Éléments de la théorie des groupes

Série pour M1 / bac + 4

Alexey Muranov

14 avril 2026

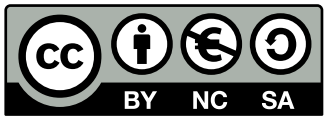


Table des matières

2026-04-14T17:29

Introduction

Les origines de la théorie des groupes

Les origines de la *théorie des groupes* contemporaine se trouvent apparemment dans les travaux de Joseph Louis de Lagrange (1736–1813), de Paolo Ruffini (1765–1822), d'Augustin Louis Cauchy (1789–1857), de Niels Henrik Abel (1802–1829), et d'Évariste Galois (1811–1832).

Avant de se transformer en un terme mathématique avec une définition abstraite sans rapport évident avec le sens usuel du mot, le mot « groupe » avait été parfois utilisé pour designer certains ensembles de permutations d'un ensemble fini, ainsi que certains ensembles de transformations d'un *espace géométrique*, lesquels, dans un certain sens, était « autonomes » ou « isolés » du reste de l'ensemble des permutations ou des transformations. En termes de l'algèbre moderne, cela pouvait vouloir dire que cet ensemble de permutations ou de transformations formait un *groupe* par rapport à l'opération de composition, mais cela pouvait aussi avoir un autre sens.

Par exemple, Galois utilisait le mot « groupe », entre autres, pour designer ce qu'en théorie moderne l'on appelle les *classes suivant un sous-groupe*. Dans sa lettre a Auguste Chevalier (1832), Galois écrit[1] :

> En d'autres termes, quand un groupe G en contient un autre H, le groupe G peut se partager en groupes, que l'on obtient chacun en opérant sur les permutations de H une même substitution ; en sorte que
>
> $$G = H + HS + HS' + \cdots .$$
>
> Et aussi il peut se diviser en groupes qui ont tous les mêmes substitutions, en sorte que
>
> $$G = H + TH + T'H + \cdots .$$

[1] Évariste Galois. *Œuvres mathématiques d'Évariste Galois*. Avec une introd. d'Emile Picard. Paris : Gauthier-Villars, 1897. x+61. URL : https://www.e-rara.ch/zut/content/titleinfo/6262819 ; Évariste Galois. *Œuvres mathématiques d'Évariste Galois*. Avec une introd. d'Emile Picard. Project Gutenberg, 2012. vi+61. URL : https://www.gutenberg.org/ebooks/40213.

Felix Klein dans *Vergleichende Betrachtungen über neuere geometrische Forschungen* [Considérations comparatives sur les recherches géométriques récentes] (1872), écrit[2] :

> L'idée la plus essentielle requise dans la discussion qui suit est celle d'un *groupe* de transformations spatiales.
>
> La combinaison d'un nombre quelconque de transformations d'espace est toujours équivalente à une seule transformation. Si maintenant un système donné de transformations a la propriété que toute transformation obtenue en combinant n'importe quelles transformations du système appartient à ce système, on l'appellera un *groupe de transformations*.

Observons qu'il n'est pas précisé que les transformations inverses des transformations du système soient dans le système. Il est possible pourtant qut cette hypothèse ait été sous-entendue.

Groupes de symétries et groupes d'automorphismes

Les exemples les plus « typiques » de groupes sont les groupes de *symétries* (au sens large) et les groupes d'*automorphismes*.

Une *symétrie* d'un « espace géométrique » est une application bijective de l'ensemble des points de cet espace sur lui-même qui « respecte » la « structure géométrique » de l'espace. On peut aussi parler d'une *symétrie* d'une « figure » ou d'une « configuration » de points, de « figures » ou d'« objets géométriques » dans un espace, qui sont les symétries de l'espace laissant *invariant* cette « figure » ou cette « configuration ». En tout cas, la composition de deux symétries est une symétrie, l'application identité est une symétrie (la symétries *triviale*), et l'application réciproque d'une symétrie est une symétrie.

Un *automorphisme* d'une *structure algébrique* est une application bijective de l'ensemble des éléments de cette structure sur lui-même qui « respecte » toutes les opérations et toutes les relations de la structure. La composition de deux automorphismes est un automorphisme, l'application identité est un

[2] Felix Klein. "A comparative review of recent researches in geometry". Anglais. Trad. de l'allemand par Mellen Woodman Haskell. In : *Bulletin of the New York Mathematical Society* 2.10 (juill. 1893), p. 215-249. URL : https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society-new-series/volume-2/issue-10/A-comparative-review-of-recent-researches-in-geometry/bams/1183407629.full.

automorphisme (l'automorphisme *trivial*), et l'application réciproque d'un automorphisme est un automorphisme.

Semi-groupes, monoïdes, groupes, catégories et groupoïdes

Si on considère un ensemble S d'applications $X \to X$, et que S est clos par composition, on dit que S est un *semi-groupe* par rapport à l'opération de composition. Si, en plus, l'application identité $\mathrm{id}_X : X \to X$ est dans S, alors S est un *monoïde* par rapport à la composition. Si, en plus, S est composé uniquement des permutations (des application bijectives de X sur X), et que l'application inverse de chaque élément de S est dans S, alors S est un *groupe*.

Cependant, tout ce qu'on demande d'un *semi-groupe*, c'est que son opération de composition soit *associative*. Pour qu'un semi-groupe soit un *monoïde*, on demande uniquement l'existence d'un *élément neutre* pour la composition. Pour qu'un monoïde soit un groupe, on demande uniquement que tous les éléments soient *inversibles* par rapport à la composition.

Il est ainsi possible qu'un ensemble S d'applications $X \to X$ soit un monoïde, et même un groupe, sans que l'application identité id_X appartient à S. Par exemple, quel que soit un ensemble non-vide X et une application constante $e : X \to X$ ($e(x) = e(y)$ pour tous $x, y \in X$), l'ensemble $\{e\}$ est un groupe par rapport à l'opération de composition (vu que $e \circ e = e$).

À part de la composition de fonctions, un exemple courant et assez ample d'une opération associative est la multiplication de matrices.

L'ensemble des matrices carrées d'une certaine taille $n \times n$ à coefficients dans $\mathbf{Z}$, dans $\mathbf{R}$, ou dans un n'importe quel corps ou anneau unitaire, forment un monoïde par rapport à la multiplication. Ceux parmi elles qui sont inversibles forment un groupe, noté « $\mathrm{GL}_n(\mathbf{K})$ » si $\mathbf{K}$ est le corps des coefficients.

Si on considère l'ensemble de toutes les matrices de toutes tailles à coefficients dans un corps ou dans un anneau unitaire, on ne peut pas les toujours multiplier, mais dans le cas ou les produits sont définis, la multiplication est associative. En plus, pour tout n, il y a un *élément neutre* en dimension n – la matrice identité $n \times n$. Une telle structure est dite une *catégorie*.

Entre les catégories et les groupes se trouvent les *groupoïdes*, où on ne peut pas toujours composer (multiplier), mais on peut toujours inverser. Par exemple, si on considère une famille d'ensembles disjoints non vides, les bijections entre les membres de la famille forment un groupoïde par rapport à l'opération de composition.

I. Généralités

I.1. « Opérations » au sens algébrique du terme

Commençons par discuter la notion d'une *opération*. On s'intéresse ici à l'usage de ce terme dans le contexte des opérations arithmétiques et algébriques, comme celles d'addition, de soustraction, de multiplication.

Le mot « opération » est couramment utilisé en mathématique d'une manière informelle ou semi-formelle, sans aucune définition, et pourtant d'habitude sans risque de confusion.

En plus des usages informels, ce terme est parfois muni d'une définition formelle. Ceci n'est pas entièrement sans risque de confusion, car les définitions formelles ne correspondent pas exactement aux usages informelles, et parce que plusieurs définitions non équivalentes sont envisageables.[1]

Poursuivant la tradition mathématique moderne de formaliser tout et n'importe quoi, donnons une définition formelle au terme « opération » qui nous convient.

Rappelons-nous que :

- si X et Y sont deux ensembles, on note « $X \times Y$ » le *produit cartésien* de X et Y, qui est l'ensemble de tous les couples (x, y) avec $x \in X$ et $y \in Y$,
- si $n \in \mathbf{N}$ et X est un ensemble, on note « X^n » la n-ième *puissance cartésienne* de X, qui est l'ensemble de tous les *n-uples* des éléments de X.

[1] Comme une illustration de ce genre de difficulté, considérons une tentative de formaliser la notion de l'opération *sinus*, qui donne le sinus d'un angle, ou d'une quantité réelle. On peut souhaiter dire que sin est une *fonction* (au sens « moderne » du terme). Alors, quel est son domain de définition ? Est-il $\mathbf{R}$? Peut-être non, car on sais bien que les valeurs $\sin z$, $\cos z$, et e^z sont définies pour toute quantité complexe z. Alors, est-ce que le domaine de définition de sin est $\mathbf{C}$? Rappelons-nous ici que $\sin A$, $\cos A$, et e^A sont définis pour toute matrice carrée A à coefficients réelles ou complexes. Faut-il alors définir plusieurs fonctions toutes nommées « sin » ? Si oui, combien de définitions faut-il donner, et faut-il préciser à chaque usage de sin de laquelle on parle ? Notons par ailleurs qu'il y a différentes formalisations courantes de la notion d'une *fonction*, et qu'elles toutes différent du sens original de ce terme, où on pouvait parler d'une *variable* qui était *fonction* d'une autre *variable*.

Pour faire simple, et parce que les produits cartésiens des ensemble ne jouent qu'un rôle auxiliaire dans ce texte, on va prétendre que les identités suivantes soient vraies :[2]

$$X^0 = \{\varnothing\}, \qquad X^1 = X, \qquad X^2 = X \times X,$$
$$X^3 = (X \times X) \times X = X \times (X \times X), \qquad \dots$$

Définition. Définissons une *opération* d'*arité* $n \in \mathbf{N}$, ou une *opération* n*-aire*, sur un ensemble X comme une application $X^n \to X$. Une opération

- d'arité 0 sera dite *nulaire*,
- d'arité 1 sera dite *unaire*,
- d'arité 2 sera dite *binaire*,
- d'arité 3 sera dite *ternaire*,

et ainsi de suite.

Observons que donner une opération nulaire sur X revient à donner un élément de X (l'image de l'unique élément de X^0 par cette opération), et que donner une operation unaire sur X revient à donner une application $X \to X$ (car X^1 peut être « identifié » avec X grâce à la bijection canonique entre eux).

On n'aura pas besoin d'opérations d'arité supérieure à deux.[3]

Remarque. On a choisi une définition convenable, sans chercher la généralité. Notamment, l'opération de division des nombres rationnels n'est pas une opération sur $\mathbf{Q}$ selon notre définition (car elle n'est pas défini sur $\mathbf{Q} \times \mathbf{Q}$). Aussi, l'opération de multiplication d'un vecteur par un scalaire n'entre pas dans le cadre de cette définition. On pourrait donner une définition plus générale, et après distinguer différentes espèces d'opérations en les qualifiant comme *totales* ou *partielles*, *internes* ou *externes*.

Remarque. L'appellation « loi de composition », ou « loi de composition interne », pour ce qu'on appelle ici une *opération binaire* est assez courante.[4]

[2] En tout cas, il y a des *bijections canoniques* entre les parties gauche et droite de ces identités prétendues, et la première identité est peut-être vraie pour le vrai.

[3] En fait, il n'est pas évident de donner un exemple d'une opération « intéressante » d'arité supérieure à 2 qui ne soit pas exprimable comme une combinaison d'opérations « intéressantes » d'arités au plus 2.

[4] N. Bourbaki. *Algèbre. Chapitres 1 à 3.* 2e éd. Réimpression inchangée de la « nouvelle édition » de 1970. Berlin, Heidelberg : Springer, 11 déc. 2006. xiii+636. DOI : 10.1007/978-3-540-33850-5, Introduction, pp. xi–xii.

I.2. Opérations binaires

Définition. Soient S un ensemble et $\gamma\colon S \times S \to S$ une opération binaire sur S.

(1) L'opération γ est dite *associative* si et seulement si

$$\gamma(y_1, \gamma(x, y_2)) = \gamma(\gamma(y_1, x), y_2) \qquad \text{pour tous } x, y_1, y_2 \in S.$$

(2) L'opération γ est dite *commutative* si et seulement si

$$\gamma(y, x) = \gamma(x, y) \qquad \text{pour tous } x, y \in S.$$

(3) Un élément $a \in S$ est dit un *élément neutre à gauche*[5] pour γ si et seulement si

$$\gamma(a, x) = x \qquad \text{pour tout } x \in S.$$

(4) Un élément $b \in S$ est dit un *élément neutre à droite*[6] pour γ si et seulement si

$$\gamma(x, b) = x \qquad \text{pour tout } x \in S.$$

(5) Un élément de S est dit un *élément neutre* pour γ si et seulement s'il est neutre à gauche et à droite pour γ.

Proposition. *Soient S un ensemble et $\gamma\colon S \times S \to S$ une opération binaire associative sur S. Soient a un élément neutre à gauche pour γ et b un élément neutre à droite pour γ. Alors $a = b$.*

Démonstration. $a = \gamma(a, b) = b$. □

Ainsi, si une opération binaire associative admet un élément neutre, il y en a un seul et unique.

Définition. Soient S un ensemble et $\gamma\colon S \times S \to S$ une opération binaire associative sur S qui admet un élément neutre.

[5] Le terme « à gauche » vient de notre façon d'écrire de gauche à droite. Si on écrivait de droite à gauche, on dirait « neutre à droite » au lieu de « neutre à gauche », et si on écrivait de haut en bas, on dirait « neutre en haut », et ainsi de suite.

[6] Voir la note précédente.

(1) Pour deux éléments $x, y \in S$, on dit que x est *inverse à gauche* de y pour γ, ou, ce qui est la même chose, que y est *inverse à droite* de x, si et seulement si $\gamma(x, y)$ est l'élément neutre pour γ. Un élément qui admet un inverse à gauche est dit *inversible à gauche*, et un élément qui admet un inverse à droite est dit *inversible à droite*.

(2) Pour deux éléments $x, y \in S$, on dit qu'ils sont *inverses* l'un de l'autre pour γ si et seulement si $\gamma(x, y)$ est l'élément neutre et $\gamma(y, x)$ l'est aussi. Un élément qui admet un inverse est dit *inversible*.

(3) Un élément de S est dit être une *involution* pour γ si et seulement si il est inverse de lui-même pour γ.

Proposition. *Soient S un ensemble et $\gamma\colon S \times S \to S$ une opération binaire associative sur S qui admet un élément neutre. Soient $x, y_1, y_2 \in S$ tels que y_1 soit inverse de x à gauche et y_2 soit inverse de x à droite pour γ. Alors $y_1 = y_2$.*

Démonstration. $y_1 = \gamma(y_1, \gamma(x, y_2)) = \gamma(\gamma(y_1, x), y_2) = y_2$. □

Autrement dit, si un élément x admet un inverse à gauche et un inverse à droite (pour une opération binaire associative), alors les deux coïncident, et cet élément est l'unique inverse de x.

Théorème. *Soient S un ensemble et $(\circ)$ une opération binaire associative sur S qui satisfait les deux propriétés suivantes* :

(1) *pour tous $z, y \in S$, il existe $x \in S$ tel que $x \circ y = z$,*

(2) *pour tous $z, y \in S$, il existe $x \in S$ tel que $y \circ x = z$.*

Alors, quels que soient $x_1, x_2, y_1, y_2 \in S$:

(1) *si $x_1 \circ y_1 = y_1$ et $x_2 \circ y_2 = y_2$, alors $x_1 = x_2$,*

(2) *si $y_1 \circ x_1 = y_1$ et $y_2 \circ x_2 = y_2$, alors $x_1 = x_2$,*

(3) *si $x_1 \circ y_1 = y_1$ et $y_2 \circ x_2 = y_2$, alors $x_1 = x_2$.*

Le lemme suivant sera utilisé dans la démonstration de ce théorème :

Lemme. *Sous les hypothèses du théorème, quels que soient $x_1, x_2, y \in S$, on a :*

(1) *si $x_1 \circ y = x_2 \circ y$, alors $x_1 = x_2$,*

(2) *si* $y \circ x_1 = y \circ x_2$, *alors* $x_1 = x_2$.

Démonstration. Adoptons l'écriture « xy » pour $x \circ y$.

Soient $x_1, x_2, y \in S$ tels que $x_1 y = x_2 y$. Posons

$$z = x_1 y = x_2 y.$$

Notons « x_2/x_1 » et « $z\backslash x_1$ » des éléments de S tels que :

$$(x_2/x_1)x_1 = x_2 \qquad \text{et} \qquad z(z\backslash x_1) = x_1$$

(n'importe lesquels s'il y en plusieurs). Alors :

$$\begin{aligned} x_1 &= z(z\backslash x_1) = x_2 y(z\backslash x_1) = (x_2/x_1)x_1 y(z\backslash x_1) \\ &= (x_2/x_1)z(z\backslash x_1) = (x_2/x_1)x_1 = x_2. \end{aligned}$$

Ainsi, la partie (1) est démontrée. La partie (2) se démontre de la même manière. □

Démonstration du théorème. Adoptons l'écriture « xy » pour $x \circ y$.

Vu le lemme précédent, définissons les opérations $(/)$ de « quotient à droite » et $(\backslash)$ de « quotient à gauche » par les identités suivantes :

$$(x/y)y = x = y(y\backslash x), \qquad \text{pour tous } x, y \in S.$$

Montrons la partie (1). Soient $x_1, x_2, y_1, y_2 \in S$ tels que $x_1 y_1 = y_1$ et $x_2 y_2 = y_2$. Alors :

$$x_1 y_1 = y_1 = y_2(y_2\backslash y_1) = x_2 y_2(y_2\backslash y_1) = x_2 y_1,$$

d'où, $x_1 = x_2$ d'après le lemme.

La partie (2) se montre de la même manière.

Observons que, d'après la partie (1) de la conclusion (déjà démontrée) et d'après l'hypothèse (1), si $x, y \in S$ et que $xy = y$, alors x est un et unique élément neutre à gauche pour $(\circ)$, et donc $xz = z$ pour tout $z \in S$. De même, d'après la partie (2) de la conclusion et d'après l'hypothèse (2), si $x, y \in S$ et que $yx = y$, alors x est un et unique élément neutre à droite pour $(\circ)$, et donc $zx = z$ pour tout $z \in S$. On appliquera cela pour montrer la partie (3) de la conclusion.

Montrons donc la partie (3). Soient $x_1, x_2, y_1, y_2 \in S$ tels que $x_1 y_1 = y_1$ et $y_2 x_2 = y_2$. Alors, $x_1 x_2 = x_2$ (car $x_1 y_1 = y_1$) et $x_1 x_2 = x_1$ (car $y_2 x_2 = y_2$). D'où, $x_2 = x_1$. □

Corollaire. *Sous les hypothèses du théorème précédent, et à condition que l'ensemble S ne soit pas vide, il existe un unique couple (e, δ), avec $e \in S$ et $\delta\colon S \to S$, tel que, pour tout $x \in S$,*

(1) $x \circ e = x = e \circ x$,

(2) $x \circ \delta(x) = e = \delta(x) \circ x$.

Exercice. Démontrer ce corollaire.

I.3. Structure de groupe

Définition. Munir un ensemble S d'une *structure de groupe* signifie désigner :

(1) une opération binaire $\gamma\colon S \times S \to S$, qui sera appelée la *loi de composition*, ou l'*opération de composition*, ou l'*opération de groupe* tout simplement,

(2) un élément $e \in S$, qui sera appelé l'*identité*, ou l'*unité*, ou l'*élément neutre*,

(3) une opération unaire $\delta\colon S \to S$, qui sera appelée l'*inversion*,

de sorte que :

(1) γ soit associative :

$$\gamma(y_1, \gamma(x, y_2)) = \gamma(\gamma(y_1, x), y_2)$$

pour tous $x, y_1, y_2 \in S$,

(2) e soit l'élément neutre pour γ :

$$\gamma(x, e) = x = \gamma(e, x)$$

pour tout $x \in S$,

(3) $\delta(x)$ soit l'inverse de x pour γ :

$$\gamma(x, \delta(x)) = e = \gamma(\delta(x), x)$$

pour tout $x \in S$.

Si on note $\gamma(x, y)$ comme « $x \cdot y$ », e comme « 1 », et $\delta(x)$ comme « $x\backslash$ », ces identités s'écrivent ainsi :

(1) $y_1 \cdot (x \cdot y_2) = (y_1 \cdot x) \cdot y_2$,

(2) $x \cdot 1 = x = 1 \cdot x$,

(3) $x \cdot (x\backslash) = 1 = (x\backslash) \cdot x$.

Un *groupe* est un ensemble muni d'une structure de groupe. Si un groupe G est donné comme un ensemble S muni d'une structure de groupe, alors l'ensemble S est dit l'*ensemble sous-jacent* du groupe G.

Observons que, vu l'obligation d'avoir l'élément identité, on ne peut pas munir l'ensemble vide $\varnothing$ d'une structure de groupe.

Définition. L'*ordre* d'un groupe est le nombre cardinal (la taille) de l'ensemble de ses éléments (de son ensemble sous-jacent).

Notation. L'ordre d'un groupe G est noté « $|G|$ ».

Observons que pour donner une application/fonction/opération avec un certain domaine de définition D, il suffit d'en donner une avec un domaine plus large dont la restriction sur D sera convenable. Ainsi, pour munir un ensemble S d'une structure de groupe, il suffit de désigner des opérations dont les *restrictions* appropriées forment une structure de groupe sur S. Par exemple, pour munir l'ensemble $2\mathbf{Z}$ des entiers pairs d'une structure de groupe, on peut désigner l'opération d'addition d'entiers comme l'opération de ce groupe (alors que le domaine de définition de cette opération est $\mathbf{Z} \times \mathbf{Z}$), car il suffit de prendre la restriction de cette opération sur $(2\mathbf{Z}) \times (2\mathbf{Z})$ pour satisfaire la lettre de la définition (dont l'esprit devrait déjà être satisfait).

En général on est assez libre dans le choix de symboles pour nommer l'opération de groupe, l'élément identité, et l'opération d'inversion. Les appellations utilisées peuvent aussi varier, tant que les rôles des opérations et des éléments désignés restent clairs.

Vu le rôle principal de l'opération de groupe $\gamma\colon S \times S \to S$, on va souvent noter l'image de (x, y) par cette opération comme « xy » tout court (plutôt que « $\gamma(x, y)$ », ou « $x \cdot y$ », etc.).[7]

On peut définir un groupe plus formellement comme un quadruple (S, γ, e, δ), où S est un ensemble (non vide) et $\gamma\colon S \times S \to S$, $e \in S$, $\delta\colon S \to S$ forment une structure de groupe sur S comme dans la définition ci-dessus. En fait, on

[7] Observons qu'à priori rien n'empêche de noter l'image de (x, y) par l'opération de groupe comme « yx » ou « $y \cdot x$ ». Sauf qu'il y a une tradition d'écrire le premier argument d'une opération à gauche et le second à droite, parce qu'on écrit de gauche à droite. Cependant, cette tradition n'est pas toujours évidente à appliquer : dans « x^y », « $\log_y x$ », « $\frac{x}{y}$ », quel argument est le premier et quel est le second ?

verra bientôt que l'opération de groupe $\gamma\colon S \times S \to S$ toute seule suffit pour déterminer la structure de groupe, et ainsi on peut définir un groupe comme un couple (S, γ).

Tout ensemble qui contient plus d'un élément peut être muni de plusieurs structures de groupe différentes. Ainsi, différents groupes peuvent avoir le même ensemble sous-jacent.

Cependant, pour des raisons pratique et par pénurie de lettres dans les alphabets communs, on peut se permettre d'utiliser un même symbole (une même lettre) pour nommer un groupe et son ensemble sous-jacent, tant que le contexte permet d'éviter toute ambiguïté. Souvent ce symbole sera « G ».

Comme il est de coutume dans un discours mathématique, lorsque dans un certain contexte il y a une façon évidente de munir un certain ensemble d'une structure de groupe, on ne va pas préciser tous les détails, et on pourra traiter cet ensemble comme un groupe.

On peut dire qu'un certain ensemble *forme un groupe* par rapport à une ou plusieurs opérations données pour dire que ces opérations (avec leurs rôles indiquées ou entendus) munissent cet ensemble d'une unique structure de groupe. Par exemple, l'ensemble des nombres rationnels non nuls forme un groupe par rapport à l'opération de multiplication.

D'après le corollaire du théorème de la section précédente, pour munir un ensemble d'une structure de groupe, il suffit d'y désigner l'opération de composition de ce groupe.

Notation. Lorsqu'on utilise la terminologie *multiplicative* pour les opérations d'un groupe G, en appelant l'opération de composition la *multiplication*, les notations suivantes seront utilisées :

(1) on note « $x \cdot y$ » ou « xy » le *produit* de x et y, c'est-à-dire, l'image de $(x, y) \in G \times G$ par l'opération de composition de G (par la multiplication),

(2) on note « 1 » ou « 1_G » l'identité (l'élément neutre) de G,

(3) on note « x/y » le *quotient à droite* de $x \in G$ par $y \in G$, défini par l'équation :

$$(x/y) \cdot y = x,$$

(4) on note « $y\backslash x$ » le *quotient à gauche* de $x \in G$ par $y \in G$, défini par l'équation :

$$y \cdot (y\backslash x) = x,$$

(5) on note « x^n », où $n \in \mathbf{N}$ et $x \in G$, l'élément défini par la formule :

$$x^n \overset{\text{déf}}{=} 1\underbrace{\cdot x \cdot \cdots \cdot x}_{n \text{ fois}} = \underbrace{x \cdot \cdots \cdot x \cdot}_{n \text{ fois}} 1,$$

(6) on note « x^a », où $a \in \mathbf{Z}$, $a = n - m$ avec $m, n \in \mathbf{N}$, et $x \in G$, l'élément défini par la formule :

$$x^{n-m} \overset{\text{déf}}{=} x^n/x^m = x^m\backslash x^n.$$

Proposition. *Quels que soient $a, b \in \mathbf{Z}$ et un élément x d'un groupe, les identités suivantes sont satisfaites* :

$$x^{a+b} = x^a x^b = x^b x^a, \qquad x^{a-b} = x^a/x^b = x^b\backslash x^a, \qquad x^{ab} = (x^a)^b = (x^b)^a.$$

Exercice. Prouver cette proposition.

I.4. Commutation

Définition. On dit que deux éléments x et y d'un groupe *commutent* si et seulement si $yx = xy$.

Proposition. *Si x et y sont deux éléments d'un groupe qui commutent, alors $y\backslash x = x/y$.*

Démonstration. Si $xy = yx$, alors

$$\begin{aligned} y\backslash x &= (1/y)y(y\backslash x) = (1/y)x = (1/y)xy(y\backslash 1) \\ &= (1/y)yx(y\backslash 1) = x(y\backslash 1) = (x/y)y(y\backslash 1) = x/y. \end{aligned}$$ □

Proposition. *Si $a \in \mathbf{Z}$ et x et y sont deux éléments d'un groupe qui commutent, alors $(xy)^a = x^a y^a$ et $(x/y)^a = x^a/y^a$.*

Exercice. Prouver cette proposition.

I.5. Groupes abéliens (commutatifs)

Définition. Un groupe est dit *abélien*[8] ou *commutatif* si et seulement si son opération de composition est commutative.

[8] En hommage à Niels Henrik Abel (1802–1829).

Pour les groupes abéliens, et uniquement pour les groupes abéliens, la terminologie et la notation *additives* peuvent être utilisées, où l'opération de composition s'appelle l'*addition* et est notée avec « $+$ ».

Notation. Lorsqu'on utilise la terminologie *additive* pour les opérations d'un groupe abélien G, en appelant l'opération de composition l'*addition*, les notations suivantes seront utilisées :

(1) on note « $x+y$ » la *somme* de x et y, c'est-à-dire, l'image de $(x, y) \in G \times G$ (et, au même temps, de (y, x)) par l'opération de composition de G (par l'addition),

(2) on note « 0 » ou « 0_G » l'identité (l'élément neutre) de G,

(3) on note « $x - y$ » la *différence* de $x \in G$ et $y \in G$, définie par l'équation :

$$(x - y) + y = x,$$

(4) on note « nx », où $n \in \mathbf{N}$ et $x \in G$, l'élément défini par la formule :

$$nx \overset{\text{déf}}{=} 0 \underbrace{+ x \cdots + x}_{n \text{ fois}} = \underbrace{x + \cdots x +}_{n \text{ fois}} 0,$$

(5) on note « ax », où $a \in \mathbf{Z}$, $a = n - m$ avec $m, n \in \mathbf{N}$, et $x \in G$, l'élément défini par la formule :

$$(n - m)x \overset{\text{déf}}{=} nx - mx.$$

Notation. Les notations abrégées suivantes sont utilisées :

(1) au lieu d'écrire « $0 + x$ », on peut écrire « $+x$ » tout court,

(2) au lieu d'écrire « $0 - x$ », on peut écrire « $-x$ » tout court.

I.6. Groupes opposés

Définition. Deux groupes G et H d'un même ensemble sous-jacent S sont dits *opposés* l'un de l'autre si et seulement si pour tous $x, y \in S$, l'image de (x, y) par l'opération de composition de G coïncide avec l'image de (y, x) par l'opération de composition de H.

Pour exprimer cette définition par une formule, considérons deux groupes G et H d'un même ensemble sous-jacent S, notons $(\circ_G)$ l'opération de composition de G, et notons $(\circ_H)$ l'opération de composition de H. Alors G et H sont opposés l'un de l'autre si et seulement si l'identité suivante est satisfaite :

$$x \underset{G}{\circ} y = y \underset{H}{\circ} x \qquad \text{pour tous } x, y \in S.$$

Clairement, les groupes opposés partagent l'élément identité et l'opération d'inversion. Tout groupe a un unique groupe opposé.

Notation. Le groupe opposé d'un groupe G est noté G^{op}.

Observons qu'un groupe G est abélien si et seulement si il coïncide avec son groupe opposé (en tant qu'un groupe[9]).

I.7. Exemples

Permutations

Si X est un ensemble, alors l'ensemble des *permutations* de X, c'est-à-dire, des bijections entre X et lui-même, forme un groupe par rapport à l'opération de composition. Ce groupe est dit le *groupe symétrique* de X et est d'habitude noté « S_X » ou « $\mathfrak{S}_X$ » ou « Σ_X », ou « $S(X)$ » et ainsi de suite, ou encore « $\mathrm{Sym}(X)$ ».

Le groupe des permutations de l'ensemble $\{1, \ldots, n\}$ est souvent noté « S_n » ou « $\mathfrak{S}_n$ » ou « Σ_n ».

Transformations et symétries

Si M est un *espace métrique*, alors l'ensemble des bijections *isométriques* entre M et lui-même forme un groupe par rapport à l'opération de composition. Telles bijections isométriques d'un espace avec lui-même sont parfois appelées *transformations isométriques* ou *symétries*.

En général, les bijections entre un « espace géométrique » et lui-même qui préservent sa « structure géométrique » forment un groupe, qu'on peut appeler le *groupe de symétries* de cet « espace ».

[9] Ici la distinction entre un groupe G et son ensemble sous-jacent est assez importante : G et G^{op} partagent toujours l'ensemble sous-jacent, mais l'identité $G = G^{\mathrm{op}}$ de groupes n'a lieu que si G est abélien.

Parfois on considère une partie ou une « figure géométrique » dans un « espace » et on définit le groupe des symétries de cette « figure » dans cet « espace » comme l'ensemble de transformations de l'« espace » qui préservent sa « structure » et envoient la « figure » sur elle-même.

Le terme « transformation » est utilisé plus librement que le terme « symétrie », et son interprétation dépend des qualifications et du contexte.

Groupes diédraux

Observons qu'un polygon régulier à n sommets possède $2n$ symétries (y compté la symétrie triviale). Par exemple, les symétries d'un triangle équilatéral sont :

(1) la symétrie triviale (identité),

(2) les 2 rotations d'angles $\pm 2\pi/3$ modulo 2π,

(3) les 3 réflexions par rapport à ses 3 axes de symétrie.

Ces symétries forment un groupe par rapport à la composition. Par exemple, une rotation suivie d'une réflexion axiale équivaut une réflexion axiale.

Évidemment, pour deux polygones réguliers avec le même nombre des sommets, leurs groupes de symétries sont « identiques » du point de vu de leurs structures de groupe ; on dit qu'ils sont *isomorphes*.

D'habitude, lorsqu'on utilise les groupes des symétries des polygones réguliers en théorie de groupes, on prétend avoir choisi, pour chaque $n \geqslant 3$, un certain polygone régulier à n sommets, et ainsi, pour chaque n, on ne considère qu'un seul groupe. On appelle ces groupes les *groupes diédraux*, et on fixe une notation pour les nommer. Deux notations sont courantes :

(1) Avec la notation dite *géométrique*, le groupe diédral des symétries du polygone régulier à n sommets est noté « D_n ».

