Cours de groupes

Itaï Ben Yaacov

Itaï Ben Yaacov, Université Claude Bernard Lyon 1, Institut Camille Jordan, CNRS UMR 5208, 43 boulevard du 11 novembre 1918, 69622 Villeurbanne Cedex, France

URL: http://math.univ-lyon1.fr/~begnac/

Table des matières

Chapitre I

Groupes

1. Premières définitions

On a déjà vu des corps, qui sont des structures algébriques munies de deux opérations : $+$ et $\cdot$.

Nous allons nous concentrer sur les groupes, qui sont des structures algébriques munies d'une seule opération. Mais ce n'est pas forcément bien plus simple…

Définition I.1.1. Un **groupe** est une paire $(G, *)$, où G est un ensemble et $*$ est une loi associant à tous deux élément $x, y \in G$ un élément $x * y$, et qui vérifie les axiomes suivants :

— **Clôture :** pour tous $x, y \in G$ on a $x * y \in G$.

— **Associativité :** $x * (y * z) = (x * y) * z$ pour tous $x, y, z \in G$.

— **Neutre :** il existe un élément $e \in G$ qui est **neutre** pour l'opération $*$:

$$x * e = e * x = x \qquad \text{quel que soit } x \in G.$$

On observe, d'ailleurs, que le neutre est forcent unique. En effet, si $f \in G$ est un autre neutre, alors

$$f = f * e = e.$$

— **Inverse :** pour chaque $x \in G$ il existe un élément noté $x' \in G$ qui est **inverse** de x pour l'opération $*$:

$$x * x' = x' * x = e,$$

où e est l'unique neutre.

L'ensemble G s'appelle l'ensemble **sous-jacent** du groupe $(G, *)$, et l'opération $*$ s'appelle la **loi** du groupe. Lorsqu'il n'y a pas de risque d'ambiguïté, nous nous permettrons de noter un groupe $(G, *)$ par G seul (c'est que l'on appelle un **abus de notation**).

Puisque la loi est associative, on peut omettre les parenthèses :

$$(x * y) * z = x * (y * z) = x * y * z,$$

et pareil pour quatre éléments de G, cinq, voire plus. On mettra néanmoins les parenthèses lorsque cela rend plus clair notre raisonnement, comme c'est le cas dans la preuve du lemme suivant.

Lemme I.1.2. *Soit G un groupe. Alors G admet un unique neutre e, et chaque $x \in G$ admet un unique inverse x'.*

Démonstration. Si $f \in G$ est neutre, alors $e = e * f = f$. Si $y \in G$ est inverse de x, alors

$$y = e * y = (x' * x) * y = x' * (x * y) = x' * e = x'.$$

■

Nous pouvons ainsi considérer l'inversion comme une opération $\cdot' \colon G \to G$.

Définition I.1.3. Un groupe $(G, *)$ est dit **abélien** (ou simplement **commutatif**) si la loi est commutative : $x * y = y * x$ pour tous $x, y \in G$.

Exemple I.1.4. Voici quelques premiers exemples :
- $(\mathbf{R}, +)$ est un groupe. Son neutre est 0, et l'inverse de x est $-x$. Le soin de vérifier les axiomes un par un est laissé au lecteur.
- Par contre $(\mathbf{R}, \cdot)$ n'est pas un groupe : 1 est bien neutre, mais 0 n'a pas d'inverse pour la multiplication.
- $(\mathbf{R} \setminus \{0\}, \cdot)$ est un groupe, mais $(\mathbf{R} \setminus \{0\}, +)$ non (il n'est pas clos).
- $(\mathbf{R}^{>0}, \cdot)$ est un groupe, mais $(\mathbf{R}^{>0}, +)$ non (pas de neutre).
- $(\mathbf{Z}, +)$ est un groupe, mais $(\mathbf{Z}, \cdot)$ non (toujours souci d'inverse).
- Soit $n \in \mathbf{N}$, $n \geq 1$. $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe, $(\mathbf{Z}/n\mathbf{Z}, \cdot)$ non.
- Notons par $M(2, \mathbf{R})$ l'ensemble des matrices 2×2 à coordonnées réelles. C'est un groupe pour la loi d'addition de matrices, mais non pour la loi de multiplication.
- Notons par $\mathrm{GL}(2, \mathbf{R})$ l'ensemble des matrices 2×2 **inversibles** à coordonnées réelles. C'est un groupe pour la loi de multiplication de matrices, mais non pour la loi d'addition.

Tous les groupes énumérés ci-dessus sont abéliens, sauf $\mathrm{GL}(2, \mathbf{R})$.

Nous avons le droit d'utiliser n'importe quel symbole pour noter la loi d'un groupe. Dans les exemples précédents, le plus souvent la loi était notée ou bien par $\cdot$ (multiplication) ou bien par $+$ (addition). Ce sera en effet le cas pour la quasi-totalité des groupes :
- Le plus souvent, la loi est notée par $\cdot$. On dit alors que $(G, \cdot)$ est un groupe en **notation multiplicative** (ou tout simplement un **groupe multiplicatif**).

  Dans la notation multiplicative, on écrit souvent xy au lieux de $x \cdot y$. Le neutre est noté par 1 (parfois encore par e), et s'appelle aussi l'**identité** de G. L'inverse de x est noté x^{-1}.
- Plus rarement, et uniquement pour un groupe abélien, la loi sera notée par $+$. On dit alors que $(G, +)$ est un groupe en **notation additive** (ou tout simplement un **groupe additif**).

  Dans la notation additive, le neutre est noté par 0, et l'inverse (ou **opposé**) de x est noté $-x$. On écrira également $x - y$ au lieu de $x + (-y)$.

La notation multiplicative sera notre choix par défaut. Ainsi « soit G un groupe » doit toujours être entendu comme « soit $(G, \cdot)$ un groupe multiplicatif ».
D'ailleurs, comme dit plus haut, nous n'utiliserons la notation additive que pour les groupes abéliens !

Définition I.1.5. Soit G un groupe (puisqu'on n'a rien précisé de plus, c'est en notation multiplicative). Pour $n \in \mathbf{N}$, on défini par récurrence :

$$x^0 = e, \qquad x^{n+1} = x \cdot x^n.$$

Autrement dit, $x^n = x \cdot x \cdots x$, n fois, où il est convenu que le produit de zéro facteurs est le neutre. On étend ça à tout $n \in \mathbf{Z}$, en posant, pour $n < 0$:

$$x^n = (x')^{-n}.$$

Nous venons d'introduire une notation ambiguë !
- D'un côté, x^{-1} est une notation pour l'inverse de x, ce que l'on a appelé x' plus tôt.
- D'un autre côté, on pourrait lire x^{-1} comme x^n, avec $n = -1$. D'après Définition I.1.5, il faut interpréter cette notation comme $(x^{-1})^{-n}$, c'est à dire $(x')^1$, ou encore : x'.

Autrement dit, nous avons deux manières pour interpréter la notation x^{-1}, mais les deux lui donne le même sens. Ouf !

Nous avons donnée la Définition I.1.5 en notation multiplicative. En notation additive, on écrira nx au lieu de x^n, et pour n négatif, $nx = (-n)(-x)$. Voir l'Exercice I.4.

Lemme I.1.6. *Soit G un groupe, et $x \in G$. Alors*

$$x = e \iff x^2 = x.$$

De surcroît, pour tout $y \in G$:

$$x = e \iff xy = y \iff yx = y,$$

et pour tout $z \in G$

$$z = x^{-1} \iff xz = e \iff zx = e.$$

Démonstration. Montrons d'abord que $x = e \iff xy = y$. En effet, $\Longrightarrow$ est par définition. Pour $\Longleftarrow$, on suppose que $xy = y$. Alors

$$x = xe = x(yy^{-1}) = (xy)y^{-1} = yy^{-1} = e.$$

On démontre que $x = e \iff yx = y$ de la même façon. Comme y est arbitraire, on peut prendre $y = x$, d'où $x = e \iff x^2 = x$. La preuve de la dernière équivalence est laissé en exercice. ■

2. Isomorphismes, isomorphie

Le reste du chapitre est principalement consacré aux exemples de groupes. Une question qui va se poser, et qui n'est pas du tout anodine, est : étant donné deux groupes, sont-ils vraiment distincts ? ou a-t-on donné par inadvertance deux fois le même exemple ?

Exemple I.2.1. Considérons quelques groupes :
- Soit $G_1 = \{e, x\}$ muni de la loi $e^2 = x^2 = e$ et $ex = xe = x$. On laisse au lecteur le soin de vérifier qu'il s'agit bien d'un groupe.
- Soit $G_2 = \{\pm 1\}$ muni du produit habituel : $1^2 = (-1)^2 = 1$ et $1 \cdot (-1) = (-1) \cdot 1 = -1$. Ça aussi, c'est un groupe.
- Soit $G_3 = \{\spadesuit, \clubsuit\}$ muni de la loi $\spadesuit^2 = \clubsuit^2 = \spadesuit$ et $\spadesuit\clubsuit = \clubsuit\spadesuit = \clubsuit$. C'est toujours un groupe. Quel est son neutre ?
- Et pour finir, soit $G_4 = (\mathbf{Z}/2\mathbf{Z}, +)$. C'est un groupe additif, cette fois-ci, avec loi $\overline{0} + \overline{0} = \overline{1} + \overline{1} = \overline{0}$ et $\overline{0} + \overline{1} = \overline{1} + \overline{0} = \overline{1}$.

Pourquoi a-t-on l'impression d'avoir défini de quatre manière différentes « le même groupe » ? Qu'entendons-nous par cela ?

Définition I.2.2. Soit G et H deux groupes (ici, en notation multiplicative, mais rien n'empêche l'un ou l'autre, voire les deux, d'être en notation additive, voire d'avoir une loi notée

encore par un autre symbole). Un **isomorphisme de groupes** entre G et H est une application bijective $\varphi\colon G \to H$ qui respecte la loi :

$$\varphi(xy) = \varphi(x)\varphi(y). \tag{1}$$

S'il existe un isomorphisme entre G et H on dit que G et H sont **isomorphes**, et on le note $G \cong H$, ou plus explicitement (en incluant φ), $\varphi\colon G \xrightarrow{\sim} H$.

Notez bien que dans (1), à gauche nous employons la loi de G et à droite, de H. Si on le souhaite, on peut rendre ça plus explicite en écrivant :

$$\varphi(x \cdot_G y) = \varphi(x) \cdot_H \varphi(y).$$

C'est plus clair, mais aussi plus lourd. D'ailleurs, si on suit bien, il ne devrait pas y avoir d'ambiguïté, donc cette notation plus lourde n'est par forcément nécessaire.

La relation d'isomorphie est une relation d'équivalence (Exercice I.11). Lorsque deux groupes sont isomorphes, on obtient l'un de l'autre en renommant les éléments, et éventuellement même en renommant la loi : ce ne sont que des changements « cosmétiques », laissant l'objet algébrique essentiellement le même.

Maintenant on peut répondre à la question qui suit l'Exemple I.2.1 : les quatre groupes sont, en effet, isomorphes (Exercice I.12), et ne présentent qu'un seul et même exemple (que l'on appellera dans la section suivante « le groupe cyclique d'ordre deux »).

Définition I.2.3. Un groupe qui consiste en un seul élément (forcément son neutre) est dit **trivial**. En notation multiplicative, un groupe trivial peut être noté $\{1\}$, et en notation additive $\{0\}$.

On appelle souvent un tel groupe « **le** groupe trivial », bien qu'il en existe plusieurs, puisqu'il sont tous isomorphes (Exercice I.14). On exprimera la même idée en disant que : à isomorphie près, le groupe trivial est unique.

3. Groupes monogènes

Notons par $\mathbf{N}^\star$ l'ensemble $\mathbf{N} \smallsetminus \{0\}$, c'est à dire les entiers naturels strictement positifs.

Définition I.3.1. Soit G un groupe et $x \in G$. L'**ordre** de x, noté $\mathrm{ord}(x)$, est le plus petit $m \in \mathbf{N}^\star$ tel que $x^m = e$, s'il en existe un, ou ∞ sinon.

On constate que $x \in G$ est le neutre si et seulement si $\mathrm{ord}(x) = 1$.

Lemme I.3.2. *Soit G un groupe et $x \in G$.*

— *Si $\mathrm{ord}(x) = m$ est fini, alors pour tout $n, n' \in \mathbf{Z}$:*

$$x^n = x^{n'} \iff n \equiv n' \mod m.$$

En particulier,

$$x^n = e \iff n \equiv 0 \mod m \iff m \mid n.$$

— *Si $\mathrm{ord}(x) = \infty$, alors pour tout $n, n' \in \mathbf{Z}$:*

$$x^n = x^{n'} \iff n = n'.$$

En particulier,

$$x^n = e \iff n = 0.$$

Démonstration. Supposons d'abord que $\mathrm{ord}(x) = m$ est fini. Pour chaque $n \in \mathbf{Z}$ il existe $q \in \mathbf{Z}$ et $0 \leq r < m$ tels que $n = mq + r$ (division avec reste). Alors

$$x^n = x^{mq+r} = (x^m)^q x^r = x^r.$$

Puisque m est minimal dans $\mathbf{N}^\star$ tel que $x^m = e$, on ne peut avoir $x^r = e$ que si $r = 0$. On conclut que $x^n = e$ si et seulement si $m \mid n$. Par conséquent, $x^n = x^{n'}$ si et seulement si $x^{n-n'} = e$, si et seulement $m \mid (n - n')$, si et seulement si $n \equiv n' \mod m$.

Supposons maintenant que $\mathrm{ord}(x) = \infty$, et soit $n \in \mathbf{Z}$. Si $n = 0$, alors $x^n = x^0 = e$. Si $n > 0$, alors $x^n \neq e$ (car $x^m \neq e$ pour tout $m \in \mathbf{N}^\star$). Si $n < 0$, alors $-n > 0$, donc $x^{-n} \neq e$, donc $x^n = (x^{-n})^{-1} \neq e$ également. ■

Définition I.3.3. L'**ordre d'un groupe** G est son cardinal (ou plus précisément, le cardinal de son ensemble sous-jacent).

Définition I.3.4. Soit G un groupe et $x \in G$. On définit :

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

Bien évidemment, l'ensemble $\langle x \rangle$ ne dépend pas que de x, mais aussi de G, et s'il y a le risque d'ambiguïté on le notera plutôt par $\langle x \rangle_G$. Si $G = \langle x \rangle$, on dit que x est un **générateur** de G, ou que G est **engendré** par x. (Ceci est un cas particulier d'une définition plus générale que nous verrons plus tard.)

Définition I.3.5. Un groupe G est dit **monogène** (= engendré par un élément) s'il existe $x \in G$ tel que $G = \langle x \rangle$. Un groupe monogène fini (c'est-à-dire d'ordre fini) et non trivial est dit **cyclique**.

Exemple I.3.6. Voici quelque exemples de groupes monogènes. On verra bientôt qu'à isomorphie près, ce sont **tous** les groupes monogènes.

- Le groupe $(\mathbf{Z}, +)$ est un groupe monogène infini, avec générateur 1.
- Pour chaque $n \in \mathbf{N}$, $n \geq 2$, le groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ est cyclique d'ordre n. En effet, son ensemble sous-jacent est $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ (sans répétition), et il est engendré par $\overline{1}$.
- Pour $n = 1$, on a $\mathbf{Z}/1\mathbf{Z} = \{\overline{0}\}$, et $(\mathbf{Z}/1\mathbf{Z}, +)$ est le groupe trivial (que nous ne considérons pas comme cyclique).

Lemme I.3.7. *Soit $G = \langle x \rangle$ un groupe monogène. Alors de deux choses l'une :*

- *Si $\mathrm{ord}(x) < \infty$, disons $\mathrm{ord}(x) = m$, alors*

$$G = \{e, x, \ldots, x^{m-1}\} = \{x^n : 0 \leq n < m\}$$

  sans répétition, si bien que $|G| = m$.
- *Si $\mathrm{ord}(x) = \infty$, alors*

$$G = \{x^n : n \in \mathbf{Z}\} \tag{2}$$

  sans répétition : si $m \neq n$ alors $x^m \neq x^n$.

Dans un cas comme dans l'autre, on a égalité d'ordre, fini ou infini,

$$|G| = \mathrm{ord}(x).$$

Démonstration. Découle immédiatement du Lemme I.3.2. ■

Bien évidemment, si le groupe G est additif, il faudrait écrire nx au lieu de x^n. En particulier, $\mathrm{ord}(x)$ serait le plus petit $m \in \mathbf{N}^\star$ tel que $mx = 0$, s'il en existe un, et ∞ sinon.

