f$.*

Démonstration. Pour x dans G, on a $f(x \operatorname{Ker} f) = f(x)$. D'où $x \operatorname{Ker} f$ appartient au noyau de $\overline{f}$ si et seulement si x appartient au noyau de x. Le noyau de $\overline{f}$ est donc trivial. D'où le résultat. □

Exemples 3.39.

1. Le quotient S_n/A_n est canoniquement isomorphe au groupe cyclique à deux éléments.
2. Soit k un corps. Le quotient $GL_n(k)/SL_n(k)$ est canoniquement isomorphe à k^*.