(2) Avec la notation dite *algébrique*, le groupe diédral des symétries du polygone régulier à n sommets est noté « D_{2n} » (vu que son ordre est $2n$).

Dans ces notes on va suivre la convention géométrique.

Cependant, la définition des groupes diédraux comme les groupes des symétries des polygones réguliers n'est pas complètement satisfaisante, car elle ne définit le groupe D_n que pour $n \geqslant 3$, alors qu'il y a une manière naturelle de définir D_n pour tout $n \geqslant 1$. En plus, il est possible de définir D_∞ par analogie.

Quel que soit $n \geqslant 1$, on peut définir le *groupe diédral* D_n comme le groupe des applications $\mathbf{C} \to \mathbf{C}$ (de l'ensemble des nombres complexes sur lui-même)

qui sont de la forme $z \mapsto uz$ ou de la forme $z \mapsto u\bar{z}$ avec $u \in \mathbf{C}$ tel que $u^n = 1$. (Ici $\bar{z}$ est le conjugué complexe de z.) Observons que les éléments de D_n, défini ainsi, envoient le cercle unité $\mathbf{U} = \{ z \in \mathbf{C} \mid |z| = 1 \}$ sur lui même en laissant invariant l'ensemble des racines n-ièmes de 1.

On peut aussi définir le groupe diédral D_n comme le groupe des isométries d'un cercle de longueur n qui laissent invariant un ensemble de n points repartis uniformément sur le cercle à intervalles de longueur 1.

Par analogie, en regardant une droite comme un « cercle de longueur infinie », on définit alors le groupe diédral D_∞ comme le groupe des isométries d'une droite qui laissent invariant un ensemble discret des points uniformément reparties. Plus concrètement, on peut définir le groupe diédral D_∞ comme le groupe des applications $\mathbf{R} \to \mathbf{R}$ qui sont de la forme $t \mapsto n + t$ ou de la forme $t \mapsto n - t$ avec $n \in \mathbf{Z}$. (On peut aussi bien définir D_∞ comme le groupe des applications $\mathbf{Z} \to \mathbf{Z}$ de ces deux formes.)

Tresses

Différentes manières de tresser n fils ou n brins peuvent être composées : une tresse peut être prolongée par une autre. Ainsi on obtient un *groupe de tresses* à n brins, d'habitude noté « B_n ».

Automorphismes

Si V est un espace vectoriel, alors l'ensemble des automorphismes de V forme un groupe par rapport à l'opération de composition. Ce groupe est dit le *groupe général linéaire* sur V ; il est noté « $\mathrm{GL}(V)$ ». On peut aussi appeler ce groupe le *groupe d'automorphismes* de V tout simplement, et le noter « $\mathrm{Aut}(V)$ ».

En général, les *automorphismes* de toute *structure algébrique* (y compris ceux d'un groupe) forment un groupe par rapport à la composition. Le groupe d'automorphismes de d'une structure algébrique A est noté « $\mathrm{Aut}(A)$ ».

Les groupes additif et multiplicatif d'un anneau

Soit R est un *anneau*, comme $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{Z}[X]$, $\mathbf{Q}[X]$, $\mathbf{R}[X]$, ou, encore, comme l'ensemble des matrices carrées d'une taille donnée à coefficients dans un autre anneau. Alors :

(1) l'ensemble d'élément de R forme un groupe abélien par rapport à l'opération d'addition de R, dit le *groupe additif* de R,

(2) si l'anneau R est unitaire (c'est-à-dire, possède l'élément neutre pour la multiplication), alors l'ensemble des élément inversibles de R forme un groupe par rapport à l'opération de multiplication de R, dit le *groupe multiplicatif* de R.

Le groupe additif d'un anneau R est d'habitude noté « R » tout simplement, et son groupe multiplicatif est d'habitude noté « $R^\times$ ».

Par exemple, comme les seuls éléments inversibles dans l'anneau $\mathbf{Z}$ des entiers relatifs sont $+1$ et -1, on a que $\mathbf{Z}^\times = \{\pm 1\}$, avec la multiplication pour l'opération de groupe.

Si V est un espace vectoriel, alors $\mathrm{GL}(V)$ est le groupe multiplicatif de l'anneau des endomorphismes de V.

Sous-groupes

Étant donné un groupe, il peut y en avoir une partie qui forme un groupe par rapport aux mêmes opérations (au sens de leurs restrictions).

Par exemple, l'ensemble $2\mathbf{Z}$ des entiers pairs forme un groupe par rapport à l'addition. Ce groupe est un sous-groupe du groupe additif $\mathbf{Z}$ (ainsi que de $\mathbf{Q}$, de $\mathbf{R}$, et de $\mathbf{C}$, si l'on admet que $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$).

L'ensemble $\mathbf{U}$ des nombres complexes de valeur absolue 1 forme un groupe par rapport à l'opération de multiplication. Ce groupe est un sous-groupe du groupe multiplicatif $\mathbf{C}^\times$.

Pour tout $n \in \mathbf{N} \setminus \{0\}$, l'ensemble $\mathbf{U}_n$ des racines complexes n-ièmes de 1 forme un sous-groupe de $\mathbf{U}$. En plus, si $m, n \in \mathbf{N} \setminus \{0\}$ et que m divise n, alors $\mathbf{U}_m$ est un sous-groupe de $\mathbf{U}_n$.

Produits directs

Étant donnés deux groupes G et H, on peut munir le produit cartésien $G \times H$ (de leurs ensembles sous-jacents) d'une structure de groupe en définissant l'opération de composition par la règle :

$$(g_1, h_1)(g_2, h_2) \overset{\text{déf}}{=} (g_1 g_2,\ h_1 h_2).$$

Le groupe défini ainsi est dit le *produit direct* (externe) de G et H et est noté aussi comme « $G \times H$ ».

I.8. Opérations sur les parties

Notation. Pour un élément x d'un groupe G et pour une partie U de G, définissons « xU » et « Ux » ainsi :

$$xU \overset{\text{déf}}{=} \{\, xy \mid y \in U \,\}, \qquad Ux \overset{\text{déf}}{=} \{\, yx \mid y \in U \,\}.$$

Notation. Pour deux parties U et V d'un groupe G, définissons « UV » ainsi :

$$UV \overset{\text{déf}}{=} \{\, xy \mid x \in U,\ y \in V \,\}.$$

Notation. Pour une partie U d'un groupe G, définissons « U^- » et « $U^\pm$ » ainsi :

$$U^- \overset{\text{déf}}{=} \{\, x^{-1} \mid x \in U \,\}, \qquad U^\pm \overset{\text{déf}}{=} U \cup U^-.$$

Remarque. Des nombreux auteurs notent « U^{-1} » ce qu'on note « U^- » ici.

Notation. Pour $n \in \mathbf{N}$ et pour une partie U d'un groupe G, définissons « U^n » ainsi :

$$U^n \overset{\text{déf}}{=} \{1\} \underbrace{U \cdots U}_{n \text{ fois}} = \underbrace{U \cdots U}_{n \text{ fois}} \{1\}.$$

Remarque. Les notations « UV », « U^- », « $U^\pm$ », « U^n » introduites ci-dessus n'ont pas de sens hors du contexte d'un certain groupe dont on considère les parties. (Déjà, il faut pouvoir identifier « 1 » dans la formule pour « U^n » comme l'élément neutre d'un certain groupe.)

Exercice. Considérons la partie vide $\varnothing$ d'un groupe G. Déterminer les ensembles $\varnothing\varnothing$, $\varnothing G$, $\varnothing^-$, $\varnothing^\pm$, $\varnothing^0$, $\varnothing^1$.

I.9. Sous-groupes et parties génératrices

Définition. Un groupe H est dit un *sous-groupe* d'un groupe G si et seulement si :

(1) l'ensemble sous-jacent de H est une partie de l'ensemble sous-jacent de G,

(2) l'opération de composition de H est la restriction de l'opération de composition de G (sur $H \times H$),

(3) l'élément identité de H est le même que l'élément identité de G,

(4) l'opération d'inversion de H est la restriction de l'opération d'inversion de G (sur H).

Si une partie de l'ensemble sous-jacent d'un groupe G possède une structure d'un sous-groupe de G, cette structure est unique. Ainsi, pour donner un sous-groupe H d'un groupe déjà donné G, il suffit de donner l'ensemble sous-jacent de H, car la structure de groupe y sera induite par celle de G.

On va continuer à confondre les groupes et leurs ensembles sous-jacents tant que le contexte permet de démêler l'ambiguïté ainsi créée.

Proposition. *Soit H une partie d'un groupe G. Alors H est un sous-groupe de G si et seulement si* :

(1) *pour tous $x, y \in H$, on a $xy \in H$,*

(2) $1 \in H$,

(3) *pour tout $x \in H$, on a $x^{-1} \in H$.*

Tout groupe est sous-groupe de lui même. L'élément neutre d'un n'importe quel groupe forme le *sous-groupe trivial* de ce groupe (qu'on peut confondre avec son ensemble sous-jacent $\{1\}$).

Définition. Soient G un groupe et H un sous-groupe de G. On va dire que H est un sous-groupe *trivial* de G si et seulement si H est un groupe trivial, c'est-à-dire, si et seulement si H ne contient que l'élément neutre. On va dire que H est un sous-groupe *propre* de G si et seulement si $H \neq G$.

Notation. On peut noter le sous-groupe trivial de G comme « $\mathbf{1}_G$ » ou « $\mathbf{1}$ ». Si G est abélien, et qu'on utilise la notation additive, on peut noter le sous-groupe trivial de G comme « $\mathbf{0}_G$ » ou « $\mathbf{0}$ ».

Remarque. Certains auteurs définissent un sous-groupe *propre* de G comme un sous-groupe différent de G et de $\mathbf{1}_G$. Certains appellent les sous-groupes G et $\mathbf{1}_G$ de G les sous-groupes *triviaux*, et alors les autres sont dits *non triviaux*.

Notation. On va écrire « $H \leqslant G$ » ou « $G \geqslant H$ » pour dire que H est un sous-groupe de G, et on va écrire « $H < G$ » ou « $G > H$ » pour dire que H est un sous-groupe de G et que $H \neq G$.

Proposition. *Tout sous-groupe de tout sous-groupe d'un groupe G est un sous-groupe de G.*

Proposition. *L'intersection de tout ensemble de sous-groupes d'un groupe G est un sous-groupe de G.*

Exercice. Prouver cette proposition.

Notation. Si H et K sont deux sous-groupes d'un groupe G, leur intersection peut être notée « $H \wedge K$ », lorsqu'elle est vue comme un sous-groupe de G (et pas comme une simple partie de G).[10] Si $(H_i)_{i\in I}$ est une famille de sous-groupes de G, leur intersection peut être notée « $\bigwedge_{i\in I} H_i$ ».

Proposition. *Soient H et K deux sous-groupes d'un groupe G. Supposons que $kh = hk$ pour tous $h \in H$ et $k \in K$. Alors $KH = HK$ est un sous-groupe de G.*

Exercice. Prouver cette proposition.

Définition. Une partie U d'un groupe G est dit *engendrer* le groupe G si et seulement si G n'a aucun sous-groupe H tel que $U \subset H < G$. Une partie d'un groupe qui engendré ce groupe est dite une partie *génératrice* ou un *ensemble de générateurs* de ce groupe.

Proposition. *Quelle que soit une partie U d'un groupe G, il y a un unique sous-groupe de G engendré par U : c'est l'intersection de tous les sous-groupes de G contenant U.*

Exercice. Prouver cette proposition.

Notation. Le sous-groupe engendré par un ensemble U peut être noté « $\langle U \rangle$ ».
Le sous-groupe engendré par un ensemble $\{x_1, \ldots, x_n\}$ peut être noté « $\langle x_1, \ldots, x_n \rangle$ ».

Théorème. *Soient G un groupe et U une partie de G. Alors*

$$\langle U \rangle = \bigcup_{n\in\mathbf{N}} (U^{\pm})^n.$$

Exercice. Prouver ce théorème.

Définition. Un groupe est dit *de type fini* si et seulement si il admet une partie génératrice finie.

Définition. Un groupe est dit *cyclique* ou *monogène* si et seulement si il admet une partie génératrice réduite à un seul élément.

En général, si x est un élément d'un groupe G, on peut considérer le sous-groupe cyclique $\langle x \rangle$ engendré par x dans G. Clairement,

$$\langle x \rangle = \{\, x^n \mid n \in \mathbf{Z} \,\}.$$

[10] Cet usage n'est pas très courant, mais il fait partie de l'usage standard du symbole « $\wedge$ » dans le contexte des *treillis*.

Définition. L'*ordre* d'un élément x d'un groupe est le nombre d'élément dans le sous-groupe $\langle x \rangle$ engendré par x. (Il peut être infini.)

Tout groupe possède un unique élément d'ordre 1 : c'est son élément identité. Les éléments d'ordre 2 sont les involutions non triviales (autres que l'identité).

Remarque. La notion de l'ordre d'un élément x est parfois utilisée, à tort ou par manque de terminologie adaptée, dans des situations où on aurait l'intérêt d'utiliser plutôt le PGCD positif de l'ensemble

$$\{\, n \in \mathbf{Z} \mid x^n = 1 \,\}.$$

Les deux coïncident lorsque x est d'ordre fini. Dans le cas contraire,

$$\{\, n \in \mathbf{Z} \mid x^n = 1 \,\} = \{0\},$$

et 0 est l'unique PGCD de cet ensemble.

I.10. Conjugaison

Observons que, pour tous éléments x, y, z d'un groupe, on a les équivalences :

$$zx = yz \quad \Leftrightarrow \quad zxz^{-1} = y \quad \Leftrightarrow \quad xz^{-1} = z^{-1}y \quad \Leftrightarrow \quad x = z^{-1}yz.$$

Définition. On dit que deux éléments x et y d'un groupe G sont *conjugués* dans G si et seulement si il existe $z \in G$ tel que $zx = yz$.

Exercice. Montrer que la relation d'être conjugués est symétrique, réflexive, et transitive.

Définition. Si x et y sont deux éléments d'un groupe, on va appeler l'élément yxy^{-1} le *conjugué* de x par y.

Remarque. Deux définitions différentes du termes « le conjugué » sont courantes : certains textes définissent le *conjugué* de x par y comme yxy^{-1}, d'autre le définissent comme $y^{-1}xy$. Peut-être il est raisonnable d'appeler yxy^{-1} le *conjugué* de x par y *à gauche*, et d'appeler $y^{-1}xy$ le *conjugué* de x par y *à droite*.

Notation. Parfois les notations suivantes sont utilisées :

$$x^y \overset{\text{déf}}{=} y^{-1}xy, \qquad {}^yx \overset{\text{déf}}{=} yxy^{-1}.$$

I.11. Isomorphismes et automorphismes

Définition. Un *isomorphisme* entre deux groupes est une bijection entre leurs ensembles sous-jacents qui respecte les structures de groupe au sens suivant. Si G et H sont deux groupes, dont les ensembles sous-jacents sont aussi notés G et H, et qu'on note $(\circ_G)$ et $(\circ_H)$ leurs opérations de composition, e_G et e_H leurs identités, et δ_G et δ_H leurs opérations d'inversion, alors une bijection f entre les ensembles G et H est un *isomorphisme* entre les groupes G et H si et seulement si :

(1) $f(x \circ_G y) = f(x) \circ_H f(y)$ pour tous $x, y \in G$,

(2) $f(e_G) = e_H$,

(3) $f(\delta_G(x)) = \delta_H(f(x))$ pour tout $x \in G$.

Si, au lieu d'utiliser différents symboles, ou symboles « décorés », pour distinguer les opérations correspondantes dans différents groupes, on laissera le contexte faire la différence, les 3 conditions de la définition peuvent être écrites ainsi :

(1) $f(xy) = f(x)f(y)$,

(2) $f(1) = 1$,

(3) $f(x^{-1}) = (f(x))^{-1}$.

Proposition. *Soient G et H deux groupes et $f\colon G \to H$ une bijection entre leurs ensemble sous-jacents telle que $f(xy) = f(x)f(y)$ pour tous $x, y \in G$. Alors f est un isomorphisme entre G et H.*

Exercice. Prouver cette proposition.

Notation. On va écrire « $f\colon G \xrightarrow{\sim} H$ » ou « $f\colon H \xleftarrow{\sim} G$ » pour dire que l'application $f\colon G \to H$ est un isomorphisme entre G et H.

Parfois au lieu de « $f\colon G \xrightarrow{\sim} H$ », on écrit « $G \overset{f}{\simeq} H$ » ou « $f\colon G \simeq H$ ».
Observons que :

(1) l'application identité id_G (de l'ensemble sous-jacent) d'un groupe G est un isomorphisme entre G et lui-même : $\mathrm{id}_G\colon G \xrightarrow{\sim} G$.

(2) l'application réciproque d'un isomorphisme est un isomorphisme : si $f\colon G \xrightarrow{\sim} H$, alors $f^{-1}\colon G \xleftarrow{\sim} H$.

(3) l'application composée de deux isomorphismes est un isomorphisme : si $\alpha\colon G \xrightarrow{\sim} H$ et $\beta\colon H \xrightarrow{\sim} K$, alors $\beta \circ \alpha\colon G \xrightarrow{\sim} K$.

Définition. Deux groupes sont dits *isomorphes* l'un à l'autre si et seulement s'il existe un isomorphisme entre eux.

Notation. On va écrire « $G \simeq H$ » pour dire que G et H sont isomorphes.

Exemple. Le groupe additif $\mathbf{R}$ de tous les réels et le group multiplicatif $\mathbf{R}_+^\times$ des réels strictement positifs sont isomorphes, les isomorphismes dans les deux sens sont établis par les fonctions exponentielles $x \mapsto a^x$ et par les fonctions logarithmes $x \mapsto \log_a x$ (avec $a > 0$, $a \neq 1$).

Proposition. *Tout groupe est isomorphe à son groupe opposé. Plus précisément, si G est un groupe et que S est son ensemble sous-jacent, alors l'application $\delta\colon S \to S$ qui à chaque $x \in S$ associe son inverse dans G (qui est aussi son inverse dans G^{op}) est un isomorphisme entre G et G^{op}, aussi bien qu'entre G^{op} et G :*

$$\delta\colon G \xrightarrow{\sim} G^{\mathrm{op}} \quad \textit{et} \quad \delta\colon G \xleftarrow{\sim} G^{\mathrm{op}}.$$

Exercice. Prouver cette proposition.

Définition. Un isomorphisme entre un groupe et lui-même est dit un *automorphisme* de ce groupe.

L'automorphisme identité id_G d'un groupe G est dit l'automorphisme *trivial* de G ; les autres automorphismes de G sont donc dits *non triviaux*.

Proposition. *L'ensemble des automorphismes d'un groupe forme un groupe par rapport à l'opération de composition.*

Exercice. Prouver cette proposition.

Notation. Le groupe d'automorphismes d'un groupe G est noté « $\mathrm{Aut}(G)$ ».

Proposition. *Si a est un élément d'un groupe G, l'application $G \to G$ de conjugaison par a (définie comme $x \mapsto axa^{-1}$) est un automorphisme de G.*

Exercice. Prouver cette proposition.

Définition. Un automorphisme *intérieur* d'un groupe G est un automorphisme de la forme $x \mapsto axa^{-1}$ avec $a \in G$.

Proposition. *L'ensemble des automorphismes intérieures est un sous-groupe du groupe de tous les automorphismes.*

Exercice. Prouver cette proposition.

Notation. Le groupe d'automorphismes intérieurs d'un groupe G est noté « $\mathrm{Inn}(G)$ ».

Remarque. Le terme « automorphisme *extérieur* » est aussi utilisé, mais c'est un piège. Ce qu'on appelle un « automorphisme extérieure » n'est pas un automorphisme, mais c'est une « classe de congruence » d'automorphismes modulo le sous-groupe des automorphismes intérieurs.

I.12. Théorème de Cayley

Théorème (Théorème de Cayley)**.** *Soit G un groupe, et posons Γ l'ensemble des permutation de (l'ensemble sous-jacent de) G qui sont de la forme $x \mapsto ax$ avec $a \in G$:*

$$\Gamma = \left\{ \sigma \colon G \to G \,\middle|\, (\exists a \in G)(\forall x \in G)\big(\sigma(x) = ax\big) \right\}.$$

Alors, par rapport à l'opération de composition, Γ forme un groupe isomorphe à G. Plus précisément :

(1) *Γ est un sous-groupe du groupe S_G de toutes les permutations de l'ensemble sous-jacent de G,*

(2) *si on définit $f \colon G \to \Gamma$ par la formule :*

$$f(x)(y) = xy \qquad \text{pour tous } x, y \in G,$$

alors f est un isomorphisme entre G et Γ.

Démonstration. Observons d'abord qu'il est facile de vérifier que toute application $G \to G$ de la forme $x \mapsto ax$, avec $a \in G$, est bien une permutation de G.

Pour tous $x, y \in G$, posons

$$f(x)(y) = xy.$$

Alors, pour tout $x \in G$, $f(x) \colon G \to G$ est une permutation de G. En plus :

(1) pour tous $x, y, z \in G$,

$$f(xy)(z) = xyz = f(x)(yz) = f(x)\big(f(y)(z)\big) = \big((f(x) \circ f(y)\big)(z),$$

(2) pour tout $x \in G$,

$$f(1)(x) = 1x = x = \mathrm{id}_G(x).$$

D'où :

(1) $f(xy) = f(x) \circ f(y)$ pour tous $x, y \in G$,

(2) $f(1) = \mathrm{id}_G$.

Il en résulte que, pour tout $x \in G$,

$$f(x^{-1}) \circ f(x) = f(x^{-1}x) = f(1) = \mathrm{id}_G$$

et

$$f(x) \circ f(x^{-1}) = f(xx^{-1}) = f(1) = \mathrm{id}_G,$$

d'où, les permutations $f(x)$ et $f(x^{-1})$ sont inverses l'une de l'autre ($f(x^{-1}) = f(x)^{-1}$).

Par définition de Γ,

$$\Gamma = \{\, f(x) \mid x \in G \,\} = f(G).$$

Pour montrer que Γ est un sous-groupe du groupe S_G des permutations de l'ensemble G, il suffit de vérifier que :

(1) si $\sigma, \tau \in \Gamma$, alors $\tau \circ \sigma \in \Gamma$,

(2) $\mathrm{id}_G \in \Gamma$,

(3) si $\sigma \in \Gamma$, alors $\sigma^{-1} \in \Gamma$.

Ceci est maintenant facile à faire :

(1) si $\sigma, \tau \in \Gamma$, $\sigma = f(x)$ et $\tau = f(y)$, alors $\tau \circ \sigma = f(yx) \in \Gamma$,

(2) $\mathrm{id}_G = f(1) \in \Gamma$,

(3) si $\sigma = f(x) \in \Gamma$, alors $\sigma^{-1} = f(x^{-1}) \in \Gamma$.

Comme on a déjà vérifié que $f(xy) = f(x) \circ f(y)$ pour tous $x, y \in G$, pour montrer que f est un isomorphisme entre G et Γ, il ne reste qu'à vérifier que f est une bijection entre G et Γ. Par définition de Γ, f est surjective sur Γ. Donc il suffit de montrer que f est injective.

Soient $x, y \in G$ tels que $x \neq y$. Montrons que $f(x) \neq f(y)$. Pour cela il suffit d'observer que

$$f(x)(1) = x \neq y = f(y)(1)$$

(en fait, $f(x)(z) = xz \neq yz = f(y)(z)$ pour tout $z \in G$). □

Remarque. Le théorème de Cayley se généralise aux catégories, où sa version s'appelle le *lemme de Yoneda*.

I.13. Produits directs et sommes directes

Définition. Soient G et H deux groupes, dont les ensembles sous-jacent sont notés ici comme « G » et « H » aussi. Le *produit direct externe* de G et H est le produit cartésien de leurs ensembles sous-jacents

$$G \times H = \{\, (g, h) \mid g \in G,\ h \in h \,\}$$

muni de l'opération de composition définie par la formule :

$$(g_1,\, h_1)(g_2,\, h_2) \overset{\text{déf}}{=} (g_1 g_2,\, h_1 h_2).$$

Notation. Le produit direct externe de deux groupes G et H peut être noté « $G \times H$ ».

Proposition. *Soient G et H deux groupes. Alors*

$$G \times H \simeq H \times G.$$

Plus précisément, il y a un isomorphisme f défini ainsi :

$$\begin{aligned} f \colon G \times H &\xrightarrow{\sim} H \times G, \\ (g, h) &\mapsto (h, g). \end{aligned}$$

Proposition. *Soient G, H, K trois groupes. Alors*

$$(G \times H) \times K \simeq G \times (H \times K).$$

Plus précisément, il y a un isomorphisme f défini ainsi :

$$\begin{aligned} f \colon (G \times H) \times K &\xrightarrow{\sim} G \times (H \times K), \\ ((g, h),\, k) &\mapsto (g,\, (h, k)). \end{aligned}$$

Ainsi, si un groupe défini comme $(G \times H) \times K$ ou comme $G \times (H \times K)$ ne nous intéresse qu'*à un isomorphisme près*, on peut le noter comme « $G \times H \times K$ », sans parenthèses.

On peut aussi éviter les parenthèses peu utiles dans l'écriture d'un produit direct (externe) d'une famille finie de groupes en définissant directement le *produit direct* d'une famille.

Définition. Soit $G_1, \dots, G_n$ une famille finie de groupes. Le *produit direct externe* de cette famille est son produit cartésien

$$\{\, (g_1, \dots, g_n) \mid (\forall k)(g_k \in G_k) \,\}$$

muni de l'opération de composition évidente.

Pour une famille de 0 groupes, cette définition donne un groupe trivial (réduit à un seul élément neutre). Pour une famille de 1 groupe, cette définition donne un groupe isomorphe à G_1. Pour 2 groupes, cette définition donne le produit direct (externe) $G_1 \times G_2$ défini précédemment. Pour plus de 2 groupes, le groupe défini est clairement isomorphe à un n'importe quel produit direct externe parenthésé de $G_1, \dots, G_n$.

Notation. Le produit direct externe d'une famille finie de groupes $G_1, \dots, G_n$ peut être noté « $G_1 \times \cdots \times G_n$ » ou « $\bigtimes_{k=1}^{n} G_k$ ».

Proposition. *Pour tous groupes G et H,*

$$G \simeq G \times \mathbf{1}_H \leqslant G \times H \quad \textit{et} \quad H \simeq \mathbf{1}_G \times H \leqslant G \times H.$$

Proposition. *Soient G un groupe et H et K deux sous-groupes de G. Considérons l'application $f\colon H \times K \to G$ donnée par la formule $f(h,k) = hk$. Alors* :

(1) *l'application f est un homomorphisme si et seulement si $kh = hk$ pour tous $h \in H$ et $k \in K$,*

(2) *l'application f est injective si et seulement si $H \cap K = \mathbf{1}$.*

Exercice. Prouver cette proposition.

Les deux dernières propositions suggèrent une version *interne* du *produit direct* :

Définition. Soient G un groupe et H et K deux sous-groupes de G.

(1) Si tout élément de H commute avec tout élément de K, et que H et K n'ont que l'élément identité pour un élément commun, alors le sous-groupe $KH = HK$ de G est dit le *produit direct interne* de H et K dans G, et on peut dire que H et K *forment un produit direct* (interne) HK dans G.

(2) Dans le cas contraire, il n'y a pas de produit direct interne de H et K dans G, et on peut dire que H et K ne forment pas de produit direct (interne) dans G.

Notation. Le produit direct interne de deux sous-groupes H et K d'un n'importe quel groupe peut être noté « $H \times K$ ».

Ainsi, lorsque H et K sont sous-groupes d'un groupe G, et qu'on utilise « $\times$ » au sens interne, on a :

(1) $H \times K = HK = KH$ si H et K forment un produit direct interne dans G,

(2) l'expression « $H \times K$ » n'a pas de sens si H et K ne forment pas de produit direct interne dans G.

Remarque. La notation pour le produit direct interne étant la même que pour l'externe, il ne reste qu'à compter sur le contexte pour lever l'ambiguïté. On peut toujours noter le produit direct interne de H et K comme « HK » ou « KH », mais cette notation ne communique pas l'information que H et K forment un produit direct.

Proposition. *Soient H et K deux sous-groupes d'un certain groupe qui y forment un produit direct interne. Alors leur produit direct interne HK est isomorphe à leur produit direct externe $H \times K$, et un isomorphisme $H \times K \xrightarrow{\sim} HK$ est donné par la règle $(h, k) \mapsto hk$.*

Exercice. Prouver cette proposition.

Proposition. *Soient H et K deux sous-groupes d'un groupe G qui forment un produit direct interne dans G. Alors, en utilisant « $\times$ » au sens interne, on a :*

$$H \times K = HK = KH = K \times H.$$

Proposition. *Soient H, K, L trois sous-groupes d'un groupe G. En utilisant « $\times$ » au sens interne, on a que le produit « $(H \times K) \times L$ » est défini si et seulement si le produit « $H \times (K \times L)$ » est défini, et dans ce cas on a :*

$$(H \times K) \times L = (HK)L = H(KL) = H \times (K \times L).$$

Exercice. Prouver cette proposition. (La partie « si et seulement si » n'est pas complètement évidente.)

Définition. Dans le contexte des groupes abéliens, lorsqu'on utilise la notation additive, on parle des *sommes directes* (externes et internes) au lieu des produits directs (externes et internes).

Notation. Les sommes directes sont notées avec « $\oplus$ » à la place de « $\times$ ».

Remarque. Si G et H sont deux groupes, $g \in G$, et $h \in H$, alors l'élément correspondant de $G \times H$ ou de $G \oplus H$ peut être noté « $g \times h$ » ou « $g \oplus h$ », respectivement, tant qu'on arrive à éviter les confusions possibles. Un tel usage est peu courant, mais il est cohérent avec l'usage du symbole « $\otimes$ » dans le contexte des *produits tensoriels*. Pour « $\oplus$ », on peut trouver un tel usage dans *Algebra* de Serge Lang.[11]

Exercice. Soient $m, n \in \mathbf{Z}$. Montrer que les énoncés suivants sont équivalents :

(1) $\mathbf{Z}/(m\mathbf{Z}) \oplus \mathbf{Z}/(n\mathbf{Z}) \simeq \mathbf{Z}/(mn\mathbf{Z})$,

(2) m et n sont *premiers entre eux*.[12]

Lorsque ces conditions sont satisfaites, expliciter un isomorphisme

$$\mathbf{Z}/(mn\mathbf{Z}) \xrightarrow{\sim} \mathbf{Z}/(m\mathbf{Z}) \oplus \mathbf{Z}/(n\mathbf{Z}).$$

Remarque. On peut montrer que lorsque m et n sont deux entiers premiers entre eux, on a un isomorphisme *des anneaux* $\mathbf{Z}/(mn\mathbf{Z}) \simeq \mathbf{Z}/(m\mathbf{Z}) \oplus \mathbf{Z}/(n\mathbf{Z})$, où à droite on a la somme directe externe *des anneaux*. Ce fait peut être vu comme une forme du *théorème des restes chinois*.

Exercice. Soient $m, n \in \mathbf{Z}$ premiers entre eux.

(1) Dans le groupe $\mathbf{Z}/(mn\mathbf{Z})$, déterminer un élément a d'ordre m et un élément b d'ordre n.

(2) Soient $a, b \in \mathbf{Z}/(mn\mathbf{Z})$ d'ordres m et n, comme dans la question précédente. Montrer que $\mathbf{Z}/(mn\mathbf{Z}) = \langle a \rangle \oplus \langle b \rangle$ au sens interne si et seulement si m et n sont premiers entre eux.

I.14. Produits cartésiens et produits directs infinis

Rappelons-nous que si $(X_i)_{i \in I}$ est une famille d'ensembles (indexée par les éléments de I), alors le *produit cartésien* $\prod_{i \in I} X_i$ est l'ensemble des fonctions $x \colon I \to \bigcup_{i \in I} X_i$ telles que $x(i) \in X_i$ pour tout $i \in I$.

[11] Serge Lang. *Algebra*. Anglais. 3e éd. Graduate Texts in Mathematics 211. Publié à l'origine par Addison-Wesley, 1993. New York, NY : Springer, 2002. xv+914. DOI : 10.1007/978-1-4613-0041-0, p. 152.

[12] Rappel : deux entiers sont dits *premiers entre eux* si et seulement si tout leur diviseur commun divise 1.

Si l'on tente généraliser la définition du produit direct de la section précédente au cas d'une famille infinie $(G_i)_{i\in I}$, deux choix de l'ensemble sous-jacent d'un tel produit se présentent :

(1) le produit cartésien $\prod_{i\in I} G_i$ des ensembles sous-jacents,

(2) l'ensemble des $g \in \prod_{i\in I} G_i$ tels que l'ensemble $\{\, i \in I \mid g(i) \neq 1_{G_i} \,\}$ soit fini.

Si on fait le premier choix, le groupe obtenu ainsi est dit le *produit cartésien* de la famille $(G_i)_{i\in I}$.