Dans l'Exercice I.15 nous montrons que deux groupes monogènes de même ordre sont isomorphes. D'ailleurs, deux groupes isomorphes doivent avoir le même ordre (si deux ensembles sont en bijection, c'est qu'il ont le même cardinal). Compte tenu de l'Exemple I.3.6, il existe, à isomorphie près, exactement un groupe monogène de chaque ordre.

Nous obtenons en particulier que :

> Deux groupes monogènes sont isomorphes si et seulement s'ils ont le même ordre (Exercice I.16).

Formulé sous cette forme, on appelle ça un résultat de **classification** : il classifie (identifie, à isomorphie près) tous les groupes dans une famille donnée (ici, la famille des groupes monogènes) en utilisant une propriété du groupe qui ne change pas entre deux groupes isomorphes (ici, l'ordre).

Nous verrons d'autres résultats de classification plus tard : la classification des groupes (ou des familles assez larges de groupes) est l'un des buts majeurs de la théorie des groupes !

Notation I.3.8. Nous notons par C_n le groupe cyclique d'ordre n, en notation multiplicative.

4. Le groupe symétrique

Nous présenterons ici une famille d'exemples particulièrement importants : les groupes de permutations, appelés aussi groupes symétriques.

Définition I.4.1. Soit X un ensemble. Une application bijective $\sigma\colon X \to X$ s'appelle une **permutation** de X. Si σ et τ sont deux permutations de X, on note par $\sigma\tau = \sigma \circ \tau$ leur composition en tant qu'applications :

$$(\sigma\tau)(x) \equiv \sigma(\tau(x)).$$

L'ensemble de toutes les permutations de X est noté S_X (parfois $\mathfrak{S}_X$, avec « S gothique »). Lorsque $X = \{1, \dots, n\}$, on note S_X aussi par S_n.

Définition I.4.2. L'ensemble S_X muni de la loi de composition, notée $\cdot$, est appelé le **groupe de permutations** de X, ou le **groupe symétrique** de X. Son neutre est $e = 1 = \mathrm{id}_X$.

Nous utiliserons l'une de deux notations pour les membres de S_n. D'abord, une notation « explicite » :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Exemple I.4.3. Dans S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \tag{3}$$

Si on multiplie dans l'ordre inverse :

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tag{4}$$

En particulier, S_3 n'est pas un groupe abélien. Cet exemple peut être adapté pour montrer que S_X n'est pas abélien dès que $|X| \geq 3$.

Étudions maintenant une autre notation pour les permutations, en produit de cycles à supports disjoints. Commençons par la partie « supports disjoints, » qui nous fournit d'ailleurs un critère suffisant pour que des permutations commutent entre elles.

Définition I.4.4. Soit X un ensemble et $\sigma \in S_X$ une permutation. Le **support** de σ est l'ensemble de $x \in X$ qui sont « déplacés » par σ :

$$\operatorname{supp}(\sigma) = \{x \in X : \sigma(x) \neq x\}.$$

On laisse en exercice (Exercice I.25) de montrer que si $x \in \operatorname{supp}(\sigma)$, alors $\sigma^n(x) \in \operatorname{supp}(\sigma)$ aussi pour tout $n \in \mathbf{Z}$.

Lemme I.4.5. *Soit $\tau_1, \ldots, \tau_k \in S_X$ de supports deux-à-deux disjoints. Soit σ la composition des τ_i dans un ordre arbitraire. Alors pour chaque $x \in X$ on a :*

$$\sigma(x) = \begin{cases} \tau_i(x) & \text{si } x \in \operatorname{supp}(\tau_i) \text{ pour un } i, \\ x & \text{si } x \notin \operatorname{supp}(\tau_i) \text{ pour tout } i. \end{cases}$$

En particulier, σ ne dépend pas de l'ordre de la composition, et

$$\operatorname{supp}(\sigma) = \bigcup_{i=1}^{k} \operatorname{supp}(\tau_i).$$

Démonstration. Supposons d'abord qu'il existe i tel que $x \in \operatorname{supp}(\tau_i)$. Alors $\tau_i(x) \in \operatorname{supp}(\tau_i)$. Puisque les supports sont disjoints, $x, \tau_i(x) \notin \operatorname{supp}(\tau_j)$ pour tout $j \neq i$. Il en découle que $\sigma(x) = \tau_i(x)$.

Dans l'autre cas, x n'appartient à $\operatorname{supp}(\tau_i)$ pour aucun i, donc $\tau_i(x) = x$ pour tout i, et $\sigma(x) = x$.

Il en découle que $\sigma(x) \neq x$ si et seulement s'il existe i tel que $x \in \operatorname{supp}(\tau_i)$, d'où la dernière formule. ■

Par conséquent, lorsque $T \subseteq S_X$ est une famille finie de permutations à supports disjoints, alors on peut définir

$$\prod T = \prod_{\tau \in T} T$$

comme étant la composition des membres de T dans un ordre quelconque, sachant que le résultat de cette composition ne dépend pas de l'ordre.

Définition I.4.6. Soit X un ensemble, $m \geq 2$, et $x_1, x_2, x_3, \ldots x_m$ une suite finie (de longueur m) dans X, sans répétitions. On notera par $(x_1\ x_2\ \ldots\ x_m)$ (les x_i séparés par des espaces, sans virgule) l'application $\sigma\colon X \to X$ définie par :

$$\sigma(y) = \begin{cases} x_{i+1} & \text{si } y = x_i,\ i < m \\ x_1 & \text{si } y = x_m \\ y & \text{si } y \neq x_i \text{ pour tout } 1 \leq i \leq m. \end{cases}$$

Une application qui peut s'écrire de cette manière est appelée un **cycle** de longueur m, ou un m**-cycle**. Un 2-cycle $(x\ y)$ s'appelle aussi une **transposition**.

Un cycle est toujours une permutation (Exercice I.24). Le cycle $(x_1\ x_2\ \ldots\ x_m)$ envoie x_1 à x_2, x_2 à x_3, et ainsi de suite, jusqu'à x_m qui s'envoie au point de départ x_1, clôturant le cycle. Mais le choix de x_1 comme point de départ est tout à fait arbitraire : on aurait pu commencer le cycle avec tout autre x_i :

$$(x_1\ x_2\ \ldots\ x_m) = (x_i\ x_{i+1}\ \ldots\ x_m\ x_1\ x_2\ \ldots\ x_{i-1}).$$

L'identité n'est pas considérée comme cycle, et il n'existe pas de cycles de longueur un (pourquoi ?)

Exemple I.4.7. Dans S_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2) = (2\,1),$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3) = (3\,2),$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) = (2\,3\,1) = (3\,1\,2).$$

L'identité (3) peut être écrite sous forme de cycles comme :

$$(1\,2)(2\,3) = (1\,2\,3)$$

ce qui est bien plus compact.

Toutes les permutations ne sont pas des cycles. Par exemple, dans S_4, le produit $(1\,2)(3\,4)$ n'est pas un cycle (cela exige encore un argument !) Si $\sigma = (x_1\ x_2\ \dots\ x_m) \in S_X$ est un m-cycle, alors $\operatorname{supp}(\sigma)$ est l'ensemble $\{x_1, x_2, \dots, x_m\}$. En effet, l'inclusion $\subseteq$ est par définition, et l'inclusion $\supseteq$ vient de notre insistance que la longueur d'un cycle est au moins deux. Il en découle que $m = |\operatorname{supp}(\sigma)|$.

Lemme I.4.8. *Soit σ un cycle, et $x \in \operatorname{supp}(\sigma)$ quelconque. Alors*

$$\sigma = (x\ \sigma(x)\ \sigma^2(x)\ \dots\ \sigma^{m-1}(x)),$$

où $m > 0$ est minimal tel que $\sigma^m(x) = m$.

Démonstration. Puisque σ est un cycle, on peut l'écrire sous la forme $\sigma = (x_1\ x_2\ \dots\ x_k)$. Comme $x \in \operatorname{supp}(\sigma)$, on a $x = x_i$ pour un certain i. Alors $k > 0$ est minimal tel que $\sigma^k(x) = x$, donc $k = m$, et

$$\sigma = (x_i\ x_{i+1}\ \dots\ x_k\ x_1\ x_2\ \dots\ x_{i-1}) = (x\ \sigma(x)\ \sigma^2(x)\ \dots\ \sigma^{m-1}(x)).$$ ■

Lemme I.4.9. *Soit $\sigma \in S_X$ une permutation à support fini et soit $x \in \operatorname{supp}(\sigma)$.*

(i) *Il existe $m > 0$ tel que $\sigma^m(x) = x$.*

(ii) *Fixons le plus petit $m > 0$ tel que $\sigma^m(x) = x$. Alors $m \geq 2$ et*

$$\sigma_x = (x\ \sigma(x)\ \sigma^2(x)\ \dots\ \sigma^{m-1}(x)) \tag{5}$$

définit un cycle.

(iii) *On a $\operatorname{supp}(\sigma_x) \subseteq \operatorname{supp}(\sigma)$, et si $y \in \operatorname{supp}(\sigma_x)$ alors $\sigma_x = \sigma_y$.*

Démonstration. Puisque $x \in \operatorname{supp}(\sigma)$, on a aussi $\sigma^n(x) \in \operatorname{supp}(\sigma)$ pour tout n. Puisque $\operatorname{supp}(\sigma)$ est fini, il doit exister $p < q$ tels que $\sigma^p(x) = \sigma^q(x) = \sigma^p(\sigma^{q-p}(x))$. Puisque σ^p est une permutation, et en particulier une application injective, $x = \sigma^m(x)$, où $m = q - p > 0$.

Pour la suite on se fixe le plus petit $m > 0$ tel que $x = \sigma^m(x)$. On a $x \in \operatorname{supp}(\sigma)$, donc $x \neq \sigma(x)$ et forcément $m \geq 2$. Supposons que l'on ait encore $\sigma^p(x) = \sigma^q(x)$ avec $0 \leq p < q < m$. Alors $\sigma^{q-p}(x) = x$ comme plus haut, ce qui contredit la minimalité de m. Ainsi, (5) définit bien un cycle (car les éléments entre parenthèses sont sans répétition).

Si $y \in \operatorname{supp}(\sigma_x)$, alors il existe $0 \leq r < m$ tel que $y = \sigma^r(x)$. D'abord, ceci implique que $y \in \operatorname{supp}(\sigma)$, et comme y est arbitraire, $\operatorname{supp}(\sigma_x) \subseteq \operatorname{supp}(\sigma)$. Puis $\sigma^m(y) = \sigma^{m+r}(x) = \sigma^r(x) = y$, et

$$\begin{aligned} \sigma_x &= (\sigma^r(x)\ \sigma^{r+1}(x)\ \dots\ \sigma^{m-1}(x)\ x\ \dots\ \sigma^{r-1}(x)) \\ &= (\sigma^r(x)\ \sigma^{r+1}(x)\ \dots\ \sigma^{m-1}(x)\ \sigma^m(x)\ \dots\ \sigma^{m+r-1}(x)) \\ &= (y\ \sigma(y)\ \dots\ \sigma^{m-1}(y)). \end{aligned}$$

En particulier $m > 0$ est minimal tel que $\sigma^m(y) = y$, d'où $\sigma_x = \sigma_y$. ■

Théorème I.4.10 (Décomposition de permutations en produit de cycles disjoints)**.** *Soit $\sigma \in S_X$ une permutation à support fini (si X est fini, toute permutation est à support fini). Alors σ se décompose d'une manière unique comme produit de cycle disjoints.*

Autrement dit, il existe une unique famille $T = \{\tau_1, \dots, \tau_k\}$ de cycles à supports deux-à-deux disjoints, dont σ est le produit.

Démonstration. Montrons d'abord l'unicité. Soit donc T une famille finie de cycles à supports disjoints, et supposons que $\sigma = \prod T$. D'après le Lemme I.4.5, on a $\mathrm{supp}(\sigma) = \bigcup_{\tau \in T} \mathrm{supp}(\tau)$ (et c'est une réunion disjointe). Si $x \in \mathrm{supp}(\sigma)$, alors $x \in \mathrm{supp}(\tau)$ pour un unique $\tau \in T$, que l'on notera τ_x. Montrons que

$$T = \{\tau_x : x \in \mathrm{supp}(\sigma)\}.$$

En effet, l'inclusion $\supseteq$ est par définition de τ_x. Pour l'autre, $\tau \in T$, alors $\mathrm{supp}(\tau) \neq \varnothing$, donc il existe $x \in \mathrm{supp}(\tau) \subseteq \mathrm{supp}(\sigma)$, et $\tau = \tau_x$.

Fixons $x \in \mathrm{supp}(\sigma)$, et montrons que $\sigma^n(x) = \tau_x^n(x)$ pour tout $n \in \mathbf{N}$.

— Pour $n = 0$ c'est juste $x = x$.

— Supposons que $\sigma^n(x) = \tau_x^n(x)$. On sait que $\tau_x^n(x) \in \mathrm{supp}(\tau_x)$ (puisque $x \in \mathrm{supp}(\tau_x)$), et d'après Lemme I.4.5 :

$$\sigma^{n+1}(x) = \sigma(\sigma^n(x)) = \sigma(\tau_x^n(x)) = \tau_x(\tau_x^n(x)) = \tau_x^{n+1}(x).$$

D'après le Lemme I.4.8,

$$\begin{aligned}\tau_x &= (x\ \tau_x(x)\ \dots\ \tau_x^{m-1}(x)) \\ &= (x\ \sigma(x)\ \dots\ \sigma^{m-1}(x)) = \sigma_x,\end{aligned}$$

où m est minimal tel que $\tau_x^m(x) = \sigma^m(x) = x$ et σ_x est comme dans Lemme I.4.9. On conclut que $T = \{\sigma_x : x \in \mathrm{supp}(\sigma)\}$ est déterminé par σ, d'où l'unicité.

Montrons l'existence. Compte tenu de la preuve d'unicité, nous n'avons de choix que de poser $T = \{\sigma_x : x \in \mathrm{supp}(\sigma)\}$, et montrer que c'est une famille finie de cycles à supports disjoints, dont le produit est σ.

— Finie : puisque $\mathrm{supp}(\sigma)$ est fini.

— De cycles : nous savons que chaque σ_x est un cycle.

— À supports disjoints : supposons que $z \in \mathrm{supp}(\sigma_x) \cap \mathrm{supp}(\sigma_y)$. Alors, d'après le Lemme I.4.9, $\sigma_x = \sigma_z = \sigma_y$. La contraposée est : si $\sigma_x \neq \sigma_y$, c'est que $\mathrm{supp}(\sigma_x) \cap \mathrm{supp}(\sigma_y) = \varnothing$.

Il nous reste à montrer que $\sigma = \prod T$. Prenons $x \in X$ et considérons deux cas. Si $x \in \mathrm{supp}(\sigma)$ alors $x \in \mathrm{supp}(\sigma_x)$, et d'après le Lemme I.4.5 :

$$\left(\prod T\right)(x) = \sigma_x(x) = \sigma(x).$$

Par contre, si $x \notin \mathrm{supp}(\sigma)$, alors $x \notin \mathrm{supp}(\sigma_y)$ pour tout $y \in \mathrm{supp}(\sigma)$ (car $\mathrm{supp}(\sigma_x) \subseteq \mathrm{supp}(\sigma)$), et

$$\left(\prod T\right)(x) = x = \sigma(x).$$

Donc $\sigma = \prod T$ et la preuve est complète. ■

Pour résumer, si $\sigma \in S_n$ est donné, nous parcourons les $i \in \{1, \dots, n\}$ un par un (par exemple, dans l'ordre) :

— Si $\sigma(i) = i$, ou si $i \in \mathrm{supp}(\sigma_j)$ pour un σ_j que l'on a déjà construit, on oublie i.

— Sinon, on construit le cycle

$$\sigma_i = (i\ \sigma(i)\ \sigma^2(i)\ \dots\ \sigma^{m-1}(i)),$$

nous arrêtant juste avant la première répétition (le plus petit $m > 0$ tel que $\sigma^m(i) = i$). Son support est :

$$\mathrm{supp}(\sigma_i) = \{i, \sigma(i), \dots, \sigma^{m-1}(i)\}.$$

Procédant ainsi on obtient l'**unique** famille de cycles disjoints dont σ est le produit.