Le produit cartésien est « externe », et il n'a pas de version « interne ».

Si on fait le second choix, le groupe obtenu ainsi est dit le *produit direct externe* de la famille $(G_i)_{i\in I}$.

Une décomposition d'un groupe en *produit direct interne* d'une famille infinie de ses sous-groupes se définit d'une manière alogique au cas d'une famille finie.

Notation. Le produit cartésien d'une famille de groupes $(G_i)_{i\in I}$ est noté « $\prod_{i\in I} G_i$ ». Son produit direct est noté « $\bigtimes_{i\in I} G_i$ ». Lorsqu'il s'agit de groupes abéliens et qu'on utilise la notation additive, la somme directe de $(G_i)_{i\in I}$ est notée « $\bigoplus_{i\in I} G_i$ ». Lorsque $G_i = G$ pour tout $i \in I$, on peut écrire « G^I » au lieu de « $\prod_{i\in I} G$ », « $G^{\times I}$ » au lieu de « $\bigtimes_{i\in I} G$ » et « $G^{\oplus I}$ » au lieu de « $\bigoplus_{i\in I} G$ ».

II. Groupes symétriques

II.1. Permutations

Définition. Une *permutation* d'un ensemble X est une bijection de X sur X.

Clairement, l'ensemble des permutations d'un ensemble X forme un groupe par rapport à l'opération de composition ($\circ$).

Pour le reste de ce chapitre, on va écrire la permutation composée $\tau \circ \sigma$ comme « $\tau\sigma$ » tout court. On va garder la notation « $\beta \circ \alpha$ » pour des cas où α et β ne sont pas supposées être permutations d'un même ensemble.

Définition. Le groupe de toutes les permutations d'un ensemble X est dit le *groupe symétrique* de X. Tout sous-groupe du groupe symétrique de X est dit un *groupe de permutations* de X.

Notation. On va noter « S_X » le groupe des permutations d'un ensemble X. On va noter « S_n » le groupe des permutations de l'ensemble $\{1, \ldots, n\}$.

Par exemple, $S_0 = S_\varnothing$ est le groupe trivial composé d'un seul élément : la permutation vide de l'ensemble vide. Le groupe S_1 est également trivial, réduit à la permutation identité $\{1\} \to \{1\}$ $(1 \mapsto 1)$.

Le groupe S_2 est composé des deux permutations de l'ensemble $\{1, 2\}$, à savoir : $\{1 \mapsto 1,\ 2 \mapsto 2\}$ et $\{1 \mapsto 2,\ 2 \mapsto 1\}$. Ce groupe est isomorphe à tout autre groupe d'ordre 2 (comme $\mathbf{Z}/(2\mathbf{Z})$).

Proposition. *Si le cardinal (le nombre d'éléments) d'un ensemble X est $n \in \mathbf{N}$, alors l'ordre du groupe S_X est $n!$. En particulier, $|S_n| = n!$.*

Exercice. Prouver cette proposition.

Proposition. *Si X et Y sont deux ensembles d'un même cardinal (avec le même nombre d'éléments), alors les groupes S_X et S_Y sont isomorphes ($S_X \simeq S_Y$). Plus précisément, si $\varphi\colon X \to Y$ est une bijection entre X et Y, et qu'on définit $f\colon S_X \to S_Y$ par la formule :*

$$f(\sigma) = \varphi \circ \sigma \circ \varphi^{-1},$$

alors f est un isomorphisme entre S_X et S_Y ($f\colon S_X \xrightarrow{\sim} S_Y$).

Si on note $\varphi \circ \sigma \circ \varphi^{-1}$ comme « ${}^{\varphi}\sigma$ », alors la formule dans le théorème devient :

$$f(\sigma) = {}^{\varphi}\sigma.$$

Exercice. Prouver cette proposition.

Pour écrire les permutations d'un ensemble fini, une notation standard utilise les tableaux à deux lignes, où dans la première ligne on écrit tous les éléments de l'ensemble, et en dessous de chaque élément de la première ligne on écrit son image par la permutation. Par exemple, si $X = \{a, b, c\}$ est un ensemble à 3 éléments, et que

$$\sigma = \{a \mapsto b,\ b \mapsto a,\ c \mapsto c\} \colon X \to X,$$

alors on peut donner ce σ par le tableau :

$$\begin{matrix} a & b & c \\ b & a & c \end{matrix}$$

On peut aussi envisager une écriture abrégée, où on n'écrit pas les éléments fixés par σ :

$$\begin{matrix} a & b \\ b & a \end{matrix}$$

Cependant, pour pouvoir bien interpréter la notation abrégée, il faut connaître l'ensemble X, car sinon on ne voit pas que σ est définie en c.

En utilisant la notation « en deux lignes », si

$$\sigma = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \qquad \text{et} \qquad \tau = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix},$$

on peut composer σ avec τ ainsi :

$$\sigma\tau = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \begin{pmatrix} \boxed{a} & c & \boxed{b} \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ \boxed{a} & c & \boxed{b} \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}.$$

Avec la notation abrégée, le calcul peut s'écrire ainsi :

$$\sigma\tau = \begin{pmatrix} a & \boxed{b} \\ b & a \end{pmatrix} \begin{pmatrix} b & c \\ c & \boxed{b} \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}.$$

II.2. Points fixes, support, parties invariantes

Définition. Si σ est un permutation de X, alors $x \in X$ est dit un *point fixe* de σ si et seulement si $\sigma(x) = x$.

Notation. L'ensemble des points fixes d'une permutation σ d'un ensemble X sera noté « $\operatorname{Fix}\sigma$ » ou « X^σ ».

Définition. Le *support* d'une permutation de X est le complément dans X de l'ensemble de ses points fixes.

Remarque. Il existe un autre usage courant du terme « support » dans le contexte des fonctions à valeurs dans un anneau : on définit le *support* d'une fonction comme l'ensemble de ses arguments sur lesquels la fonction ne s'annule pas.

Notation. Le support d'une permutation σ sera noté « $\operatorname{Supp}\sigma$ ».

Ainsi, pour toute $\sigma \in S_X$,

$$X = \operatorname{Fix}\sigma \sqcup \operatorname{Supp}\sigma.$$

Proposition. *Les permutations à supports disjoints commutent : si $\sigma, \tau \in S_X$ et que $\operatorname{Supp}\sigma \cap \operatorname{Supp}\tau = \varnothing$, alors $\tau\sigma = \sigma\tau$.*

Exercice. Prouver cette proposition.

Définition. Soit $\sigma \in S_X$. Une partie Y de X est dite *invariante* par σ si et seulement si l'image de Y par σ est Y.

Observons que $\operatorname{Fix}\sigma$ et $\operatorname{Supp}\sigma$ sont invariants par σ.

Proposition. *Soient $\rho, \sigma, \tau \in S_X$ tels que $\tau\rho = \rho\sigma$. Alors*

(1) *la restriction de ρ sur $\operatorname{Fix}\sigma$ est une bijection entre $\operatorname{Fix}\sigma$ et $\operatorname{Fix}\tau$,*

(2) *la restriction de ρ sur $\operatorname{Supp}\sigma$ est une bijection entre $\operatorname{Supp}\sigma$ et $\operatorname{Supp}\tau$.*

Exercice. Prouver cette proposition.

II.3. Restrictions et prolongements

Définition. Soient X un ensemble, Y une partie de X, $\sigma \in S_X$ et $\tau \in S_Y$. On va dire que la permutation τ de Y est la *restriction* de σ sur Y si et seulement si pour tout $y \in Y$, on a que $\tau(y) = \sigma(y)$. On va dire que σ est un *prolongement* de τ sur X si et seulement si τ est la restriction de σ sur Y.

Observons que la restriction de σ sur Y n'est définie en tant qu'une permutation de Y que si Y est invariant par σ.

Remarque. Peut-être la restriction d'une permutation sur son support mérite un nom spécial.

Définition. Soient X un ensemble, Y une partie de X, $\sigma \in S_X$ et $\tau \in S_Y$. On va dire que σ est le *prolongement trivial* de τ sur X si et seulement si les deux conditions suivantes sont satisfaites :

(1) $\sigma(y) = \tau(y)$ pour tout $y \in Y$,

(2) $\sigma(x) = x$ pour tout $x \in X \setminus Y$.

Notation. Soient X un ensemble et Y une partie de X. Si $\sigma \in S_X$ et que Y est invariante par σ, alors la restriction de σ sur Y sera notée « $\sigma\big\rfloor_Y$ ».[1] Si $\tau \in S_Y$, alors le prolongement trivial de τ sur X sera noté « $\tau\big\rceil^X$ ».[2]

Remarque. Lorsque on veut considérer une restriction d'une permutation $\sigma \in S_X$ sur une partie $Y \subset X$ qui n'est pas forcement invariante par σ, on peut continuer à utiliser la notation « $\sigma|_Y$ », comme pour une n'importe quelle fonction.

Proposition. *Soient X un ensemble et $Y \subset X$. Posons*

$$H = \{\, \sigma \in S_X \mid (\forall y \in Y)(\sigma(y) = y) \,\}.$$

Alors H est un sous-groupe de S_X.

Exercice. Prouver cette proposition.

[1] Cette notation est complètement originale. La notation standard serait « $\sigma|_Y$ », mais elle s'applique à une n'importe quelle application avec une n'importe quelle partie de son domaine de définition. La notation « $\sigma|_Y$ » désigne dans ce cas une application $Y \to X$, elle ne souligne pas les faits que σ est une permutation, que Y est invariante par σ, et que le résultat sera traité comme une permutation de Y.

[2] Cette notation est complètement originale aussi.

Proposition. *Soient X un ensemble, $Y \subset X$, et*

$$H = \{\, \sigma \in S_X \mid (\forall x \in X \setminus Y)(\sigma(x) = x) \,\}.$$

Alors le sous-groupe H de S_X est isomorphe à S_Y ($H \simeq S_Y$). Plus précisément, si on définit $f\colon H \to S_Y$ par la formule :

$$f(\sigma) = \sigma\rfloor_Y\,,$$

alors f est un isomorphisme entre H et S_Y ($f\colon H \xrightarrow{\sim} S_Y$).

Exercice. Prouver cette proposition.

II.4. Orbites

Définition. Soient X un ensemble et H un sous-groupe de S_X. Deux éléments $x, y \in X$ sont dits *conjugués* par H si et seulement si il existe $\sigma \in H$ telle que $\sigma(x) = y$ et $\sigma^{-1}(y) = x$.

Proposition. *Si X est un ensemble et $H \leqslant S_X$, alors la relation d'être conjugués par H est une relation d'équivalence sur X.*

Exercice. Prouver cette proposition.

Définition. Soit X un ensemble. Les classes d'équivalence d'éléments de X par la relation d'être conjugués par un sous-groupe H de S_X sont dites les *orbites* sous H, ou les *H-orbites*. Lorsque $H = \langle\sigma\rangle$ est un sous-groupe cyclique de S_X engendré par une permutation σ, les orbites sous H peuvent être dites les *orbites* sous σ, ou les *σ-orbites*.

Observons que la H-orbite d'un élément $x \in X$ est

$$\{\, \sigma(x) \mid \sigma \in H \,\}.$$

Notation. Soit X un ensemble. Si $H \leqslant S_X$ et $x \in X$, alors l'orbite de x sous H peut être notée « Hx ».

Ainsi, l'orbite de $x \in X$ sous $\sigma \in S_X$ peut être notée « $\langle\sigma\rangle x$ ».

Notation. Soit X un ensemble. Si $H \leqslant S_X$, alors l'ensemble des orbites dans X sous H peut être noté « $H\backslash X$ » (le « quotient à gauche » de X par H) ou « X/H » ou « X_H ». Si $\sigma \in S_X$, alors l'ensemble des orbites dans X sous $\langle\sigma\rangle$ peut être noté « X_σ » au lieu de « $X_{\langle\sigma\rangle}$ ».

II.5. Transporteurs et stabilisateurs

Définition. Soient X un ensemble, H un sous-groupe de S_X, et $x \in X$. Le *transporteur* de $x \in X$ vers $y \in X$ dans H est l'ensemble des permutations $\sigma \in H$ telles que $\sigma(x) = y$. Le *fixateur* ou le *stabilisateur* de $x \in X$ dans H est l'ensemble des permutations $\sigma \in H$ telles que $\sigma(x) = x$.

Remarque. L'usage de la notion de *transporteur* n'est pas courant. Ce terme est défini dans *Algèbre* de Bourbaki,[3] mail il n'y est mentionné qu'une dizaine de fois. Cependant, cette notion peut être utile.[4]

Proposition. *Si X est un ensemble, $H \leqslant S_X$, et $x \in X$, alors le stabilisateur de x dans H est un sous-groupe de H.*

Exercice. Prouver cette proposition.

Notation. Le stabilisateur de $x \in X$ dans $H \leqslant S_X$ peut être noté « H_x » ou « $\mathrm{Stab}_H(x)$ ».

Remarque. Il est difficile de trouver une notation courante pour les transporteurs, peut-être il n'y en a pas. On peut toutefois envisager de noter le transporteur de x vers y dans H comme « ${}_yH_x$ » ou comme « $\mathrm{Tran}_H(x, y)$ ».

II.6. Transpositions et cycles

Définition. Soient a et b deux éléments distincts d'un ensemble X. La *transposition* de a et b dans X est la permutation $\sigma \in S_X$ de support $\{a, b\}$ telle que $\sigma(a) = b$ et $\sigma(b) = a$.

Définition. Une permutation σ d'un ensemble X est dit un *cycle* si et seulement si le support de σ est une orbite sous σ. Le nombre d'élément dans le support d'un cycle est dit sa *longueur*.

Ainsi, une transposition est un cycle de longueur deux.

Proposition. *La longueur d'un cycle est égale à son ordre.*

Exercice. Prouver cette proposition.

Dans ce chapitre, on ne va traite en détail que les groupes symétriques d'ensembles finis, et ainsi les cycles seront d'habitude de longueur finie.

[3] Bourbaki, *Algèbre*, Chapitre I, § 5, N° 2, p. I.51.
[4] En termes de la *théorie des catégories*, les transporteurs sont les *hom-ensembles* du *groupoïde d'action*.

Notation. Si $\sigma \in S_X$ est un cycle de longueur n et de support $\{x_1, \dots, x_n\}$ tel que $\sigma(x_i) = x_{i+1}$ pour $i \in \{1, \dots, n-1\}$ et que $\sigma(x_n) = x_1$, on peut désigner σ comme « $(x_1, \dots, x_n)$ ».

Cette notation n'explicite par l'ensemble X, et ainsi une même expression de cette forme peut designer différents cycles sur différents ensembles. En pratique cette ambiguïté est bénigne, car tous ces cycles auront le même support et la même restriction sur leur support.

Observons que tout cycle de longueur n s'écrit comme un produit de $n-1$ transpositions de manière suivante :[5]

$$(x_1, \dots, x_n) = (x_1, x_2)(x_2, x_3) \cdots (x_{n-1}, x_n).$$

Théorème. *Toute permutation σ à support fini s'écrit comme un produit de cycles à supports disjoints deux à deux. Cette décomposition est unique à l'ordre près des facteurs (qui commutent entre eux), et les supports des cycles facteurs forment une partition du support de σ en σ-orbites.*

Ce théorème se déduit facilement du lemme suivant :

Lemme. *Soient X un ensemble fini et $\sigma \in S_X$. Soient $\tau_1, \dots, \tau_k \in S_X$. Alors les énoncés suivants sont équivalents* :

(1) *$\tau_1, \dots, \tau_k$ sont des cycles à supports disjoints deux à deux tels que $\tau_k \cdots \tau_1 = \sigma$.*

(2) *$\tau_1, \dots, \tau_k$ sont des permutations de X à supports disjoints deux à deux telles que* :

  (a) $\operatorname{Supp} \tau_i$ *est une σ-orbite pour tout i,*

  (b) $\bigsqcup_{i=1}^{k} \operatorname{Supp} \tau_i = \operatorname{Supp} \sigma$,

  (c) $\tau_i\rfloor_{\operatorname{Supp} \tau_i} = \sigma\rfloor_{\operatorname{Supp} \tau_i}$ *pour tout i.*

Exercice. Prouver ce lemme. En déduire le théorème.

Proposition. *Soit σ une permutation à support fini. Soient $\tau_1, \dots, \tau_k$ des cycles à supports disjoints deux à deux tels que $\tau_k \cdots \tau_1 = \sigma$. Alors l'ordre de σ est le PPCM positif des ordres de $\tau_1, \dots, \tau_k$.*

Démonstration. Pour tout $n \in \mathbf{Z}$, $\sigma^n = \tau_k^n \cdots \tau_1^n$, (car $\tau_1, \dots, \tau_k$ commutent deux à deux).

[5] Attention à l'ordre d'application : c'est comme dans « $(g \circ f)(x) = g(f(x))$ ».

Pour tout $n \in \mathbf{Z}$, $\operatorname{Supp} \tau_i^n \subset \operatorname{Supp} \tau_i^n$. Ainsi, les supports de $\tau_1^n, \ldots, \tau_k^n$ sont toujours disjoints. D'où, $\sigma^n = \mathrm{id}_X$ si et seulement si $\tau_1^n = \cdots = \tau_k^n = \mathrm{id}_X$. D'où, pour tout $n \in \mathbf{Z}$, l'ordre de σ divise n si et seulement les ordres de τ_1, $\ldots$, τ_k tous divisent n. D'où, l'ordre de σ est un PPCM des ordres de τ_1, $\ldots$, τ_k. □

Proposition. *Deux cycles sur un ensemble fini X sont conjugués dans S_X si et seulement si ils ont la même longueur.*

Démonstration. Si deux permutations de X sont conjuguées dans S_X, alors, d'après une proposition de la section II.2, il existe une bijection entre leurs supports. En particuliers, si deux cycles sont conjugués, ils ont la même longueur.

Considérons maintenant deux cycles σ et τ sur X de longueur k tous les deux. Avec la notation introduite ci-dessus, posons

$$\sigma = (x_1, \ldots, x_k) \quad \text{et} \quad \tau = (y_1, \ldots, y_k).$$

En particulier, on a :

$$\operatorname{Supp} \sigma = \{x_1, \ldots, x_k\} \quad \text{et} \quad \operatorname{Supp} \tau = \{y_1, \ldots, y_k\},$$

et donc $\operatorname{Supp} \sigma$ et $\operatorname{Supp} \tau$ ont le même nombre d'éléments.

Rappelons-nous que

$$\operatorname{Fix} \sigma \sqcup \operatorname{Supp} \sigma = X = \operatorname{Fix} \tau \sqcup \operatorname{Supp} \tau.$$

Comme X est fini, $\operatorname{Fix} \sigma$ et $\operatorname{Fix} \tau$ ont le même nombre d'éléments.

Soit $\rho_0 \colon \operatorname{Fix} \sigma \to \operatorname{Fix} \tau$ une bijection arbitraire, et définissons $\rho \colon X \to X$ par la formule :

$$\rho(x) = \begin{cases} \rho_0(x) & \text{si } x \in \operatorname{Fix} \sigma, \\ y_i & \text{si } x = x_i \in \operatorname{Supp} \sigma. \end{cases}$$

Alors on peut vérifier facilement que ρ est une permutation de X et que $\tau\rho = \rho\sigma$. □

II.7. Quelques parties génératrices d'un groupe symétrique fini

Proposition. *Soit X un ensemble fini. Alors S_X est engendré par l'ensemble des transpositions dans X.*

Exercice. Prouver cette proposition.

Proposition. *Soit X un ensemble fini qui est l'ensemble des* sommets *d'un* graphe connexe Γ. *Alors S_X est engendré par l'ensemble des transpositions des sommets* adjacents *de* Γ.

Exercice. Prouver cette proposition.

Proposition. *Soient X un ensemble fini et σ un cycle dans X tel que* $\operatorname{Supp}\sigma = X$. *Soient $x \in X$ et τ la transposition de x et $\sigma(x)$ dans X : $\tau = (x, \sigma(x))$. Alors S_X est engendré par σ et τ.*

Exercice. Prouver cette proposition.

II.8. Classes de conjugaison d'un groupe symétrique fini

Proposition. *Soit X un ensemble fini. Alors deux permutations de X sont conjuguées dans S_X si et seulement si elles ont le même nombre de cycles de chaque longueur dans leurs décompositions en produis de cycles à supports disjoints.*

Exercice. Prouver cette proposition.

II.9. Parité et signature

Dans cette section, on va provisoirement[6] adopter la définition suivante :

Définition. Un *homomorphisme* d'un groupe G vers un groupe H est une application $f\colon G \to H$ telle que $f(xy) = f(x)f(y)$ pour tous $x, y \in G$.

Proposition. *Soient X un ensemble, A un groupe abélien pour lequel on va utiliser la notation additive, et $f\colon S_X \to A$ un homomorphisme* :

$$f(\tau\sigma) = f(\tau) + f(\sigma) \qquad \text{pour tous } \sigma, \tau \in S_X.$$

Soit $a \in A$ l'image par f d'une (n'importe quelle) transposition dans X. Alors :

(1) $2a = 0$,

[6] La notion de *homomorphisme* sera traitée dans le chapitre suivant.

(2) *si $\sigma \in S_X$ est une transposition, alors $f(\sigma) = a$,*

(3) *si $\sigma \in S_X$ s'écrit comme un produit de n transpositions, alors*

$$f(\sigma) = na = \begin{cases} 0 & \text{si } n \text{ est pair,} \\ a & \text{si } n \text{ est impair.} \end{cases}$$

Observons que dans cette proposition on ne suppose pas que $a \neq 0$, et qu'on ne suppose pas que l'ensemble X soit fini.

Exercice. Prouver cette proposition.

Dans la suite on va parfois traiter l'ensemble $\{\pm 1\}$ comme un groupe multiplicatif.

Théorème. *Si X est un ensemble fini, alors il existe un unique homomorphisme*

$$f\colon S_X \to \{\pm 1\}$$

tel que $f(\tau) = -1$ pour toute transposition $\tau \in S_X$.

Vu que S_X est engendré par ses transpositions (pour X fini), l'unicité dans ce théorème est évidente.

Pour démontrer l'existence, on peut passer par une *action non triviale* du groupe S_X sur un ensemble à 2 éléments. C'est-à-dire, on choisit un certain ensemble B à 2 éléments, et à chaque permutation σ de X on associe une certain permutation $\varphi(\sigma)$ de B de sorte que $\varphi(\tau\sigma) = \varphi(\tau)\varphi(\sigma)$ pour tous $\sigma, \tau \in S_X$. Puis, on pose $f(\sigma) = 1$ si $\varphi(\sigma) = \mathrm{id}_B$, et $f(\sigma) = -1$ sinon.

Pour que l'application f définie ainsi satisfasse les conditions de la conclusion du théorème, il suffit qu'il existe $\sigma \in S_X$ telle que $\varphi(\sigma) \neq \mathrm{id}_B$.

On peut effectuer diverses constructions plus ou moins naturelles de tels B et φ. Entre autres, on peut prendre pour B un ensemble de certaines classes d'équivalence d'*orientations* d'un *graphe complet*.

Un *graphe simple* est composé d'un ensemble de *sommets* et d'un ensemble d'*arêtes* non orientées, lesquelles on va « identifier » avec les couples (non ordonnés) des sommets qu'elles relient. Un couple de sommets distincts est soit relié par une seule arête, soit n'est relié par aucune arête. Un sommet ne peut pas être relié à lui même.

On va « identifier » un simple graphe Γ avec le couple (V, E) de son ensemble de sommets V et de son ensemble d'arêtes E.

À chaque arête non orientée $\{u, v\}$, on va associé deux *orientations* possibles, qui sont *opposées* l'une de l'autre : une *de u vers v*, et l'autre *de v vers u*, et on va les « identifier » aux couples (u, v) et (v, u). On peut aussi appeler les orientations d'une arête non orientée les *arêtes orientées*.

(On peut adopter la notation « $u - v$ » pour l'arête non orientée $\{u, v\}$, et les notations « $u \to v$ » et « $v \to u$ » pour ses orientations de u vers v et de v vers u.)

Un choix d'une de ses deux orientations pour chaque arête non orientée d'un graphe simple Γ sera dit une *orientation complète*, ou tout simplement une *orientation*, de Γ. Le nombre d'orientations complètes d'un graphe avec n arêtes non orientées est 2^n.

Une orientations complète d'un graphe peut être vue comme une fonction qui à chaque arête non orientée associe son orientation choisie, ou comme un simple ensemble des orientations choisies, car il n'y a pas d'ambiguïté sur quelle orientation soit associée à quelle arête non orientée.

On va « identifier » toute orientation complète de $\Gamma = (V, E)$ avec la partie de $V \times V$ composée des orientations choisies. Ainsi, dans le reste de cette section, une orientation complète de Γ est une partie $\Omega \subset V \times V$ telle que :

(1) pour toute arête orientée $(u, v) \in \Omega$, on a que $u \neq v$ et $(v, u) \notin \Omega$,

(2) pour toute arête non orienté $\{u, v\} \in E$, on a que soit $(u, v) \in \Omega$, soit $(v, u) \in \Omega$.

Dans cette section, l'ensemble des orientations complètes d'un graphe Γ sera noté « $\mathcal{O}(\Gamma)$ ».

Étant données deux orientations complètes d'un graphe Γ, on peut considérer le nombre des arête de Γ sur lesquels elles différent.

Proposition. *Soient Γ un graphe et $\Omega_0, \ldots, \Omega_n$ une suite de ses orientations complètes telle que chaques deux orientations successives différent sur exactement une arête. Alors Ω_0 et Ω_n différent :*

(1) *sur un nombre pair d'arêtes si n est pair,*

(2) *sur un nombre impair d'arêtes si n est impair.*

Exercice. Prouver cette proposition.

Corollaire. *La relation sur l'ensemble d'orientations complètes d'un graphe de différer sur un nombre pair d'arêtes est une relation d'équivalence.*

Exercice. Prouver ce corollaire.

Un *graphe complet* sur un ensemble V est un graphe simple qui a V pour l'ensemble des sommets et dans lequel chaque couple de sommets distincts est relié par une arête. Un graphe complet à n sommets possède $n(n-1)/2$ arêtes non orientées.

Observons qu'une orientation complète sur un graphe complet Δ peut être vue comme une relation *totale asymétrique* sur l'ensemble des sommets de Δ.

Proposition. *Soit $\Delta = (V, E)$ un graphe complet et posons $\mathcal{O}(\Delta)$ l'ensemble des orientations complètes de Δ. Pour chaque permutation $\sigma \in S_V$ des sommets et pour chaque orientation complète $\Omega \in \mathcal{O}(\Delta)$ du graphe, posons*

$$f(\sigma)(\Omega) \stackrel{\text{déf}}{=} \{\, (\sigma(u), \sigma(v)) \mid (u, v) \in \Omega \,\}.$$

Alors :

(1) *pour toute $\sigma \in S_V$ et pout toute $\Omega \in \mathcal{O}(\Delta)$, l'ensemble $f(\sigma)(\Omega)$ est une orientation complète de Δ,*

(2) *pour toute $\sigma \in S_V$, l'application $f(\sigma)\colon \mathcal{O}(\Delta) \to \mathcal{O}(\Delta)$ ainsi définie est une permutation de $\mathcal{O}(\Delta)$,*

(3) *l'application $f\colon S_V \to S_{\mathcal{O}(\Delta)}$ ainsi définie est un homomorphisme de S_V vers $S_{\mathcal{O}(\Delta)}$.*

Exercice. Prouver cette proposition.

Démonstration du théorème. L'unicité d'une telle fonction f est évidente, car S_X est engendré par ses transpositions. Il ne reste qu'à montrer son existence.

Soit $\Delta = (X, E)$ le graphe complet sur X.

En appliquant la proposition précédente, définissons l'homomorphisme $\varphi\colon S_X \to S_{\mathcal{O}(\Delta)}$ par la formule :

$$\varphi(\sigma)(\Omega) = \{\, (\sigma(x), \sigma(y)) \mid (x, y) \in \Omega \,\} \qquad \text{où } \sigma \in S_X,\ \Omega \in \mathcal{O}(\Delta), \text{ et } x, y \in X.$$

Considérons la relation d'équivalence $(\sim)$ sur l'ensemble $\mathcal{O}(\Delta)$ d'orientations complètes de Δ définie ainsi : $\Psi \sim \Omega$ si et seulement le cardinal de $\Psi \setminus \Omega$, qui est le même que le cardinal de $\Omega \setminus \Psi$, est pair. Autrement dit, deux orientations complètes sont équivalentes par $(\sim)$ si et seulement si elles différent sur un nombre pair d'arêtes.

Dès que l'ensemble X contient au moins 2 éléments, le graphe Δ a au moins une arête, et alors il y a exactement 2 classes d'équivalence des orientations complètes de Δ par rapport à $(\sim)$.

Posons $B = \mathcal{O}(\Delta)/\sim$ l'ensemble des classes d'équivalence d'éléments de $\mathcal{O}(\Delta)$ par $(\sim)$.

Il est facile de vérifier que quelle que soit $\sigma \in S_X$, la relation $(\sim)$ est respecté par $\varphi(\sigma)$: si $\Psi \sim \Omega$ alors $\varphi(\sigma)(\Psi) \sim \varphi(\sigma)(\Omega)$.

Posons $\tilde{\varphi}(\sigma)$ l'application $B \to B$ induite par $\varphi(\sigma)$. Alors $\tilde{\varphi}(\sigma)$ est une permutation de B, et l'application $\tilde{\varphi}\colon S_X \to S_B$ ainsi définie est un homomorphisme de S_X dans S_B.

Posons $\beta \in S_B$ la permutation non triviale de B. Alors $S_B = \{\mathrm{id}_B, \beta\}$.

Définissons $f\colon S_X \to \{\pm 1\}$ par la formule :

$$f(\sigma) = \begin{cases} +1 & \text{si } \tilde{\varphi}(\sigma) = \mathrm{id}_B, \\ -1 & \text{si } \tilde{\varphi}(\sigma) = \beta. \end{cases}$$

Alors f est un homomorphisme de S_X vers le groupe multiplicatif $\{\pm 1\}$.

Pour assurer que l'homomorphisme f ainsi défini satisfait les conditions requises, il suffit de vérifier que si $\sigma \in S_X$ est une transposition, alors $\tilde{\varphi}(\sigma) \neq \mathrm{id}_B$.

Soient $a, b \in X$ deux éléments distincts, et soit $\tau \in S_X$ la transposition de a avec b. Soit Ω une orientation complète de Δ telle que :

(1) $(a, b) \in \Omega$,

(2) $(a, x) \in \Omega$ et $(b, x) \in \Omega$ pour tout $x \in X \setminus \{a, b\}$.

(Clairement, une telle orientation complète existe.) Posons

$$\Psi = \varphi(\tau)(\Omega) = \{\, (\tau(x), \tau(y)) \mid (x, y) \in \Omega \,\}.$$

Alors :

(1) $(b, a) \in \Psi$,

(2) pour tout $x \in X \setminus \{a, b\}$, on a que $(b, x) \in \Psi$ et $(a, x) \in \Psi$,

(3) pour tous $x, y \in X \setminus \{a, b\}$, on a que $(x, y) \in \Psi$ si et seulement si $(x, y) \in \Omega$.

Ainsi, les orientations complètes Ψ et Ω ne différent que sur l'unique arête non orientée (a, b). Donc, $\varphi(\tau)(\Omega) = \Psi \not\sim \Omega$, $\varphi(\tau)([\Omega]_\sim) = [\Psi]_\sim \neq [\Omega]_\sim$, où $[\Omega]_\sim$ et $[\Psi]_\sim$ sont les classes d'équivalence de Ω et de Ψ. Donc, $\tilde{\varphi}(\tau) \neq \mathrm{id}_B$ et $f(\tau) = -1$. □

Voici une présentation informelle d'une construction d'une action de S_X sur un ensemble à deux éléments qui est proche de celle utilisée dans la démonstration du théorème :

(1) Prendre un graphe complet Δ sur X.

(2) Prendre le produite cartesien Π des arêtes de Δ en les considérant être des intérevalles. Alors Π est un (hyper-) cube.

(3) L'action de S_X sur X induit les actions de S_X sur Δ et sur Π, et ainsi sur l'ensemble des sommets de Π et sur le 1-*squelette* de Π.

(4) Le 1-squelette d'un (hyper-) cube est un graphe *biparti* connexe, ce qui détermine un partage de ses sommets en deux classes de sorte que ce partage soit invariant par toute symétrie du (hyper-) cube.

(5) Ainsi, S_X agit sur l'ensemble composé des deux classes des sommets de Π, où le partage est fait celon la structure d'un graphe biparti sur le 1-squelette de Π.

Corollaire. *Si X est un ensemble (fini ou infini) et qu'on note « $(S_X)_{\text{fin}}$ » le sous-groupe de S_X composé de toutes les permutations à support fini, alors il existe un unique homomorphisme*

$$f\colon (S_X)_{\text{fin}} \to \{\pm 1\}$$

tel que $f(\tau) = -1$ pour toute transposition $\tau \in S_X$.

Exercice. Prouver ce corollaire.

Corollaire. *Dans aucun ensemble, un produit d'un nombre pair de transpositions ne peut être un produit d'un nombre impair de transpositions.*

Définition. Une permutation qui est un produit de n transpositions est dite :

(1) *paire* si et seulement si n est pair,

(2) *impaire* si et seulement si n est impair.

Cette définition est correcte d'après le corollaire précédent.

Voici une méthode pratique pour déterminer la parité d'une permutation σ d'un ensemble fini X (voir la figure II.1) :

(1) Tracer deux droites parallèles dans un plan et marque sur chacune autant de points distincts que le nombre d'éléments dans X.

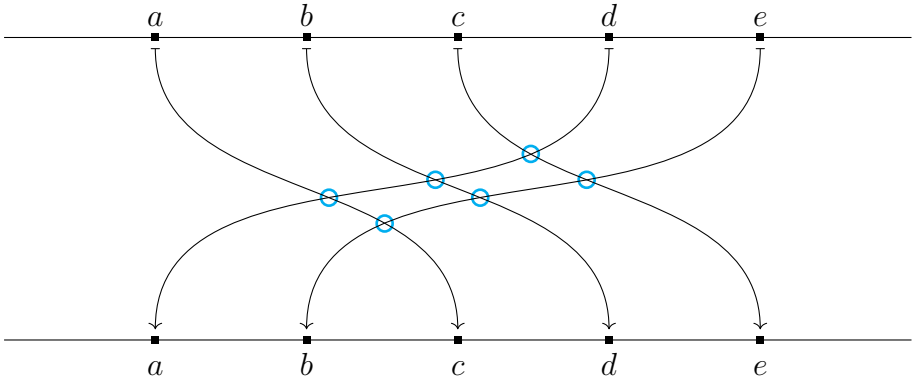


FIG. II.1. : Comme le nombre des croisements (six) est pair, la permutation $\begin{pmatrix} a & b & c & d & e \\ c & d & e & a & b \end{pmatrix}$ l'est aussi.

(2) Établir une bijection arbitraire entre les éléments de l'ensemble X et les points marqués de la première droite. Établir la bijection entre les éléments de l'ensemble X et les points marqués de la deuxième droite de sorte que les images des éléments de X soient rangées dans le même ordre sur les deux droites.

(3) Pour chaque $x \in X$, relier le point qui représente x sur la première droite au point qui représente $\sigma(x)$ sur la deuxième par une courbe de sorte que :

- (a) chacune des courbes soit complètement comprise entre les deux droites,
- (b) aucune des courbes ne se croise,
- (c) lorsque deux courbes différentes se croisent, elles le font de manière *transversale* (en passant d'un côté à l'autre),
- (d) aucunes trois courbes différentes ne se croisent toutes en un même point.

(4) Compter le nombre des points de croisement des courbes. La parité de ce nombre est la parité de σ.

Pour comprendre comment fonctionne cette méthode, considérons, pour chacune des droites, un graphe complet sur l'ensemble de ses points marqués. Choisissons les orientations des deux droites dans un même sens. Les orientations des droites induisent des orientations complètes des graphes complets sur

les points marqués. On peut aussi considérer l'orientation du second graphe induit du premier par σ. On aura ainsi deux orientations du second graphe complet, et la parité de σ est la parité du nombre d'arêtes pour lesquelles les deux orientations différent. Or, les arêtes pour lesquelles les deux orientations différent sont celles pour lesquelles les courbes qui relient leurs extrémités aux points marqués de la première droit se croisent un nombre impair de fois.

Proposition. *Les permutations paires d'un ensemble X forment un sous-groupe de S_X.*

Exercice. Prouver cette proposition.

Définition. Soit σ une permutation qui est un produit de n transpositions. Alors la *signature*[7] de σ est $(-1)^n$.

Cette définition est correcte d'après le corollaire précédent.

Notation. La signature d'une permutation σ sera notée « $\operatorname{sign}\sigma$ ».

Ainsi, une permutation σ à support fini est impaire si est seulement si $\operatorname{sign}\sigma = -1$.

Si σ et τ sont deux permutations à supports finis d'un même ensemble, alors

$$\operatorname{sign}(\tau\sigma) = (\operatorname{sign}\tau)(\operatorname{sign}\sigma).$$

Voici encore une méthode pour déterminer la signature d'une permutation σ d'un ensemble fini X.

Soit R un anneau commutatif unitaire (muni de 1) tel que :

(1) R est intègre (sans diviseurs de 0 autres que 0),

(2) la caractéristique de R est différente de 2 ($2 \neq 0$ dans R),

(3) le cardinal de R est supérieur au égal au cardinal de X ($|R| \geqslant |X|$).

(On peut toujours choisir $R = \mathbf{Z}$.) Soit $(\lambda_x)_{x\in X}$ une famille d'éléments deux à deux distincts de R.

Soit $(\curvearrowright)$ une relation *totale asymétrique* sur X. En particulier, toute relation totale $(\curvearrowright)$ d'ordre strict sur X convient. Si l'anneau R est muni d'une relation totale $(<)$ d'ordre strict (comme l'ordre usuel sur $\mathbf{Z}$), alors on peut définir un

[7] En anglais, pour parler de la signature d'une permutation, le terme « *sign* » (signe) est courant. Ce choix paraît adéquat pour parler de quelque chose qui prend les valeurs ± 1, et cela évite de surcharger le terme « signature », qui sert en algèbre et en logique formelle à d'autres fins.

ordre total strict ($\curvearrowright$) sur X par la condition que $x \curvearrowright y$ si et seulement si $\lambda_x < \lambda_y$.

Alors :

$$\frac{\displaystyle\prod_{x,y\in X\,|\,x\curvearrowright y} \big(\lambda_{\sigma(y)} - \lambda_{\sigma(x)}\big)}{\displaystyle\prod_{x,y\in X\,|\,x\curvearrowright y} (\lambda_y - \lambda_x)} = \operatorname{sign}\sigma = \frac{\displaystyle\prod_{x,y\in X\,|\,x\curvearrowright y} (\lambda_y - \lambda_x)}{\displaystyle\prod_{x,y\in X\,|\,x\curvearrowright y} \big(\lambda_{\sigma(y)} - \lambda_{\sigma(x)}\big)}.$$

(On a confondu ici la valeur $\pm 1 \in \mathbf{Z}^\times \subset \mathbf{Z}$ de $\operatorname{sign}\sigma$ avec un élément $\pm 1 \in R^\times \subset R$.)

En particulier, pour $\sigma \in S_n$,

$$\frac{\displaystyle\prod_{1\leqslant i<j\leqslant n} \big(\sigma(j) - \sigma(i)\big)}{\displaystyle\prod_{1\leqslant i<j\leqslant n} (j - i)} = \operatorname{sign}\sigma = \frac{\displaystyle\prod_{1\leqslant i<j\leqslant n} (j - i)}{\displaystyle\prod_{1\leqslant i<j\leqslant n} \big(\sigma(j) - \sigma(i)\big)}.$$

Cette méthode de calcul peut aussi servir de base pour une autre démonstration du théorème principal de cette section.

II.10. Groupes alternés

Définition. Si X est un ensemble fini, alors le sous-groupe de S_X composé des permutations paires est dit le *groupe alterné* sur X.

Notation. On va noter « A_X » le groupe alterné sur un ensemble fini X. On va noter « A_n » le groupe alterné sur l'ensemble $\{1, \ldots, n\}$.

Exercice. Soient σ et τ deux transpositions sur un ensemble X. Monter que :

(1) $\tau\sigma = \mathrm{id}_X$ lorsque $\operatorname{Supp}\tau = \operatorname{Supp}\sigma$,

(2) $\tau\sigma$ est un cycle de longueur 3 lorsque $\operatorname{Supp}\tau \cap \operatorname{Supp}\sigma$ est un singleton,

(3) $\tau\sigma$ est un produit de 2 cycles de longueur 3 lorsque $\operatorname{Supp}\tau \cap \operatorname{Supp}\sigma$ est vide.

Proposition. *Si X est un ensemble fini, alors le groupe alterné A_X est engendré par l'ensemble des cycles de longueur 3 sur X.*

Exercice. Prouver cette proposition.

III. Homomorphismes

III.1. Homomorphismes

Comme d'habitude, on va utiliser le même symbole pour noter un groupe et son ensemble sous-jacent, et on va utiliser la même notation pour les opérations usuelles dans différents groupes, tant que le contexte permet d'éviter la confusion.

Définition. Un *homomorphisme*, ou un *morphisme*, d'un groupe G vers un groupe H est une application $f\colon G \to H$ telle que :

(1) $f(xy) = f(x)f(y)$ pour tous $x, y \in G$,

(2) $f(1_G) = 1_H$,

(3) $f(x^{-1}) = (f(x))^{-1}$ pour tout $x \in G$.

Exercice. Soit $f\colon G \to H$ un homomorphisme de groupes. Montrer que $f(x^n) = f(x)^n$ pour tous $n \in \mathbf{Z}$ et $x \in G$.

Proposition. *Soient G et H deux groupes d'ensembles sous-jacents S et T, respectivement, et soit $f\colon S \to T$ une application. Alors f est un homomorphisme de G vers H si et seulement si f est un homomorphisme de G^{op} vers H^{op}.*

Proposition. *Si G et K sont deux groupes, H est un sous-groupe de G, et f est un homomorphisme $G \to K$, alors la restriction de f sur H est un homomorphisme $H \to K$.*

Proposition. *Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. Alors :*

(1) *l'image par f de tout sous-groupe de G est un sous-groupe de H,*

(2) *l'image réciproque par f de tout sous-groupe de H est un sous-groupe de G.*

En particulier, si $f\colon G \to H$ est un homomorphisme, alors son ensemble image est un sous-groupe de H, et l'image réciproque du sous-groupe trivial $\mathbf{1}_H$ de H est un sous-groupe de G :

$$f(G) \leqslant H, \qquad f^{-1}(\mathbf{1}_H) \leqslant G.$$

Exercice. Prouver la dernière proposition.

Exemple. L'application signature $\operatorname{sign}\colon S_n \to \{\pm 1\}$ est un homomorphisme du groupe symétrique S_n dans le groupe multiplicatif $\mathbf{Z}^\times = \{\pm 1\}$. On peut aussi l'interpréter comme un homomorphisme $S_n \to \mathbf{R}^\times$ ou $S_n \to \mathbf{C}^\times$.

III.2. Images et noyaux

Définition. Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. L'*image* de f, notée « $\operatorname{Im} f$ », est l'ensemble image de l'application f, muni de structure d'un sous-groupe de H. Vu comme un ensemble,

$$\operatorname{Im} f \overset{\text{déf}}{=} f(G) = \{\, f(x) \mid x \in G \,\}.$$

Le noyau de f, noté « $\operatorname{Ker} f$ », est l'image réciproque du sous-groupe trivial $\mathbf{1}_H$ de H, muni de structure d'un sous-groupe de G. Vu comme un ensemble,

$$\operatorname{Ker} f \overset{\text{déf}}{=} f^{-1}(\mathbf{1}_H) = \{\, x \in G \mid f(x) = 1_H \,\}.$$

Proposition. *Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. Alors, pour tous éléments $x, y \in G$, les énoncés suivants sont équivalents* :

(1) $f(x) = f(y)$,

(2) $xy^{-1} \in \operatorname{Ker} f$,

(3) $x^{-1}y \in \operatorname{Ker} f$.

Exercice. Prouver cette proposition.

Corollaire. *Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. Alors l'application f est injective si et seulement si* $\operatorname{Ker} f = \mathbf{1}_G$.

Exercice. Montrer que si $\tau \in S_3$ est une transposition (cycle de longueur 2), alors le sous-groupe $H = \langle \tau \rangle$ engendré par τ n'est le noyau d'aucun homomorphisme $f\colon S_3 \to G$.

III.3. Correspondance des sous-groupes sous un homomorphisme

Proposition. *Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. Alors* :

(1) *pout tout $K \leqslant G$, $f(K) \leqslant H$ et $f(K) \leqslant \operatorname{Im} f$,*

(2) *pout tout $L \leqslant H$, $f^{-1}(L) \leqslant G$ et $\operatorname{Ker} f \leqslant f^{-1}(L)$.*

Rappelons-nous que quelle que soit une application $f\colon X \to Y$,

(1) pout tout $A \subset X$, $f^{-1}(f(A)) \supset A$,

(2) pout tout $B \subset Y$, $f(f^{-1}(B)) \subset B$.

Le théorème suivant donne des critères pour les inclusions inverses dans le cadre des images et des pré-images de sous-groupes sous un homomorphisme.

Théorème. *Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. Alors* :

(1) *pout tout $K \leqslant G$, $f^{-1}(f(K)) = K$ si et seulement si $\operatorname{Ker} f \leqslant K$,*

(2) *pout tout $L \leqslant H$, $f(f^{-1}(L)) = L$ si et seulement si $L \leqslant \operatorname{Im} f$.*

En particulier, tout homomorphisme $f\colon G \to H$ determine deux bijections réciproques entre les ensembles

$$\{\, K \leqslant G \mid \operatorname{Ker} f \leqslant K \,\} \quad \text{et} \quad \{\, L \leqslant H \mid L \leqslant \operatorname{Im} f \,\}$$

données comme

$$K \mapsto f(K) \quad \text{et} \quad L \mapsto f^{-1}(L).$$

Exercice. Prouver le dernier théorème.

III.4. Iso-, épi-, mono-

Définition. Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme. Alors f est dit être :

- un *isomorphisme* entre G et H si et seulement si l'application F est bijective entre G et H,

- un *épimorphisme* sur H si et seulement si l'application f est surjective sur H,
- un *monomorphisme* si et seulement si l'application f est injective (sur son domaine de définition G).

En termes de l'image et du noyau, un homomorphisme $f\colon G \to H$ est :

- un épimorphisme si et seulement si $\operatorname{Im} f = H$,
- un monomorphisme si et seulement si $\operatorname{Ker} f = \mathbf{1}_G$.

Remarque. Pour deux groupes G et H, un homomorphisme $f\colon G \to H$ est un isomorphisme entre G et H si et seulement si f est un épimorphisme sur H et un monomorphisme (sur G). Cependant, il existe des définitions assez générales et assez standards des notions d'*isomorphisme*, d'*épimorphisme* et de *monomorphisme* qui s'appliquent dans le contexte d'une n'importe quelle *catégorie*. Ici on les utilise dans le contexte de la *catégorie des groupes*, et les définitions données ne sont pas les définitions générales. En général, il n'est pas toujours le cas qu'un morphisme qui est épi- et mono- soit iso-.

Notation. On va écrire « $f\colon G \twoheadrightarrow H$ » ou « $f\colon H \twoheadleftarrow G$ » pour dire que l'application $f\colon G \to H$ est un épimorphisme de G sur H. On va écrire « $f\colon G \rightarrowtail H$ » ou « $f\colon H \leftarrowtail G$ » pour dire que l'application $f\colon G \to H$ est un monomorphisme de G dans H. On va écrire « $f\colon G \xrightarrow{\sim} H$ » ou « $f\colon H \xleftarrow{\sim} G$ » pour dire que l'application $f\colon G \to H$ est un isomorphisme entre G et H.

Remarque. Deux formes de flèches sont courantes pour indiquer un monomorphisme : « $\rightarrowtail$ » et « $\hookrightarrow$ ».

Proposition. *Soient G, H, K trois groupes et $\alpha\colon G \to H$ et $\beta\colon H \to K$ deux homomorphismes. Alors :*

(1) *si $\alpha\colon G \xrightarrow{\sim} H$ et $\beta\colon H \xrightarrow{\sim} K$, alors $\beta \circ \alpha\colon G \xrightarrow{\sim} K$,*

(2) *si $\alpha\colon G \twoheadrightarrow H$ et $\beta\colon H \twoheadrightarrow K$, alors $\beta \circ \alpha\colon G \twoheadrightarrow K$,*

(3) *si $\alpha\colon G \rightarrowtail H$ et $\beta\colon H \rightarrowtail K$, alors $\beta \circ \alpha\colon G \rightarrowtail K$,*

(4) *$\beta \circ \alpha\colon G \twoheadrightarrow K$ si et seulement si $\beta\colon H \twoheadrightarrow K$ et*

$$(\operatorname{Im}\alpha)(\operatorname{Ker}\beta) = H = (\operatorname{Ker}\beta)(\operatorname{Im}\alpha),$$

(5) *$\beta \circ \alpha\colon G \rightarrowtail K$ si et seulement si $\alpha\colon G \rightarrowtail H$ et*

$$\operatorname{Im}\alpha \wedge \operatorname{Ker}\beta = \mathbf{1}_H.$$

Exercice. Prouver cette proposition.

Proposition. *Si $f\colon G \to H$ est un isomorphisme entre deux groupes G et H, alors l'application inverse $f^{-1}\colon H \to G$ est un isomorphisme entre H et G.*

Exercice. Prouver cette proposition. (Comme l'application inverse d'une bijection est une bijection, il suffit de vérifier que $f^{-1}\colon H \to G$ est un homomorphisme.)

Corollaire. *Un homomorphisme $\alpha\colon G \to H$ d'un groupe G vers un groupe H est un isomorphisme entre G et H si et seulement si il existe un homomorphisme $\beta\colon H \to G$ tel que :*

$$\beta \circ \alpha = \mathrm{id}_G \quad \textit{et} \quad \alpha \circ \beta = \mathrm{id}_H\,.$$

Proposition. *Soient G, H, K trois groupes, $\alpha, \beta\colon H \to G$ deux homomorphismes, et $\varepsilon\colon K \twoheadrightarrow H$ un épimorphisme tels que $\alpha \circ \varepsilon = \beta \circ \varepsilon$. Alors $\alpha = \beta$.*

Exercice. Prouver cette proposition.

Remarque. En utilisant la notion du *produit libre amalgamé*, on peut montrer que si $\gamma\colon K \to H$ est un homomorphisme de groupes qui n'est pas un épimorphisme sur H, alors il existe un groupe G ($= H *_{\mathrm{Im}\,\gamma} H$) et deux homomorphismes $\alpha, \beta\colon H \to G$ tels que $\alpha \circ \gamma = \beta \circ \gamma$, mais $\alpha \neq \beta$.

Proposition. *Soient G, H, K trois groupes, $\alpha, \beta\colon G \to H$ deux homomorphismes, et $\mu\colon H \rightarrowtail K$ un monomorphisme tels que $\mu \circ \alpha = \mu \circ \beta$. Alors $\alpha = \beta$.*

Exercice. Prouver cette proposition.

Exercice. Soient H et K deux groupes et $\gamma\colon H \to K$ un homomorphisme. Posons $G = \mathrm{Ker}\,\gamma$. Montrer que si γ n'est pas un monomorphisme, alors il existe deux homomorphismes $\alpha, \beta\colon G \to H$ tels que $\gamma \circ \alpha = \gamma \circ \beta$, mais $\alpha \neq \beta$.

III.5. Endo- et auto-

Définition. Un *endomorphisme* d'un groupe G est un homomorphisme $G \to G$. Un *automorphisme* d'un groupe G est un isomorphisme $G \xrightarrow{\sim} G$.

Pour tout groupe G, l'application identité $\mathrm{id}_G\colon G \to G$ est un automorphisme de G (son automorphisme *trivial*).

L'ensemble des endomorphismes d'un groupe forme un *monoïde* par rapport à l'opération de composition.

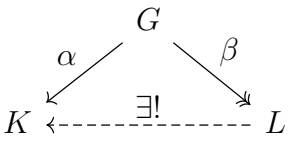
L'ensemble des automorphismes d'un groupe forme un groupe par rapport à l'opération de composition.

Notation. Si G est un groupe, alors l'ensemble, ou le monoïde, des endomorphismes de G est noté « $\mathrm{End}(G)$ », et l'ensemble, ou le groupe, des automorphismes de G est noté « $\mathrm{Aut}(G)$ ».

III.6. Homomorphismes induits

Théorème. *Si $\alpha\colon G \to K$ est un homomorphisme et $\beta\colon G \twoheadrightarrow L$ est un épimorphisme tels que $\operatorname{Ker}\beta \leqslant \operatorname{Ker}\alpha$, alors il existe un unique homomorphisme $\gamma\colon L \to K$ tel que $\gamma \circ \beta = \alpha$. En plus, dans ce cas, $\operatorname{Ker}\gamma = \beta(\operatorname{Ker}\alpha)$ et $\beta^{-1}(\operatorname{Ker}\gamma) = \operatorname{Ker}\alpha$.*

Voici un schéma pour ce théorème :



$\operatorname{Ker}\alpha \geqslant \operatorname{Ker}\beta.$

Démonstration. L'unicité est évidente. (C'est un cas particulier d'une proposition de la section III.4.) Montrons l'existence.

Soient $\alpha\colon G \to K$ un homomorphisme et $\beta\colon G \twoheadrightarrow L$ un épimorphisme tels que $\operatorname{Ker}\beta \leqslant \operatorname{Ker}\alpha$. D'après une proposition de la section III.2, on a, pour tous $x, y \in G$, l'implication :

$$\beta(x) = \beta(y) \quad \Rightarrow \quad \alpha(x) = \alpha(y).$$

Grâce à cette implication et à l'hypothèse que $\operatorname{Im}\beta = L$, on voit qu'il existe une unique application $\gamma\colon L \to K$ telle que :

$$\gamma(\beta(x)) = \alpha(x) \qquad \text{pour tout } x \in G.$$

Il est facile de vérifier qu'une telle application $\gamma\colon L \to K$ est un homomorphisme (de L vers K), ce qui terminera la démonstration de l'existence.

Soit donc $\gamma\colon L \to K$ l'homomorphisme tel que $\gamma \circ \beta = \alpha$. Montrons que $\operatorname{Ker}\gamma = \beta(\operatorname{Ker}\alpha)$ et que $\beta^{-1}(\operatorname{Ker}\gamma) = \operatorname{Ker}\alpha$.

Soit $u \in \operatorname{Ker}\gamma$ arbitraire. Soit $x \in G$ tel que $u = \beta(x)$ (il existe car $u \in L = \operatorname{Im}\beta$). Alors $\alpha(x) = \gamma(\beta(x)) = \gamma(u) = 1$. Donc, $x \in \operatorname{Ker}\alpha$. D'où, $u = \beta(x) \in \beta(\operatorname{Ker}\alpha)$. Ainsi on a montré que

$$\operatorname{Ker}\gamma \subset \beta(\operatorname{Ker}\alpha).$$

Soit $u \in \beta(\operatorname{Ker}\alpha)$ arbitraire. Soit $x \in \operatorname{Ker}\alpha$ tel que $u = \beta(x)$. Alors $\gamma(u) = \gamma(\beta(x)) = \alpha(x) = 1$. Donc, $u \in \operatorname{Ker}\gamma$. Ainsi on a montré que

$$\operatorname{Ker}\gamma \supset \beta(\operatorname{Ker}\alpha).$$

Soit $x \in \beta^{-1}(\operatorname{Ker}\gamma)$ arbitraire. Alors $\beta(x) \in \operatorname{Ker}\gamma$, et donc $\alpha(x) = \gamma(\beta(x)) = 1$. D'où, $x \in \operatorname{Ker}\alpha$. Ainsi on a montré que

$$\beta^{-1}(\operatorname{Ker}\gamma) \subset \operatorname{Ker}\alpha.$$

Soit $x \in \operatorname{Ker}\alpha$ arbitraire. Alors $\gamma(\beta(x)) = \alpha(x) = 1$. D'où, $\beta(x) \in \operatorname{Ker}\gamma$, et donc $x \in \beta^{-1}(\operatorname{Ker}\gamma)$. Ainsi on a montré que

$$\beta^{-1}(\operatorname{Ker}\gamma) \supset \operatorname{Ker}\alpha. \qquad \square$$

Corollaire. *Si deux épimorphismes $\alpha\colon G \twoheadrightarrow K$ et $\beta\colon G \twoheadrightarrow L$ ont le même noyau, alors il existe un unique isomorphisme $\gamma\colon L \xrightarrow{\sim} K$ tel que $\gamma \circ \beta = \alpha$.*

Démonstration. D'après le précédent théorème, il existe un unique homomorphisme $\gamma\colon L \to K$ tel que $\gamma \circ \beta = \alpha$. Il suffit de montrer qu'un tel γ est un isomorphisme entre L et K.

Soit donc $\gamma\colon L \to K$ un homomorphisme tel que $\gamma \circ \beta = \alpha$. Soit $\delta\colon K \to L$ un homomorphisme tel que $\delta \circ \alpha = \beta$. (Un tel δ existe d'après le précédent théorème, vu que $\alpha\colon G \twoheadrightarrow K$ et que $\operatorname{Ker}\alpha \leqslant \operatorname{Ker}\beta$.) Alors

$$\gamma \circ \delta \circ \alpha = \gamma \circ \beta = \alpha = \mathrm{id}_K \circ \alpha$$

et

$$\delta \circ \gamma \circ \beta = \delta \circ \alpha = \beta = \mathrm{id}_L \circ \beta,$$

d'où :

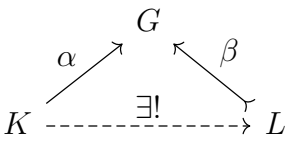
$$\gamma \circ \delta = \mathrm{id}_K \quad \text{et} \quad \delta \circ \gamma = \mathrm{id}_L$$

(d'après l'unicité dans la conclusion du dernier théorème, ou d'après une proposition de la section III.4, car $\alpha\colon G \twoheadrightarrow K$ et $\beta\colon G \twoheadrightarrow L$). D'où, $\gamma\colon L \xrightarrow{\sim} K$ (et $\delta\colon K \xrightarrow{\sim} L$.) $\square$

Remarque. Ce corollaire appliqué à la *projection canonique* β d'un groupe G sur un *groupe quotient* $L = G/N$ est parfois appelé le *premier théorème d'isomorphisme*.

Théorème. *Si $\alpha\colon K \to G$ est un homomorphisme et $\beta\colon L \rightarrowtail G$ est un monomorphisme tels que $\operatorname{Im}\beta \geqslant \operatorname{Im}\alpha$, alors il existe un unique homomorphisme $\gamma\colon K \to L$ tel que $\alpha = \beta \circ \gamma$. En plus, dans ce cas, $\operatorname{Im}\gamma = \beta^{-1}(\operatorname{Im}\alpha)$ et $\beta(\operatorname{Im}\gamma) = \operatorname{Im}\alpha$.*

Voici un schéma pour ce théorème :



$\operatorname{Im}\alpha \leqslant \operatorname{Im}\beta.$

Exercice. Prouver ce théorème.

Corollaire. *Si deux monomorphismes $\alpha\colon K \rightarrowtail G$ et $\beta\colon L \rightarrowtail G$ ont la même image, alors il existe un unique isomorphisme $\gamma\colon K \xrightarrow{\sim} L$ tel que $\alpha = \beta \circ \gamma$.*

IV. Actions

IV.1. Actions de groupes sur des ensembles

Définition. Soient G un groupe et X un ensemble. Une *action* de G sur X *à gauche* est une application $\alpha\colon G \times X \to X$ telle que :

(1) $\alpha(h,\, \alpha(g,x)) = \alpha(hg,\, x)$ pour tous $g,h \in G$ et $x \in X$,

(2) $\alpha(1,x) = x$ pour tout $x \in X$.

Une *action* de G sur X *à droite* est une application $\beta\colon X \times G \to X$ telle que :

(1) $\beta(\beta(x,g),\, h) = \beta(x,\, gh)$ pour tous $g,h \in G$ et $x \in X$,

(2) $\beta(x,1) = x$ pour tout $x \in X$.

Exemple. Quel que soit un groupe G, il existe une unique action de G sur l'ensemble vide $\varnothing$ à gauche et une unique action de G sur $\varnothing$ à droite (les actions qui ne font rien de rien).

Exemple. Soient un groupe G et un ensemble X. Pour tous $g \in G$ et $x \in X$, posons :

$$\alpha(g,x) \overset{\text{déf}}{=} x \quad \text{et} \quad \beta(x,g) \overset{\text{déf}}{=} x.$$

Alors α est une action de G sur X à gauche et β est une action de G sur X à droite (dites les actions *triviales*).

Exemple. Soit un ensemble X. Pour toute permutation $\sigma\colon X \to X$ et pour tout $x \in X$, posons :

$$\alpha(\sigma,x) \overset{\text{déf}}{=} \sigma(x) \quad \text{et} \quad \beta(x,\sigma) \overset{\text{déf}}{=} \sigma(x).$$

Alors α est une action du groupe symétrique S_X sur X à gauche et β est une action du groupe opposé S_X^{op} sur X à droite (dites les actions *canoniques* des groupes S_X et S_X^{op} sur X).

Exemple. Soit G un groupe d'ensemble sous-jacent X. Pour tous $g, x \in G$, posons :

$$\alpha(g,x) \overset{\text{déf}}{=} gx \quad \text{et} \quad \beta(x,g) \overset{\text{déf}}{=} xg.$$

Alors α est une action de G sur X à gauche et β est une action de G sur X à droite (dites les actions *canoniques* de G sur son ensemble sous-jacent).

Remarque. Dans le dernier exemple, on parle d'actions d'un groupe G sur *son ensemble sous-jacent*, plutôt que sur *lui-même*, parce que ces actions ne respectent pas la structure de groupe. Pour pouvoir dire que $\alpha\colon G \times H \to H$ est une action du groupe G *sur le groupe* H à droite, il faut que l'identité

$$\alpha(g,\, h \cdot k) = \alpha(g,h) \cdot \alpha(g,k)$$

soit satisfaite (pour tous $g \in G$ et $h, k \in H$). Un exemple d'une véritable action (non triviale) d'un groupe (non trivial) G sur *lui-même* à gauche est l'application $\alpha\colon G \times G \to G$ définie par :

$$\alpha(g,h) \overset{\text{déf}}{=} ghg^{-1}.$$

Définition. Soient G un groupe et X un ensemble.

(1) Si $\alpha\colon G \times X \to X$ est une action de G sur X à gauche et $g \in G$, alors l'*action* de g sur X dans le contexte de l'action α est l'application $X \to X$ définie comme $x \mapsto \alpha(g,x)$.

(2) Si $\beta\colon X \times G \to X$ est une action de G sur X à droite et $g \in G$, alors l'*action* de g sur X dans le contexte de l'action β est l'application $X \to X$ définie comme $x \mapsto \beta(x,g)$.

On peut montrer que lorsqu'un groupe G opère sur un ensemble X, l'action de chaque élément de G sur X est une permutation de X. En plus :

(1) toute action d'un groupe G sur un ensemble X à gauche peut être vue comme un homomorphisme $G \to S_X$, et

(2) toute action d'un groupe G sur un ensemble X à droite peut être vue comme un homomorphisme $G \to S_X^{\text{op}}$.

Proposition. *Soient G un groupe et X un ensemble. Pour toute action α de G sur X à gauche, posons f_α l'application qui à chaque élément de G associe une application $X \to X$ selon la formule* :

$$f_\alpha(g)(x) = \alpha(g,x) \qquad \textit{pour tous } g \in G \textit{ et } x \in X.$$

Alors :

(1) *$f_\alpha(g)\colon X \to X$ est une permutation de X, quels que soient une action α de G sur X à gauche et $g \in G$,*

(2) *$f_\alpha\colon G \to S_X$ est un homomorphisme de G vers le groupe symétrique de X, quelle que soit une action α de G sur X à gauche,*

(3) *l'application $\alpha \mapsto f_\alpha$ est une bijection entre l'ensemble des actions de G sur X à gauche et l'ensemble des homomorphismes $G \to S_X$.*

Exercice. Prouver cette proposition.

Proposition. *Soient G un groupe et X un ensemble. Pour toute action β de G sur X à droite, posons f_β l'application qui à chaque élément de G associe une application $X \to X$ selon la formule :*

$$f_\beta(g)(x) \overset{\text{déf}}{=} \beta(x, g) \qquad \text{pour tous } g \in G \text{ et } x \in X.$$

Alors :

(1) *$f_\beta(g)\colon X \to X$ est une permutation de X, quels que soient $g \in G$ et une action β de G sur X à droite,*

(2) *$f_\beta\colon G \to S_X^{\mathrm{op}}$ est un homomorphisme de G vers le groupe opposé du groupe symétrique de X, quelle que soit une action β de G sur X à droite,*

(3) *l'application $\beta \mapsto f_\beta$ est une bijection entre l'ensemble des actions de G sur X à droite et l'ensemble des homomorphismes $G \to S_X^{\mathrm{op}}$.*

Exercice. Prouver cette proposition.