Exemple I.4.11. Appliquons cette procédure à

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 4 & 3 & 1 & 5 & 7 \end{pmatrix} \in S_7.$$

— $\sigma(1) \neq 1$, donc on calcule : $\sigma_1 = (1\ 6\ 5)$ et $\mathrm{supp}(\sigma_1) = \{1, 5, 6\}$,
— $\sigma(2) = 2$, on ne fait rien,
— $3 \neq \sigma(3)$ et $3 \notin \mathrm{supp}(\sigma_1)$, donc on calcule : $\sigma_3 = (3\ 4)$ et $\mathrm{supp}(\sigma_3) = \{3, 4\}$,
— $4 \in \mathrm{supp}(\sigma_3)$,
— $5 \in \mathrm{supp}(\sigma_1)$,
— $6 \in \mathrm{supp}(\sigma_1)$,
— $\sigma(7) = 7$,

et c'est fini :

$$\sigma = (1\ 6\ 5)(3\ 4).$$

Puisque les cycles sont disjoint, l'ordre des cycles importe peu, et on a aussi

$$\sigma = (3\ 4)(1\ 6\ 5).$$

5. Groupes associés à d'autres structures algébriques

Commençons par une structure algébrique bien familière : un espace vectoriel E au-dessus d'un corps $\mathbf{F}$ ($\mathbf{F}$ pourrait être $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}$, ou tout autre corps). Il s'agit d'un ensemble E muni de deux sortes d'opérations : une addition $+ \colon E \times E \to E$, et une multiplication par scalaires $\cdot \colon \mathbf{F} \times E \to E$. Ces opérations vérifient une liste d'axiomes que nous considérons inutile de rappeler ici dans leur ensemble : le lecteur devrait les connaît, et vérifiera facilement qu'ils implique que $(E, +)$ est un groupe abélien. On l'appel le **groupe additif** de l'espace vectoriel E (notez bien que dans le groupe abélien de E nous avons perdu toute trace du corps $\mathbf{F}$ ainsi que de l'opération de multiplication par scalaire).

On verra de nombreux exemples de cette sorte, par exemple $(\mathbf{R}^n, +)$ (le groupe additif du $\mathbf{R}$-espace vectoriel $\mathbf{R}^n$), ou $(\mathbf{C}^n, +)$ (le groupe additif du $\mathbf{C}$-espace vectoriel $\mathbf{C}^n$), voire $(\mathbf{F}^n, +)$, où $\mathbf{F}$ est n'importe quel corps. Pour l'instant nous n'avons pas beaucoup de choses intéressantes à dire de ces groupes, hormis le fait de leur existence.

Passons à une famille bien plus intéressante d'exemples. Ceci nous oblige à introduire une nouvelle définition :

Définition I.5.1. Un **anneau** $(A, +, \cdot)$ consiste d'un ensemble A muni de deux opérations binaires $+$ et $\cdot$, tel que :
— $(A, +)$ est un groupe abélien, dont le neutre sera noté comme d'habitude par 0.
— A est clos pour la multiplication : si $a, b \in A$ alors $ab \in A$.
— La multiplication est associative :

$$a(bc) = (ab)c.$$

— La multiplication est distributive au-dessus de l'addition, des deux côtés :

$$(a+b)c = ac + bc, \qquad a(b+c) = ab + ac.$$

Nous exigeons l'associativité des deux côtés, car la multiplication n'est pas forcément commutative. D'ailleurs :

— Un anneau A est dit **commutatif** si la multiplication de A est commutative.
— Un anneau A est dit **unitaire** s'il admet un neutre multiplicatif (c'est à dire un neutre, des deux côtés, pour la multiplication), noté 1. On appelle ce neutre l'**identité** de A.

Si A est un anneau et $a \in A$, alors

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a,$$

d'où $0 \cdot a = 0$. On démontre de la même manière que $a \cdot 0 = 0$.

Si A est unitaire alors le neutre multiplicatif est unique. En effet, si $1'$ est un autre neutre multiplicatif, alors $1 = 1 \cdot 1' = 1'$.

Si A est un anneau, alors $(A, +)$ est un groupe, c'est bien ça la définition d'un anneau. On l'appelle le **groupe additif** de A. Lorsque A est unitaire, on peut lui associer un deuxième groupe, un peu plus intéressant.

Définition I.5.2. Soit A un anneau unitaire et $a \in A$. Un élément $a' \in A$ est dit **inverse** de a si $aa' = a'a = 1$. On dit que a est **inversible** s'il admet un inverse.

L'ensemble des éléments inversibles de A sera noté $A^\times$.

Lemme I.5.3. *Soit A un anneau unitaire. Alors $1 \in A^\times$, et $(A^\times, \cdot)$ (les éléments inversibles de A, avec la multiplication de A) est un groupe.*

Démonstration. On a $1 \cdot 1 = 1$, donc 1 est son propre inverse. Vérifions maintenant les axiomes de groupe pour $(A^\times, \cdot)$:

(i) Si $a, b \in A^\times$, avec inverses respectifs a' et b' alors :

$$(b'a')(ab) = b'1b = b'b = 1 = aa' = a1a' = (ab)(b'a').$$

Ainsi, $b'a'$ est inverse de ab, donc $ab \in A^\times$.

(ii) la multiplication est associative : on a $a(bc) = (ab)c$ pour tous $a, b, c \in A$, et *a fortiori* pour tous $a, b, c \in A^\times$.

(iii) Existence d'un neutre : on a déjà $1 \in A^\times$, et c'est un neutre multiplicatif.

(iv) Existence d'inverse à gauche : si $a \in A^\times$ et a' est inverse de a, alors a est inverse de a'. Ainsi $a' \in A^\times$, et on a bien $a'a = 1$.

■

Il en découle que l'inverse multiplicatif, s'il existe, est unique (on aurait pu aussi le démontrer directement).

Définition I.5.4. Soit A un anneau unitaire. Le groupe $(A^\times, \cdot)$ s'appelle le **groupe multiplicatif** de A.

Notez bien la distinction entre $\star$ et $\times$:
- Nous avons utilisé la notation $\mathbf{N}^\star$ pour « $\mathbf{N}$ privé de zéro », et on peut faire pareil pour d'autres ensembles : $\mathbf{Z}^\star = \mathbf{Z} \smallsetminus \{0\}$, $\mathbf{R}^\star = \mathbf{R} \smallsetminus \{0\}$,...
- La notation $A^\times$ veut dire autre chose : les éléments inversibles de A, et ce n'est pas la même chose !
- Puisque zéro n'est jamais inversible (sauf si $0 = 1$...est-ce possible, dans un anneau ? mais écartons ce cas particulièrement pathologique), on aura toujours $A^\times \subseteq A^\star$. Parfois on a égalité ($\mathbf{R}^\times = \mathbf{R}^\star$, voir Exercice I.29) et parfois non ($\mathbf{Z}^\times = \{\pm 1\} \neq \mathbf{Z}^\star$, voir Exercice I.31).
- Finalement, $\mathbf{N}^\star = \mathbf{N} \smallsetminus \{0\}$, mais $\mathbf{N}^\times$ n'a pas de sens puisque $\mathbf{N}$ n'est pas un anneau ! (Pourquoi ne l'est-il pas ?)

Exercices

Exercice I.1. Vérifier les affirmations de l'Exemple I.1.4.

Exercice I.2. Soit G un groupe. Montrer que pour tout $x, y \in G$:

$$e^{-1} = e \qquad (xy)^{-1} = x^{-1}y^{-1}, \qquad (x^{-1})^{-1} = x.$$

Énoncer les identités analogues en notation additive. A-t-on besoin de les démontrer elles aussi ?

Exercice I.3. Soit G un groupe. Montrer que pour tout $x \in G$ et $n, m \in \mathbf{Z}$:

$$x^{-n} = (x^n)^{-1}, \qquad x^{m+n} = x^m x^n, \qquad x^{mn} = (x^m)^n.$$

Attention : pour certaines identités il y a plusieurs cas à considérer, selon si m, n (et $m+n$) sont positifs, négatifs, ou nuls.

Exercice I.4. Soit G un groupe en notation additive.

Définir nx pour chaque $x \in G$ et $n \in \mathbf{Z}$, en traduisant Définition I.1.5 à la notation additive. Traduire également les identités de l'Exercice I.3 à la notation additive. A-t-on besoin de les démontrer elles aussi ?

Exercice I.5. Montrer qu'un ensemble à un seul élément $\{e\}$ admet une unique loi de groupe. Montrer que ce groupe est abélien et que e est nécessairement le neutre de ce groupe.

D'ailleurs, un ensemble vide peut-il être muni d'une loi de groupe ?

Exercice I.6. Soit G un groupe et $x, y \in G$. Alors :

$$x = y \iff x^{-1}y = e \iff xy^{-1} = e.$$

Exercice I.7. Soit G un groupe et $x, y, z \in G$. Alors :

$$x = y \iff zx = zy \iff xz = yz \iff x^{-1} = y^{-1}.$$

En déduire que les applications suivantes sont des bijections de G avec lui-même :
- La **translation à gauche** par z : $x \mapsto zx$.
- La **translation à droite** par z : $x \mapsto xz$.
- L'inverse : $x \mapsto x^{-1}$.

Exercice I.8. Soit $(G, \cdot)$ un groupe. Définissons une nouvelle opération $\cdot^{\mathrm{op}}$ par :

$$x \cdot^{\mathrm{op}} y = y \cdot x.$$

Montrer que $(G, \cdot^{\mathrm{op}})$ est aussi un groupe il est appelé le **groupe opposé** de $(G, \cdot)$. Lorsque le groupe est noté par G seul, son groupe opposé sera noté G^{op}.

Exercice I.9. Soit G un ensemble muni d'une opération binaire $*$. Supposons que les propriétés suivantes sont vérifiées :

— **Clôture :** pour tous $x, y \in G$ on a $x * y \in G$.
— **Associativité :** $x * (y * z) = (x * y) * z$ pour tous $x, y, z \in G$.
— **Neutre à gauche :** il existe un $e \in G$ tel que $e * x = x$ pour tout $x \in G$. On fixe un tel e (même si, pour l'instant, on ne sait pas s'il en existe un seul ou plusieurs).
— **Inverse à gauche :** pour chaque $x \in G$ il existe $x' \in G$ tel que $x' * x = e$.

Alors $(G, *)$ est un groupe, e est son neutre, et pour chaque $x \in G$, x' est son inverse.
Indication : Il faudrait procéder par plusieurs étapes, en démontrant que :

— Un élément $x \in G$ est égal à e si est seulement si $x * x = x$.
— Pour chaque $x \in G$, x' est également inverse à droite : $x * x' = e$.
— L'élément e est aussi neutre à droite : $x * e = x$ pour tout $x \in G$.

Exercice I.10. Soit $\varphi\colon G \xrightarrow{\sim} H$ un isomorphisme de groupes. Montrer que $\varphi(e) = e$ (ou plus explicitement, $\varphi(e_G) = e_H$, où e_G est le neutre de G et e_H de H), et que $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Exercice I.11. Soit G, H et K des groupes.

— Montrer que l'application identité $\mathrm{id}\colon G \to G$ est un isomorphisme.
— Montrer que si $\varphi\colon G \xrightarrow{\sim} H$, alors φ est une application inversible et $\varphi^{-1}\colon H \xrightarrow{\sim} G$ (autrement dit, l'inverse d'un isomorphisme de groupes en est un).
— Montrer que si $\varphi\colon G \xrightarrow{\sim} H$ et $\psi\colon H \xrightarrow{\sim} K$, alors $\psi \circ \varphi\colon G \xrightarrow{\sim} K$ (autrement dit, la composition de deux isomorphismes de groupes en est un).

Déduire que la relation d'isomorphie est une **relation d'équivalence** : elle est réflexive, symétrique et transitive.

Exercice I.12. Montrer que les quatre groupes de l'Exemple I.2.1 sont en effet deux-à-deux isomorphes. Cela fait $\binom{4}{2} = 6$ paires de groupes à considérer. A-t-on vraiment besoin de les considérer toutes, ou peut-on faire des économies d'effort ?

Exercice I.13. Revenant à l'Exercice I.8, montrer que G et G^{op} sont toujours isomorphes.

Exercice I.14. Soit G et H deux groupe triviaux. Montrer qu'ils sont isomorphes. De surcroît, montrer qu'il existe un **unique** isomorphisme $\varphi\colon G \xrightarrow{\sim} H$.

Exercice I.15. Soit $G = \langle x \rangle$ et $H = \langle y \rangle$ deux groupe monogène de même ordre (fini ou infini). Nous aimerions définir une application $\varphi\colon G \to H$ par :

$$\varphi(x^n) = y^n \qquad n \in \mathbf{Z}.$$

(i) Montrer que φ est bien définie. Autrement dit, si $x^n = x^k$ alors $y^n = y^k$.
(ii) Montrer que φ est un isomorphisme.
(iii) Montrer que c'est l'unique isomorphisme entre G et H qui vérifie $\varphi(x) = y$.

Exercice I.16. Déduire de l'exercice précédent que deux groupes monogènes G et H sont isomorphes si et seulement si $|G| = |H|$.

Exercice I.17. Montrer que tout groupe monogène est abélien.

Exercice I.18. Montrer que tous les groupes d'ordre deux sont cycliques. En déduire qu'à isomorphie près il existe un unique groupe d'ordre deux.

Exercice I.19. Montrer que tous les groupes d'ordre trois sont cycliques. En déduire qu'à isomorphie près il existe un unique groupe d'ordre trois.

Exercice I.20. Soit G un groupe et $x \in G$ d'ordre fini $\mathrm{ord}(x) = n$. Soit $m \in \mathbf{Z}$. Exprimer $\mathrm{ord}(x^m)$ en termes de n et m.
Indication : avant de considérer le cas général, on pourrait considérer les cas suivants : $m = 0$, $m = -1$, $m > 0$ divise n, ou $m > 0$ est premier avec n.

Exercice I.21. Pour $n \in \mathbf{N}^\star$, soit $\varphi(n)$ le nombre des entiers $0 \leq m < n$ qui sont premier avec n. Ceci définit une fonction $\varphi\colon \mathbf{N}^\star \to \mathbf{N}^\star$ appelée l'**indicatrice d'Euler**. On se rappelle que C_n est l'unique groupe cyclique d'ordre n.

(i) Montrer que pour chaque $n \in \mathbf{N}^\star$ et $d \mid n$ il existe dans C_n exactement $\varphi(d)$ éléments d'ordre d.

(ii) En déduire l'identité suivante :

$$\varphi(n) = \sum_{d|n} \varphi(d).$$

Exercice I.22. Montrer que si X est fini alors $|S_X| = |X|!$ En particulier, $|S_n| = n!$

Ceci est valable aussi lorsque X est vide, ou lorsque $n = 0$, avec la convention que $0! = 1$ (c'est l'unique valeur possible, pour que l'identité $(n+1)! = n! \cdot (n+1)$ soit valable aussi pour $n = 0$).

Exercice I.23. Soit X un ensemble.

(i) Montrer que la composition de deux permutations de X est encore une permutation de X.

(ii) Montrer que la composition de permutations est associative (pour tout dire, c'est vrai pour n'importe quel composition d'applications, dès lors qu'elle est bien définie !)

(iii) Montrer que l'application identité id_X est neutre (à gauche, ou des deux côtés, comme il vous plaît) pour la composition de permutations.

(iv) Montrer que pour toute permutation $\sigma \in S_X$ il existe une permutation $\sigma' \in S_X$ qui est sont inverse pour la loi de composition (à gauche ou des deux côtés, encore).

(v) Montrer que S_X, muni de la loi de composition, est une groupe.

Exercice I.24. Un cycle $\sigma = (x_1\ x_2\ \ldots\ x_m)$ est toujours une permutation, et on a $\sigma^k(x_i) = x_j$ si et seulement si $j \equiv i + k \mod m$.

Exercice I.25. Soit $\sigma \in S_X$. Alors

(i) $\mathrm{supp}(\sigma^n) \subseteq \mathrm{supp}(\sigma)$ pour tout $n \in \mathbf{Z}$.

(ii) $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$.

(iii) $\sigma = e$ si et seulement si $\mathrm{supp}(\sigma)$ est vide.

(iv) Si $x \in \mathrm{supp}(\sigma)$ alors $\sigma(x) \in \mathrm{supp}(\sigma)$, d'où $\sigma^n(x) \in \mathrm{supp}(\sigma)$ pour tout $n \in \mathbf{N}$ (voire $n \in \mathbf{Z}$).

(v) Le cardinal de $\mathrm{supp}(\sigma)$ n'est jamais égal à un.

Exercice I.26. L'ordre d'un m-cycle est m. Plus généralement, si σ est le produit de k cycles disjoints de longueurs $m_1, \ldots, m_k$, alors $\mathrm{ord}(\sigma) = \mathrm{ppcm}(m_1, \ldots, m_k)$.

Donner un exemple où c'est faux lorsque les cycles ne sont pas disjoints (il en existe un dans S_3).

Exercice I.27. Soit $G = S_n$ (ou plus généralement, $G = S_X$). Soit

$$\sigma = (a_1\ a_2\ \ldots\ a_k) \in G$$

un cycle, et $\tau \in G$ une permutation quelconque. Alors

$$\tau\sigma\tau^{-1} = \big(\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k)\big).$$

En déduire une formule pour $\tau\sigma\tau^{-1}$ étant donnée la décomposition de σ en produit de cycles disjoints.