Remarque. Dans la littérature, le terme « *action à gauche* » pour un groupe G et pour un ensemble X peut désigner soit une application $G \times X \to X$, comme dans la définition donnée ci-dessus, soit un homomorphisme $G \to S_X$. De même, le terme « *action à droite* » pour G et X peut désigner soit une application $X \times G \to X$, soit un homomorphisme $G \to S_X^{\mathrm{op}}$. D'après les deux dernières propositions, il y a une correspondance canonique entre les deux interprétations des ces deux termes. Pourtant, dans le contexte d'actions de *groupes topologiques* sur des *espaces topologiques*, il est naturel d'exiger que les actions soient *continues* dans un sens approprié, ce qui s'exprime par la condition que les application correspondantes $G \times X \to X$ ou $X \times G \to X$ soient continues, mais ne s'exprime pas facilement en termes des homomorphismes $G \to S_X$ ou $G \to S_X^{\mathrm{op}}$. En outre, pour une action à gauche $\alpha\colon G \times X \to X$, on

peut avoir l'intérêt de regarder l'application associée $G \times X \to X \times X$ définie comme $(g, x) \mapsto (\alpha(g, x),\, x)$. De même, pour une action à droite $\beta\colon X \times G \to X$, on peut avoir l'intérêt de regarder l'application associée $X \times G \to X \times X$ définie comme $(x, g) \mapsto (x,\, \beta(x, g))$.

Définition. Soient G un groupe et X un ensemble.

(1) Si $\alpha\colon G \times X \to X$ est une action de G sur X à gauche, alors on va appeler l'homomorphisme associé $G \to S_X$ l'homomorphisme *associé* à l'action α.

(2) Si $\beta\colon X \times G \to X$ est une action de G sur X à droite, alors on va appeler l'homomorphisme associé $G \to S_X^{\mathrm{op}}$ l'homomorphisme *associé* à l'action β.

Notation. Si G est un groupe, X est un ensemble, et $\alpha\colon G \times X \to X$ est une action de G sur X à gauche, alors, pour $g \in G$ et $x \in X$, l'élément $\alpha(g, x) \in X$ peut être noté comme « gx » ou « ${}^g x$ » ou « $g \cdot x$ » ou « $g.x$ », lorsque cela n'introduit pas d'ambiguïté. On peut aussi envisager d'autres notations, comme « $g \triangleleft x$ ». De même, si $\beta\colon X \times G \to X$ est une action de G sur X à droite, alors, pour $g \in G$ et $x \in X$, l'élément $\beta(x, g) \in X$ peut être noté comme « xg » ou « x^g » ou « $x \cdot g$ » ou « $x.g$ », et on peut envisager d'autres notations, comme « $x \triangleright g$ ».

Proposition. *Soient G un groupe, X un ensemble, et $\alpha\colon G \times X \to X$ et $\beta\colon X \times G \to X$ deux applications telles que :*

$$\alpha(g, x) = \beta(x, g) \qquad \text{pour tous } g \in G \text{ et } x \in X.$$

Alors :

(1) *α est une action de G sur X à gauche si et seulement si β est une action de G^{op} sur X à droite, et*

(2) *β est une action de G sur X à droite si et seulement si α est une action de G^{op} sur X à gauche.*

Exercice. Prouver cette proposition.

Proposition. *Soient G un groupe, X un ensemble, et $\alpha\colon G \times X \to X$ et $\beta\colon X \times G \to X$ deux applications telles que :*

$$\alpha(g, x) = \beta(x,\, g^{-1}) \qquad \text{pour tous } g \in G \text{ et } x \in X,$$

ce qui équivaut à :

$$\beta(x, g) = \alpha(g^{-1}, x) \qquad \textit{pour tous } g \in G \textit{ et } x \in X.$$

Alors α est une action de G sur X à gauche si et seulement si β est une action de G sur X à droite.

Exercice. Prouver cette proposition.

Définition. Soit G un groupe.

(1) Un *G-ensemble gauche* est un ensemble muni d'une action de G à gauche.

(2) Un *G-ensemble droit* est un ensemble muni d'une action de G à droite.

Remarque. Lorsqu'on cherche à munir un même ensemble X à la fois d'une structure d'un G-ensemble gauche et d'une structure d'un H-ensemble droite, d'habitude on exige que l'action de G à gauche *commute* avec l'action de H à droite au sens que :

$$g(xh) = (gx)h \qquad \text{pour tous } g \in G,\ h \in H \text{ et } x \in X.$$

Remarque. Dans la littérature, on parle plus souvent des actions à gauche (qu'on appelle « *actions* » tout court) que des actions à droite. Cette disparité provient du faut qu'une action de G sur X à gauche représente un homomorphisme $G \to S_X$ (qui peut aussi être vu comme un homomorphisme $G^{\mathrm{op}} \to S_X^{\mathrm{op}}$), alors qu'une action de G sur X à droite représente un homomorphisme $G \to S_X^{\mathrm{op}}$ (qui peut aussi être vu comme un homomorphisme $G^{\mathrm{op}} \to S_X$), ce qui paraît moins naturel. La source de cette disparité est le fait que l'image d'un élément x par une application f est d'habitude écrite comme « $f(x)$ », plutôt que comme « $(x)f$ ».[1]

Vue que les traitements des actions à gauche et à droite sont presque identiques (ou, plutôt, « symétriques »), dans le reste de ce chapitre on va principalement nous occuper des actions à gauche, qu'on va appeler « *actions* » tout court. De même, si G est un groupe, un « *G-ensemble* » va par défaut signifier un G-ensemble gauche.

[1] La notation « $(x)f$ », ainsi que « x^f », pour l'image de x sous f peut aussi être trouvée dans la littérature, notamment dans le domaine de la théorie des groupes. Voir par exemple, Hall. (Marshall Hall. *The theory of groups*. Anglais. AMS Chelsea Publishing 288. Publié à l'origine par Macmillan Company, New York, 1959. American Mathematical Society, 1976. xiii+434. URL : `https://bookstore.ams.org/chel-288/`, chapitre 5, p. 53)

IV.2. Actions induites sur le même ensemble

Observons que si $H \leqslant G$, alors tout G-ensemble gauche est, *par restriction*, un H-ensemble gauche, et tout G-ensemble droit est, par restriction, un H-ensemble droit. Plus généralement :

Proposition. *Soient G et H deux groupes et $f\colon H \to G$ un homomorphisme. Alors :*

(1) *tout G-ensemble gauche X est un H-ensemble gauche par rapport à l'action définie ainsi :*

$$hx \overset{\text{déf}}{=} f(h)x \qquad \text{pour tous } h \in H \text{ et } x \in X,$$

(2) *tout G-ensemble droit X est un H-ensemble droit par rapport à l'action définie ainsi :*

$$xh \overset{\text{déf}}{=} xf(h) \qquad \text{pour tous } h \in H \text{ et } x \in X.$$

Exercice. Prouver cette proposition.

Proposition. *Soient G et K deux groupes et $f\colon G \twoheadrightarrow K$ un épimorphisme.*

(1) *Si X est un G-ensemble gauche tel que pour tous $g_1, g_2 \in G$ tels que $f(g_1) = f(g_2)$, et pour tout $x \in X$, on a que $g_1 x = g_2 x$, alors X est un K-ensemble gauche par rapport à l'action définie ainsi :*

$$f(g)x \overset{\text{déf}}{=} gx \qquad \text{pour tous } g \in G \text{ et } x \in X,$$

(2) *Si X est un G-ensemble droit tel que pour tous $g_1, g_2 \in G$ tels que $f(g_1) = f(g_2)$, et pour tout $x \in X$, on a que $xg_1 = xg_2$, alors X est un K-ensemble droit par rapport à l'action définie ainsi :*

$$xf(g) \overset{\text{déf}}{=} xg \qquad \text{pour tous } g \in G \text{ et } x \in X.$$

Exercice. Prouver cette proposition.

IV.3. Actions induites du même groupe

Si G est un groupe et X est un G-ensemble (gauche), alors :

(1) pour tout $n \in \mathbf{N}$, l'ensemble X^n est un G-ensemble par rapport à l'action définie ainsi :

$$g(x_1, \ldots, x_n) \overset{\text{déf}}{=} (gx_1, \ldots, gx_n) \qquad \text{pour tous } g \in G \text{ et } (x_1, \ldots, x_n) \in X^n,$$

(2) pour tout ensemble I, l'ensemble X^I des applications $I \to X$ est un G-ensemble par rapport à l'action définie ainsi :

$$(gf)(i) \overset{\text{déf}}{=} g(f(i)) \qquad \text{pour tous } g \in G,\ f\colon I \to X, \text{ et } i \in I,$$

(3) pour tout ensemble J, l'ensemble J^X des applications $X \to J$ est un G-ensemble par rapport à l'action définie ainsi :

$$(gf)(x) \overset{\text{déf}}{=} f(g^{-1}x) \qquad \text{pour tous } g \in G,\ f\colon X \to J, \text{ et } x \in X,$$

(4) l'ensemble $\mathscr{P}(X)$ des parties de X est un G-ensemble par rapport à l'action définie ainsi :

$$gY \overset{\text{déf}}{=} \{\, gx \mid x \in Y \,\} \qquad \text{pour tous } g \in G \text{ et } Y \subset X,$$

(5) l'ensemble des *partitions* de X est un G-ensemble par rapport à l'action définie ainsi :

$$gP \overset{\text{déf}}{=} \{\, gY \mid Y \in P \,\} \qquad \text{pour tout } g \in G \text{ et pour toute partition } P \text{ de } X.$$

On peut prolonger cette liste en y ajoutant, par exemple, le G-ensemble des relations d'équivalence sur un G-ensemble X, et ainsi de suite.

Définition. Soient G un groupe et X un G-ensemble. Une partie Y de X est dite *invariante* par l'action de G si et seulement si $gY = Y$ pour tout $g \in G$.

Proposition. *Soient G un groupe, X un G-ensemble, et Y une partie de X invariante par l'action de G. Alors Y est un G-ensemble* par restriction.

Exercice. Prouver cette proposition.

Définition. Soient G un groupe et X un G-ensemble. Une relation d'équivalence $(\sim)$ sur X est dite *invariante* par l'action de G si et seulement si, pour tout $g \in G$ et pour tous $x, y \in X$, on a l'équivalence logique :

$$gx \sim gy \quad \Leftrightarrow \quad x \sim y.$$

Proposition. *Soient G un groupe, X un G-ensemble, et $(\sim)$ une relation d'équivalence sur X invariante par l'action de G. Alors l'ensemble quotient $X/\sim$ (l'ensemble des classes d'équivalence par $(\sim)$) est un G-ensemble par rapport à l'action définie ainsi :*

$$g[x] \overset{\text{déf}}{=} [gx] \qquad \text{pour tous } g \in G \text{ et } x \in X,$$

où « $[x]$ » dénote la classe d'équivalence de $x \in X$.

Démonstration. Premièrement, on a besoin de vérifier que la formule

$$g[x] \overset{\text{déf}}{=} [gx]$$

définit correctement un élément $g[x] \in X/\sim$ pour tout couple $(g, [x]) \in G \times (X/\sim)$, c'est-à-dire, que l'élément $[gx] \in X/\sim$ ne dépende que du couple $(g, [x]) \in G \times (X/\sim)$. Cela résulte de l'invariance de la relation d'équivalence $(\sim)$ par l'action de G :

$$[x] = [y] \quad \Leftrightarrow \quad x \sim y \quad \Leftrightarrow \quad gx \sim gy \quad \Leftrightarrow \quad [gx] = [gy]$$

pour tout $g \in G$ et pour tous $x, y \in X$.

Il ne reste qu'à vérifier que l'application $G \times (X/\sim) \to (X/\sim)$ donnée comme

$$(g, [x]) \mapsto g[x] \overset{\text{déf}}{=} [gx]$$

est une action de G sur $X/\sim$ (à gauche).

On a :

$$h(g[x]) = h[gx] = [h(gx)] = [(hg)x] = (hg)[x]$$

pour tous $g, h \in G$ et $x \in X$. On a aussi :

$$1[x] = [1x] = [x]$$

pour tout $x \in X$. □

En plus de différentes façons de construire des nouveaux G-ensembles à partir d'un G-ensemble donné, on peut construire des nouveau G-ensembles à partir de plusieurs G-ensembles donnés. Par exemple, si X et Y sont deux G-ensembles, alors le produit cartésien $X \times Y$ est un G-ensemble par rapport à l'action définie ainsi :

$$g(x, y) \overset{\text{déf}}{=} (gx, gy) \qquad \text{pour tous } g \in G, x \in X \text{ et } y \in Y.$$

IV.4. Actions d'un groupe sur son ensemble sous-jacent

Soit G un groupe d'ensemble sous-jacent X.
Il y a toujours les quatre actions suivantes de G sur X à gauche :

$$(g,x)\mapsto x,\qquad (g,x)\mapsto gx,\qquad (g,x)\mapsto xg^{-1},\qquad (g,x)\mapsto {}^{g}x\overset{\text{déf}}{=}gxg^{-1}.$$

La première est dite l'action *triviale* à gauche, la deuxième est dite l'action par *translation* à gauche (aussi dite l'action *canonique* à gauche), et la dernière est dite l'action par *conjugaison*, ou l'action *adjointe*,[2] à gauche. La troisième peut être appelée l'action à gauche par *translation inverse à droite*.

De même, il y a les quatre actions suivantes de G sur X à droite :

$$(x,g)\mapsto x,\qquad (x,g)\mapsto xg,\qquad (x,g)\mapsto g^{-1}x,\qquad (x,g)\mapsto x^{g}\overset{\text{déf}}{=}g^{-1}xg.$$

La première est dite l'action *triviale* à droite, la deuxième est dite l'action par *translation* à droite, (aussi dite l'action *canonique* à droite), et la dernière est dite l'action par *conjugaison*, ou l'action *adjointe*,[3] à droite. La troisième peut être appelée l'action à droite par *translation inverse à gauche*.

Parmi ces actions, les actions triviales et les actions par conjugaison respectent la structure de groupe au sens suivant :

(1) si on note « $g.x$ » l'image de l'action triviale ou de l'action par conjugaison à gauche de $g\in G$ sur $x\in G$, alors, pour tous $g,x,y\in G$,

$$g.(xy)=(g.x)(g.y).$$

(2) si on note « $x.g$ » l'image de l'action triviale ou de l'action par conjugaison à droite de $g\in G$ sur $x\in G$, alors, pour tous $g,x,y\in G$,

$$(xy).g=(x.g)(y.g).$$

Pour cette raison, on peut dire que les actions triviales et par conjugaison son les actions du groupe G sur *lui-même* (sur G), et pas uniquement sur son *ensemble sous-jacent* (sur X).

[2] Le terme « action adjointe » est principalement utilisé dans le contexte des *groupes de Lie*.
[3] Voir la note précédente.

IV.5. Points fixes, support, parties stables, parties invariantes

Définition. Soient X un ensemble et $\varphi\colon X \to X$ une application.

- Un élément $x \in X$ est dit un *point fixe* de φ si et seulement si $\varphi(x) = x$.
- Une partie $Y \subset X$ est dite *stable* par φ si et seulement si $\varphi(Y) \subset Y$.
- Une partie $Y \subset X$ est dite *invariante* par φ si et seulement si $\varphi(Y) = Y$.

Dans le reste de cette section, G est un groupe et X est un G-ensemble.

Définition. Un élément $x \in X$ est dit :

- un *point fixe* de (l'action de) $g \in G$ si et seulement si $gx = x$,
- un *point fixe* de (l'action de) G si et seulement si $gx = x$ pour tout $g \in G$,
- un *point fixe* de (l'action de) $U \subset G$ si et seulement si $gx = x$ pour tout $g \in U$.

Notation. L'ensemble des points fixes de $g \in G$ dans X sera noté « X^g » ou « $\operatorname{Fix}_X g$ » ou « $\operatorname{Fix} g$ ». L'ensemble des points fixes de G dans X peut être noté « X^G » ou « $\operatorname{Fix}_X G$ » ou « $\operatorname{Fix} G$ ». L'ensemble des points fixes de $U \subset G$ dans X peut être noté « X^U » ou « $\operatorname{Fix}_X U$ » ou « $\operatorname{Fix} U$ ».

La notation avec « Fix » peut être préférable pour des usages occasionnels.

Définition. Le *support* de $g \in G$ dans X est le complément dans X de l'ensemble des points fixes de g. Le *support* de $U \subset G$ dans X est le complément dans X de l'ensemble des points fixes de U.

Remarque. Il existe un autre usage courant du terme « support » dans le contexte des fonctions à valeurs dans un anneau : on définit le *support* d'une fonction comme l'ensemble de ses arguments sur lesquels la fonction ne s'annule pas.

Notation. Le support de $g \in G$ sera noté « $\operatorname{Supp}_X g$ » ou « $\operatorname{Supp} g$ ». Le support de $U \subset G$ peut être noté « $\operatorname{Supp}_X U$ » ou « $\operatorname{Supp} U$ ».

Ainsi, pour tout $g \in G$,

$$X = X^g \sqcup \operatorname{Supp}_X g.$$

Définition. Une partie $Y \subset X$ est dite :

- *stable* par (l'action de) $g \in G$ si et seulement si $gY \subset Y$,
- *stable* par (l'action de) G si et seulement si $gY \subset Y$ pour tout $g \in G$,
- *stable* par (l'action de) $U \subset G$ si et seulement si $gY \subset Y$ pour tout $g \in U$.

Définition. Une partie $Y \subset X$ est dite :

- *invariante* par (l'action de) $g \in G$ si et seulement si $gY = Y$.
- *invariante* par (l'action de) G si et seulement si $gY = Y$ pour tout $g \in G$.
- *invariante* par (l'action de) $U \subset G$ si et seulement si $gY = Y$ pour tout $g \in U$.

Observons que $X^g = \mathrm{Fix}_X\, g$ et $\mathrm{Supp}_X\, g$ sont invariants par $g \in G$.

Exercice. Montrer que :

(1) Toute partie finie de X stable par $g \in G$ est invariante par g.

(2) Si $g \in G$ est d'ordre fini, alors toute partie de X stable par g est invariante par g.

(3) Toute partie de X stable par G est invariante par G.

IV.6. Orbites

Dans cette section, G est un groupe et X est un G-ensemble.

Définition. Deux éléments $x, y \in X$ sont dits *conjugués* par l'action de G si et seulement si il existe $g \in G$ tel que $gx = y$ (et $x = g^{-1}y$).

Proposition. *La relation d'être conjugués par l'action de G est une relation d'équivalence sur X.*

Exercice. Prouver cette proposition.

Définition. Les classes d'équivalence d'éléments de X par la relation d'être conjugués par l'action de G sont dites les *orbites* de l'action de G, ou les *G-orbites*. Lorsque $G = \langle g \rangle$ est un groupe cyclique engendré par $g \in G$, les orbites de l'action de G peuvent être dites les *g-orbites*.

Observons que la G-orbite d'un élément $x \in X$ est

$$\{\, gx \mid g \in G \,\}.$$

Définition. Le nombre cardinal d'une orbite (sa taille, son nombre d'éléments) est dite sa *longueur*.

Notation. La G-orbite de $x \in X$ sera notée, en fonction de la notation utilisée pour l'image de x sous l'action d'un élément $g \in G$, comme « Gx », ou comme « ${}^{G}x$ », ou comme « $G \cdot x$ », ou comme « $G.x$ », et ainsi de suite. (C'est pour le cas d'un G-ensemble *gauche* ; les notations correspondantes pour la G-orbite de $x \in X$ dans un G-ensemble *droit* sont « xG », « x^G », « $x \cdot G$ », « $x.G$ », et ainsi de suite.)

Notation. L'ensemble des G-orbites dans X peut être noté « $G\backslash X$ » (pour une action à gauche, mais « X/G » pour une action à droite) ou « X_G » (que l'action soit à gauche ou à droite).

Remarque. À toute action à gauche $\alpha\colon G \times X \to X$ de G sur X, on peut associer l'action à droite $\beta\colon X \times G \to X$ par la formule :

$$\beta(x, g) \overset{\text{déf}}{=} \alpha(g^{-1}, x).$$

Réciproquement, à toute action à droite $\beta\colon X \times G \to X$, on peut associer l'action à gauche $\alpha\colon G \times X \to X$ par la formule :

$$\alpha(g, x) \overset{\text{déf}}{=} \beta(x, g^{-1}).$$

(Voir une proposition à cet effet dans la section IV.1.) Dans les deux cas, les orbites de l'action à gauche α coïncident avec les orbites de l'action à droite β. Cette observation peut servir de prétexte pour noter l'ensemble d'orbites d'un G-ensemble gauche X comme « X/G », aussi bien que pour noter l'ensemble d'orbites d'un G-ensemble droit X comme « $G\backslash X$ ».

IV.7. Transporteurs et stabilisateurs

Dans cette section, G est un groupe et X est un G-ensemble.

Définition. Le *transporteur* de $x \in X$ vers $y \in X$ (par l'action de G) est l'ensemble

$$\{\, g \in G \mid gx = y \,\}.$$

Le *fixateur* ou le *stabilisateur* de $x \in X$ (par l'action de G) est l'ensemble

$$\{\, g \in G \mid gx = x \,\}.$$

Remarque. L'usage de la notion de *transporteur* n'est pas courant. Ce terme est défini dans *Algèbre* de Bourbaki,[4] mail il n'y est mentionné qu'une dizaine de fois. Cependant, cette notion peut être utile.[5]

Proposition. *Le stabilisateur de $x \in X$ est un sous-groupe de G.*

Exercice. Prouver cette proposition.

Notation. Le stabilisateur de $x \in X$ dans G peut être noté « G_x » ou « $\mathrm{Stab}_G(x)$ » ou « $\mathrm{Stab}(x)$ ».

Notation. Il est difficile de trouver une notation courante pour les transporteurs, peut-être il n'y en a pas. On peut toutefois envisager de noter le transporteur de x vers y par l'action de G comme « ${}_yG_x$ » (pour une action à gauche, mais comme « ${}_xG_y$ » pour une action à droite) ou comme « $\mathrm{Tran}_G(x,y)$ » ou « $\mathrm{Tran}(x,y)$ ».

Exercice. Soient $x \in X$ et $H = \mathrm{Stab}_G(x)$.

(1) Considérons l'action *canonique* de H sur l'ensemble sous-jacent de G à gauche donnée comme $(h,g) \mapsto hg$. Montrer que les orbites de cette action sont les transporteurs $\mathrm{Tran}_G(y,x)$ pour $y \in Gx$.

(2) Considérons l'action *canonique* de H sur l'ensemble sous-jacent de G à droite donnée comme $(g,h) \mapsto gh$. Montrer que les orbites de cette action sont les transporteurs $\mathrm{Tran}_G(x,y)$ pour $y \in Gx$.

Donner une caractérisation analogiques des orbites des actions canoniques de $H = \mathrm{Stab}_G(x)$ sur l'ensemble sous-jacent de G à gauche et à droite dans le cas où X est un G-ensemble *droit*.

Proposition. *Soient $h, k \in G$, et considérons la permutation $\sigma_{h,k} \colon G \to G$ de (l'ensemble sous-jacent de) G définie par :*

$$\sigma_{h,k}(g) \overset{\text{déf}}{=} kgh.$$

Alors, pour tous $x, y \in X$, $\sigma_{h,k}$ établit une bijection entre $\mathrm{Tran}(hx, y)$ et $\mathrm{Tran}(x, ky)$.

Exercice. Prouver cette proposition.

[4] Bourbaki, *Algèbre*, Chapitre I, § 5, N° 2, p. I.51.

[5] En termes de la *théorie des catégories*, les transporteurs sont les *hom-ensembles* du *groupoïde d'action*.

Corollaire. *Pour tous $g, h \in G$ et pour tous $x, y \in X$,*

$$h \operatorname{Tran}(x, y) g^{-1} = \operatorname{Tran}(gx, hy).$$

En utilisant la notation de la forme « ${}_yG_x$ » au lieu de « $\operatorname{Tran}(x, y)$ », la formule du dernier corollaire s'écrit ainsi :

$$h({}_yG_x)g^{-1} = {}_{hx}G_{gy}.$$

Corollaire. *Pour tout $g \in G$ et pour tout $x \in X$,*

$$g \operatorname{Stab}(x) g^{-1} = \operatorname{Stab}(gx).$$

Corollaire. *Pour tout $g \in G$ et pour tous $x, y \in X$,*

$$\operatorname{Stab}_G(gx) = \operatorname{Stab}_G(gy) \quad \Leftrightarrow \quad \operatorname{Stab}_G(x) = \operatorname{Stab}_G(y).$$

Ainsi, la relation entre les éléments de X de partager le même stabilisateur est une relation d'équivalence invariante par l'action de G.

Corollaire. *Si $x, y, u, v \in X$, $Gx = Gu$ et $Gy = Gv$, alors* $|\operatorname{Tran}(x, y)| = |\operatorname{Tran}(u, v)|$.

Corollaire. *Si $x, y \in X$ et $Gx = Gy$, alors* $|\operatorname{Stab}(x)| = |\operatorname{Stab}(y)|$.

Corollaire. *Pour tout $x \in X$,*

$$|Gx| \cdot |\operatorname{Stab}_G(x)| = |G|.$$

La formule dans ce corollaire a le sens clair lorsque G est d'ordre fini, et elle reste vraie, au sens standard, pour G d'ordre infini.

Démonstration. Soit $x \in X$. Alors

$$G = \bigsqcup_{y \in X} \operatorname{Tran}_G(x, y) = \bigsqcup_{y \in Gx} \operatorname{Tran}_G(x, y),$$

d'où,

$$|G| = \sum_{y \in Gx} |\operatorname{Tran}_G(x, y)| = \sum_{y \in Gx} |\operatorname{Stab}_G(x)| = |Gx| \cdot |\operatorname{Stab}_G(x)|. \qquad \square$$

Corollaire. *Si l'ordre de G est fini, alors :*

(1) *la longueur de toute G-orbite divise l'ordre de G,*

(2) *l'ordre du stabilisateur de tout élément de X divise l'ordre de G.*

Corollaire.

$$\sum_{x \in X} |\operatorname{Stab}_G(x)| = |G \backslash X| \cdot |G|.$$

Exercice. Prouver ce corollaire.

IV.8. Lemme de Cauchy-Frobenius-Burnside

Lemme (*Lemme de Cauchy-Frobenius-Burnside*[6])**.** *Soient G un groupe et X un G-ensemble. Alors* :

$$\sum_{g\in G} |\mathrm{Fix}_X(g)| = \sum_{x\in X} |\mathrm{Stab}_G(x)| = |G\backslash X| \cdot |G|\,.$$

Démonstration. En « comptant » de deux manières différentes le nombre des couples $(g,x) \in G \times X$ tels que $gx = x$, on trouve que :

$$\sum_{g\in G} |\mathrm{Fix}_X(g)| = |\{\,(g,x) \in G \times X \mid gx = x\,\}| = \sum_{x\in X} |\mathrm{Stab}_G(x)|\,.$$

D'après un corollaire d'une proposition dans la section IV.7,

$$\sum_{x\in X} |\mathrm{Stab}_G(x)| = |G\backslash X| \cdot |G|\,. \qquad \square$$

IV.9. Transporteurs, stabilisateurs et fixateurs de parties

Dans cette section, G est un groupe et X est un G-ensemble.

Définition. Le *transporteur* de $Y \subset X$ dans $Z \subset X$ (par l'action de G) est l'ensemble

$$\{\,g \in G \mid gY \subset Z\,\}.$$

Le *transporteur strict* de $Y \subset X$ dans $Z \subset X$ (par l'action de G) est l'ensemble

$$\{\,g \in G \mid gY = Z\,\}.$$

Le *stabilisateur* de $Y \subset X$ (par l'action de G) est l'ensemble

$$\{\,g \in G \mid gY \subset Y\,\}.$$

Le *stabilisateur strict* de $Y \subset X$ (par l'action de G) est l'ensemble

$$\{\,g \in G \mid gY = Y\,\}.$$

Le *fixateur* de $Y \subset X$ (par l'action de G) est l'ensemble

$$\{\,g \in G \mid (\forall y \in Y)(gy = y)\,\}.$$

[6] Aussi connu comme le *lemme de Burnside* et comme le *lemme qui n'est pas de Burnside*.

Clairement, le fixateur de toute partie $Y \subset X$ fait partie du stabilisateur strict de Y, lequel fait partie du stabilisateur ordinaire de Y.

Si Y est une partie finie de X, alors il n'y a pas de différence entre le stabilisateur et le stabilisateur strict de Y.

Si $Y = \{y\} \subset X$, alors il n'y a pas de différence entre le stabilisateur de Y, le fixateur de Y, et le stabilisateur de y.

Pour toute partie Y de X, le fixateur et le stabilisateur strict de Y forment des groupes par rapport à l'opération de composition. En plus, le fixateur de Y est le noyau de l'homomorphisme évident du stabilisateur strict de Y vers le groupe symétrique S_Y.

Le stabilisateur de $Y \subset X$ ne forme un groupe que s'il coïncide avec le stabilisateur strict de Y. Par contre, il forme toujours un *monoïde*.

IV.10. Actions transitives, libres, fidèles

Définition. Soient G un groupe et X un G-ensemble (gauche). L'action de G sur X est dite :

- *transitive* si et seulement si pour tous $x, y \in X$, il existe $g \in G$ tel que $gx = y$,
- *libre* si et seulement si pour tout $g \in G \setminus \{1\}$ et pour tout $x \in X$, on a que $gx \neq x$,
- *fidèle*, ou *effective*, si et seulement si pour tout $g \in G \setminus \{1\}$, il existe $x \in X$ tel que $gx \neq x$.

Les conditions pour une action de G sur X d'être transitive, libre, ou fidèle peuvent être écrites ainsi :

transitive :

$$(\forall x \in X)(\forall y \in X \setminus \{x\})(\exists g \in G \setminus \{1\})(gx = y),$$

libre :

$$(\forall g \in G \setminus \{1\})(\forall x \in X)(\exists y \in X \setminus \{x\})(gx = y),$$

fidèle :

$$(\forall g \in G \setminus \{1\})(\exists x \in X)(\exists y \in X \setminus \{x\})(gx = y).$$

Proposition. *Soient G un groupe et X un G-ensemble. Alors l'action de G sur X est* :

(1) transitive *si et seulement si, pour tous $x, y \in X$,*

$$|\mathrm{Tran}_G(x, y)| \geqslant 1,$$

(2) libre *si et seulement si, pour tous $x, y \in X$,*

$$|\mathrm{Tran}_G(x, y)| \leqslant 1.$$

Exercice. Prouver cette proposition.

Proposition. *Soient G un groupe et X un G-ensemble. Alors l'action de G sur X est fidèle si et seulement si l'homomorphisme associé $G \to S_X$ est injectif (est un monomorphisme).*

Exercice. Prouver cette proposition.

Proposition. *Toute action libre sur un ensemble non vide est fidèle.*

Exercice. Prouver cette proposition.

Exercice. Montrer que l'action canonique d'un groupe sur son ensemble sous-jacent (à gauche) est libre et transitive.

Exercice. Soient G un groupe et X et Y deux G-ensembles (gauches) non vides tels que les actions de G sur X et sur Y sont libres et transitives. Soient $x_0 \in X$ et $y_0 \in Y$. Montrer qu'il existe une unique bijection φ entre X et Y telle que :

(1) $\varphi(gx) = g\varphi(x)$ pour tout $g \in G$ et pour tout $x \in X$,

(2) $\varphi(x_0) = y_0$.

IV.11. Actions commutantes

Dans cette section, G et H sont deux groupes et X est un ensemble muni à la fois d'une action de G à gauche ou à droite et d'une action de H à gauche ou à droite.

Pour tout $g \in G$, posons $\sigma_g \in S_X$ l'action de g sur X selon l'action du groupe G. Pour tout $h \in H$, posons $\tau_h \in S_X$ l'action de h sur X selon l'action du groupe H.

Définition. On dit que les actions de G et de H sur X *commutent* si et seulement si $\sigma_g \circ \tau_h = \tau_h \circ \sigma_g$ pour tous $g \in G$ et $h \in H$.

Proposition. *Si les actions de G et de H sur X commutent, alors la relation d'équivalence sur X d'être dans une même G-orbite est invariante par l'action de H, et la relation d'équivalence d'être dans une même H-orbite est invariante par l'action de G.*

Exercice. Prouver cette proposition.

Pour des raisons syntactiques, il est plus agréable de travailler avec deux actions commutantes lorsqu'une d'elles est une action à gauche, et l'autre est une action à droite. Par exemple, si G opère sur X à gauche et H opère sur X à droite, alors, lorsque le contexte le permet, on peut noter $\sigma_g(x)$ comme « gx » et $\tau_h(x)$ comme « xh », et, avec cette notation, la condition de la commutation des actions s'écrit ainsi :

$$g(xh) = (gx)h \qquad \text{pour tous } g \in G,\ h \in H \text{ et } x \in X.$$

IV.12. Actions de groupes sur des structures algébriques

Lorsqu'on parle d'une *action* (à gauche ou à droite) d'un groupe G sur une *structure algébrique* S (par exemple, sur un autre groupe, ou sur un anneau, ou sur un espace vectoriel), d'habitude on sous-entend une action de G sur l'ensemble sous-jacent de S avec la propriété que chaque élément de G opère sur S par un *automorphisme* de S. Parfois dans ce cas on précise que G opère sur S *par des automorphismes*.