Exercice I.28. Soit $G = S_n$ (ou plus généralement, $G = S_X$, avec X fini). À chaque $\sigma \in G$ on définit sa **structure de cycles** comme étant la liste, en ordre croissant (et avec répétition), des longueurs des cycles dans la décomposition de σ en cycles disjoints. On pourra la noter par $SC(\sigma)$, de sorte que, par exemple

$$\sigma = (2\,5)(3\,8\,6)(4\,7) \quad \Longrightarrow \quad SC(\sigma) = (2,2,3).$$

(i) À l'aide de l'Exercice I.27, montrer que $SC(\sigma) = SC(\tau\sigma\tau^{-1})$ pour tous $\sigma, \tau \in G$.

(ii) Montrer que pour tous $\sigma, \tau \in G$ sont équivalents :
— $SC(\sigma) = SC(\tau)$
— Il existe $\rho \in G$ tel que $\tau = \rho\sigma\rho^{-1}$ (on dit alors que σ et τ sont **conjugués**).

Exercice I.29. Montrer que :

(i) $(\mathbf{R}, +, \cdot)$ est un anneau unitaire commutatif.

(ii) Son groupe additif est $(\mathbf{R}, +)$.

(iii) Son groupe multiplicatif est $\big(\mathbf{R} \smallsetminus \{0\}, \cdot\big)$ (c'est à dire que $\mathbf{R}^\times = \mathbf{R} \smallsetminus \{0\}$).

Exercice I.30. Répéter l'Exercice I.29, avec $\mathbf{R}$ remplacé par un corps quelconque F. Au fait, cet exercice nous fournit une définition équivalente d'un corps : un corps F est un anneau unitaire commutatif dans lequel tout élément non-nul est inversible.

Exercice I.31. Montrer que :

(i) $(\mathbf{Z}, +, \cdot)$ est un anneau unitaire.

(ii) Son groupe additif est $(\mathbf{Z}, +)$, l'unique groupe monogène infini.

(iii) Son groupe multiplicatif est $\big(\{\pm 1\}, \cdot\big)$. Il est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

Exercice I.32. Soit $n \in \mathbf{N}^\star$, $n \geq 2$ Montrer que :

(i) $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$ est un anneau unitaire.

(ii) Son groupe additif est $(\mathbf{Z}/n\mathbf{Z}, +)$, le groupe cyclique d'ordre n.

Son groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ sera très intéressant à étudier par la suite.

Exercice I.33. Soit $n \in \mathbf{N}^\star$. Soit $M(n, \mathbf{R})$ l'ensemble des matrices $n \times n$ à coefficients réels. Soit $\mathrm{GL}(n, \mathbf{R}) \subseteq M(n, \mathbf{R})$ l'ensemble des matrices inversibles. Montrer que :

(i) $\big(M(n, \mathbf{R}), +, \cdot\big)$ est un anneau unitaire (où $+$ et $\cdot$ représentent la somme et le produit de matrices).

(ii) Son groupe additif est $\big(M(n, \mathbf{R}), +\big)$, c'est le même que le groupe additif de $M(n, \mathbf{R})$ en tant que $\mathbf{R}$-espace vectoriel.

(iii) Son groupe multiplicatif est $\big(\mathrm{GL}(n, \mathbf{R}), \cdot\big)$.

Exercice I.34. Un **anneau intègre** est un anneau commutatif unitaire A, tel que si $a, b \in A$ et $ab = 0$, alors $a = 0$ ou $b = 0$.

(i) Montrer qu'un anneau commutatif unitaire A est intègre si et seulement si pour tous $a, b, c \in A$, si $ca = cb$ et $c \neq 0$, alors $a = b$.

(ii) Montrer que tout corps est un anneau intègre.

(iii) Montrer que tout anneau intègre fini est un corps.

(iv) Montrer que $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$ est un corps si et seulement si n est premier.

Chapitre II

Sous-groupes

1. Définitions et critères

Définition II.1.1. Soit G un groupe. Un **sous-groupe** de G est une partie $H \subseteq G$ qui est elle même un groupe pour la loi de G restreinte à H. Dans ce cas on écrit $H \leq G$.

Lemme II.1.2. *Soit G un groupe et $H \leq G$ un sous-groupe. Alors G et H ont le même neutre, que l'on pourra noter sans ambiguïté par e (en particulier, le neutre de G appartient à H). Si $x \in H$ alors l'inverse de x est le même au sens de G et au sens de H, et on pourra le noter sans ambiguïté par x^{-1}.*

Démonstration. Notons par e_G et e_H les neutres respectifs de G et de H. On a $e_H^2 = e_H$ dans H, et par conséquent aussi dans G, car $e_H \in H \subseteq G$ et la loi de H est la restriction de celle de G. On conclut que $e_H = e_G$ (voir Lemme I.1.6), on le notera simplement par e. De la même manière, si $x \in H$ et x' est son inverse au sens de H, c'est que $x'x = e$ dans H, donc dans G, et on conclut que x' est aussi l'inverse au sens de G. ■

Exemple II.1.3. On a $(\mathbf{R}^{>0}, \cdot) \leq (\mathbf{R}^{\times}, \cdot)$. Par contre, ni $(\mathbf{R}^{\times}, \cdot)$ ni $(\mathbf{R}^{\times}, +)$ n'est un sous-groupe de $(\mathbf{R}, +)$. Pourquoi ?

Exemple II.1.4. Tout groupe G admet au moins les sous-groupes suivants :
— G lui-même.
— Le sous-groupe trivial $\{e\}$.

Remarque II.1.5. Un sous-groupe de G est déterminé par son ensemble sous-jacent. Autrement dit, si $H, K \leq G$ ont le même ensemble sous-jacent, alors $H = K$ en tant que groupes. En effet, leur loi doit être la restriction de celle de G à l'ensemble sous-jacent commun.

Grâce à cette remarque, nous pourrons nous permettre, par la suite, de confondre un sous-groupe H de G avec son ensemble sous-jacent (qui sera également noté par H). Il reste encore à déterminer si une partie de G est un sous-groupe (c'est à dire, l'ensemble sous-jacent d'un tel).

Lemme II.1.6. *Soit G un groupe et $H \subseteq G$ une partie. Alors les conditions suivantes sont équivalentes :*

(i) *H est un sous-groupe de G (c'est à dire, H est l'ensemble sous-jacent d'un sous-groupe).*

(ii) *Les deux conditions suivantes sont vérifiées :*

$$H \neq \varnothing, \qquad x, y \in H \Longrightarrow x^{-1}y \in H.$$

(iii) *Les trois conditions suivantes sont vérifiées :*

$$e \in H, \qquad x \in H \Longrightarrow x^{-1} \in H, \qquad x, y \in H \Longrightarrow xy \in H.$$

Démonstration. (i) $\Longrightarrow$ (ii). Puisque H est un groupe, il n'est pas vide. Si $x, y \in H$ alors $x^{-1} \in H$, d'où $x^{-1}y \in H$.

(ii) $\Longrightarrow$ (iii). Puisque $H \neq \varnothing$, il existe $x \in H$. Ainsi, $e = x^{-1}x \in H$. Si $x \in H$, alors (puisque $e \in H$) $x = e^{-1}x \in H$. Si $x, y \in H$ alors $x^{-1} \in H$, et donc $xy = (x^{-1})^{-1}y \in H$.

(iii) $\Longrightarrow$ (i). Vérifions axiome par axiome que H, muni de la restriction de la loi de G, est un groupe :
— Clôture : si $x, y \in H$ alors $xy \in H$, par hypothèse.
— Associativité : on sait que $x(yz) = (xy)z$ pour tous $x, y, z \in G$ et *a fortiori* pour tous $x, y, z \in H$.
— Neutre : $e \in H$ par hypothèse. On a $ex = x$ pour tout $x \in G$, et *a fortiori* pour tout $x \in H$.
— Inverse : si $x \in H$ alors $x^{-1} \in H$ par hypothèse, et $x^{-1}x = e$.
Ainsi H (muni de la restriction de la loi de G), est bien un groupe. ■

Nous souhaitons proposer une formulation équivalente du même énoncé.

Définition II.1.7. Soit G un groupe. On étend la loi et l'inverse à des parties $A, B \subseteq G$ de la manière suivante :

$$AB = \{xy : x \in A,\, y \in B\}, \qquad A^{-1} = \{x^{-1} : x \in A\}.$$

Si $B = \{x\}$ est un singleton on écrit Ax au lieu de $A\{x\}$, et pareil pour xA.

Dans l'Exercice II.2 nous montrons que cette opération de produit d'ensembles est associative, et que toutes les manières naturelles pour définir les produit de trois ensembles coïncident. En particulier, on aura toujours

$$Axx^{-1} = Ae = A = xx^{-1}A.$$

⚠ Pour une partie $B \subseteq G$ qui n'est pas un singleton (pourquoi cette restriction ?), et $B^{-1} = \{y^{-1} : y \in B\}$, on peut très bien avoir

$$ABB^{-1} \neq A.$$

Voir aussi l'Exercice II.2.

Lemme II.1.8. *Soit G un groupe et $H \subseteq G$ une partie. Alors les conditions suivantes sont équivalentes :*

(i) $H \leq G$.

(ii) $H \neq \varnothing$ *et* $H^{-1}H \subseteq H$.

(iii) $e \in H$, $H^{-1} \subseteq H$, *et* $HH \subseteq H$.

D'ailleurs, si ces conditions équivalentes sont vérifiées, alors pour tout $x \in H$ on a des égalités :

$$H = H^{-1}H = H^{-1} = HH = Hx = xH. \tag{6}$$

Démonstration. Les trois conditions sont des reformulations des conditions correspondantes du Lemme II.1.6. La preuve de (6) sous l'hypothèse que $H \leq G$ est laissée en exercice. ■

Lemme II.1.9. *Soit G un groupe et $\mathcal{H}$ une famille non vide de sous-groupes de G. Posons*

$$K = \bigcap \mathcal{H} = \bigcap_{H \in \mathcal{H}} H$$

Alors K est un sous-groupe de G.

Démonstration. D'après le Lemme II.1.6 (en utilisant n'importe lequel des deux critères). ■

Définition II.1.10. Soit G un groupe.

(i) Le **centralisateur** dans G d'un élément $x \in G$ consiste des éléments de G qui commutent avec x :

$$C_G(x) = \{y \in G : xy = yx\}.$$

(ii) Plus généralement, le **centralisateur** dans G d'une partie $A \subseteq G$ consiste des éléments de G qui commutent avec tous les éléments de A :

$$C_G(A) = \{x \in G : xy = yx \text{ pour tout } y \in A\} = \bigcap_{y \in A} C_G(y).$$

(iii) Un cas d'intérêt particulier est lorsque $A = G$. Le centralisateur de G dans lui-même s'appelle le **centre** de G (noté par Z pour l'allemand *Zentrum*). Il consiste des éléments de G qui commutent avec tout élément de G :

$$Z(G) = C_G(G) = \{x \in G : xy = yx \text{ pour tout } y \in G\}.$$

Lemme II.1.11. *Les centralisateurs $C_G(x)$, $C_G(A)$, et le centre $Z(G)$ sont des sous-groupes de G.*

Démonstration. Soit $x \in G$, et $y, z \in C_G(x)$. Alors

$$\begin{aligned} ex = xe &\qquad\Longrightarrow\qquad e \in C_G(x) \\ y^{-1}x = y^{-1}(xy)y^{-1} = y^{-1}(yx)y^{-1} = xy^{-1} &\qquad\Longrightarrow\qquad y^{-1} \in C_G(x) \\ yzx = yxz = xyz &\qquad\Longrightarrow\qquad yz \in C_G(x) \end{aligned}$$

D'après le Lemme II.1.6, $C_G(x) \leq G$.

D'après le Lemme II.1.9 $C_G(A) = \bigcap_{x \in A} C_G(x)$ est également un sous-groupe, et c'est en particulier le cas du centre $Z(G) = C_G(G)$. ■

La notion de centralisateur sera principalement utilisée lorsque A est un singleton (centralisateur de x) ou G tout entier (le centre de G). Pour des parties de G, et notamment les sous-groupes de G, une notion proche mais distincte sera utile :

Définition II.1.12. Soit G un groupe et $A \subseteq G$. Nous définissons le **normalisateur** de A dans G comme :

$$N_G(A) = \{x \in G : xA = Ax\}.$$

Nous remarquerons la similarité avec la définition de $C_G(x)$. D'ailleurs, lorsque $A = \{x\}$ est un singleton, on a :

$$C_G(x) = C_G(A) = N_G(A).$$

D'une manière générale, $N_G(A)$ est toujours un sous-groupe de G, et si $H \leq G$ alors $H \leq N_G(H)$ (Exercice II.12).

2. Sous-groupe engendré

Définition II.2.1. Soit G un groupe et $S \subseteq G$ une partie quelconque, et $H \leq G$ un sous-groupe. Nous disons que H est **engendré** par S (dans G) s'il est le plus petit (pour l'inclusion) sous groupe de G contenant S.

Autrement dit, H est engendré par S si :

(i) $S \subseteq H \leq G$,

(ii) si $S \subseteq K \leq G$, alors $H \subseteq K$.

Si G est engendré par S, nous dirons que S est une **partie génératrice** de G.

Lemme II.2.2. *Soit G un groupe et $S \subseteq G$ une partie. Alors il existe un unique sous-groupe de G qui est engendré par S.*

Démonstration. **Unicité :** Supposons que H et K sont deux sous-groupes engendrés par S. En particulier, $S \subseteq K \leq G$, donc $H \subseteq K$, et par l'argument symétrique $K \subseteq H$. On déduit que $H = K$ en tant qu'ensembles, et donc en tant que groupes (voir la Remarque II.1.5).

Existence : Posons

$$\mathcal{H}_S = \{K \leq G : S \subseteq K\},$$

la famille des sous-groupes de G qui contiennent S. On a toujours $G \in \mathcal{H}_S$, et d'après le Lemme II.1.9

$$H = \bigcap \mathcal{H}_S = \bigcap_{K \in \mathcal{H}_S} K$$

est un sous-groupe de G. On a forcément $S \subseteq H$, donc $H \in \mathcal{H}_S$. Ainsi, $H \subseteq K$ pour tout $K \in \mathcal{H}_S$: c'est exactement dire que H est engendré par S. ■

Notation II.2.3. Le sous-groupe engendré par S dans G sera noté par $\langle S \rangle_G$, ou par $\langle S \rangle$ s'il n'y a pas possibilité de confusion. Si $S = \{x_1, x_2, \ldots\}$ nous écrirons $\langle x_1, x_2, \ldots \rangle$ plutôt que $\langle \{x_1, x_2, \ldots\} \rangle$.

Encore une fois, nous avons introduit une notation ambiguë ! En effet, soit G un groupe et $x \in G$. Dans la Définition I.3.4 nous avons donné un sens à la notation $\langle x \rangle$, et dans la Notation II.2.3 nous avons donné à $\langle x \rangle$ encore un sens. Nous devons donc démontrer que les deux sens coïncident.

Lemme II.2.4. *Soit G un groupe, $x \in G$, et $H = \{x^n : n \in \mathbf{Z}\}$. Alors H est le sous-groupe de G engendré par x. Autrement dit, les deux sens donnés à la notation $\langle x \rangle$ coïncident.*

Démonstration. Tout d'abord, $x = x^1 \in H$, donc $H \neq \varnothing$. Si $y, z \in H$, c'est que $y = x^n$ et $z = x^m$ pour $n, m \in \mathbf{Z}$. Alors $y^{-1}z = x^{m-n} \in H$. Ainsi, d'après le Lemme II.1.6, $H \leq G$ – et il contient x.

Soit maintenant $K \leq G$ un autre sous-groupe contenant x. C'est en particulier un groupe, donc $x^n \in K$ pour tout $n \in \mathbf{Z}$, et $H \subseteq K$.

On conclut que H est bel et bien le plus petit sous-groupe de G contenant x, c'est-à-dire le sous-groupe engendré par x. ■

Ceci justifie également la terminologie introduite dans la Définition I.3.5 : G est monogène si et seulement si il peut être engendré par un élément. Dans le cas où G n'est pas forcément monogène, pour tout $x \in G$ le sous-groupe $\langle x \rangle \leq G$ est monogène, et il est cyclique si et seulement si $1 < \mathrm{ord}(x) < \infty$.