Exemple. Si S est une structure algébrique et $G = \mathrm{Aut}(S)$ est le groupe d'automorphismes de S, alors G opère sur S à gauche selon la règle :

$$(\varphi, x) \mapsto \varphi(x),$$

et G^{op} opère sur S à droite selon la règle :

$$(x, \varphi) \mapsto \varphi(x).$$

Exemple. Tout groupe opère sur lui-même par des automorphismes intérieurs à gauche et à droite selon les règles :

$$(g, x) \mapsto gxg^{-1} \quad \text{et} \quad (x, g) \mapsto g^{-1}xg.$$

Exemple. Si R est un anneau unitaire (pas nécessairement commutatif), alors son groupe multiplicatif $R^\times$ opère sur son groupe additif R à gauche et à droite selon les règles :

$$(u, x) \mapsto ux \quad \text{et} \quad (x, u) \mapsto xu.$$

V. Classes suivant un sous-groupe

V.1. Décomposition d'un groupe suivant un sous-groupe

Dans cette section, G est un groupe, et H est un sous-groupe de G. On va noter l'ensemble sous-jacent de G par « G » aussi.

Toute action du groupe G sur son ensemble sous-jacent, que ce soit à gauche ou à droite, induit, par restriction, une action de H sur l'ensemble G.

Considérons les actions canoniques (par translations à gauche et à droite) de G et de H sur l'ensemble G. Observons que ces actions sont libres.

Dans cette section, il sera sous-entendu que lorsqu'on parle d'une action de G ou de H, à gauche ou à droite, sur l'ensemble G, il s'agit de l'action canonique par translations.

La proposition suivante n'est qu'une expression de la liberté des actions de H sur G :

Proposition. *Soit $x \in G$. Alors :*

(1) *l'application $H \to Hx$ donnée comme $h \mapsto hx$ est une bijection entre H et Hx,*

(2) *l'application $H \to xH$ donnée comme $h \mapsto xh$ est une bijection entre H et xH.*

Le groupe (l'ensemble) G se décompose en H-orbites pour l'action de H à gauche. Il se décompose aussi en H-orbites pour l'action de H à droite.

Notation. L'ensemble des H-orbites dans G pour l'action de H à gauche sera noté « $H\backslash G$ » :

$$H\backslash G \overset{\text{déf}}{=} \{\, Hx \mid x \in G \,\}.$$

L'ensemble des H-orbites dans G pour l'action de H à droite sera noté « G/H » :

$$G/H \overset{\text{déf}}{=} \{\, xH \mid x \in G \,\}.$$

Proposition. *Pour tous $x, y \in G$, $Hx = Hy$ si et seulement si $x^{-1}H = y^{-1}H$.*

Exercice. Prouver cette proposition.

Corollaire. *L'application d'inversion $x \mapsto x^{-1}$ dans G induit deux bijections réciproques entre $H\backslash G$ et G/H par la règle $U \mapsto U^{-}$.*

V.2. Classes suivant un sous-groupe

Définition. Soient G un groupe, $H \leqslant G$, et $x \in G$.

(1) L'ensemble Hx est dit la *classe* de x *à droite* suivant (ou modulo) H.

(2) L'ensemble xH est dit la *classe* de x *à gauche* suivant (ou modulo) H.

Il n'est pas difficile d'apprendre par cœur quelles classes sont *à gauche* et quelles sont *à droite* :

(1) si H agit à *gauche*, les H-orbites sont les classes à *droite*, et

(2) si H agit à *droite*, les H-orbites sont les classes à *gauche*.

Donc, c'est à l'inverse.

En revanche, il est moins facile de justifier ces appellations. Voici une justification tentative :

> Une *classe à gauche* gH est l'image de l'ensemble H par la *translation à gauche* $x \mapsto gx$, et une *classe à droite* Hg est l'image de l'ensemble H par la *translation à droite* $x \mapsto xg$.

(En plus, toute translation à gauche induit une permutation des classes à gauche, et toute translation à droite induit une permutation des classes à droite, de sorte que le groupe G agit sur l'ensemble G/H *à gauche* et sur l'ensemble $H\backslash G$ *à droite*.)

En tout cas, le choix entre « classes à gauche » et « classes à droite » est assez arbitraire, car, en plus des actions canoniques par translations, le groupe G agit sur son ensemble sous-jacent par translations inverses : à droite par la règle $(x, g) \mapsto g^{-1}x$, et à gauche par la règle $(g, x) \mapsto xg^{-1}$.

Remarque. En choisissant les appellations de « classes à droite » et de « classes à gauche » pour les orbites des actions de H à gauche et à droite, on a suivi la convention qui semble être prévalente en ce moment. Parmi les exceptions à cette convention, il y a *The theory of groups* de Marshall Hall[1] et *Algebra*

[1] Hall, *The theory of groups*, p. 10.

de Saunders Mac Lane et Garrett Birkhoff,[2] où les orbites de l'action de H *à gauche* s'appellent *left cosets* (de H), et les orbites de l'action de H *à droite* s'appellent *right cosets* (de H).

V.3. Action d'un groupe sur l'ensemble des classes modulo un sous-groupe

Dans cette section, G est un groupe, et H est un sous-groupe de G.

Proposition. *Pour tous* $g, x, y \in G$,

(1) $Hx = Hy$ *si et seulement si* $Hxg = Hyg$,

(2) $xH = yH$ *si et seulement si* $gxH = gyH$.

Exercice. Prouver cette proposition.

Corollaire. (1) *L'action du groupe* G *sur son ensemble sous-jacent par translations à droite induit une action de* G *sur l'ensemble* $H\backslash G$ *à droite par la règle* $(U, g) \mapsto Ug$.

(2) *L'action de* G *sur son ensemble sous-jacent par translations à gauche induit une action de* G *sur l'ensemble* G/H *à gauche par la règle* $(g, U) \mapsto gU$.

Dans le reste de cette section, on va parler de l'action de G sur G/H à gauche selon la règle

$$g.xH \overset{\text{déf}}{=} gxH.$$

(Les propriétés de l'action de G sur $H\backslash G$ à droite selon la règle $Hx.g \overset{\text{déf}}{=} Hxg$ sont les mêmes, à l'échange du « droite » avec le « gauche » près.)

Observons que :

(1) l'action de G sur G/H est transitive,

(2) $\mathrm{Stab}_G(H) = H$,

(3) $\mathrm{Tran}_G(H, xH) = xH$ pour tout $x \in G$,

[2] Saunders Mac Lane et Garrett Birkhoff. *Algebra*. Anglais. 3e éd. AMS Chelsea Publishing 330. Publié à l'origine par Chelsea Publishing Company, 1988. American Mathematical Society, 10 oct. 2023. 626 p. URL : https://bookstore.ams.org/chel-330/, p. 72.

(4) $\mathrm{Tran}_G(xH, H) = Hx^{-1}$ pour tout $x \in G$,

(5) $\mathrm{Stab}_G(xH) = xHx^{-1}$ pour tout $x \in G$,

(6) $\mathrm{Tran}_G(xH, yH) = yHx^{-1}$ pour tous $x, y \in G$,

(7) le noyau de l'homomorphisme associé $G \to S_{G/H}$ est $\bigwedge_{g \in G} gHg^{-1}$.

V.4. L'indice d'un sous-groupe

Définition. Si G est un groupe et $H \leqslant G$, alors l'*indice* de H dans G est le nombre cardinal de l'ensemble $H\backslash G$ des orbites de l'action de H sur G à gauche, ainsi que le nombre cardinal de l'ensemble G/H des orbites de l'action de H sur G à droite.

Notation. L'indice d'un sous-groupe H dans un groupe G peut être noté « $[G : H]$ »,[3] ou « $(G : H)$ »,[4] ou « $|G : H|$ ».[5] Ici on va adopter la notation « $[G : H]$ ».

Observons que $[G : \mathbf{1}] = |G|$.

Proposition. *Soient G un groupe et $H \leqslant G$. Alors*

$$|G| = [G : H] \cdot |H| .$$

Démonstration. Comme $G = \bigsqcup_{U \in G/H} U$, on a :

$$|G| = \bigsqcup_{U \in G/H} |U| = \bigsqcup_{U \in G/H} |H| = |G/H| \cdot |H| = [G : H] \cdot |H| . \qquad \square$$

Corollaire (Théorème de Lagrange)**.** *Si G est un groupe d'ordre fini et $H \leqslant G$, alors l'ordre de H divise l'ordre de G.*

Corollaire. *Si G est un groupe d'ordre fini et $g \in G$, alors $g^{|G|} = 1$.*

[3] Hall, *The theory of groups*, p. 11 ; Mac Lane et Birkhoff, *Algebra*, p. 73.
[4] Bourbaki, *Algèbre*, p. I.34 ; Lang, *Algebra*, p. 12.
[5] Mikhail Kargapolov et Yuriĭ Merzlyakov. *Éléments de la théorie des groupes*. Trad. du russe par V. Kotliar. Moscou : Éditions Mir, 1985. 263 p. URL : https://archive.org/details/kargapolov-merzliakov-elements-de-la-theorie-des-groupes-mir-1985fc.

Exercice. Prouver le *petit théorème de Fermat* : si p est un nombre premier et r est un entier qui n'est pas multiple de p, alors r^{p-1} est congru à 1 modulo p. En déduire que pour tout nombre premier p et pour tout entier r, r^p est congru à r modulo p.

La dernière proposition peut être généralisée[6] ainsi :

Proposition. *Soient G un groupe, $H \leqslant G$, et $K \leqslant H$. Alors*

$$[G : K] = [G : H] \cdot [H : K].$$

Exercice. Prouver cette proposition.

Proposition. *Soient X un G-ensemble et $x \in G$. Alors la longueur de l'orbite de x est égale à l'indice de sont stabilisateur dans G :*

$$|G.x| = [G : \mathrm{Stab}_G(x)].$$

Exercice. Prouver cette proposition.

V.5. Correspondance des décompositions sous un homomorphisme

Théorème. *Soient G_1 et G_2 deux groupes et $f : G_1 \to G_2$ un homomorphisme. Soient H_1 et K_1 deux sous-groupes de G_1, et H_2 et K_2 deux sous-groupes de G_2 tels que :*

$$f(H_1) = H_2, \qquad f^{-1}(H_2) = H_1, \qquad f(K_1) = K_2, \qquad f^{-1}(K_2) = K_1.$$

Alors $K_1 \leqslant H_1$ si et seulement si $K_2 \leqslant H_2$. Dans le cas où $K_1 \leqslant H_1$ et $K_2 \leqslant H_2$, les règles $U \mapsto f(U)$ et $V \mapsto f^{-1}(V)$ déterminent deux bijections réciproques entre $K_1 \backslash H_1$ et $K_2 \backslash H_2$, ainsi que deux bijections réciproques entre H_1/K_1 et H_2/K_2. En particulier, dans ce cas, $[H_1 : K_1] = [H_2 : K_2]$.

Exercice. Prouver ce théorème.

[6] En posant $K = \mathbf{1}$ dans l'énoncé, on retrouve la proposition précédente.

V.6. Transversales d'un sous-groupe

Dans cette section, G est un groupe, et H est un sous-groupe de G.

Définition. Une *transversale à droite* de H dans G est une partie $T \subset G$ telle que toute classe à droite de H dans G a exactement un élément en commun avec T. De même, une *transversale à gauche* de H dans G est une partie $T \subset G$ telle que toute classe à gauche de H dans G a exactement un élément en commun avec T.

Observons que, pour un sous-groupe donné dans un groupe donné, T est une transversale à droite si et seulement si $T^- = \{ x^{-1} \mid x \in T \}$ est une transversale à gauche (et inversement).

Un choix d'une transversale de H dans G peut servir, par exemple, à construire une (« petite ») partie génératrice de H à partir d'une (« petite ») partie génératrice de G : une telle construction est connue comme le *lemme de Schreier*. Notamment, on peut montrer ainsi que si H est d'indice fini dans G et que G admet une partie génératrice finie, alors H, lui aussi, admet une une partie génératrice finie.

VI. Congruences, sous-groupes normaux, quotients

VI.1. Congruences

Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme.
Définissons une relation $(\sim)$ sur G par l'équivalence :

$$x \sim y \quad \Leftrightarrow \quad f(x) = f(y) \qquad \text{pour tous } x, y \in G.$$

Alors $(\sim)$ est une relation d'équivalence sur G. Mais elle n'est pas une n'importe quelle relation d'équivalence, elle a les propriétés supplémentaires :

(1) si $x \sim u$ et $y \sim v$, alors $xy \sim uv$,

(2) si $x \sim y$, alors $x^{-1} \sim y^{-1}$.

Définition. Une *congruence* sur un groupe G est une relation d'équivalence $(\sim)$ sur G telle que :

(1) pour tous $x, y, u, v \in G$ tels que $x \sim u$ et $y \sim v$, on a $xy \sim uv$,

(2) pour tous $x, y \in G$ tels que $x \sim y$, on a $x^{-1} \sim y^{-1}$.

Exemple. Si n est un entier, la relation de congruence modulo n est une congruence sur le groupe additif $\mathbf{Z}$.

Exercice. Soit $(\sim)$ une congruence sur le groupe additif $\mathbf{Z}$. Montrer qu'il existe $n \in \mathbf{Z}$ tel que $(\sim)$ est la relation de congruence modulo n.

VI.2. Sous-groupes normaux (distingués)

Soient G et H deux groupes et $f\colon G \to H$ un homomorphisme.
Posons $N = \operatorname{Ker} f$ (le noyau de f). Alors N est un sous-groupe de G. Mais N n'est pas un n'importe quel sous-groupe, il a une propriété supplémentaire : si $x \in N$ et $g \in G$, alors $gxg^{-1} \in N$ (et $g^{-1}xg \in N$). En effet, pour tous $x \in N$ et $g \in G$, on a :

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)1_H f(g)^{-1} = 1_H.$$

Définition. Un sous-groupe N d'un groupe G est dit *normal* ou *distingué* dans G si et seulement si pour tous $x \in N$ et $g \in G$, on a que $gxg^{-1} \in N$ (ainsi que $g^{-1}xg \in N$).

Observons que dans un groupe abélien, tout sous-groupe est normal (normal).

Proposition. *Soient G un groupe et H un sous-groupe de G. Alors les conditions suivantes sont équivalentes* :

(1) $gHg^{-1} = H$ *pour tout* $g \in G$,

(2) $gHg^{-1} \supset H$ *pour tout* $g \in G$,

(3) $gHg^{-1} \subset H$ *pour tout* $g \in G$,

(4) H *est normal dans* G.

Exercice. Prouver cette proposition.

Ainsi, les sous-groupes normaux sont les sous-groupes invariants par tous les automorphismes intérieurs.

Notation. On va écrire « $N \trianglelefteqslant G$ » ou « $G \trianglerighteqslant N$ » pour dire que N est un sous-groupe normal (distingué) de G, et on va écrire « $H \lhd G$ » ou « $G \rhd N$ » pour dire que N est un sous-groupe normal de G et que $N \neq G$.

Proposition. *Un sous-groupe H d'un groupe G est normal dans G si et seulement si $gH = Hg$ pour tout $g \in G$.*

Exercice. Prouver cette proposition.

Proposition. *Soient G un groupe et $(\sim)$ une congruence sur G. Posons*

$$N = \{\, x \in G \mid x \sim 1 \,\}.$$

Alors $N \trianglelefteqslant G$.

Exercice. Prouver cette proposition.

Si G est un groupe et H est un sous-groupe de G, on a deux relations d'équivalence sur G qui correspondent aux partitions de G en classes à gauche et à droite suivant H. On va dire que deux éléments $x, y \in G$ sont :

(1) *équivalents suivante H à gauche* si et seulement si $xH = yH$,

(2) *équivalents suivante H à droite* si et seulement si $Hx = Hy$.

Proposition. *Soient G un groupe et H un sous-groupe de G. Alors les conditions suivantes sont équivalentes* :

(1) *la relation d'équivalence dans G suivant H à gauche est une congruence sur G,*

(2) *la relation d'équivalence dans G suivant H à droite est une congruence sur G,*

(3) *les relations d'équivalence dans G suivant H à gauche et suivant H à droite coïncident,*

(4) $H \trianglelefteqslant G$.

Exercice. Prouver cette proposition.

Proposition. *L'intersection de tout ensemble de sous-groupes normaux d'un groupe G est un sous-groupe normal de G.*

Exercice. Prouver cette proposition.

Proposition. *Soient G un groupe, $N \trianglelefteqslant G$ et $H \leqslant G$. Alors $HN = NH \leqslant G$. En plus, si $H \trianglelefteqslant G$, alors $NH \trianglelefteqslant G$.*

Exercice. Prouver cette proposition.

Exercice. Soient G un groupe et H un sous-groupe de G d'indice 2. Montrer que $H \triangleleft G$.

Exercice. Soit G un groupe. Montrer que le groupe des automorphismes intérieurs $\mathrm{Inn}(G)$ est un sous-groupe normal du groupe $\mathrm{Aut}(G)$ de tous les automorphismes de G.

Théorème. *Soient G un groupe et $H \leqslant G$ un sous-groupe. Posons*

$$N = \bigwedge_{g \in G} gHg^{-1}.$$

Alors $N \trianglelefteqslant G$. Si l'indice $m = [G : H]$ est fini, alors l'indice $[G : N]$ est fini et divise $m!$.

Exercice. Prouver ce théorème.

VI.3. Quotients

Considérons un groupe G et une application surjective $p\colon G \to Q$ de (l'ensemble sous-jacent de) G sur un ensemble Q.

On peut se demander si Q admet une structure de groupe qui rend p un homomorphisme de groupes. On peut aussi se demander si une telle structure de groupe sur Q, lorsqu'elle existe, est unique.

Si $(\circ)$ est une opération binaire sur Q par rapport à laquelle Q est un groupe tel que $p\colon G \to Q$ est un homomorphisme, alors

$$p(x) \circ p(y) = p(xy) \qquad \text{pour tous } x, y \in G.$$

Vu que p est surjective, cette condition complètement détermine l'opération $(\circ)$. Il est toutefois possible qu'aucune opération binaire $(\circ)$ ne satisfasse cette condition, et ce qui voudrait dire qu'aucune structure de groupe sur Q ne rendrait $p\colon G \to Q$ un homomorphisme.

Considérons la relation d'équivalence $(\sim_p)$ sur G définie par la condition :

$$x \sim_p y \quad \Leftrightarrow \quad p(x) = p(y) \qquad \text{pour tous } x, y \in G.$$

D'après la section VI.1, si Q admet une structure de groupe qui rend p un homomorphisme, alors la relation $(\sim_p)$ est une congruence sur G.

Supposons donc maintenant que $(\sim_p)$ est une congruence sur G. Définissons alors une opération binaire $(\circ_p)$ sur Q par la règle :

$$p(x) \circ_p p(y) \overset{\text{déf}}{=} p(xy) \qquad \text{pour tous } x, y \in G.$$

(Cette définition est correcte et complète, vu que $(\sim_p)$ est une congruence sur G, et que p est surjective sur Q.)

Il est facile de vérifier que l'ensemble Q muni de l'opération $(\circ_p)$ est un groupe.

Exercice. Vérifier que l'ensemble Q muni de l'opération $(\circ_p)$ est un groupe.

Maintenant considérons un groupe G et une congruence quelconque $(\sim)$ sur G. Posons $Q = G/\!\sim$, et soit $\pi\colon G \to Q$ la *projection canonique* ($\pi(x)$ est la classe d'équivalence de x).

Alors il existe une unique structure de groupe sur $Q = G/\!\sim$ qui rend π un homomorphisme de groupes. Concrètement, dans cette structure, l'opération de groupe est définie par la règle :

$$[x][y] \overset{\text{déf}}{=} [xy] \qquad \text{pour tous } x, y \in G,$$

où $[x] = \pi(x)$ et $[y] = \pi(x)$ sont les classes d'équivalence de x et de y par rapport à la congruence $(\sim)$.

Définition. Soient G un groupe et $(\sim)$ une congruence sur G. Alors le groupe *quotient* de G par $(\sim)$ est l'ensemble quotient $G/\sim$ muni de la structure de groupe qui rend la projection canonique $G \to G/\sim$ un homomorphisme, où l'opération de groupe est définie par la règle :

$$[x][y] \overset{\text{déf}}{=} [xy] \qquad \text{pour tous } x, y \in G,$$

où $[x]$ et $[y]$ sont les classes d'équivalence de x et de y par rapport à $(\sim)$.

Définition. Soient G un groupe et $N \trianglelefteqslant G$. Alors le groupe *quotient* de G par N est l'ensemble quotient G/N muni de la structure de groupe qui rend la projection canonique $G \to G/N$ un homomorphisme, où l'opération de groupe est définie par la règle :

$$(xN)(yN) \overset{\text{déf}}{=} xyN \qquad \text{pour tous } x, y \in G.$$

D'après la section VI.2, le noyau de tout homomorphisme de groupes $G \to H$ est un sous-groupe normal dans G. Maintenant on voit que tout sous-groupe normal d'un groupe G est le noyau d'un épimorphisme $G \twoheadrightarrow Q$:

Proposition. *Soient G un groupe et $N \trianglelefteqslant G$. Soit $\pi\colon G \twoheadrightarrow G/N$ la projection canonique. Alors* $\operatorname{Ker}\pi = N$.

Observons que tout sous-groupe d'un quotient est un quotient d'un sous-groupe :

Proposition. *Soient G un groupe, $N \trianglelefteqslant G$ et $K \leqslant G/N$. Soit $\pi\colon G \twoheadrightarrow G/N$ la projection canonique, et posons $H = \pi^{-1}(K)$. Alors $K = H/N$.*

Définition. Un *sous-quotient* d'un groupe G est un quotient d'un sous-groupe de G.

VI.4. Groupes simples

Définition. Un groupe G est dit *simple* si et seulement si il a exactement deux sous-groupes normaux différents : le sous-groupe trivial $\mathbf{1}$ et G lui-même.

Autrement dit, les groupes triviaux (réduits à un seul élément) ne sont pas simples, et un groupe non trivial G est simple si et seulement si tout homomorphisme non trivial $G \to H$ est un monomorphisme.

Remarque. Des nombreux auteurs considéraient les groupes triviaux simples.

Proposition. *Un groupe abélien est simple si et seulement si il est isomorphe à* $\mathbf{Z}/p\mathbf{Z}$ *pour un certain* p *premier.*

Exercice. Prouver cette proposition.

Exercice. Montrer que le groupe alterné A_n est simple pour tout $n \geqslant 5$, ainsi que pour $n = 3$. Montrer que A_4 n'est pas simple.

Exercice. Montrer qu'aucun groupe infini qui possède un sous-groupe d'indice fini n'est simple.

Il existe une classification prétendue[1] des groupes finis simples.

VI.5. Correspondance des sous-quotients sous un homomorphisme

Théorème. *Soient* G_1 *et* G_2 *deux groupes et* $f\colon G_1 \to G_2$ *un homomorphisme. Soient* H_1 *et* K_1 *deux sous-groupes de* G_1*, et* H_2 *et* K_2 *deux sous-groupes de* G_2 *tels que :*

$$f(H_1) = H_2, \qquad f^{-1}(H_2) = H_1, \qquad f(K_1) = K_2, \qquad f^{-1}(K_2) = K_1.$$

Alors $K_1 \leqslant H_1$ *si et seulement si* $K_2 \leqslant H_2$*. Supposons que* $K_1 \leqslant H_1$ *et* $K_2 \leqslant H_2$*. Alors* $K_1 \trianglelefteqslant H_1$ *si et seulement si* $K_2 \trianglelefteqslant H_2$*. Supposons que* $K_1 \trianglelefteqslant H_1$ *et* $K_2 \trianglelefteqslant H_2$*. Alors* $H_1/K_1 \simeq H_2/K_2$*, et les règles* $U \mapsto f(U)$ *et* $V \mapsto f^{-1}(V)$ *déterminent deux isomorphismes réciproques entre* H_1/K_1 *et* H_2/K_2*.*

Exercice. Prouver ce théorème.

VI.6. Théorèmes d'isomorphisme

Théorème. *Soient* G *et* K *deux groupes et* $f\colon G \to K$ *un homomorphisme. Alors*

$$G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

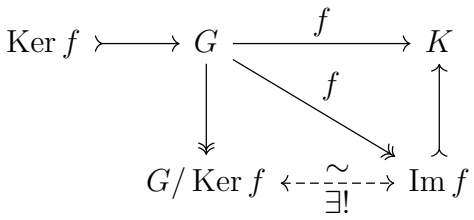
Plus précisément, il existe un unique isomorphisme

$$\hat{f}\colon G/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$$

tel que $f = \hat{f} \circ \pi$*, où* π *est la projection canonique* $G \twoheadrightarrow G/\operatorname{Ker} f$*.*

[1] L'auteur de ces notes de l'a jamais étudiée.

Voici un schéma pour ce théorème :



Ce théorème est un corollaire du premier théorème de la section III.6.

Théorème. *Soient G un groupe, $N \trianglelefteqslant G$, et $H \leqslant G$. Alors $H \wedge N \trianglelefteqslant H$, et*

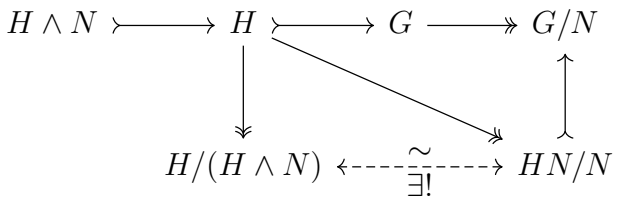
$$H/(H \wedge N) \simeq HN/N.$$

Plus précisément, si $f\colon H \to G/N$ est l'homomorphisme « évident », donné par la formule $f(h) = hN$, alors $\operatorname{Im} f = HN/N$ et $\operatorname{Ker} f = H \wedge N$, et donc il existe un unique isomorphisme

$$\hat{f}\colon H/(H \wedge N) \xrightarrow{\sim} HN/N$$

tel que $f = \hat{f} \circ \pi$, où $\pi\colon H \twoheadrightarrow H/(H \wedge N)$ est la projection canonique.

Voici un schéma pour ce théorème :



Théorème. *Soient G un groupe, $N \trianglelefteqslant G$, et $N \leqslant M \trianglelefteqslant G$ (et donc, $N \trianglelefteqslant M$). Alors $M/N \trianglelefteqslant G/N$, et*

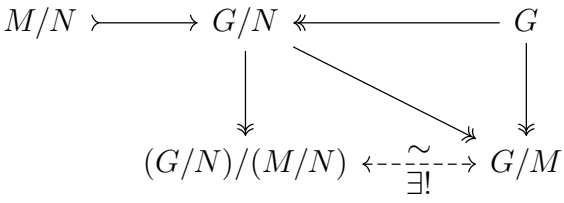
$$(G/N)/(M/N) \simeq G/M.$$

Plus précisément, si $f\colon G/N \twoheadrightarrow G/M$ est l'épimorphisme « évident », donné par la formule $f(gN) = gM$, alors $\operatorname{Ker} f = M/N$, et donc il existe un unique isomorphisme

$$\hat{f}\colon (G/N)/(M/N) \xrightarrow{\sim} G/M$$

tel que $f = \hat{f} \circ \pi$, où $\pi\colon G/N \twoheadrightarrow (G/N)/(M/N)$ est la projection canonique.

Voici un schéma pour ce théorème :



VII. Commutation et conjugaison

VII.1. Commutation et commutateurs

Définition. On dit que deux éléments x et y d'un groupe *commutent* si et seulement si $yx = xy$.

Observons que la relation de commutation est symétrique et réflexive :

(1) si x commute avec y, alors y commute avec x,

(2) tout élément commute avec lui-même.

Proposition. *Soient x et y deux éléments d'un groupe qui commutent. Alors x^m commute avec y^n pour tous $m, n \in \mathbf{Z}$.*

Exercice. Prouver cette proposition.

Corollaire. *Soient x et y deux éléments d'un groupe. Alors les conditions suivantes sont équivalentes* :

(1) *x commute avec y,*

(2) *x commute avec y^{-1},*

(3) *x^{-1} commute avec y,*

(4) *x^{-1} commute avec y^{-1}.*

Si x et y sont deux éléments d'un groupe, alors on a les équivalences suivantes :

$$xy = yx \quad \Leftrightarrow \quad xyx^{-1} = y \quad \Leftrightarrow \quad xyx^{-1}y^{-1} = 1,$$

et

$$xy = yx \quad \Leftrightarrow \quad y^{-1}xy = x \quad \Leftrightarrow \quad x^{-1}y^{-1}xy = 1.$$

Définition. Si x et y sont deux éléments d'un groupe, alors on va appeler l'élément $xyx^{-1}y^{-1}$ le *commutateur* de x et y.

Observons que le commutateur de x^{-1} et y^{-1} est $x^{-1}y^{-1}xy$.

Remarque. La définition des commutateurs donnée ci-dessus est partiellement arbitraire : on pourrait aussi bien définir le commutateur de x et y comme $x^{-1}y^{-1}xy$. Cependant, dans les contextes où on les utilise, le choix entre les deux formes souvent n'a pas d'importance.

Notation. Le commutateur de x et y est noté « $[x, y]$ ».

Observons que si $f\colon G \to H$ est un homomorphisme entre deux groupes G et H, alors $f([x, y]) = [f(x),\ f(y)]$ pour tous $x, y \in G$.

VII.2. Sous-groupe dérivé et abélianisation

Étant donné un groupe G, on peut en dériver divers sous-groupes et groupe quotients. Entre autres, on peut en dériver son sous-groupe engendré par l'ensemble des commutateurs. Vu le rôle important de ce sous-groupe, il est dit le sous-groupe *dérivé* tout court.

Définition. Si G est un groupe, alors le sous-groupe engendré par tous les commutateurs d'éléments de G est dit le sous-groupe *dérivé* de G.

Notation. Le sous-groupe dérivée d'un groupe G peut être noté « $[G, G]$ » ou « $G^{(1)}$ » ou « G' ».

Le sous-groupe dérivé du sous-groupe dérivé d'un groupe G peut être noté « $G^{(2)}$ » ou « G'' ».

Si H et K sont deux sous-groupes d'un groupe G, alors le sous-groupe de G engendré par tous les commutateurs $[h, k]$ avec $h \in H$ et $k \in K$ peut être noté « $[H, K]$ ».

Proposition. *Le sous-groupe dérivé d'un groupe G est un sous-groupe normal de G.*

Démonstration. Comme l'image d'un commutateur $[x, y]$ sous un homomorphisme f est le commutateur $[f(x),\ f(y)]$, l'ensemble des commutateurs de G est stable sous tout endomorphisme de G. En particulier, il est invariant sous tout automorphisme de G. Donc, le sous-groupe engendré par l'ensemble des commutateurs est invariant sous tout automorphisme de G. Or, pour qu'un sous-groupe de G soit normal, il suffit qu'il soit invariant (ou stable) sous tout automorphisme intérieur de G. Donc, le sous-groupe engendré par l'ensemble des commutateurs est normal. □

Théorème. *Soient G et H deux groupes, G' le sous-groupe dérivée de G, et $f\colon G \to H$ un homomorphisme. Alors* $\operatorname{Im} f$ *est abélien si et seulement si* $G' \leqslant \operatorname{Ker} f$.

Exercice. Prouver ce théorème.

Proposition. *Soient G un groupe, G' le sous-groupe dérivée de G, et H un sous-groupe de G tel que $G' \leqslant H$. Alors $H \trianglelefteqslant G$.*

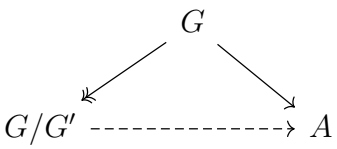
Exercice. Prouver cette proposition.

Le sous-groupe dérivé G' de G, étant normal, est le noyau de la projection canonique $G \twoheadrightarrow G/G'$. Le groupe quotient G/G' est abélien.

Définition. Si G est un groupe de G' est son sous-groupe dérivé, alors le quotient G/G' est dit l'*abélianisé* de G.

Théorème. *Soient G un groupe, G' son sous-groupe dérivée, et π la projection canonique $G \twoheadrightarrow G/G'$. Soient A un groupe abélien et $f\colon G \to A$ un homomorphisme. Alors il existe un (unique) homomorphisme $\hat{f}\colon G/G' \to A$ tel que $f = \hat{f} \circ \pi$.*

Voici un schéma pour ce théorème :



Exercice. Prouver ce théorème.

VII.3. Conjugaison

Définition. Deux éléments x et y d'un groupe G sont dits *conjugués*[1] dans G si et seulement si il existe $z \in G$ tel que $yz = zx$.

Exercice. Montrer que la relation d'être conjugués est symétrique, réflexive, et transitive.

Pour tous éléments x, y, z d'un groupe, on a les équivalences :

$$y = zxz^{-1} \quad \Leftrightarrow \quad yz = zx \quad \Leftrightarrow \quad z^{-1}yz = x.$$

Définition. Si x et y sont deux éléments d'un groupe, on va appeler l'élément yxy^{-1} le *conjugué* de x par y *à gauche*, et on va appeler l'élément $y^{-1}xy$ le *conjugué* de x par y *à droite*.

[1] Ils devraient être dits plutôt « conjougués », car ils font penser à deux bœufs attelés par un même *joug* (z).

Observons que le conjugué de x par y à droite est le conjugué de x par y^{-1} à gauche.

On peut dire « conjugué » tout court, au lieu de « conjugué à gauche » ou « conjugué à droite » si cela se fait sans ambiguïté.

Dans ce texte on va privilégier la conjugaison à gauche.

Notation. On va adopter les notations suivantes :

$$x^y \overset{\text{déf}}{=} y^{-1}xy, \qquad {}^yx \overset{\text{déf}}{=} yxy^{-1}.$$

Définition. Si G est un groupe, $a, b \in G$ et $ab = 1$, alors l'application $G \to G$ donnée par la règle $x \mapsto axb$ est dite une application de *conjugaison par a à gauche*, ou une application de *conjugaison par b à droite*.

Pour tout groupe G, les application $G \to G$ de conjugaison par des éléments de G sont des automorphismes de G, dits les automorphismes *intérieurs*.

Ainsi, tout groupe opère sur lui-même par des automorphismes intérieurs à gauche et à droite selon les règles :

$$(g, x) \mapsto gxg^{-1} \quad \text{et} \quad (x, g) \mapsto g^{-1}xg.$$

On va appeler ces actions les actions par *conjugaison* à gauche et à droite.

Définition. Si G est un groupe et $x \in G$, alors la *classe de conjugaison* de x dans G est l'ensemble des élément de G conjugués à x dans G :

$$\{\, gxg^{-1} \mid g \in G \,\} = \{\, axb \mid a, b \in G,\ ab = 1 \,\} = \{\, g^{-1}xg \mid g \in G \,\}.$$

Ainsi, la classe de conjugaison de x dans G est l'orbite de x sous l'action de G sur lui-même par conjugaison à gauche ou à droite (les orbites sont les mêmes).

Notation. La classe de conjugaison de $x \in G$ dans G peut être notée « ${}^Gx$ » ou « x^G ».

VII.4. Centralisateurs et centre

Dans cette section, G est un groupe.

Proposition. *Pour tout $x \in G$, l'ensemble des éléments de G qui commutent avec x forme un sous-groupe de G.*

Exercice. Prouver cette proposition.

Corollaire. *Pour toute partie $U \subset G$, l'ensemble des éléments de G qui commutent avec chaque élément de U forme un sous-groupe de G.*

Corollaire. *L'ensemble des éléments de G qui commutent avec tous les éléments de G forme un sous-groupe de G.*

Définition. Le *centralisateur* d'un élément $x \in G$ dans G est l'ensemble des éléments de G qui commutent avec x :

$$\{\, g \in G \mid gx = xg \,\} = \{\, g \in G \mid gxg^{-1} = x \,\} = \{\, g \in G \mid x = g^{-1}xg \,\}.$$

Ainsi, le centralisateur de x dans G est le stabilisateur de x sous l'action de G sur lui-même par conjugaison à gauche ou à droite (les stabilisateurs sont les mêmes).

Observons que le centralisateur d'un élément d'un groupe non trivial ne peut pas être trivial.

Définition. Le *centralisateur* d'une partie U de G dans G est l'ensemble des éléments de G qui commutent avec chaque élément de U :

$$\{\, g \in G \mid (\forall u \in U)(gu = ug) \,\}.$$

Notation. Le centralisateur de $x \in G$ dans G peut être noté « $C_G(x)$ » ou « $Z_G(x)$ ».[2] Le centralisateur de $U \subset G$ dans G peut être noté « $C_G(U)$ » ou « $Z_G(U)$ ».

Pour le reste de ce chapitre, on va adopter les notations « $Z_G(x)$ » et « $Z_G(U)$ » pour les centralisateurs. Cependant, les notations « $C_G(x)$ » et « $C_G(U)$ » sont actuellement plus courantes.

Définition. Le sous-groupe de G formé de tous les élément de G qui commutent avec tous les élément de G est dit le *centre* de G.

Notation. Le centre de G est noté « $Z(G)$ ».

Ainsi, $Z(G) = Z_G(G) = \bigwedge_{x \in G} Z_G(x)$.

Proposition. *Si $H \leqslant Z(G)$, alors $H \trianglelefteqslant G$. En particulier, $Z(G) \trianglelefteqslant G$.*

Exercice. Prouver cette proposition.

Comme la longueur de l'orbite est l'indice du stabilisateur, la proposition suivante en découle :

[2] Le « Z » vient de « *Zentrum* » en allemand.

Proposition. *Pour tout $x \in G$,*

$$\left|x^G\right| = [G : Z_G(x)].$$

Lemme (*« Équation aux classes »*)**.** *Soit T un ensemble de représentants des classes de conjugaison des éléments de $G \setminus Z(G)$:*

$$G = Z(G) \sqcup \bigsqcup_{x \in T} x^G.$$

Alors

$$|G| = |Z(G)| + \sum_{x \in T} [G : Z_G(x)] \quad \textit{et} \quad |G \setminus Z(G)| = \sum_{x \in T} [G : Z_G(x)].$$

Corollaire. *Soit G un groupe fini non abélien. Alors :*

(1) *l'ordre du centre de G se factorise par tout commun diviseur[3] des indices des centralisateurs de tous les éléments non centraux de G,*

(2) *l'indice du centre de G divise tout commun multiple[4] des ordres des centralisateurs de tous les éléments non centraux de G.*

Indication d'une démonstration. Le premier énoncé est facile à voir.

Le deuxième résulte du premier par une espèce de *dualité* : si $a, \bar{a}, b, \bar{b} \in \mathbf{Z}$ et $0 \neq a\bar{a} = b\bar{b}$, alors a divise b si et seulement si $\bar{b}$ divise $\bar{a}$. En considérant un commun multiple m des ordres des centralisateurs de tous les éléments non centraux de G, on peut supposer, sans perte de généralité, que m divise l'ordre de G (sinon, il suffit de passer à un PGCD de m et $|G|$). □

Il est intéressant de combiner l'« équation aux classes » avec la factorisation

$$|G| = \overbrace{[G : Z_G(x)] \cdot \underbrace{[Z_G(x) : Z(G)]}_{|Z_G(x)|} \cdot |Z(G)|}^{[G:Z(G)]} \qquad \text{(pour tout } x \in G\text{)}.$$

Lemme. *Soient G un groupe fini non abélien, p un nombre premier, et $m, n \in \mathbf{N}$ tels que p^m divise $|G|$, p^{n+1} ne divise pas $|Z(G)|$, et que $n \leqslant m$. Alors il existe $x \in G \setminus Z(G)$ tel que p^{m-n} divise $|Z_G(x)|$.*

[3] Observons que se factoriser par tout commun diviseur équivaut à se factoriser par un PGCD (par le positif ou par le négatif).

[4] Observons que diviser tout commun multiple équivaut à diviser un PPCM.

Ce lemme peut être énoncé plus aisément en termes de la *valuation p-adique*.

Définition. Pour un entier premier p et pour un entier non nul a, la *valuation p-adique* de a est $n \in \mathbf{N}$ tel que p^n divise a, mais p^{n+1} ne divise pas a.

Notation. Pour un entier premier p et pour un entier non nul a, on va noter « $v_p(a)$ »[5] la valuation p-adique de a.

Avec cette notation, le dernier lemme dit que si G est fini non abélien et p est un nombre premier, alors il existe $x \in G \setminus Z(G)$ tel que

$$v_p(|Z_G(x)|) + v_p(|Z(G)|) \geqslant v_p(|G|).$$

Exercice. Prouver le dernier lemme.

Corollaire. *Soient G un groupe fini non abélien, p un nombre premier et $n \in \mathbf{N}$ tels que p^{2n+1} divise $|G|$. Alors il existe $x \in G \setminus Z(G)$ tel que p^{n+1} divise $|Z_G(x)|$.*

En termes de la valuation p-adique, ce corollaire dit que si G est fini non abélien et p est un nombre premier, alors il existe $x \in G \setminus Z(G)$ tel que

$$2v_p(|Z_G(x)|) \geqslant v_p(|G|).$$

VII.5. Normalisateurs

Dans cette section, G est un groupe.

Définition. Soit $U \subset G$.

- Un élément $g \in G$ est dit *normaliser* U si et seulement si $gU = Ug$.
- Une partie $V \subset G$ est dite *normaliser* U si et seulement si $gU = Ug$ pour tout $g \in V$.

Proposition. *Pour toute partie $U \subset G$, l'ensemble*

$$\{\, g \in G \mid gUg^{-1} = U \,\} = \{\, g \in G \mid gU = Ug \,\} = \{\, g \in G \mid U = g^{-1}Ug \,\}$$

est un sous-groupe de G.

Exercice. Prouver cette proposition.

[5] On suit ici la notation de Bourbaki. (Bourbaki, *Algèbre*, Chapitre I, § 4, N° 10, p. I.49)

Définition. Le *normalisateur* d'une partie U de G dans G est l'ensemble des éléments de G conjugaison par lesquels laisse U invariante :

$$\{\, g \in G \mid gUg^{-1} = U \,\} = \{\, g \in G \mid gU = Ug \,\} = \{\, g \in G \mid U = g^{-1}Ug \,\}.$$

Notation. Le normalisateur de $U \subset G$ dans G est noté « $N_G(U)$ ».

Observons que pour tous $H \leqslant G$ et $K \leqslant G$, on a l'équivalence :

$$H \trianglelefteqslant K \quad \Leftrightarrow \quad H \leqslant K \leqslant N_G(H).$$

Proposition. *Pour toute partie $U \subset G$, $Z_G(U) \trianglelefteqslant N_G(U)$.*

Exercice. Prouver cette proposition.

Proposition. *Soient un G-ensemble X et une partie $U \subset G$. Alors les parties $\mathrm{Fix}_X U$ et $\mathrm{Supp}_X U$ de X sont invariantes par l'action de tout $g \in N_G(U)$.*

Exercice. Prouver cette proposition.

Lorsque G opère sur un ensemble X, la relation d'avoir le même stabilisateur est une relation d'équivalence sur X, et cette relation d'équivalence est invariante par l'action de G. Ainsi, G opère sur l'ensemble des classes d'équivalence. On peut alors montrer que les stabilisateurs des classes d'équivalence des éléments de X sont les normalisateurs des stabilisateurs des éléments de X :

Proposition. *Soit X un G-ensemble. Considérons la relation d'équivalence $(\sim)$ sur X définie par l'équivalence* :

$$x \sim y \quad \Leftrightarrow \quad \mathrm{Stab}_G(x) = \mathrm{Stab}_G(y).$$

Cette relation d'équivalence étant invariante par l'action de G, considérons le quotient $X/\!\sim$ comme un G-ensemble par rapport à l'action induite. Alors

$$\mathrm{Stab}_G([x]) = N_G(\mathrm{Stab}_G(x))$$

pour tout $x \in X$, où $[x] \in X/\!\sim$ est la classe d'équivalence de x.

Exercice. Prouver cette proposition.

VIII. Extension de groupes

VIII.1. « Extensions » en théorie des groupes

L'usage du terme « *extension* » en théorie des groupes a évolué au cours de l'histoire.

À l'origine, l'usage du terme « *extension* » en théorie des groupes ressemblait son usage habituel en théorie des corps : lorsque H était un sous-groupe d'un groupe G, on pouvait dire que G soit une *extension* de H.[1] Plus généralement, G était dit une *extension* de H lorsque il existait un monomorphisme $H \rightarrowtail G$.

Puis, ce terme a été utilisé davantage dans le cadre d'un sous-groupe normal N de G, où on disait toujours que G soit une *extension* de N, mais en plus, si $K \simeq G/N$, on disait que G soit une *extensions* de N *par* K. Plus généralement, si H et K était deux groupes, on disait qu'un groupe G soit une *extensions* de H par K lorsque G avait un sous-groupe normal N isomorphe à H tel que le quotient G/N soit isomorphe à K.

Autrement dit, dans ce dernier sens, un groupe G était dit une *extension* de H par K si et seulement si il existait un monomorphisme $\iota\colon H \rightarrowtail G$ et un épimorphisme $\pi\colon G \twoheadrightarrow K$ tels que $\operatorname{Im}\iota = \operatorname{Ker}\pi$. Voici un schéma pour cette situation :

$$H \overset{\iota}{\rightarrowtail} G \overset{\pi}{\twoheadrightarrow} K \qquad (\operatorname{Im}\iota = \operatorname{Ker}\pi).$$

Ici, on va adopter une terminologie « moderne », selon laquelle, dans la situation décrite ci-dessus, G est dit plutôt une extension *de* K *par* H.

Définition. Soit H un groupe. Un groupe G sera dit une *extension* de H si et seulement si il existe un épimorphisme $G \twoheadrightarrow H$. Un groupe G sera dit une *extension* de H par un groupe K si et seulement si il existe un épimorphisme $G \twoheadrightarrow H$ dont le noyau est isomorphe à K. Plus précisément,

(1) une *extension* d'un groupe H est un groupe G *avec* un épimorphisme $\pi\colon G \twoheadrightarrow H$,

[1] Hall, *The theory of groups*, section 15.1, p. 218.

(2) une *extension* d'un groupe H par un groupe K est un groupe G *avec* un épimorphisme $\pi\colon G \twoheadrightarrow H$ et *avec* un monomorphisme $\iota\colon K \rightarrowtail G$ tels que $\operatorname{Im}\iota = \operatorname{Ker}\pi$:

$$K \xrightarrow{\ \iota\ } G \xrightarrow{\ \pi\ } H \qquad (\operatorname{Im}\iota = \operatorname{Ker}\pi).$$

Exemple. Quels que soient deux groupes H et K, considérons leur produit direct $H \times K$, l'épimorphisme $\pi\colon H \times K \twoheadrightarrow H$ donné par la règle $(h, k) \mapsto h$, et le monomorphisme $\iota\colon K \to H \times K$ donné par la règle $k \mapsto (1, k)$. Alors $\operatorname{Im}\iota = \operatorname{Ker}\pi$, et donc le groupe $H \times K$, avec le monomorphisme ι et l'épimorphisme π, est une extension de H par K :

$$K \xrightarrow{k \mapsto (1,k)} H \times K \xrightarrow{(h,k) \mapsto h} H.$$

Au même temps, $H \times K$ est une extension de K par H :

$$H \xrightarrow{h \mapsto (h,1)} H \times K \xrightarrow{(h,k) \mapsto k} K.$$

VIII.2. Épimorphismes scindés et extensions scindées

Définition. Soit $p\colon G \twoheadrightarrow H$ un épimorphisme. Une *sections* de p est un homomorphisme $s\colon H \to G$ (qui sera forcement un monomorphisme) tel que $p \circ s = \mathrm{id}_H$.

Proposition. *Soient $p\colon G \twoheadrightarrow H$ un épimorphisme de groupes et $s_1, s_2\colon H \rightarrowtail G$ deux sections de p telles que $\operatorname{Im} s_2 = \operatorname{Im} s_1$. Alors $s_2 = s_1$.*

Exercice. Prouver cette proposition.

Définition. Un épimorphisme est dit *scindé* si et seulement si il admet une section.

Exercice. Montrer que l'unique épimorphisme $\mathbf{Z}/4\mathbf{Z} \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$ n'est pas scindé.

Exercice. Soit $n \geqslant 2$ un entier. Considérons l'épimorphisme du groupe symétrique S_n sur le groupe additif $\mathbf{Z}/2\mathbf{Z}$ qui à chaque permutation $\sigma \in S_n$ associe un des deux éléments de $\mathbf{Z}/2\mathbf{Z}$ selon la parité de σ. Montrer que cet épimorphisme est scindé.

Définition. Une extension $(G,\ p\colon G \twoheadrightarrow H)$ d'un groupe H est dite *scindée* si et seulement si son épimorphisme p est scindé.

Quels que soient deux groupes H et K, leur produit direct $H \times K$ est une extension scindée de H (par K) et de K (par H).

Proposition. *Soient G et H deux groupes et $p\colon G \twoheadrightarrow H$ un épimorphisme scindé avec une section $s\colon H \rightarrowtail G$. Posons $N = \operatorname{Ker} p$ et $K = \operatorname{Im} s$. Alors $N \wedge K = \mathbf{1}$ et $NK = KN = G$.*

Exercice. Prouver cette proposition.

Proposition. *Soient G un groupe, $N \trianglelefteqslant G$ et $K \leqslant G$ tels que*

$$N \wedge K = \mathbf{1} \quad \textit{et} \quad NK = KN = G.$$

Alors $G/N \simeq K$ et, en plus, la projection canonique $G \twoheadrightarrow G/N$ est scindée et admet une (unique) section $s\colon G/N \rightarrowtail G$ telle que $\operatorname{Im} s = K$.

Exercice. Prouver cette proposition.

Sous les hypothèses de la dernière proposition, on peut dire que le groupe G est un *produit semi-direct interne* de ses sous-groupes N et K, avec K *normalisant* N.

VIII.3. Produits semi-directs

Définition. Soient G un groupe et N et K deux sous-groupes de G.

(1) Si K est contenu dans le normalisateur de N dans G ($K \leqslant N_G(N)$), et que N et K n'ont que l'élément identité pour un élément commun, alors le sous-groupe $NK = KN$ de G est dit le *produit semi-direct interne* de N et K dans G, avec K *normalisant* N.

(2) Dans le cas contraire, il n'y a pas de produit semi-direct interne de N et K avec K *normalisant* N (mais il peut y en avoir un avec N normalisant K).

Observons certaines implications des conditions qui forment la définition d'un produit semi-direct interne :

(1) Soient N et K deux sous-groupes d'un groupe G tels que $K \leqslant N_G(N)$. Alors K agit sur N par conjugaisons à gauche et à droite. En utilisant les notations

$$^{y}x \overset{\text{déf}}{=} yxy^{-1} \quad \text{et} \quad x^{y} \overset{\text{déf}}{=} y^{-1}xy,$$

on a, pour tous $n_1, n_2 \in N$ et $k_1, k_2 \in K$:

$$(n_1k_1)(n_2k_2) = (n_1\,{}^{k_1}n_2)(k_1k_2) \quad \text{et} \quad (k_1n_1)(k_2n_2) = (k_1k_2)(n_1^{k_2}\,n_2).$$

(2) Si N et K sont deux sous-groupes d'un groupe G tels que $N \wedge K = \mathbf{1}$, alors chaque élément de l'ensemble $NK \subset G$ s'écrit d'une unique façon sous la forme « nk » avec $n \in N$ et $k \in K$, et chaque élément de l'ensemble $KN \subset G$ s'écrit d'une unique façon sous la forme « kn » avec $k \in K$ et $n \in N$.

Notation. Le produit semi-direct interne de deux sous-groupes N et K d'un même groupe, avec K normalisant N, peut être noté « $N \rtimes K$ » ou « $K \ltimes N$ ».

Exercice. Montrer que le groupe diédral d'ordre $2n$ se décompose en un produit semi-direct interne $\langle r\rangle \rtimes \langle s\rangle$ de deux sous-groupes cycliques d'ordres n et 2.

Pour définir une version *externe* du *produit semi-direct*, on va utiliser la définition suivante :

Définition. Soit G un groupe.

(1) Un *G-groupe gauche* est un groupe muni d'une action de G à gauche par des automorphismes.

(2) Un *G-groupe droit* est un groupe muni d'une action de G à droite par des automorphismes.

Remarque. Toute action d'un groupe à gauche induit une action à droite et vice versa : on peut définir l'action par un élément g à droite comme l'action par g^{-1} à gauche, et réciproquement.

Dans le reste de cette section, lorsque G est un groupe et H est un G-groupe gauche, on va noter l'image de $h \in H$ par l'action de $g \in G$ comme « $g.h$ ». Dans le cas où H est un G-groupe droit, on va noter l'image de $h \in H$ par l'action de $g \in G$ comme « $h.g$ ». On va préciser dans le contexte qui agit sur qui.

Proposition. *Soient K un groupe et N un K-groupe gauche. Définissons une opération binaire $(\circ)$ sur le produit cartésien des ensembles sous-jacents de N et K par la formule* :

$$(n_1, k_1) \circ (n_2, k_2) \overset{\text{déf}}{=} \big(n_1(k_1.n_2),\, k_1k_2\big), \qquad \text{où } n_1, n_2 \in N \text{ et } k_1, k_2 \in K.$$

Alors le produit cartésien des ensembles $N \times K$ muni de l'opération $(\circ)$ est un groupe.

Exercice. Prouver cette proposition.

Proposition. *Soient K un groupe et N un K-groupe droit. Définissons une opération binaire $(\circ)$ sur le produit cartésien des ensembles sous-jacents de K et N par la formule* :

$$(k_1, n_1) \circ (k_2, n_2) \overset{\text{déf}}{=} \big(k_1 k_2,\ (n_1.k_2)n_2\big), \qquad \text{où } n_1, n_2 \in N \text{ et } k_1, k_2 \in K.$$

Alors le produit cartésien des ensembles $K \times N$ muni de l'opération $(\circ)$ est un groupe.

Exercice. Prouver cette proposition.

Définition. Soit K un groupe.

(1) Si N est un K-groupe gauche, alors le *produit semi-direct externe* de N et K est le groupe dont l'ensemble sous-jacent est le produit cartésien des ensembles sous-jacents de N et K, et dont l'opération de composition est définie par la formule :

$$(n_1, k_1)(n_2, k_2) \overset{\text{déf}}{=} \big(n_1(k_1.n_2),\ k_1 k_2\big).$$

(2) Si N est un K-groupe droit, alors le *produit semi-direct externe* de K et N est le groupe dont l'ensemble sous-jacent est le produit cartésien des ensembles sous-jacents de K et N, et dont l'opération de composition est définie par la formule :

$$(k_1, n_1)(k_2, n_2) \overset{\text{déf}}{=} \big(k_1 k_2,\ (n_1.k_2)n_2\big).$$

Notation. Si K est un groupe et N est un K-groupe gauche, alors le produit semi-direct externe de N et K est noté « $N \rtimes K$ ». Si K est un groupe et N est un K-groupe droit, alors le produit semi-direct externe de K et N est noté « $K \ltimes N$ ».

Comme d'habitude, on compte sur le contexte pour lever l'ambiguïté entre les produits semi-directs internes et externes.

Dans le cas d'un produit semi-direct externe, l'action d'un groupe sur l'autre peut être indiquée dans la notation. Par exemple, si un groupe K agit sur un groupe N à gauche, et que $\varphi\colon K \to \mathrm{Aut}(N)$ est l'homomorphisme associé à cette action, alors le produit semi-direct externe de N et K déterminé par cette action (ainsi que par φ) peut être noté « $N \rtimes_\varphi K$ ».

Exercice. Considérons l'action α du groupe additif $\mathbf{Z}$ sur le groupe additif $\mathbf{Q}$ donnée par la règle : $n.x \overset{\text{déf}}{=} 2^n x$ pour tous $n \in \mathbf{Z}$ et $x \in \mathbf{Q}$. Posons $G = \mathbf{Q} \rtimes_\alpha \mathbf{Z}$. Donner un exemple de $H < G$ et de $g \in G$ tels que

$$H \neq gHg^{-1} \subset H.$$

IX. Groupes finis

IX.1. Théorème de Cauchy

Dans cette section, $p \in \mathbf{N}$ est un nombre premier.

On va voir que si l'ordre d'un groupe fini est multiple de p, alors ce groupe contient un élément d'ordre p. Ce fait a été démontré par Cauchy[1] et porte le nom de *théorème de Cauchy*.

Lemme. *Si l'ordre d'un élément x dans un groupe est mn, avec $m, n \in \mathbf{N}\backslash\{0\}$, alors l'ordre de x^m est n.*

Lemme. *Si $f : G \to H$ est un homomorphisme de groupes et que $x \in G$ est un élément d'ordre fini, alors l'ordre de $f(x)$ divise l'ordre de x.*

Lemme. *Tout groupe fini abélien dont l'ordre est multiple de p possède un élément dont l'ordre est multiple de p.*

Démonstration. On va appliquer un principe de récurrence.

Soit un groupe abélien A d'ordre fini n multiple de p tel que tout groupe abélien dont l'ordre est multiple de p et strictement plus petit que n possède un élément dont l'ordre est multiple de p.

Soit a un élément non trivial de A.

Si l'ordre de a est multiple de p, on a la conclusion souhaitée.

Supposons maintenant que l'ordre de a ne soit pas multiple de p. Posons $B = A/\langle a \rangle$. Alors l'ordre de B est multiple de p et strictement plus petit que l'ordre de A. Soit b un élément de B dont l'ordre est multiple de p. (On a appliqué l'hypothèse de récurrence.) Soit $c \in A$ une image réciproque de b par la projection canonique $A \twoheadrightarrow B$. Alors l'ordre de c est multiple de l'ordre de b, et donc multiple de p.

L'énoncé du lemme s'en déduit par récurrence. □

[1] Augustin-Louis Cauchy. "Mémoire sur les arrangements que l'on peut former avec des lettres données". Et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre. In : *Exercices d'analyse et de physique mathématique*. T. 3. Paris : Bachelier, 1844, p. 151-250. URL : https://gallica.bnf.fr/ark:/12148/bpt6k96417945, p. 250.

Théorème (Théorème de Cauchy abélien)**.** *Tout groupe fini abélien dont l'ordre est multiple de p possède un élément d'ordre p.*

Démonstration. Il suffit d'appliquer deux lemmes précédents. □

Rappelons-nous que « $Z(G)$ » désigne le centre de G et que « $C_G(x)$ » désigne le centralisateur de x dans G.

Lemme. *Si G est un groupe fini non abélien dont l'ordre est multiple de p, alors il existe $x \in G \setminus Z(G)$ tel que l'ordre de $C_G(x)$ est multiple de p.*

Démonstration. Si l'ordre du centre de G est multiple de p, alors l'ordre de tout centralisateur est multiple de p.

Si l'ordre de $Z(G)$ n'est pas multiple de p, alors il suffit de regarder l'« équation aux classes » pour conclure qu'il y a au moins un élément $x \in G \setminus Z(G)$ tel que l'indice $[G : C_G(x)]$ n'est pas multiple de p, et donc l'ordre de $C_G(x)$ est multiple de p. □

Théorème (Théorème de Cauchy)**.** *Tout groupe fini dont l'ordre est multiple de p possède un élément d'ordre p.*

Démonstration. On peut à nouveau appliquer une récurrence sur l'ordre du groupe.

Soit un groupe G d'ordre fini n multiple de p tel que tout groupe dont l'ordre est multiple de p et strictement plus petit que n possède un élément d'ordre p.

Si G est abélien, il suffit d'appliquer le théorème précédent pour conclure que G possède un élément d'ordre p.

Supposons donc que G soit non abélien. Alors, d'après le lemme précédent, G contient un sous-groupe propre dont l'ordre est multiple de p. D'après l'hypothèse de récurrence, il y a un élément d'ordre p dans ce sous-groupe.

L'énoncé du théorème s'en découle par récurrence. □

IX.2. Groupes dont l'ordre est une puissance d'un nombre premier

Dans cette section, $p \in \mathbf{N}$ est un nombre premier.

Pour le reste de ce chapitre, on va adopter la définition suivante (où p est toujours un nombre premier) :

Définition. Un élément d'un groupe sera dit un *p-élément* si et seulement si son ordre est une puissance de p.[⚠2]

[2] Cette définition est complètement originale.

Lemme. *L'image d'un p-élément sous un homomorphisme est un p-élément.*

Définition. Un *p-groupe* est un groupe dont tout élément est un p-élément.

Lemme. *Un sous-groupe d'un p-groupe est un p-groupe.*

Lemme. *Un quotient d'un p-groupe est un p-groupe.*

Théorème. *Un groupe fini est un p-groupe si et seulement si son ordre est une puissance de p.*

Démonstration. Il suffit d'appliquer le théorème de Cauchy. □

Lemme. *Soient G un p-groupe fini et X un G-ensemble. Alors la longueur de toute G-orbite dans X est une puissance de p. En particulier, la longueur de toute G-orbite non triviale est multiple de p.*

Théorème. *L'ordre du centre d'un p-groupe fini et multiple de p.*

Démonstration. Il suffit de considérer l'action du groupe sur lui-même par conjugaison et d'appliquer le lemme précédent. Voir l'« équation aux classes ». □

IX.3. Sous-groupes de Sylow

Peter Ludvig Meidell Sylow (1832–1918) est un mathématicien norvégien. Il étudia la théorie des groupes et démontra, en 1872, des théorèmes sur les sous-groupes qui porteraient son nom.

Dans cette section, $p \in \mathbf{N}$ est un nombre premier, et G est un groupe fini.

Rappelons-nous que « $N_G(H)$ » désigne le normalisateur de H dans G.

Lemme. *Soit H un sous-groupe de G tel que l'indice $[N_G(H) : H]$ soit multiple de p. Alors il existe un sous-groupe K de G tel que $H \lhd K$ et $[K : H] = p$.*

Démonstration. Comme l'ordre du quotient $N_G(H)/H$ est multiple de p, $N_G(H)/H$ possède un sous-groupe (cyclique) d'ordre p, d'après le théorème de Cauchy.

Soit L un sous-groupe de $N_G(H)/H$ d'ordre p. Soit K l'image réciproque de L par la projection canonique $N_G(H) \twoheadrightarrow N_G(H)/H$. Alors $H \lhd K$ et $[K : H] = |L| = p$. □

Lemme. *Soit H un p-sous-groupe de G dont l'indice $[G : H]$ soit multiple de p. Alors l'indice $[N_G(H) : H]$ est aussi multiple de p.*

Démonstration. Soit X un G-ensemble gauche transitif tel que H soit le stabilisateur d'un élément de X. (On peut prendre $X = G/H$.)

Notons que $|X| = [G : H]$ est multiple de p.

Posons $Y = \mathrm{Fix}_X H$ et $Z = \mathrm{Supp}_X H$.

Notons que $X = Y \sqcup Z$, et que Y et Z sont invariants par l'action de $N_G(H)$.

Comme H est un p-groupe, la longueur de toute H-orbite non triviale est multiple de p, et donc $|Z|$ l'est aussi.

Ainsi, $|Y| = |X| - |Z|$ est multiple de p.

Notons que

$$Y = \{\, x \in X \mid \mathrm{Stab}_G(x) \supset H \,\}.$$

Comme G est fini et que l'action de G sur X est transitive, on a :

$$Y = \{\, x \in X \mid \mathrm{Stab}_G(x) = H \,\}.$$

D'où, si $g \in G$, $x \in Y$, et $gx \in Y$, alors $g \in N_G(H)$. Comme l'action de G sur X est transitive, l'action de $N_G(H)$ sur Y l'est aussi. Ainsi, $[N_G(H) : H] = |Y|$. □

Théorème. *Soit H un p-sous-groupe de G dont l'indice $[G : H]$ soit multiple de p. Alors il existe un p-sous-groupe K de G tel que $H \lhd K$ et $[K : H] = p$.*

Démonstration. Il suffit de combiner les deux lemmes précédents. □

Corollaire (Premier théorème de Sylow)**.** *Soit $n \in \mathbf{N}$ tel que p^n divise l'ordre de G. Alors G possède un p-sous-groupe d'ordre p^n. En plus, si p^{n+1} divise l'ordre de G, alors pour tout p-sous-groupe H d'ordre p^n, il existe un p-sous-groupe K d'ordre p^{n+1} tel que $H \lhd K$.*

Définition. Soient G un groupe fini et $p \in \mathbf{N}$ un nombre premier. Un sous-groupe H de G est dit un p-sous-groupe *de Sylow*, ou un p-*Sylow* sous-groupe, si et seulement si H est un p-groupe et p ne divise pas son indice $[G : H]$.[3]

Observons que l'image d'un p-Sylow sous-groupe de G sous un automorphisme de G est aussi un p-Sylow sous-groupe de G. En particulier, un sous-groupe de G conjugué dans G à un p-Sylow sous-groupe de G est un p-Sylow sous-groupe de G.

Lemme. *Si S est un p-Sylow sous-groupe de G, alors tout p-élément de $N_G(S)$ est un (p-) élément de S.*

[3] Bourbaki, *Algèbre*, Chapitre I, § 6, N° 6, p. I.74.

Démonstration. Comme p ne divise pas l'ordre du quotient $N_G(S)/S$, il ne divise l'ordre d'aucun élément de ce quotient.

Soit $x \in N_G(S)$ un p-élément arbitraire. Alors l'image de x dans $N_G(S)/S$ sous la projection canonique $N_G(S) \twoheadrightarrow N_G(S)/S$ (la classe xS) est un p-élément aussi. Donc, x est dans le noyau S de la projection. □

Corollaire. *Si S est un p-Sylow sous-groupe de G, alors tout p-sous-groupe de $N_G(S)$ est un (p-) sous-groupe de S.*

Corollaire. *Si S et T sont deux p-Sylow sous-groupes de G tels que $T \leqslant N_G(S)$, alors $T = S$.*

Théorème. *Si S est un p-Sylow sous-groupe de G, et H est un p-sous-groupe de G, alors il existe $g \in G$ tel que $H \leqslant gSg^{-1}$.*

Démonstration. Posons $X = \{\, gSg^{-1} \mid g \in G \,\}$ et montrons qu'il existe $T \in X$ tel que $H \leqslant T$.