Le Lemme I.3.7 s'applique donc à $\langle x \rangle$:

— ou bien $\mathrm{ord}(x) = m < \infty$, et

$$\langle x \rangle = \{e, x, \ldots, x^{m-1}\}$$

sans répétition,

— ou bien $\mathrm{ord}(x) = \infty$ et

$$\langle x \rangle = \{x^n : n \in \mathbf{Z}\}$$

sans répétition.

Dans un cas comme dans l'autre, l'ordre de x est égal à l'ordre du sous-groupe engendré $\langle x \rangle$ (d'où la terminologie).

3. Classes modulo un sous-groupe

Définition II.3.1. Soit G un groupe et $H \leq G$. Soit $x \in G$. L'ensemble

$$xH = \{xh : h \in H\}$$

s'appelle la **classe à gauche** de x modulo H. La famille de toutes les classes à gauche modulo H est :

$$G/H = \{xH : x \in G\}.$$

On définit la **classe à droite** et la famille des classes à droite de la même manière :

$$Hx = \{hx : h \in H\}, \qquad H \setminus G = \{Hx : x \in G\}.$$

On remarque que $H = eH = He$ est toujours une classe à la fois à gauche et à droite.

Si G est abélien, alors $xH = Hx$: toute classe à gauche est aussi une classe à droite, et vice versa. Ceci peut aussi se produire également pour un groupe non abélien – on verra ça plus tard.

En notation additive, la classe de x modulo H sera notée $x + H$ (un groupe additif est toujours abélien : $x + H = H + x$, et il n'est pas nécessaire de préciser classe à gauche ou à droite).

Lemme II.3.2. *Soit G un groupe et $H \leq G$, et soit $x, y \in G$. Alors sont équivalents :*

(i) $xH = yH$

(ii) $y \in xH$

(iii) $xH \cap yH \neq \varnothing$

(iv) $x^{-1}y \in H$

Démonstration. (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Puisque $y \in yH$.

(iii) $\Longrightarrow$ (iv). Soit $z \in xH \cap yH$. Alors il existe $u, v \in H$ tels que $z = xu = yv$, d'où $x^{-1}y = uv^{-1} \in H$.

(iv) $\Longrightarrow$ (i). Supposons que $x^{-1}y \in H$. Alors pour tout $h \in H$ on a $(x^{-1}y)h \in H$, donc $yh = x(x^{-1}y)h \in xH$, si bien que $yH \subseteq xH$. Mais nous avons aussi $y^{-1}x = (x^{-1}y)^{-1} \in H$, et le même argument sert à montrer que $xH \subseteq yH$. Ainsi, $xH = yH$. ■

En particulier, deux classes à gauche modulo H sont ou bien égales, ou bien disjointes. Autrement dit, la famille G/H des classes à gauche modulo H est une **partition** de G. On montre de la même manière que la famille $G \setminus H$ de classes à droite est une partition G (Exercice II.21).

Ceci associe à chaque sous-groupe $H \leq G$ **deux** partitions de G.

Lemme II.3.3. *Soit G un groupe et $H \leq G$. Soit $\Phi \colon G/H \to H \setminus G$ l'application $xH \mapsto Hx^{-1}$. Alors Φ est bien définie, et c'est une bijection.*

Démonstration. Pour montrer que Φ est bien définie, il faut montrer que si $xH = yH$, alors $Hx^{-1} = Hy^{-1}$. En effet, si $xH = yH$ alors $x^{-1}y \in H$. Or $x^{-1}y = x^{-1}(y^{-1})^{-1}$, donc $Hx^{-1} = Hy^{-1}$ (on utilise l'Exercice II.21).

De la même manière, on montre que l'application $\Psi \colon Hx \mapsto x^{-1}H$ est bien définie. Ces deux applications sont inverses. ■

En particulier, on a égalité de cardinaux $|G/H| = |H \setminus G|$ (possiblement infini).

Définition II.3.4. Le cardinal $|G/H|$ (égal à $|H \setminus G|$) s'appelle l'**indice** de H dans G, noté $[G : H]$.

Lemme II.3.5. *Soit G un groupe fini et $H \leq G$. Alors $|G| = |H| \cdot [G : H]$.*

Démonstration. Soit $x \in G$, et montrons d'abord que $|H| = |xH|$. En effet, l'application $T_x : h \mapsto xh$ (translation à gauche par x) est injective par Exercice I.7. L'image de H sous cette application est xH. Ainsi, T_x se restreint en une bijection de H avec xH, d'où l'égalité de cardinaux $|H| = |xH|$.

Maintenant, puisque G/H est une partition de G, on a :

$$|G| = \sum_{xH \in G/H} |xH| = \sum_{xH \in G/H} |H| = |G/H| \cdot |H| = [G : H] \cdot |H|. \qquad \blacksquare$$

Remarque II.3.6. Au fait, le Lemme II.3.5 reste valable si G est infini, et avec la même preuve. Par contre, il faut savoir manipuler des cardinaux infini, ce qui dépasse largement notre cours.

Théorème II.3.7 (Lagrange)**.** *Soit G un groupe fini, et $H \leq G$. Alors l'ordre de H divise l'ordre de G.*

Démonstration. Immédiat du Lemme II.3.5. $\blacksquare$

Corollaire II.3.8. *Soit G un groupe fini, et $x \in G$. Alors l'ordre de x divise l'ordre de G.*

Démonstration. On applique le Théorème de Lagrange avec $H = \langle x \rangle$, sachant que $\mathrm{ord}(x) = |H|$. $\blacksquare$

Corollaire II.3.9. *Soit p premier. Alors tout groupe d'ordre p est cyclique.*

Démonstration. Soit p premier et G un groupe d'ordre p. Alors $p \geq 2$, il existe donc $x \in G \setminus \{e\}$. Soit $H = \langle x \rangle \leq G$. Alors $|H|$ divise p, et $|H| \neq 1$ (car $e, x \in H$ et $e \neq x$). Donc $|H| = p = |G|$, donc $G = H = \langle x \rangle$.

Ainsi G est monogène, fini et non trivial, donc cyclique. $\blacksquare$

Exercices

Exercice II.1. Utiliser les critères du Lemme II.1.6 pour vérifier que :

— $(\mathbf{R}^{>0}, \cdot)$ est un sous-groupe de $(\mathbf{R}^{\times}, \cdot)$.
— $(\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{R}, +)$.
— $(n\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{Z}, +)$ et de $(\mathbf{R}, +)$.

Pourquoi ces critères ne nous disent pas que $(\mathbf{R}^{>0}, \cdot)$ est un sous-groupe de $(\mathbf{R}, +)$ (il ne l'est pas) ?

Exercice II.2. Soit G un groupe et $A, B, C \subseteq G$.

(i) Montrer que
$$(AB)C = A(BC) = \{xyz : x \in A,\, y \in B,\, z \in C\}.$$

(ii) Montrer que
$$(AB)^{-1} = B^{-1}A^{-1}.$$

(iii) Donner des exemples où
$$AA^{-1} \neq \{e\}$$
(montrer que $\not\subseteq$ et $\not\supseteq$ sont possible).

Exercice II.3. La relation $H \leq G$ est un ordre partiel sur les groupes. Autrement dit, cette relation est :

— **Réflexive :** $G \leq G$

— **Antisymétrique :** $H \leq G$ et $G \leq H$ implique $G = H$ (**en tant que groupes !**)
— **Transitive :** Si $K \leq H$ et $H \leq G$ alors $K \leq G$

Exercice II.4. Si $H \leq G$ et $K \leq G$, alors : $H \leq K$ ssi $H \subseteq K$.

Autrement dit, sur la famille des sous-groupes de G, l'ordre par la relation « sous-groupe » coïncide avec l'ordre par l'inclusion.

Quel est le plus petit sous-groupe de G, selon cet ordre ?

Exercice II.5. Soit G un groupe et $H \subseteq G$ une partie quelconque. Alors sont équivalents :

(i) $H \leq G$.
(ii) Pour tout $x \in G$: $x \in H \iff xH = H$.
(iii) Pour tout $x \in G$: $x \in H \iff Hx = H$.

Remarquez bien que, contrairement aux critères des Lemme II.1.6 et Lemme II.1.8, ici nous n'avons pas besoin d'exiger que H soit non vide. Pourquoi ?

Exercice II.6. Soit G un groupe et $H, K \leq G$ deux sous-groupes.

(i) Rappeler pourquoi $H \cap K \leq G$.
(ii) Montrer que $HK \leq G$ si et seulement si $HK = KH$.
(iii) Trouver une condition nécessaire et suffisante pour que $H \cup K \leq G$.
Indication : si $x \in H \smallsetminus K$ et $y \in K \smallsetminus H$, que peut-on dire de xy ?

Exercice II.7. Trouver deux sous-groupes de S_3 dont la réunion n'est pas un sous-groupe. Ainsi, le Lemme II.1.9 est faux si on remplace « intersection » par « réunion ».

Exercice II.8. Soit G un groupe et $x \in G$.

(i) Montrer que $x \in Z(G)$ si et seulement si $C_G(x) = G$.
(ii) Montrer que G est abélien si et seulement si $Z(G) = G$.

Exercice II.9. Soit G un groupe, $H \leq G$ et $K = C_G(H)$. Montrer que $H \leq C_G(K)$.

Exercice II.10. Soit G un groupe non trivial et $x \in G$. Montrer que $C_G(x)$, le centralisateur de x dans G, n'est jamais trivial.

Exercice II.11. Soit $G = S_3$. Calculer $C_G(\sigma)$ pour chaque $\sigma \in G$, ainsi que $Z(G)$.

Pouvez-vous calculer $Z(S_n)$ pour tout $n \in \mathbf{N}$?

Exercice II.12. Soit G un groupe, $A \subseteq G$ une partie, et $H \leq G$ un sous-groupe.

(i) Montrer que le normalisateur $N_G(A)$ est un sous-groupe de G.
(ii) Montrer que $H \leq N_G(H)$.

Exercice II.13. Montrer que dans un quelconque groupe G : $\langle \varnothing \rangle = \{e\}$, et c'est l'unique sous-groupe de G qui est un groupe trivial. C'est donc **le sous-groupe trivial** de G.

Exercice II.14. Soit G un groupe. Alors $\langle G \rangle = G$. Plus généralement, si $H \leq G$ alors $\langle H \rangle = H$. Et encore plus généralement, si $S \subseteq G$, alors $S \leq G$ si et seulement si $S = \langle S \rangle$.

Exercice II.15. Si $S \subseteq H \leq G$ alors $\langle S \rangle_H = \langle S \rangle_G$.

Exercice II.16. Soit G un groupe.

(i) Pour deux parties $A, B \subseteq G$, on pose

$$AB = \{xy : x \in A,\ y \in B\} \subseteq G$$

Montrer que pour $A, B, C \subseteq G$:

$$A(BC) = (AB)C$$

(ii) Pour $A \subseteq G$ on pose

$$A^{-1} = \{x^{-1} : x \in A\}.$$

Montrer que pour $A, B \subseteq G$:

$$(A^{-1})^{-1} = A, \qquad (AB)^{-1} = B^{-1}A^{-1}.$$

(iii) Pour $A \subseteq G$ on pose, par récurrence sur $n \in \mathbf{N}$:

$$A^0 = \{e\}, \qquad A^{n+1} = A^n A.$$

Montrer que pour tout $n, m \in \mathbf{N}$:

$$A^1 = A, \qquad A^{n+m} = A^n A^m, \qquad (A^{-1})^n = (A^n)^{-1}.$$

(iv) Soit maintenant $S \subseteq G$. Montrer que $(S \cup S^{-1})^{-1} = S \cup S^{-1}$. En déduire que

$$H = \bigcup_{n \in \mathbf{N}} (S \cup S^{-1})^n$$

est un sous-groupe de G.

(v) Montrer que $H = \langle S \rangle$. Autrement dit, montrer que c'est le plus petit parmi les sous-groupes de G qui contiennent S.

Autrement dit, $x \in \langle S \rangle$ si et seulement si on peut exprimer x comme produit d'éléments pris dans S ou dans S^{-1}, où on considère e comme étant un tel produit, celui de zéro éléments. Un peu informellement, on exprimera ça sous la forme

$$x = s_1^{\pm 1} s_2^{\pm 1} \cdots s_n^{\pm 1}, \qquad s_i \in S,\ n \in \mathbf{N}.$$

Exercice II.17. Encore une variante, supposant maintenant que $(G, +)$ est un groupe additif (et donc abélien). Lorsque S est fini, disons $S = \{x_1, \ldots, x_n\}$, montrer que

$$\langle S \rangle = \{k_1 x_1 + \cdots + k_n x_n : k_1, \ldots, k_n \in \mathbf{Z}\}.$$

Exercice II.18. Supposons toujours que G est additif, et considérons le cas où $S \subseteq G$ est infini. Ajoutons quelques notations. D'abord, un membre de $\mathbf{Z}^S$ sera noté $(k_x : x \in S)$ ou simplement (k_x) (où $k_x \in \mathbf{Z}$ pour tout $x \in S$). On pose

$$\mathbf{Z}^{(S)} = \left\{(k_x) \in \mathbf{Z}^S : k_x = 0 \text{ pour tout sauf un nombre fini de } x \in S\right\} \subseteq \mathbf{Z}^S.$$

Montrer que si $(k_x) \in \mathbf{Z}^{(S)}$, alors on peut bien donner un (bon) sens à la somme infini $\sum_{x \in S} k_x x$, et que

$$\langle S \rangle = \left\{ \sum_{x \in S} k_x x : (k_x) \in \mathbf{Z}^{(S)} \right\}.$$

Exercice II.19.
— Quelles sont les classes à gauche de $(\mathbf{R} \smallsetminus \{0\}, \cdot)$ modulo $(\mathbf{R}^{>0}, \cdot)$? À droite ?
— Quelles sont les classes de $(\mathbf{Z}, +)$ modulo $(n\mathbf{Z}, +)$?

Exercice II.20. Soit $H = \left\{e, (1\,2)\right\} \subseteq S_3$.
— Montrer que $H \leq S_3$.
— Montrer que $S_3/H \neq H \setminus S_3$.
— Montrer que $|S_3/H| = |H \setminus S_3|$ en les calculant explicitement.

Exercice II.21. Soit G un groupe et $H \leq G$. Soit $x, y \in G$. Alors sont équivalents :

(i) $xy^{-1} \in H$

(ii) $Hx = Hy$

(iii) $y \in Hx$

(iv) $Hx \cap Hy \neq \varnothing$

En déduire que la famille $H \setminus G$ est une partition de G.

Exercice II.22. Montrer la version « infinie » suivante du Lemme II.3.5 : Soit G un groupe et $H \leq G$. Alors $|G|$ est infini si et seulement si au moins l'un de $|H|$ ou $[G : H]$ est infini.

Exercice II.23. Soit G un groupe monogène d'ordre n (fini).

(i) Montrer qu'il admet un unique sous-groupe d'ordre d pour chaque $d \mid n$.

(ii) Montrer qu'il admet un unique sous-groupe d'indice d pour chaque $d \mid n$.

(Pour une réciproque, voir l'Exercice VI.8.)

Exercice II.24. Soit G un groupe monogène infini. Montrer qu'il admet un unique sous-groupe d'indice d pour chaque $d \in \mathbf{N}^\star$, ainsi qu'un unique sous-groupe d'indice infini.

Exercice II.25. Soit G un groupe fini, d'ordre n. Supposons que pour chaque d, G possède au plus d membres dont l'ordre divise d. Montrer que G est monogène.

Pour cela, vous pouvez suivre les étapes suivantes :

(i) Soit $x \in G$, disons $\operatorname{ord}(x) = d$. Montrer que

$$\langle x \rangle = \big\{ y \in G : \operatorname{ord}(y) \mid d \big\}.$$

(ii) Pour chaque d, soit

$$\alpha(d) = \big| \big\{ x \in G : \operatorname{ord}(x) = d \big\} \big|.$$

Montrer que si $\alpha(d) > 0$ alors $d \mid n$ et $\alpha(d) = \varphi(d)$, où φ est l'indicatrice d'Euler que nous avons étudiée dans l'Exercice I.21.

(iii) Conclure, en comparant les deux sommes $\sum_{d \mid n} \alpha(d)$ et $\sum_{d \mid n} \varphi(d)$.

Exercice II.26. À l'aide de l'Exercice II.25, montrer que si K est un corps (commutatif !) et si $G \leq K^\times$ est un sous-groupe fini, alors G est monogène.

Exercice II.27. Montrer que pour p premier, $(\mathbf{Z}/p\mathbf{Z}^\times, \cdot) \cong \big(\mathbf{Z}/(p-1)\mathbf{Z}, +\big)$.