Considérons l'action de H sur X par conjugaison. Comme $|H|$ est une puissance de p, la longueur de toute H-orbite non triviale est multiple de p. Or, $|X| = [G : N_G(S)]$ n'est pas multiple de p. Donc, il y a des points fixes. Soit $T \in \mathrm{Fix}_X H$. Alors $H \leqslant N_G(T)$, et donc $H \leqslant T$, d'après un corollaire d'un lemme précédent. □

Corollaire (Deuxième théorème de Sylow)**.** *Les p-Sylow sous-groupes de G sont deux à deux conjugués dans G.*

Corollaire. *Le nombre des p-Sylow sous-groupes de G est $[G : N_G(S)]$, où S est un n'importe lequel parmi eux.*

Corollaire. *Le nombre des p-Sylow sous-groupes de G divise l'ordre de G et n'est pas multiple de p.*

Théorème (Troisième théorème de Sylow)**.** *Le nombre des p-Sylow sous-groupes de G est congru à 1 modulo p.*

Démonstration. Soit X l'ensemble des p-Sylow sous-groupes de G, et soit $S \in X$. Considérons l'action de S sur X par conjugaison.

Si T est un point fixe de cette action, alors $S \leqslant N_G(T)$, et donc $S = T$. Ainsi, il y a exactement 1 point fixe. Comme S est un p-groupe, la longueur de toute H-orbite non triviale est multiple de p. D'où la conclusion souhaitée. □

X. 🚧 Groupes abéliens

Dans ce chapitre, pour les groupes abéliens, on va privilégier la terminologie et la notation additives.

X.1. Anneaux et modules

La théorie des groupes abéliens est étroitement liée à la théorie des anneaux et des modules sur des anneaux. Ceci ne doit pas surprendre, vu que :

- le groupe additif d'un anneau est un groupe abélien,
- un module sur un anneau est un groupe abélien muni d'une action de l'anneau,
- tout groupe abélien possède une structure canonique d'un $\mathbf{Z}$-module,
- les endomorphismes d'un groupe abélien forment un anneau (non seulement l'on peut les composer, mais aussi additionner).

Définition. Un *anneau* est un groupe abélien, pour lequel on adopte la terminologie et la notation additives, muni d'une opération binaire associative, dite la *multiplication*, qui est distributive sur l'addition.

Définition. Un *anneau unitaire* est un anneau dans lequel l'opération de multiplication admet un (unique) élément neutre, qui est désigné comme l'*unité* de l'anneau.

Notons bien qu'un anneau unitaire n'est pas simplement un anneau dans lequel la multiplication admet un élément neutre : cet élément neutre doit en plus être « nommé » l'*unité*. En pratique cela implique, entre autres, que lorsqu'on définit les homomorphismes d'anneaux, on exiges seulement que les opérations d'addition et de multiplication soient respectées, alors que pour les homomorphismes d'anneaux unitaires, on demande en plus que l'unité soit envoyé sur l'unité (ce qui n'est pas automatique).

Définition. L'*anneau sous-jacent* d'un anneau unitaire est l'anneau qu'on en obtient en « oubliant » que l'élément neutre de la multiplication a été désigné comme l'*unité*.

Définition. Un anneau, unitaire ou non, est dite *commutatif* si et seulement si son opération de multiplication est commutative.

Comme d'habitude, on se permet d'utiliser un même symbole (une même lettre) pour nommer un anneau, unitaire ou non, et son *ensemble sous-jacent* (l'ensemble de ses éléments).

Définition. Soient R un anneau unitaire et M un groupe abélien. Une *action* de R sur M *à gauche* est une application $\alpha\colon R \times M \to M$ telle que :

(1) $\alpha(r,\, x+y) = \alpha(r,\, x) + \alpha(r,\, y)$ pour tous $r \in R$ et $x, y \in M$,

(2) $\alpha(s,\, \alpha(r,x)) = \alpha(sr,\, x)$ pour tous $r, s \in R$ et $x \in M$,

(3) $\alpha(1, x) = x$ pour tout $x \in M$,

(4) $\alpha(r+s,\, x) = \alpha(r,\, x) + \alpha(s,\, x)$ pour tous $r, s \in R$ et $x \in M$.

Une *action* de R sur M *à droite* est une application $\beta\colon M \times R \to M$ telle que :

(1) $\beta(x+y,\, r) = \beta(x,\, r) + \beta(y,\, r)$ pour tous $r \in R$ et $x, y \in M$,

(2) $\beta(\beta(x,r),\, s) = \beta(x,\, rs)$ pour tous $r, s \in R$ et $x \in M$,

(3) $\beta(x, 1) = x$ pour tout $x \in M$,

(4) $\beta(x,\, r+s) = \beta(x,\, r) + \beta(x,\, s)$ pour tous $r, s \in R$ et $x \in M$.

Pour les anneaux unitaires commutatifs, on ne fait pas de différence entre leurs actions à gauche et à droite, car il n'y a pas de différence substantielle.

Notation. Si R est un anneau unitaire, M est un groupe abélien, et $\alpha\colon R \times M \to M$ est une action de R sur M à gauche, alors, pour $r \in R$ et $x \in M$, l'élément $\alpha(r,x) \in M$ peut être noté comme « rx » ou « $r \cdot x$ » ou « $r.x$ », lorsque cela n'introduit pas d'ambiguïté. On peut aussi envisager d'autres notations, comme « $r \triangleleft x$ ». De même, si $\beta\colon M \times R \to M$ est une action de R sur M à droite, alors, pour $r \in R$ et $x \in M$, l'élément $\beta(x,r) \in M$ peut être noté comme « xr » ou « $x \cdot r$ » ou « $x.r$ », et on peut envisager d'autres notations, comme « $x \triangleright r$ ».

Définition. Soit R un anneau unitaire.

(1) Un *R-module gauche* est un groupe abélien muni d'une action de R à gauche.

(2) Un *R-module droit* est un groupe abélien muni d'une action de R à droite.

Si R est un anneau unitaire commutatif, on ne fait pas de différence entre les R-modules gauches et droits.

X.2. Groupes abéliens comme modules

Tout groupe abélien est un $\mathbf{Z}$-module par rapport à l'opération[1] usuelle de multiplication par un entier d'un élément d'un groupe abélien, lorsque la notation et la terminologie additives sont utilisées.

Soit A un groupe abélien. Son ensemble d'endomorphisme $\mathrm{End}(A)$ possède une structure canonique d'un anneau unitaire, définie ainsi :

(1) la *multiplication* est la composition :

$$(\alpha\beta)(x) \stackrel{\text{déf}}{=} \alpha(\beta(x))$$

pour tous $\alpha, \beta \in \mathrm{End}(A)$ et $x \in A$,

(2) l'*unité* est l'automorphisme identité de A,

(3) l'*addition* est l'addition « point par point » :

$$(\alpha + \beta)(x) \stackrel{\text{déf}}{=} \alpha(x) + \beta(x)$$

pour tous $\alpha, \beta \in \mathrm{End}(A)$ et $x \in A$.

Clairement, tout groupe abélien A est un $\mathrm{End}(A)$-module gauche par rapport à l'opération de l'application d'un endomorphisme à un élément : $\alpha.x \stackrel{\text{déf}}{=} \alpha(x)$.

X.3. Faits divers

Proposition. *Si $n \in \mathbf{Z}$ et A est un groupe abélien, alors l'application $A \to A$ donnée par la règle $a \mapsto na$ est un endomorphisme de A.*

Exercice. Prouver cette proposition.

Corollaire. *Si $n \in \mathbf{Z}$ et A est un groupe abélien, alors l'ensemble $nA = \{\, na \mid a \in A \,\}$ (l'image de l'endomorphisme $a \mapsto na$) et l'ensemble $\{\, a \in A \mid na = 0 \,\}$ (le noyau de l'endomorphisme $a \mapsto na$) forment sous-groupes de A.*

Proposition. *Si B et C sont deux sous-groupes d'un groupe abélien, alors $B + C$ l'est aussi, et*

$$[B + C : B \wedge C] = [B : B \wedge C] \cdot [C : B \wedge C].$$

[1] Le terme « opération » ici est utilisé au sens plus large que lorsqu'on parle des applications du type $X \times X \to X$.

Exercice. Prouver cette proposition.

Corollaire. *Si un groupe abélien A est engendré par n éléments $a_1, \ldots, a_n$ d'ordres finis $m_1, \ldots, m_n$, alors l'ordre de A est fini et divise le produit $m_1 \cdots m_n$.*

Ce corollaire peut être démontré directement en considérant l'épimorphisme

$$(\mathbf{Z}/m_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/m_n\mathbf{Z}) \twoheadrightarrow A,$$
$$([k_1], \ldots, [k_n]) \mapsto a_1^{k_1} \cdots a_n^{k_n}.$$

Corollaire. *Si un groupe abélien A est engendré par un ensemble fini à n éléments, alors pour tout $m \in \mathbf{N} \setminus \{0\}$, l'indice $[A : mA]$ est fini et divise m^n.*

Exercice. Soient G et K deux groupes, $f\colon G \to K$ un homomorphisme, $H \leqslant G$ un sous-groupe de G, et $U \subset G$ une partie de G. Supposons que

$$\langle U \cap \operatorname{Ker} f \rangle = H \wedge \operatorname{Ker} f, \qquad \langle f(U) \rangle = f(H), \qquad U \subset H.$$

Montrer que $\langle U \rangle = H$.

Théorème. *Si A est un groupe abélien qui est engendré par un ensemble à n éléments, alors tout sous-groupe de A admet un ensemble de générateurs à n éléments ou moins.*

Démonstration. Supposons que

$$A = \langle a_1, \ldots, a_n \rangle = \langle a_1 \rangle + \cdots + \langle a_n \rangle.$$

Posons

$$A_0 = \mathbf{0}, \qquad A_k = A_{k-1} + \langle a_k \rangle = \langle a_1, \ldots, a_k \rangle \quad \text{pour } k \in \{1, \ldots, n\}.$$

En particulier, $A_n = A$.

Pour tout $k \in \{1, \ldots, n\}$, le quotient A_k/A_{k-1} est un groupe (abélien) monogène engendré par l'image de a_k sous la projection canonique $A_k \twoheadrightarrow A_k/A_{k-1}$. (On peut noter cela ainsi : $A_k/A_{k-1} = \langle [a_k]_{A_{k-1}} \rangle$, où $[a_k]_{A_{k-1}} = a_k + A_{k-1}$ est la classe de a_k suivant A_{k-1} vue comme un élément de A/A_{k-1} ou de A_k/A_{k-1}.)

Soit $B \leqslant A$ un sous-groupe de A. Posons

$$B_k = B \wedge A_k \quad \text{pour } k \in \{0, \ldots, n\}.$$

En particulier, $B_n = B$.

Pour tout $k \in \{1, \ldots, n\}$,

$$B_k/B_{k-1} \simeq (B_k + A_{k-1})/A_{k-1} \leqslant A_k/A_{k-1},$$

et donc B_k/B_{k-1} est monogène. (Le quotient $(B_k + A_{k-1})/A_{k-1}$ est l'image de B_k sous la projection canonique $A_k \twoheadrightarrow A_k/A_{k-1}$.)

Pour tout $k \in \{1, \ldots, n\}$, choisissons $b_k \in B_k$ tel que :

(1) $b_k = 0$ si $B_k = B_{k-1}$,

(2) l'image de b_k sous la projection canonique $B_k \twoheadrightarrow B_k/B_{k-1}$ engendre B_k/B_{k-1} si $B_k > B_{k-1}$.

On peut montrer par récurrence que

$$B_k = B_{k-1} + \langle b_k \rangle = \langle b_1, \ldots, b_k \rangle \quad \text{pour tout } k \in \{1, \ldots, n\}.$$

En particulier, $B = B_n = \langle b_1, \ldots, b_n \rangle$. □

X.4. Groupes abéliens libres

Définition. Soient G un groupe et $U \subset G$ une partie de son ensemble sous-jacent. Le groupe G est dit *libre* sur U (dans la classe de tous les groupes) si et seulement si pour tout groupe H et pout toute application $\varphi\colon U \to H$, il existe un unique homomorphisme $f\colon G \to H$ tel que $f|_U = \varphi$.

Exemple. Un groupe monogène infini engendré par un élément x est libre sur $\{x\}$. En particulier, le groupe additif $\mathbf{Z}$ est libre sur $\{1\}$, ainsi que sur $\{-1\}$.

Dans ce chapitre, on ne va pas discuter les groupes libres dans la classe de tous les groupes, mais on va survoler la notion analogique pour la classe des groupes abéliens, laquelle est bien plus simple, et en plus peut être considérée comme un cas particulière de la notion d'un *module libre* sur un anneau commutatif.

Définition. (1) Un groupe abélien A est dit *abélien libre* sur $U \subset A$ si et seulement si pour tout groupe abélien B et pout toute application $\varphi\colon U \to B$, il existe un unique homomorphisme $f\colon A \to B$ tel que $f|_U = \varphi$.

(2) Un groupe abélien A est dit *abélien libre* sur une famille indexée $(a_i)_{i\in I}$ d'éléments de A si et seulement si pour tout groupe abélien B et pout toute famille $(b_i)_{i\in I}$ d'éléments de B, il existe un unique homomorphisme $f\colon A \to B$ tel que $f(a_i) = b_i$ pour tout $i \in I$.

On peut dire « libre » au lieu de « abélien libre » lorsqu'il est clair du contexte de quoi on parle.

Définition. Soit L un groupe abélien libre. Une partie $U \subset L$ est dite une *base* de L si et seulement si L est abélien libre sur U. Une famille $(a_i)_{i\in I}$ d'éléments de L est dite une *base* (indexée par I) de L si et seulement si L est abélien libre sur cette famille.

Si A est un groupe abélien, on va utiliser la notation « $A^{\oplus I}$ » pour la somme directe externe $\bigoplus_{i\in I} A$, dont les éléments sont les fonctions $\varphi\colon I \to A$ telles que l'ensemble $\{\, i \in I \mid \varphi(i) \neq 0 \,\}$ est fini.

Proposition. *Soit I un ensemble. Alors le groupe $\mathbf{Z}^{\oplus I}$ est abélien libre. Comme une base de $\mathbf{Z}^{\oplus I}$ on peut prendre la famille $(\delta_i)_{i\in I}$ définie par la formule* :

$$\delta_i(j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{sinon.} \end{cases}$$

Exercice. Prouver cette proposition.

Proposition. *Soient I un ensemble, A un groupe abélien libre sur une base $(a_i)_{i\in I}$ et B un groupe abélien libre sur une base $(b_i)_{i\in I}$. Alors A et B sont isomorphes. Plus précisément, si les homomorphismes $f\colon A \to B$ et $g\colon B \to A$ sont définies par les conditions* :

$$f(a_i) = b_i \quad \text{et} \quad g(b_i) = a_i \qquad \text{pour tout } i \in I,$$

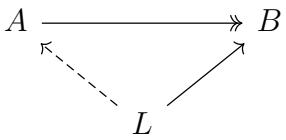
alors f et g sont deux isomorphismes réciproques entre A et B.

En particulier, tout groupe abélien libre dont une base est indexée par I (ou par un autre ensemble de même cardinal) est isomorphe à $\mathbf{Z}^{\oplus I}$.

Exercice. Prouver la dernière proposition.

Théorème. *Soient A et B deux groupes abéliens, L un groupe abélien libre, $p\colon A \twoheadrightarrow B$ un épimorphisme et $f\colon L \to B$ un homomorphisme. Alors il existe un homomorphisme $g\colon L \to A$ tel que $p \circ g = f$.*

Voici un schéma pour ce théorème :



Exercice. Prouver ce théorème.

Corollaire. *Toute extension abélienne d'un groupe abélien libre est scindée.*

Définition. Soient A et B deux groupes abéliens libres, et $f\colon A \to B$ un homomorphisme. Soient $\mathcal{A} = (a_i)_{i\in I}$ une base de A et $\mathcal{B} = (b_i)_{i\in I}$ une base de B. Alors la *matrice* de f par rapport aux bases $\mathcal{A}$ et $\mathcal{B}$ est la matrice $M = (m_{i,j})_{i\in I,\, j\in J}$ à coefficients entiers définis par la condition :

$$f(a_i) = \sum_{j\in J} m_{i,j} b_j \qquad \text{pour tout } i \in I.$$

Proposition. *Soient A, B et C trois groupes abéliens libres, et $f\colon A \to B$ et $g\colon B \to C$ deux homomorphismes. Soient $\mathcal{A}$ une base de A, $\mathcal{B}$ une base de B et $\mathcal{C}$ une base de C. Soient M la matrice de f par rapport aux bases $\mathcal{A}$ et $\mathcal{B}$ et N la matrice de g par rapport aux bases $\mathcal{B}$ et $\mathcal{C}$. Alors la matrice de $g \circ f$ par rapport aux bases $\mathcal{A}$ et $\mathcal{C}$ est la matrice produit NM.*

Exercice. Prouver cette proposition.

Lemme. *Soient L un groupe abélien libre, $U \subset L$ une base de L, et $m \in \mathbf{N}\backslash\{0\}$. Alors :*

(1) *U est fini si et seulement si l'indice $[L : mL]$ est fini,*

(2) *si U est fini, alors $[L : mL] = m^{|U|}$.*

Exercice. Prouver ce lemme.

Corollaire. *Toutes les bases d'un groupe abélien libre de type fini sont finies et avec le même nombre d'éléments. Deux groupes abéliens libres de type fini sont isomorphes si et seulement si les cardinaux de leurs bases sont les mêmes.*

En fait, il n'est pas difficile de généraliser le dernier lemme et son corollaire au cas de groupes libre arbitraires (pas forcement de type fini).

Définition. Le nombre d'élément d'une base d'un groupe abélien libre L de type fini peut s'appeler le *rang* de L.

X.5. Éléments d'ordre fini et sous-groupe de torsion

Dans cette section, A est un groupe abélien et T est l'ensemble des éléments de A d'ordres finis. On verra tout de suite que T forme un sous-groupe de A.

Proposition. *Soient a et b sont deux éléments de A, et posons $c = a + b$ ou $c = a - b$. Alors :*

(1) *si parmi les trois éléments a, b et c deux sont d'ordres finis, alors le troisième l'est aussi,*

(2) *dans le cas où les trois éléments sont d'ordres finis, l'ordre de chacun divise les PPCM des ordres des deux autres.*

Idée d'une démonstration. Il suffit de traiter le cas $c = a + b$ et observer que pour tout $n \in \mathbf{Z}$, si parmi les trois éléments na, nb et $nc = na + nb$, deux sont 0, alors le troisième l'est aussi. □

Corollaire. *L'ensemble T d'éléments de A d'ordres finis forme un sous-groupe de A.*

Exercice. Soient a, b, c trois nombres naturels dont chacun divise le PPCM des deux autre. Montrer que si a et b sont premiers entre eux, alors $c = ab$. La version suivante du lemme d'Euclide peut être utile : si c divise ab, alors il existe u et v tels que $c = uv$, u divise a, et v divise b.[2]

Lemme. *Soient a et b sont deux éléments de T dont les ordres sont premiers entre eux. Considérons le sous-groupe $\langle a, b\rangle$ engendré par a et b. Alors :*

(1) $\langle a, b\rangle = \langle a\rangle \oplus \langle b\rangle = \langle a + b\rangle = \langle a - b\rangle$,

(2) *si l'ordre de a est m et l'ordre de b est n, alors il existe un unique $c \in A$ tel que $a = nc$ et $b = mc$, et en plus ce c appartient à $\langle a, b\rangle$, et donc $\langle a, b\rangle = \langle c\rangle$.*

Démonstration. Comme $\langle a\rangle \wedge \langle b\rangle = \mathbf{0}$, on a

$$\langle a, b\rangle = \langle a\rangle + \langle b\rangle = \langle a\rangle \oplus \langle b\rangle.$$

En particulier, l'ordre de $\langle a, b\rangle$ est le produit des ordres de a et de b.

D'après la proposition précédente, l'ordre de chacun des trois éléments a, b, $a + b$ divise les PPCM des ordres des deux autres. Comme les ordres de a et de b sont premiers entre eux, il en découle que l'ordre de $a + b$ est le produit

[2] Pour démontrer cet énoncé, ainsi que le lemme d'Euclide classique, on peut se servir de l'identité $\operatorname{pgcd}(ab, ac) = a \operatorname{pgcd}(b, c)$, pour en déduire que $\operatorname{pgcd}(ab, c) = \operatorname{pgcd}(ab, ac, c) = \operatorname{pgcd}(\operatorname{pgcd}(ab, ac), c) = \operatorname{pgcd}(a \operatorname{pgcd}(b, c), c)$. Ainsi, si c divise ab, alors $c = \operatorname{pgcd}(ab, c) = \operatorname{pgcd}(a \operatorname{pgcd}(b, c), c)$, et donc c divise $a \operatorname{pgcd}(b, c)$. On peut ensuite poser $v = \operatorname{pgcd}(b, c)$.

des ordres de a et de b. Ainsi, l'ordre de $a+b$ coïncide avec l'ordre de $\langle a,\, b\rangle$. Donc,

$$\langle a,\, b\rangle = \langle a+b\rangle.$$

De la même manière on peut montrer que $\langle a,\, b\rangle = \langle a-b\rangle$.

Soient maintenant m l'ordre de a et n l'ordre de b. On « cherche » c tel que $a = nc$ et $b = mc$.

Soient $u, v \in \mathbf{Z}$ tels que $um + vn = 1$. Si on a $c \in A$ tel que $a = nc$ et $b = mc$, alors

$$c = (um+vn)c = umc + vnc = ub + va.$$

Posons donc $c = ub + va$. Alors

$$mc = m(ub+va) = umb + v\underbrace{ma} = umb = umb + v\underbrace{nb} = (um+vn)b = b$$

et

$$nc = n(ub+va) = u\underbrace{nb} + vna = vna = u\underbrace{ma} + vna = (um+vn)a = a,$$

car $ma = 0 = nb$. □

On peut aussi prover la première partie du dernier lemme en utilisant l'isomorphisme

$$\begin{aligned}\mathbf{Z}/mn\mathbf{Z} &\xrightarrow{\sim} (\mathbf{Z}/m\mathbf{Z}) \oplus (\mathbf{Z}/n\mathbf{Z}),\\ [k]_{mn} &\mapsto ([k]_m,\, [k]_n),\end{aligned}$$

pour m et n premiers entre eux.

Définition. Le *sous-groupe de torsion* de A est son sous-groupe T (formé des éléments de A d'ordres finis). Le groupe A est dit *de torsion* si et seulement si $T = A$. Le groupe A est dit *sans torsion* si et seulement si $T = \mathbf{0}$.

Proposition. *Le quotient A/T est sans torsion.*

Exercice. Prouver cette proposition.

X.6. Composantes primaires

Dans cette section, A est un groupe abélien, et T est son sous-groupe de torsion.

On va continuer à utiliser le terme *p-élément* pour un élément dont l'ordre est une puissance de p, lorsque $p \in \mathbf{N}$ est un nombre premier.

Pour tout $p \in \mathbf{N}$ premier, posons T_p l'ensemble des p-éléments de T.

Proposition. *Pour tout $p \in \mathbf{N}$ premier, T_p est un sous-groupe de T.*

Exercice. Prouver cette proposition.

Si T est d'ordre fini, alors T_p est son unique p-sous-groupe de Sylow.

Définition. Pour tout $p \in \mathbf{N}$ premier, la *composante p-primaire* de A (ou de T) est son sous-groupe T_p (formé des p-éléments de A).

Théorème. *Tout groupe abélien de torsion est la somme directe interne des ces composantes primaires* :

$$T = \bigoplus_{p \in \mathbf{N} \text{ premier}} T_p.$$

Exercice. Prouver ce théorème.

X.7. 🚧 Sommes directes finies de groupes monogènes

Théorème. *Soient $r, s \in \mathbf{N}$ et $m_1, \ldots, m_r, n_1, \ldots, n_s \in \mathbf{N} \setminus \{1\}$ tels que* :

(1) *m_{i+1} divise m_i pour tout $i \in \{1, \ldots, r-1\}$,*

(2) *n_{j+1} divise n_j pour tout $j \in \{1, \ldots, s-1\}$,*

(3) $(\mathbf{Z}/m_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/m_r\mathbf{Z}) \simeq (\mathbf{Z}/n_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_s\mathbf{Z})$.

Alors $r = s$ et $(m_1, \ldots, m_r) = (n_1, \ldots, n_s)$.

Démonstration. [...] □

X.8. 🚧 Divisibilité et sous-groupes purs

Définition. Soit A un groupe abélien. On va dire que $n \in \mathbf{Z}$ *divise* $a \in A$ si et seulement si il existe $b \in A$ tel que $a = nb$. On va dire que $b \in A$ *divise* (ou $\mathbf{Z}$-*divise*) $a \in A$ si et seulement si il existe $n \in \mathbf{Z}$ tel que $a = nb$.

Ainsi,

(1) $n \in \mathbf{Z}$ divise $a \in A$ si et seulement si $a \in nA$,

(2) $b \in A$ divise $a \in A$ si et seulement si $a \in \mathbf{Z}b$.

Lorsque A est le groupe abélien sous-jacent d'une structure muni d'une certaine opération de « multiplication », le sens de « b divise a » pour $a, b \in A$ est ambigu. On peut éviter l'ambiguïté en écrivant, par exemple, « b $\mathbf{Z}$-divise a ».

On peut utiliser de manière appropriée d'autres termes associés, comme *diviseur*, $\mathbf{Z}$-*diviseur*, *multiple*, $\mathbf{Z}$-*multiple*.

Exercice. Soient $a, b \in \mathbf{Z} \setminus \{0\}$. Montrer que $\dfrac{1}{\mathrm{ppcm}(a,b)}$ est le plus petit nombre strictement positif qui s'écrit sous la forme $\dfrac{m}{a} + \dfrac{n}{b}$ avec $m, n \in \mathbf{Z}$.

Proposition. *Soient a, b, c trois éléments d'un groupe abélien et $m, n \in \mathbf{Z}$ tels que*

$$ma = c = nb.$$

Posons $u = \mathrm{ppcm}(m, n)$. Alors il existe $d \in \langle a, b \rangle$ tel que

$$ud = c.$$

Démonstration. Soient $v, w \in \mathbf{Z}$ tels que

$$\frac{v}{m} + \frac{w}{n} = \frac{1}{u}.$$

Posons

$$d = va + wb.$$

Alors

$$ud = u(va + wb) = \frac{uv}{m}ma + \frac{uw}{n}nb = \frac{uv}{m}c + \frac{uw}{n}c = u\left(\frac{v}{m} + \frac{w}{n}\right)c = c. \square$$

Définition. Un groupe abélien A est dit *divisible* si et seulement si $nA = A$ pour tout $n \in \mathbf{Z} \setminus \{0\}$.

Définition. Un sous-groupe B d'un groupe abélien A est dit *pur*[3] si et seulement si $nB = B \wedge nA$ pour tout $n \in \mathbf{Z}$.

Proposition. *Si A est un groupe abélien, B est un sous-groupe pur de A, et C est un sous-groupe pur de B, alors C est pur dans A.*

Exercice. Prouver cette proposition.

Proposition. *Si un groupe abélien A est la somme directe interne de ses sous-groupes B et C ($A = B \oplus C$), alors B et C sont purs dans A.*

Exercice. Prouver cette proposition.

X.9. 🚧 Classification des groupes abéliens de type fini

Théorème. *Tout groupe abélien sans torsion et de type fini est libre.*

Démonstration. `[...]` □

Théorème. *Soit A un groupe abélien fini non trivial. Alors il existe $a_1, \ldots, a_n \in A \setminus \{0\}$ tels que :*

(1) $A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$,

(2) *pour tout $i \in \{1, \ldots, n-1\}$ et pour tout $m \in \mathbf{Z}$, si $ma_i = 0$, alors $ma_{i+1} = 0$.*

En plus, quelle que soit une telle famille $a_1, \ldots, a_n$, sa taille n et les ordres des ses éléments sont toujours les mêmes (ils ne dépendent que de A).

Démonstration. `[...]` □

Corollaire. *Tout groupe abélien de type fini est la somme directe d'une famille de sous-groupes monogènes.*

[3] Ce terme semble être du à Jean Braconnier (1922–1985). La notion a été introduite plus tôt par Heinz Prüfer (1896–1934), qui utilisait l'appellation *Servantzuntergruppe* en allemand.

XI. 🚧 Groupes linéaires

XI.1. 🚧

[...]

XII. 🚧 Espaces projectifs et groupes associés

XII.1. 🚧

[...]

XIII. 🚧 Transfert

https://fr.wikipedia.org/wiki/Transfert_(théorie_des_groupes)

XIII.1. 🚧

[...]

XIV. Suites de composition

https://fr.wikipedia.org/wiki/Suite_de_composition
Hall.[1]

XIV.1.

[...]

XIV.2. Théorème de Jordan-Hölder

https://fr.wikipedia.org/wiki/Théorème_de_Jordan-Hölder
Serre.[2]
Mac Lane et Birkhoff.[3]
[...]

[1] Hall, *The theory of groups*, chapitre 8.
[2] Jean-Pierre Serre. "Groupes finis". Cours à l'École Normale Supérieure de Jeunes Filles, 1978/1979. Rédigé par Martine Buhler et Catherine Goldstein (Montrouge, 1979), révisé et transcrit en LaTeX par Nicolas Billerey, Olivier Dodane et Emmanuel Rey (Strasbourg – Paris, 2004). 2004. URL : https://arxiv.org/abs/math/0503154, section 1.3.
[3] Mac Lane et Birkhoff, *Algebra*, chapitre XII, section 8.

Bibliographie

Bourbaki, N. *Algèbre. Chapitres 1 à 3*. 2e éd. Réimpression inchangée de la « nouvelle édition » de 1970. Berlin, Heidelberg : Springer, 11 déc. 2006. xiii+636. doi : 10.1007/978-3-540-33850-5.

Cauchy, Augustin-Louis. "Mémoire sur les arrangements que l'on peut former avec des lettres données". Et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre. In : *Exercices d'analyse et de physique mathématique*. T. 3. Paris : Bachelier, 1844, p. 151-250. url : https://gallica.bnf.fr/ark:/12148/bpt6k96417945.

Galois, Évariste. *Œuvres mathématiques d'Évariste Galois*. Avec une introd. d'Emile Picard. Paris : Gauthier-Villars, 1897. x+61. url : https://www.e-rara.ch/zut/content/titleinfo/6262819.

– *Œuvres mathématiques d'Évariste Galois*. Avec une introd. d'Emile Picard. Project Gutenberg, 2012. vi+61. url : https://www.gutenberg.org/ebooks/40213.

Hall, Marshall. *The theory of groups*. Anglais. AMS Chelsea Publishing 288. Publié à l'origine par Macmillan Company, New York, 1959. American Mathematical Society, 1976. xiii+434. url : https://bookstore.ams.org/chel-288/.

Kargapolov, Mikhail et Yuriï Merzlyakov. *Éléments de la théorie des groupes*. Trad. du russe par V. Kotliar. Moscou : Éditions Mir, 1985. 263 p. url : https://archive.org/details/kargapolov-merzliakov-elements-de-la-theorie-des-groupes-mir-1985fc.

Klein, Felix. "A comparative review of recent researches in geometry". Anglais. Trad. de l'allemand par Mellen Woodman Haskell. In : *Bulletin of the New York Mathematical Society* 2.10 (juill. 1893), p. 215-249. url : https://projecteuclid.org/journals/bulletin-of-the-american-mathematical-society-new-series/volume-2/issue-10/A-comparative-review-of-recent-researches-in-geometry/bams/1183407629.full.

Lang, Serge. *Algebra*. Anglais. 3e éd. Graduate Texts in Mathematics 211. Publié à l'origine par Addison-Wesley, 1993. New York, NY : Springer, 2002. xv+914. doi : 10.1007/978-1-4613-0041-0.

Mac Lane, Saunders et Garrett Birkhoff. *Algebra*. Anglais. 3e éd. AMS Chelsea Publishing 330. Publié à l'origine par Chelsea Publishing Company,

1988. American Mathematical Society, 10 oct. 2023. 626 p. URL : https://bookstore.ams.org/chel-330/.

SERRE, Jean-Pierre. “Groupes finis”. Cours à l’École Normale Supérieure de Jeunes Filles, 1978/1979. Rédigé par Martine Buhler et Catherine Goldstein (Montrouge, 1979), révisé et transcrit en LaTeX par Nicolas Billerey, Olivier Dodane et Emmanuel Rey (Strasbourg – Paris, 2004). 2004. URL : https://arxiv.org/abs/math/0503154.