Chapitre III

Morphismes et quotients

1. Morphismes de groupes

Définition III.1.1. Soit G et H deux groupes. Un **morphisme** (ou **homomorphisme**) de G vers (ou dans) H est une application $\varphi\colon G \to H$ qui respecte la loi :

$$\varphi(xy) = \varphi(x)\varphi(y)$$

Lemme III.1.2. *Soit $\varphi\colon G \to H$ un morphisme. Alors $\varphi(e) = e$ et $\varphi(x^{-1}) = \varphi(x)^{-1}$.*

Démonstration. Exercice III.1. ■

Lemme III.1.3. *Soient $\varphi\colon G \to H$ et $\psi\colon H \to K$ deux morphismes de groupes. Alors la composition $\psi \circ \varphi\colon G \to K$ est encore un morphisme.*

Démonstration. Exercice III.2. ■

Tout isomorphisme de groupes et en particulier un morphisme. On a également la réciproque suivante :

Lemme III.1.4. *Soit G et H deux groupes, et $\varphi\colon G \to H$ une application. Alors sont équivalents :*

(i) *φ est un isomorphisme.*

(ii) *φ est un morphisme bijectif.*

(iii) *φ est un morphisme inversible. Autrement dit, φ est un morphisme, et il existe un morphisme $\psi\colon H \to G$ qui est son inverse : $\psi \circ \varphi = \mathrm{id}_G$ et $\varphi \circ \psi = \mathrm{id}_H$.*

Démonstration. Les deux premières conditions sont équivalentes par définition. Montrons l'équivalence avec la troisième condition. D'après l'Exercice I.11, si φ est un isomorphisme alors c'est une application inversible et $\varphi^{-1}\colon H \to G$ est aussi un isomorphisme, donc un morphisme. Réciproquement, si φ est un morphisme inversible, alors φ est en particulier bijectif. ■

Nous pouvons définir d'autres « cas particuliers » :

Définition III.1.5.
- Un morphisme injectif est dit **monomorphisme** ou **plongement** (en anglais, **embedding**).
- Un morphisme surjectif est dit **épimorphisme**.
- Nous l'avons déjà dit, un morphisme bijectif (donc à la fois monomorphisme et épimorphisme) est un **isomorphisme**.
- Un morphisme de G dans lui-même s'appelle un **endomorphisme** de G.
- Un isomorphisme de G avec lui-même (donc à la fois isomorphisme et endomorphisme) s'appelle un **automorphisme**.

Ça fait beaucoup de définitions d'un coup. Les deux le plus importantes à retenir sont celle d'un morphisme et celle d'un automorphisme.

Exemple III.1.6.
- Si $H \leq G$ est un sous-groupe, alors l'identité $\mathrm{id}_H\colon H \to G$ (qui s'appelle aussi l'application inclusion) est un morphisme (et même un monomorphisme).

— En particulier, $\mathrm{id}_G \colon G \to G$ est un morphisme (et même un isomorphisme, voire un automorphisme).
— Soit $H = \{e\}$ le groupe trivial. L'unique application $G \to \{e\}$ est un morphisme (et même un épimorphisme). C'est le morphisme **trivial**.

Définition III.1.7. Soit $x \in G$. L'application

$$\varphi_x \colon G \to G, \qquad \varphi_x(u) = xux^{-1}$$

s'appelle la **conjugaison par** x.

Lemme III.1.8. *Soit G un groupe et $x, y \in G$. Alors :*

(i) $\varphi_x \colon G \to G$ *est un morphisme (donc un endomorphisme).*
(ii) $\varphi_x \circ \varphi_y = \varphi_{xy}$.
(iii) $\varphi_x \colon G \to G$ *est un automorphisme.*

Démonstration. D'abord, si $u, v \in G$ alors

$$\varphi_x(uv) = xuvx^{-1} = xux^{-1}xvx^{-1} = \varphi_x(u)\varphi_x(v),$$

c'est donc bien un morphisme. Maintenant,

$$\varphi_x \circ \varphi_y(u) = \varphi_x(yuy^{-1}) = xyuy^{-1}x^{-1} = xyu(xy)^{-1} = \varphi_{xy}(u).$$

Comme u est quelconque, $\varphi_x \circ \varphi_y = \varphi_{xy}$. Remarquons également que $\varphi_e = \mathrm{id}$ (car $\varphi_e(u) = eue = u$). Ainsi, $\varphi_x \circ \varphi_{x^{-1}} = \varphi_{xx^{-1}} = \varphi_e = \mathrm{id}_G$ et $\varphi_{x^{-1}} \circ \varphi_x = \mathrm{id}_G$ par le même raisonnement. Ainsi, φ_x est inversible, c'est donc un isomorphisme, donc un automorphisme de G. ■

Définition III.1.9. Soit $\varphi \colon G \to H$ un morphisme. Le **noyau** de φ est

$$\ker \varphi = \{x \in G : \varphi(x) = e\}.$$

L'**image** de φ est

$$\mathrm{img}\, \varphi = \{\varphi(x) : x \in G\}.$$

Lemme III.1.10. *Soit $\varphi \colon G \to H$ un morphisme. Alors* $\ker \varphi \leq G$ *et* $\mathrm{img}\, \varphi \leq H$.

Démonstration. Nous allons utiliser le Lemme III.1.2 plusieurs fois, sans mention explicite. En particulier, $\varphi(e_G) = e_H$, donc $e_G \in \ker \phi$, et $\ker \varphi \neq \varnothing$. On a $\ker \varphi \subseteq G$ par définition. Si $x, y \in \ker \varphi$ alors

$$\varphi(x^{-1}y) = \varphi(x^{-1})\varphi(y) = \varphi(x)^{-1}\varphi(y) = e^{-1}e = e.$$

D'après le Lemme II.1.6, $\ker \varphi \leq G$.

On a $\mathrm{img}\, \varphi \subseteq G$ par définition, et $e = \varphi(e) \in \mathrm{img}\, \varphi$. Si $u, v \in \mathrm{img}\, \varphi$ alors il existe $x, y \in G$ tels que $\varphi(x) = u$ et $\varphi(y) = v$. Ainsi

$$u^{-1}v = \varphi(x)^{-1}\varphi(y)\varphi(x^{-1}y) \in \mathrm{img}\, \varphi.$$

D'après le Lemme II.1.6, $\mathrm{img}\, \varphi \leq G$. ■

Quid d'une réciproque du Lemme III.1.10 ? Est-ce que tout sous groupe peut être le noyau ou l'image d'un morphisme ?

— Nous savons déjà que tout sous-groupe $H \leq G$ est l'image d'une morphisme : $\mathrm{id}_H \colon H \to G$ est un morphisme, et H est son image !
— Par contre, tout sous-groupe n'est pas forcément un noyau, mais on ne verra ça que plus tard.

Lemme III.1.11. *Soit $\varphi\colon G \to H$ un morphisme. Alors φ est injectif (c'est à dire un plongement, ou monomorphisme) si et seulement si* $\ker \varphi = \{e\}$.

Démonstration. Supposons que φ est injectif. Nous savons déjà que $e \in \ker \varphi$, car $\varphi(e) = e$. Si $x \in \ker \varphi$, alors $\varphi(x) = e = \varphi(e)$, donc $x = e$, d'où $\ker \varphi = \{e\}$.

Réciproquement, supposons que $\ker \varphi = \{e\}$. Si $\varphi(x) = \varphi(y) = u \in H$, c'est que :

$$\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) = u^{-1}u = e,$$

donc $x^{-1}y \in \ker \varphi$, donc $x^{-1}y = e$, et $x = y$. Ainsi, φ est injectif. ■

2. Sous-groupes distingués, quotients

Définition III.2.1. Un sous-groupe $H \leq G$ est dit **distingué** (en anglais, et parfois aussi en français, **normal**) si $xH = Hx$ pour tout $x \in G$. Le fait que H soit un sous-groupe distingué est noté $H \trianglelefteq G$.

Autrement dit, un sous-groupe est distingué si ses classes à gauche sont aussi des classes à droite (et réciproquement). Donc, pour un sous-groupe distingué $H \trianglelefteq G$ on pourra se contenter de parler de ses **classes** sans préciser le côté.

Rappelons-nous que dans la Définition II.1.12 nous avons défini le normalisateur $N_G(A)$ d'une partie $A \subseteq G$ comme :

$$N_G(A) = \{x \in G : xA = Ax\}.$$

Autrement dit, $H \trianglelefteq G$ si et seulement si :

(i) $H \leq G$, et

(ii) $N_G(H) = G$

Lemme III.2.2. *Soit $H \leq G$. Alors sont équivalents :*

(i) *H est distingué : $xH = Hx$ pour tout $x \in G$.*

(ii) *$xHx^{-1} = H$ pour tout $x \in G$.*

(iii) *$xHx^{-1} \subseteq H$ pour tout $x \in G$.*

(iv) *$xyx^{-1} \in H$ pour tout $x \in G$ et $y \in H$.*

Démonstration. (i) $\iff$ (ii). Si $xH = Hx$ alors $xHx^{-1} = Hxx^{-1} = H$, et pareil pour l'implication inverse.

(ii) $\iff$ (iii). Une implication est évidente. Pour l'autre, supposons que $xHx^{-1} \subseteq H$ pour tout $x \in G$, d'où

$$H = x^{-1}(xHx^{-1})x \subseteq x^{-1}Hx.$$

Puisque c'est vrai pour tout $x \in G$, c'est vrai également pour x^{-1}, d'où $H \subseteq xHx^{-1}$. Par la double inclusion $H = xHx^{-1}$.

(iii) $\iff$ (iv). Ce sont deux manières de dire la même chose. ■

Exemple III.2.3. Pour tout groupe G on a :
— $\{e\} \trianglelefteq G$.
— $G \trianglelefteq G$.
— $Z(G) \trianglelefteq G$.
(Voir l'Exercice III.10.)

Lemme III.2.4. *Soit $\varphi\colon G \to H$ un morphisme de groupes. Alors* $\ker \varphi \trianglelefteq G$.

Démonstration. Soit $x \in \ker\varphi$ et $y \in G$. Alors

$$\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y^{-1}) = \varphi(y)\varphi(y)^{-1} = e.$$

Ainsi $yxy^{-1} \in \ker\varphi$ également. Autrement dit, $y(\ker\varphi)y^{-1} \subseteq \ker\varphi$. D'après le Lemme III.2.2, $\ker\varphi \trianglelefteq G$. ■

Exemple III.2.5. Soit $G = S_3$, $\sigma = (1\,2)$ et $\tau = (1\,2\,3)$. Alors $H = \langle\sigma\rangle = \{e, \sigma\}$. Alors $H \leq G$ mais $H \not\trianglelefteq G$ (ce n'est pas un sous-groupe distingué). En effet, $\tau\sigma\tau^{-1} = (2\,3) \notin H$.

On en déduit qu'il est possible qu'un sous-groupe ne soit le noyau d'aucun morphisme (dès lors qu'il n'est pas distingué). Quid d'un sous-groupe distingué ?

Proposition III.2.6. *Soit G un groupe et $N \trianglelefteq G$.*

- *Pour toutes deux classes $xN, yN \in G/N$, leur produit (en tant que parties de G) est :*
$$(xN)(yN) = xyN.$$
- *Cette opération définit une loi de groupe sur l'ensemble G/N. Son neutre est $eN = N$, et $(xN)^{-1} = x^{-1}N$.*
- *L'application $\pi_N(x) = xN$ est un épimorphisme (morphisme surjectif) $\pi_N\colon G \to G/N$, avec noyau $\ker\pi_N = N$.*

Démonstration. D'abord, par l'associativité du produit de parties de G :

$$(xN)(yN) = x(Ny)N = x(yN)N = xyN.$$

Maintenant, pour tout $xN \in G/N$:

$$N(xN) = xNN = xN, \qquad (x^{-1}N)(xN) = x^{-1}xN = N.$$

Ainsi G/N, muni de cette loi, est bien un groupe avec neutre N et inverse $(xN)^{-1} = x^{-1}N$.

Finalement, on a

$$\pi_N(xy) = xyN = (xN)(yN) = \pi_N(x)\pi_N(y),$$

donc π_N est bien un morphisme, et

$$x \in \ker\pi_N \iff xN = N \iff x \in N.$$

(L'équivalence $x \in H \iff xH = H$ est valable pour tout sous-groupe H : voir l'Exercice II.5.) C'est un épimorphisme par définition de G/N. ■

Définition III.2.7. Soit G un groupe et $N \trianglelefteq G$. Le groupe G/N s'appelle **groupe quotient** de G par N. L'application $\pi_N\colon G \to G/N$ s'appelle l'**application quotient**.

Conclusion : les sous groupe distingués de G sont exactement les noyaux des morphismes de domaine G.

3. Les trois théorèmes d'isomorphie

Les résultats de cette section sont appelés traditionnellement le premier, deuxième et troisième théorèmes d'isomorphie. Ils affirment que certaines constructions de groupes (quotients, notamment) produisent des groupes isomorphes. De surcroît, chaque telle paire de groupes admets un isomorphisme **canonique**, c'est à dire un isomorphisme particulièrement naturel compte tenu de la construction en question.

Théorème III.3.1 (Premier théorème d'isomorphie)**.** *Soit $\varphi\colon G \to H$ un morphisme et $N = \ker\varphi$. Pour $x \in G$, posons $\overline{\varphi}(xN) = \varphi(x)$. Alors $\overline{\varphi}$ est bien défini, est c'est un isomorphisme :*

$$\overline{\varphi}\colon G/N \xrightarrow{\sim} \operatorname{img}\varphi.$$

Démonstration. Montrons que $\overline{\varphi}$ est bien défini. Supposons donc que $xN = yN$. Alors $x^{-1}yN = N$, donc $x^{-1}y \in N$, donc $e = \varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y)$, donc $\varphi(x) = \varphi(y)$.

Montrons que $\overline{\varphi}$ est un morphisme. En effet :

$$\overline{\varphi}\big((xN)(yN)\big) = \overline{\varphi}(xyN) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(xN)\overline{\varphi}(yN).$$

Montrons que c'est isomorphisme : Si $e = \overline{\varphi}(xN) = \varphi(x)$, alors $x \in \ker\varphi = N$, donc $xN = N$. Autrement dit, $\ker\overline{\varphi} = \{N\} = \{e_{G/N}\}$. D'après le Lemme III.1.11, $\overline{\varphi}$ est injectif. C'est donc un isomorphisme avec son image, qui est $\operatorname{img}\varphi$ (par définition de $\overline{\varphi}$). ■

On remarque également que par définition on a $\overline{\varphi} \circ \pi_N = \varphi$. Autrement dit, le diagramme suivant est **commutatif** :

$$\begin{array}{ccc} G & \xrightarrow{\quad\varphi\quad} & H \\ & {\scriptstyle\pi_N}\searrow \quad \nearrow{\scriptstyle\subseteq} & \\ & G/N \xrightarrow[\overline{\varphi}]{\sim} \operatorname{img}\varphi & \end{array}$$

Ceci signifie que toutes les différentes manières de composer des applications (des « flèches ») pour aller d'un point A à un point B (ici, de G à H) coïncident (ici, $\varphi = \mathrm{id}_{\operatorname{img}\varphi} \circ \overline{\varphi} \circ \pi_N$).

Exemple III.3.2. Soit n un entier ≥ 1 et posons $G = \mathrm{GL}(n, \mathbf{C})$. On considère l'homomorphisme $\det : \mathrm{GL}_n(\mathbf{C}) \to \mathbf{C}^\times$. Alors $\ker(\det) = \mathrm{SL}(n, \mathbf{C})$ est un sous-groupe distingué de G et $\mathrm{GL}(n, \mathbf{C})/\mathrm{SL}(n, \mathbf{C}) \cong \mathbf{C}^\times$.

Dans le théorème suivant, nous considérons deux sous-groupes $H, K \leq G$, et supposons que $H \leq N_G(K)$. On se rappelle que si $K \trianglelefteq G$, alors $N_G(K) = G$. Autrement dit,

$$K \trianglelefteq G \qquad \Longrightarrow \qquad H \leq N_G(K).$$

Le théorème sera donc valable sous l'hypothèse que $H \leq G$ et $K \trianglelefteq G$.

Théorème III.3.3 (Deuxième théorème d'isomorphie)**.** *Soient G un groupe, $H, K \leq G$ des sous-groupes, et supposons que $H \leq N_G(K)$. Alors :*

(i) *$KH = HK$, et c'est un sous-groupe de G.*

(ii) *$K \trianglelefteq HK$ et $K \cap H \trianglelefteq H$.*

(iii) *L'application*

$$\varphi\colon h(K \cap H) \mapsto hK,$$

pour $h \in H$, est bien définie, et c'est un isomorphisme

$$\varphi\colon H/(K \cap H) \xrightarrow{\sim} KH/K.$$

Démonstration. Si $h \in H$ et $k \in K$, alors $hkh^{-1} \in K$ (puisque $h \in H \leq N_G(K)$), d'où $hk = (hkh^{-1})h \in KH$. Ainsi, $HK \subseteq KH$. Il en suit que $KH = K^{-1}H^{-1} = (HK)^{-1} \subseteq (KH)^{-1} = H^{-1}K^{-1} = HK$, c'est à dire $KH \subseteq HK$ (on peut aussi donner un argument direct, similaire au premier). On conclut que $HK = KH$. D'après l'Exercice II.6, HK est un sous-groupe de G.

En particulier, HK est un groupe, et K en est un sous-groupe. Soit $h \in H$ et $k \in K$. Puisque $h \in H \leq N_G(K)$, on a $hKh^{-1} = K$, d'où également

$$hkK(hk)^{-1} = hkKk^{-1}h^{-1} = hKh^{-1} = K.$$

Puisque hk est un membre général de HK, on obtient $K \trianglelefteq HK$.

Pour conclure, considérons l'application $\psi\colon H \to HK/K$, qui envoie $h \in H$ à $\psi(h) = hK$. C'est la restriction à H du morphisme quotient $HK \to HK/K$, donc c'est un morphisme.

Tout membre de HK/K peut s'écrire comme hkK, où $h \in H$ et $k \in K$. Or, $hkK = hK = \psi(h)$, donc ψ est surjectif. Finalement,

$$\ker \psi = \{h \in H : \psi(h) = eK = K\}.$$

Or, $\psi(h) = hK$, donc $\psi(h) = K$ si et seulement si $h \in K$. Ainsi, $\ker \psi = H \cap K$.

D'après le premier théorème d'isomorphie, $H \cap K \trianglelefteq H$ et on a un isomorphisme $\overline{\psi}\colon H/(H \cap K) \xrightarrow{\sim} HK/K$, qui envoie $h(H \cap K)$ à $\psi(h) = hK$. ■

Le troisième théorème affirme une sorte d'élimination d'un terme commun dans un quotient. Il est laissé en exercice (Exercice III.15)

Théorème III.3.4 (Troisième théorème d'isomorphie)**.** *Soit G un groupe, et $H, K \trianglelefteq G$ deux sous-groupes distingués, de sorte que $K \subseteq H$. Alors $K \trianglelefteq H$, $H/K \trianglelefteq G/K$, et*

$$G/H \cong (G/K)/(H/K)$$

via l'isomorphisme

$$gH \mapsto (gK) \cdot (H/K).$$

(Ici, $gK \in G/K$, donc $(gK) \cdot (H/K) \in (G/K)/(H/K)$).

Résumons brièvement les trois théorèmes d'isomorphie (numéro, hypothèse, conclusion).

1er	$\varphi\colon G \to H$ un morphisme	$G/\ker\varphi \cong \operatorname{img}\varphi$
2e	$K, H \leq G$, $H \leq N_G(K)$	$H/(K \cap H) \cong HK/K$
3e	$K, H \trianglelefteq G$, $K \leq H$	$G/H \cong (G/K)/(H/K)$

Dans chacun, si la conclusion fait référence à un quotient G_1/G_2, c'est que l'affirmation "$G_2 \trianglelefteq G_1$" fait partie de la conclusion, et l'isomorphisme est tellement naturel qu'il ne sert à rien de le rappeler – vous devriez pouvoir le retrouver sans problème !

Exercices

Exercice III.1. Soit $\varphi\colon G \to H$ un morphisme de groupes. Montrer que $\varphi(e) = e$ (ou plus explicitement, $\varphi(e_G) = e_H$, où e_G est le neutre de G et e_H de H), et que $\varphi(x^{-1}) = \varphi(x)^{-1}$. (Comparer avec l'Exercice I.10.)

Exercice III.2. Soient $\varphi\colon G \to H$ et $\psi\colon H \to K$ deux morphismes de groupes. Alors la composition $\psi \circ \varphi\colon G \to K$ est encore un morphisme. (Comparer avec l'Exercice I.11.)

Exercice III.3. Soit G un groupe. Soit $\operatorname{Aut}(G)$ l'ensemble des automorphismes de G, muni de la loi de composition. Alors $\operatorname{Aut}(G)$ est un groupe, nommé le **groupe d'automorphismes** de G.

Y a-t-il un lien entre $\operatorname{Aut}(G)$ et S_G ?

Exercice III.4. On se rappelle que pour $x \in G$, la conjugaison par x est l'application $\varphi_x(u) = xux^{-1}$ et c'est un automorphisme de G. Montrer que l'application

$$\Phi\colon G \to \operatorname{Aut}(G), \qquad \Phi(x) = \varphi_x$$

est un morphisme de groupes.

Exercice III.5. Continuant l'Exercice III.4, montrer que G est abélien si et seulement si Φ est le morphisme trivial.

Exercice III.6. Montrer qu'un plongement $\varphi\colon G \to H$ est la même chose qu'un isomorphisme entre G et un sous-groupe de H (d'où la terminologie : on met G, ou plutôt une copie de G, dans H).

Exercice III.7. Montrer que tout groupe G se plonge (admet un plongement) dans S_G.
Indication : l'Exercice I.7 peut vous donner une idée (voire deux).

Exercice III.8. Soit $\varphi\colon G \to H$ un morphisme. Alors φ est trivial si et seulement si $\ker \varphi = G$.

Exercice III.9. Nous avons montré dans Lemme III.1.10 que toute image d'un morphisme est un sous-groupe. Montrer la réciproque : tout sous-groupe est l'image d'un morphisme.

Plus précisément, soit G un groupe et $H \leq G$ un sous-groupe. Alors il existe un troisième groupe K, et un morphisme $\varphi\colon K \to G$, tel que $H = \operatorname{img} \varphi$. Comment trouve-t-on K ?

Exercice III.10. Vérifier l'Exemple III.2.3 :
— $\{e\} \trianglelefteq G$.
— $G \trianglelefteq G$.
— $Z(G) \trianglelefteq G$.

Exercice III.11. Si G est abélien alors tout sous groupe de G est distingué.

Exercice III.12. Soit G un groupe. Alors tout sous-groupe d'indice 2 de G est distingué.

Exercice III.13. Soit G un groupe et $x, y \in G$. On appelle

$$[x, y] = xyx^{-1}y^{-1}$$

le **commutateur** de x et y.

Montrer que $[x, y] = e$ si et seulement si $xy = yx$ (d'où son nom).

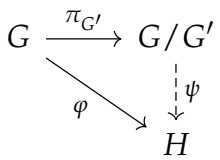
Exercice III.14. Soit G un groupe. Le sous-groupe engendré par tous les commutateurs, noté G', s'appelle le **groupe dérivé** de G :

$$G' = \big\langle [x, y] : x, y \in G \big\rangle.$$

(i) Montrer que $G' \trianglelefteq G$.

(ii) Montrer que G/G' est abélien.

(iii) Montrer que si H est un groupe abélien quelconque et $\varphi\colon G \to H$ un morphisme, alors $G' \leq \ker \varphi$ et il existe un unique morphisme $\psi\colon G/G' \to H$ tel que $\psi \circ \pi_{G'} = \varphi$. Autrement dit, il existe un unique ψ qui rend le diagramme suivant commutatif :



Exercice III.15. Démontrer le troisième théorème d'isomorphie.
Indication : une fois qu'on a démontré que $K \trianglelefteq H$ et $H/K \trianglelefteq G/K$, on peut considérer les applications quotient $G \to G/K$ et $G/K \to (G/K)/(H/K)$, et étudier leur composition.

Exercice III.16. Nous proposons de calculer le groupe $\operatorname{Aut}(\mathbf{Z}/n\mathbf{Z}, +)$, pour $n \geq 2$. Pour cela, nous allons utiliser la structure d'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$. On rappelle $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ est **inversible** s'il existe $\overline{\ell} \in \mathbf{Z}/n\mathbf{Z}$ tel que $\overline{k\ell} = \overline{1}$, et que le groupe multiplicatif de cet anneau, noté $(\mathbf{Z}/n\mathbf{Z})^\times$, est l'ensemble des ses éléments inversibles (Définition I.5.2 et Définition I.5.4).

Pour chaque $\varphi \in \operatorname{Aut}(\mathbf{Z}/n\mathbf{Z})$, posons : $\hat{\varphi} = \varphi(\overline{1})$, de sorte que $\hat{\varphi} \in \mathbf{Z}/n\mathbf{Z}$.

(i) Soit $m, k \in \mathbf{N}$. Se rappeler pourquoi, dans le groupe additif $(\mathbf{Z}/n\mathbf{Z}, +)$, la somme $\bar{k} + \cdots + \bar{k}$ (m fois), que l'on note également par $m\bar{k}$, est égale à $\overline{mk}$.

(ii) Si $\varphi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, alors $\varphi(\bar{k}) = \bar{k}\hat{\varphi}$ (le produit dans l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$) pour tout $\bar{k} \in \mathbf{Z}/n\mathbf{Z}$.

(iii) Montrer que si $\varphi, \psi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z})$, alors $\widehat{\varphi \circ \psi} = \hat{\varphi}\hat{\psi}$, et que $\hat{\mathrm{id}} = \bar{1}$.

(iv) En déduire que $\hat{\varphi} \in (\mathbf{Z}/n\mathbf{Z})^\times$ pour tout $\varphi \in \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +)$, et que l'application $\varphi \mapsto \hat{\varphi}$ est un morphisme $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +) \to \big((\mathbf{Z}/n\mathbf{Z})^\times, \cdot\big)$.

(v) Montrer que c'est un isomorphisme, d'où notre conclusion :

$$\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}, +) \cong \big((\mathbf{Z}/n\mathbf{Z})^\times, \cdot\big).$$

Exercice III.17. Utilisant les mêmes idée que dans Exercice III.16, montrer que $\mathrm{Aut}(\mathbf{Z}, +) \cong (\mathbf{Z}^\times, \cdot) = \big(\{\pm 1\}, \cdot\big)$.

Exercice III.18. Soit $(A, +, \cdot)$ un anneau commutatif unitaire (voir la Définition I.5.1). Un **idéal** de A est une partie $I \subseteq A$ tel que :
— I est un sous-groupe du groupe additif $(A, +)$.
— Pour tout $a \in A$ et $b \in I$: $ab \in I$.

(i) Rappeler pourquoi I est un sous-groupe **distingué** de $(A, +)$.

(ii) Soit $A/I = \{a + I : a \in A\}$ le quotient. Pour $a + I, b + I \in A/I$, on aimerait définir leur produit comme

$$(a + I)(b + I) = ab + I.$$

Montrer que cette opération est bien définie : c'est à dire qu'elle ne dépend que des classes $a + I$ et $b + I$, et non du choix de représentants a et b.

(iii) Montrer que $(A/I, +, \cdot)$ (où $+$ est la loi du groupe quotient A/I et $\cdot$ est le produit que nous venons de définir) est un anneau commutatif unitaire, avec $1_{A/I} = 1_A + I$.

Exercice III.19. Soit A et B deux anneaux commutatifs unitaires et soit $\varphi\colon A \to B$ une application. C'est un **morphisme d'anneaux** si :
— $\varphi(a + b) = \varphi(a) + \varphi(b)$.
— $\varphi(ab) = \varphi(ab)$.
— $\varphi(1) = \varphi(1)$.
En particulier, un morphisme d'anneaux est un morphisme de groupes additifs, donc son noyau est :

$$\ker \varphi = \big\{a \in A : \varphi(a) = 0\big\}.$$

Montrer que le noyau d'un morphisme d'anneaux $\varphi\colon A \to B$ est un idéal de A. Réciproquement, si $I \subseteq A$ est un idéal et $B = A/I$ est l'anneau quotient construit dans l'Exercice III.18, alors l'application $\pi_I\colon A \to A/I$ est un morphisme d'anneaux, dont le noyau est I.

Chapitre IV

Actions de groupes

1. Définitions

Définition IV.1.1. Soit G un groupe et X un ensemble. Une **action (à gauche)** de G sur X est une opération $G \times X \to X$, notée le plus souvent $(g, x) \mapsto gx$ (ou $g \cdot x$), qui vérifie

$$ex = x, \qquad (gh)x = g(hx).$$

Étant donné une action de G sur X, on dit aussi que G **agit** sur X, et on le note $G \curvearrowright X$.

On peut également définir une **action à droite** de G sur X comme une opération $X \times G \to X$, notée $(x, g) \mapsto xg$, qui vérifie

$$x = xe, \qquad x(gh) = (xg)h.$$

Une action à droite est notée $X \curvearrowleft G$.

Lorsqu'on parle d'une action, sans préciser de quel côté, c'est une action à gauche.

Dans l'identité $(gh)x = g(hx)$ on a quatre opérations : trois instances de l'action, et une de la loi de groupe.

Exemple IV.1.2. Il existe une action naturelle $S_n \curvearrowright \{1, \dots, n\} : \sigma \cdot k = \sigma(k)$. En effet, $e = \mathrm{id}$, donc $e \cdot k = \mathrm{id}(k) = k$, et

$$(\sigma\tau) \cdot k = (\sigma \circ \tau)(k) = \sigma\big(\tau(k)\big) = \sigma \cdot (\tau \cdot k).$$

Plus généralement, pour tout ensemble X, il existe une action naturelle $S_X \curvearrowright X$ définie par $\sigma \cdot x = \sigma(x)$.

Exemple IV.1.3. Le groupe de matrices inversibles $\mathrm{GL}(n, \mathbf{R})$ agit naturellement sur $\mathbf{R}^n$ par $(A, v) \mapsto Av$ (produit d'une matrice et d'un vecteur colonne). On peut d'ailleurs remplacer $\mathbf{R}$ par n'importe que corps ($\mathbf{C}$, $\mathbf{Q}$, …), voire par n'importe quel anneau unitaire (mais bon, ça commence à faire plus compliqué, et on s'éloigne un peu).

Exemple IV.1.4. Soit G un groupe quelconque. Sa loi $(g, h) \mapsto gh$ est aussi une action à gauche $G \curvearrowright G$. En effet, $eh = h$ et $(fg)h = f(gh)$ pour tout $f, g \in G$ et tout $h \in G$ (bref, pour tout $f, g, h \in G$). On appelle cette action **l'action à gauche** (avec l'article défini) de G sur lui-même.

De la même manière, c'est aussi une action à droite $G \curvearrowleft G$ (puisque $he = h$ et $h(fg) = (hf)g$), que l'on appelle **l'action à droite** de G sur lui-même.

Finalement, on définit l'action par conjugaison $G \curvearrowright G$ (c'est donc **une** action à gauche) par

$$(g, h) \mapsto ghg^{-1}.$$

Soit $G \curvearrowright X$ une action. Dans l'Exercice IV.2 on montre que pour chaque $g \in G$, l'application $x \mapsto gx$ est une permutation, donc en particulier injective. Autrement dit :

Pour tous $g \in G$ et $x, y \in X$:

$$x = y \qquad \Longleftrightarrow \qquad gx = gy.$$

Nous utiliserons cette propriété plusieurs fois dans la suite.

Définition IV.1.5. Soit $G \curvearrowright X$ une action. Pour $x \in X$, son **orbite** (sous l'action de G) est l'ensemble

$$O_x = G \cdot x = \{gx : g \in G\}.$$

L'orbite O_x est une partie de X.

Lemme IV.1.6. *Soit $G \curvearrowright X$ une action, et O une orbite (de n'importe quel élément de X). Alors pour tout $x \in X$:*

$$x \in O \qquad \Longleftrightarrow \qquad O = O_x.$$

Démonstration. Si $O = O_x$, alors $x = ex \in O$. Pour la réciproque, nous supposons que $x \in O$, et qu'il existe $y \in X$ tel que $O = O_y$. Alors il existe $g \in G$ tel que $x = gy$, d'où $y = g^{-1}x$. Pour tout $h \in G$ on a $hx = hgy \in O_y$ et $hy = hg^{-1}x \in O_x$, d'où $O_x = O_y = O$. ■

Résumons :
— Chaque orbite est une partie de X.
— La réunion des orbites est X (car $x \in O_x$).
— Deux orbites distinctes sont disjointes. En effet, si O, O' sont deux orbites non disjointes, et $x \in O \cap O'$, alors $O = O_x = O'$ d'après le Lemme IV.1.6.

Autrement dit, X est la réunion disjointe des orbites. Ou encore :

Soit $G \curvearrowright X$ une action, et Ω la collection de ses orbites. Alors Ω est une partition de X.

(Une **partition** d'un ensemble X est une famille de parties de X, dont X est la réunion disjointe : chaque membre de X appartient à un membre de Ω et à un seul.)

Définition IV.1.7. Soit $G \curvearrowright X$ une action. Si $g \in G$ et $x \in X$ satisfont $gx = x$, on dit que x est un **point fixe** de g. Étant donné $g \in G$, son ensemble de points fixes est :

$$\mathrm{Fix}(g) = \{x \in X : gx = x\}.$$

Et, étant donné $x \in X$, son **stabilisateur** est

$$G_x = \{g \in G : gx = x\}.$$

Lemme IV.1.8. *Chaque G_x est un sous-groupe de G, et $G_{gx} = gG_xg^{-1}$*

Démonstration. On a $ex = x$, donc $e \in G_x$ et $G_x \neq \varnothing$. Maintenant, si $g, h \in G_x$, alors $gx = hx = x$ et :

$$g^{-1}hx = g^{-1}gx = ex = x.$$

Ainsi $g^{-1}h \in G_x$, donc G_x est un sous-groupe.

Maintenant :

$$h \in gG_xg^{-1} \Longleftrightarrow g^{-1}hg \in G_x \Longleftrightarrow g^{-1}hgx = x \Longleftrightarrow hgx = gg^{-1}hgx = gx \Longleftrightarrow h \in G_{gx}.$$ ■

Lorsque $H \leq G$, nous avons toujours une action à gauche canonique $G \curvearrowright G/H$, dite aussi **action par translation**, donnée par

$$(g, fH) \mapsto gfH.$$

On vérifie aisément qu'il s'agit en effet d'une action : $efH = fH$ et $(kg)fH = k(gfH)$ pour tous $k, g, f \in G$. D'ailleurs, si $H = \{e\}$, cette action coïncide avec l'action à gauche $G \curvearrowright G$ (quitte à identifier G avec $G/\{e\}$).

Définition IV.1.9. Une action $G \curvearrowright X$ est dite **transitive** si $X \neq \varnothing$, et pour tout $x, y \in X$ il existe $g \in G$ tel que $gx = y$.

Exemple IV.1.10. L'action par translation $G \curvearrowright G/H$ est transitive. En effet, on a $H = eH \in G/H$, donc $G/H \neq \varnothing$. Aussi, pour tous $x = gH \in G/H$ et $y = fH \in G/H$ on a

$$(fg^{-1})x = fg^{-1}gH = fH = y.$$

Proposition IV.1.11. *Soit $G \curvearrowright X$ une action et $x \in X$. Alors il existe une bijection naturelle $\varphi\colon O_x \to G/G_x$, donnée par*

$$\varphi\colon gx \mapsto gG_x.$$

De surcroît, cette bijection respecte l'action de G :

$$h\varphi(y) = \varphi(hy) \qquad \forall y \in O_x.$$

Démonstration. Montrons d'abord que φ est bien définie. En effet, si $gx = hx$, c'est que $h^{-1}gx = x$ et $h^{-1}g \in G_x$. Dans ce cas $G_x = h^{-1}gG_x$ et

$$hG_x = hh^{-1}gG_x = gG_x.$$

Très bien, φ est bien définie. Au fait, dans l'argument précédent, toutes les implication sont bidirectionnelles, si bien que $hG_x = gG_x$ implique $gx = hx$, donc φ est injective. Son image est

$$\{\varphi(y) : y \in O_x\} = \{\varphi(gx) : g \in G\} = \{gG_x : g \in G\} = G/G_x.$$

Ainsi, φ est bijective.

Maintenant, soit $y = gx \in O_x$ et $h \in G$. Alors

$$h\varphi(y) = hgG_x = \varphi(hy).$$ ■

2. Restrictions

Considérons une action $G \curvearrowright X$, et un sous-groupe $H \leq G$. Si on « oublie » les éléments de G en dehors de H, on obtient une action de H sur X :

$$(h, x) \mapsto hx \qquad h \in H,\ x \in X.$$

(On vérifie aisément que c'est bien une action.) Cette action $H \curvearrowright X$ est la **restriction** de l'action $G \curvearrowright X$ au sous-groupe H.

Exemple IV.2.1. Le groupe orthogonal

$$O(n) = \{A \in M(n, \mathbf{R}) : {}^tAA = I_n\}$$

est un sous-groupe de $\mathrm{GL}(n, \mathbf{R})$. Il agit naturellement sur $\mathbf{R}^n$: $(A, v) \mapsto Av$. Cette action est la restriction de celle de $\mathrm{GL}(n, \mathbf{R})$ (voir Exemple IV.1.3). C'est une action par isométries : si $A \in O(n)$, alors l'application $v \mapsto Av$ est une isométrie, alors que ceci est faux pour $A \in \mathrm{GL}(n, \mathbf{R}) \smallsetminus O(n)$.

Encore plus généralement, tout morphisme $\varphi\colon H \to G$ et action $G \curvearrowright X$ donnent lieu à une action $H \curvearrowright X$, définie par $h \cdot x = \varphi(h) \cdot x$ (dans le cas d'une restriction de G à H, φ est l'application identité).

Quid de l'autre côté ? Si $Y \subseteq X$, peut-on restreindre une action $G \curvearrowright X$ en une action $G \curvearrowright Y$, par $(g, y) \mapsto gy$ pour tout $g \in G$ et $y \in Y$? Pour cela, il faut au moins que si $y \in Y$, alors $gy \in Y$ également pour tout $g \in G$.

Définition IV.2.2. Soit $G \curvearrowright X$ une action. Une partie $Y \subseteq X$ est dite **stable** par l'action si $gy \in Y$ pour tout $y \in Y$ et $g \in G$.

Lorsque $Y \subseteq X$ est une partie stable, on peut en effet définir la **restriction** de $G \curvearrowright X$ à Y par

$$(g, y) \mapsto gy \qquad g \in G,\ y \in Y,$$

sachant que dans ce cas on a $gy \in Y$ également. (Encore on vérifie aisément que c'est une action $G \curvearrowright Y$.)

Si $Y, Z \subseteq X$ sont des parties stables, il est de même de $Y \cap Z$ et $Y \cup Z$. Toute orbite est stable (si O est une orbite, $x \in O$, et $g \in G$, alors $gx \in O_x = O$). In en découle que toute réunion d'orbite est stable par l'action.

3. La formule des classes et la formule de Burnside

Soit $G \curvearrowright X$ une action et $x \in X$. D'après la Proposition IV.1.11 il existe une bijection entre O_x et G/G_x, d'où $|O_x| = |G/G_x| = [G : G_x]$. On a démontré le résultat suivant.

La **formule des classes** : $\qquad |O_x| = [G : G_x].$

Cette formule a de nombreuses conséquences. Considérons par exemple l'action par conjugaison $G \curvearrowright G : g \cdot k = gkg^{-1}$. Si $k \in G$, alors son stabilisateur est le centralisateur de k (voir Définition II.1.10) :

$$G_k = \{g : gkg^{-1} = k\} = \{g : gk = kg\} = C_G(k).$$

Définition IV.3.1. La **classe de conjugaison** d'un $k \in G$ est l'ensemble de ses conjugués :

$$\{gkg^{-1} : g \in G\}.$$

C'est donc l'orbite de k sous l'action par conjugaison, d'où, d'après la formule des classes :

$$|\{gkg^{-1} : g \in G\}| = \big[G : C_G(k)\big].$$

Lemme IV.3.2. *Soit p un nombre premier, G un groupe d'ordre p^n, $n > 0$. Alors son centre $Z(G)$ est non trivial.*

Démonstration. Si $g \in G \setminus Z(G)$, alors $C_G(g) \neq G$, et par conséquent, $\big[G : C_G(g)\big] > 1$. Or $\big[G : C_G(g)\big] \mid |G|$, donc $\big[G : C_G(g)\big]$ est aussi une puissance de p, et $p \mid \big[G : C_G(g)\big]$. Autrement dit, le cardinal de la classe de conjugaison d'un $g \notin Z(G)$ est divisible par p. Par contre, si $g \in Z(G)$ alors sa classe de conjugaison est $\{g\}$, de cardinal un.

Supposons, par l'absurde, que $Z(G) = \{e\}$. Les classes de conjugaison forment une partition de G (car ce sont les orbites d'une action sur G). Donc G serait la réunion disjointe de $\{e\}$ et des autres classes de conjugaison, toutes de cardinal divisible par p. Ainsi, $|G| \equiv 1 \mod p$, ce qui contredit l'hypothèse que $n > 0$. ∎

Proposition IV.3.3 (Formule de Burnside). *Soit $G \curvearrowright X$ une action, avec G et X finis, et soit Ω l'ensemble des orbites. Alors*

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Démonstration. Posons

$$Z = \big\{(g, x) \in G \times X : gx = x\big\}.$$

On peut l'exprimer comme réunion disjointe d'ensembles de deux manières différentes :

$$Z = \bigcup_{g \in G} \{g\} \times \mathrm{Fix}(g) = \bigcup_{x \in X} G_x \times \{x\}.$$

Par conséquent,

$$|Z| = \sum_{g \in G} |\mathrm{Fix}(g)| = \sum_{x \in X} |G_x|.$$

Soit $O \in \Omega$. Si $x \in O$, alors $O = O_x$ et $|O| = [G : G_x] = |G|/|G_x|$, ou encore, $|G_x| = |G|/|O|$. Ainsi

$$\sum_{x \in O} |G_x| = \sum_{x \in O} |G|/|O| = |G|.$$

Maintenant :

$$\sum_{g \in G} |\mathrm{Fix}(g)| = |Z| = \sum_{x \in X} |G_x| = \sum_{O \in \Omega} \sum_{x \in O} |G_x| = \sum_{O \in \Omega} |G| = |\Omega||G|.$$

La formule de Burnside en découle en divisant par $|G|$. ■

Exemple IV.3.4. Nombre de bracelets à 3 billes de 3 couleurs :

$$\frac{3^3 + 2 \cdot 3 + 3 \cdot 3^2}{6} = \frac{6 \cdot 3^2 + 6}{6} = 10$$

(3 monochromatiques + 6 à deux couleurs + 1 à trois couleurs)

Nombre de bracelets à 5 billes de 3 couleurs :

$$\frac{3^5 + 4 \cdot 3 + 5 \cdot 3^3}{10} = 3\frac{81 + 4 + 45}{10} = 3 \cdot 13 = 39.$$

4. Programme d'Erlangen [à élaborer]

Felix Klein (19e siècle) : correspondance entre une « géométrie » et l'action de groupe qui en préserve les concepts fondamentaux.

Exemple IV.4.1. $\mathrm{GL}(n, K) \curvearrowright K^n$. Géométrie linéaire : respecte combinaisons linéaire (et zéro)

Exemple IV.4.2. $O(n) \curvearrowright \mathbf{R}^n$ géométrie euclidienne. Distance, angles.
$U(n) \curvearrowright \mathbf{C}^n$ géométrie hermitienne.

Exemple géométrique « non linéaire » :

Exemple IV.4.3. $K^n \rtimes \mathrm{GL}(n, K) \curvearrowright K^n$. Géométrie affine : respecte combinaisons affine

Exemple IV.4.4. Géométrie projective : $PGL(2, \mathbf{C}) \curvearrowright \mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$. Cercles et droites.

Exercices

Exercice IV.1. Soit $(x, g) \mapsto xg$ une action à droite de G sur X. Définissons une autre opération $G \times X \to X$ par $(g, x) \mapsto xg^{-1}$. Montrer que c'est une action à gauche.

Montrer que nous venons de construire une bijection entre l'ensemble des actions à droite de G sur X, et l'ensemble des actions à gauche.

Exercice IV.2. Soit S_X l'ensemble des permutations de X (bijections $\sigma : X \to X$). Nous avons déjà vu que S_X est un groupe pour la loi de composition.

Si $G \curvearrowright X$ est une action et $g \in G$, alors $\sigma_g : x \to gx$ est une permutation, i.e., $\sigma_g \in S_X$. De surcroît, l'application $g \mapsto \sigma_g$ est un morphisme $G \to S_X$.

Exercice IV.3. Soit G un groupe et X un ensemble. Soit $\mathrm{Act}(G, X)$ l'ensemble des actions $G \curvearrowright X$. Soit $\mathrm{Hom}(G, S_X)$ l'ensemble des morphismes de groupes $G \to S_X$.

L'exercice précédent met en évidence une application $\mathrm{Act}(G, X) \to \mathrm{Hom}(G, S_X)$. Montrer que cette application est une bijection. Autrement dit, la donnée d'une action $G \curvearrowright X$ revient exactement à la donnée d'un morphisme de groupes $G \to S_X$.

Indication : soit $\Sigma : G \to S_X$ un morphisme, et pour $g \in G$ notons $\sigma_g = \Sigma(g) \in S_X$. Montrer que $(g, x) \mapsto gx = \sigma_g(x)$ définit une action $G \curvearrowright X$. Utiliser pour construire l'application inverse.

Exercice IV.4. Soit $G \curvearrowright X$ une action. Sont équivalents :

(i) L'action est transitive (Définition IV.1.9).

(ii) Elle admet une unique orbite O (donc $O = O_x$ pour tout $x \in X$).

Exercice IV.5. Une action $G \curvearrowright X$ est dite **fidèle** si pour tout $g \neq e$ il existe $x \in X$ tel que $gx \neq x$. Sont équivalents :

(i) L'action est fidèle.

(ii) $\bigcap_{x \in X} G_x = \{e\}$.

(iii) Le morphisme $G \to S_X$ de l'Exercice IV.2 est injectif.

Exercice IV.6. Une action $G \curvearrowright X$ est dite **libre** si pour tout $g \neq e$ et tout $x \in X$: $gx \neq x$. Sont équivalents :

(i) L'action est libre.

(ii) $G_x = \{e\}$ pour tout $x \in X$.

(iii) Pour tout $x, y \in X$ il existe au plus un g tel que $gx = y$.

Si l'action est libre, alors $|G| = |O|$ pour toute orbite O.

Exercice IV.7. Soit $G \curvearrowright X$ une action. Sont équivalents :

(i) L'action est libre et transitive.

(ii) Il existe $x \in X$ tel que pour tout $y \in X$ il existe un unique g tel que $gx = y$.

(iii) $X \neq \varnothing$ et pour tout $x, y \in X$ il existe un unique g tel que $gx = y$.

Si l'action est libre et transitive, alors $|G| = |X|$.

Exercice IV.8. Si une action $G \curvearrowright X$ est libre alors elle est aussi fidèle. Ou presque : il manque encore une hypothèse, laquelle ?

Exercice IV.9. L'action à gauche $G \curvearrowright G$ est transitive et libre. Elle est donc fidèle.

Exercice IV.10. Pour tout groupe G il existe un morphisme injectif $G \hookrightarrow S_G$.

Pour tout groupe G d'ordre n il existe un morphisme injectif $G \hookrightarrow S_n$.

Exercice IV.11. Soit G un groupe et $H \leq G$.
— L'action $G \curvearrowright G/H$ est transitive, et $G_H = H$.
— Elle est libre si et seulement si $H = \{e\}$.
— Fidèle si et seulement si $\bigcap_{g\in G} gHg^{-1} = \{e\}$.

Exercice IV.12. Soit $H \trianglelefteq G$. Sous quelle condition l'action $G \curvearrowright G/H$ est-elle fidèle ?

Exercice IV.13. L'action naturelle $S_n \curvearrowright \{1, \dots, n\}$ est transitive et fidèle, mais non libre (dès que $n \geq 3$).

Exercice IV.14. Soit $G \curvearrowright X$ une action. Nous avons vu que toute réunion d'orbites est stable par l'action. Montrer la réciproque : toute partie stable $Y \subseteq X$ est une réunion d'orbites : $Y = \bigcup_{x\in Y} O_x$.

Exercice IV.15. Tout groupe d'ordre p^2, avec p premier, est abélien.
Indication : on sait déjà, d'après le Lemme IV.3.2, que $Z(G)$ est non trivial. Supposons que $g \in G \smallsetminus Z(G)$ et étudions son centralisateur $C_G(g)$ pour trouver une contradiction.

Exercice IV.16. Soit p premier. Soit $G_1 = C_{p^2}$ et $G_2 = C_p \times C_p$.
— Montrer que $G_1 \ncong G_2$.
— Montrer que tout groupe d'ordre p^2 est isomorphe à l'un des deux (et à un seul).
Indication : s'il n'existe pas $x \in G$ tel que $o(x) = p^2$, alors on peut essayer de choisir $x \in G \smallsetminus \{e\}$ et $y \in G \smallsetminus \langle x\rangle$. Puis, à l'aide de l'Exercice IV.15, on peut essayer de montrer que G est le produit directe interne $\langle x\rangle \times \langle y\rangle$.

Exercice IV.17. Soit G un groupe fini, et $H \leq G$. Soit

$$\mathfrak{C} = \{gHg^{-1} : g \in G\}$$

l'ensemble des conjugués de H.

(i) Montrer que $g \cdot K = gKg^{-1}$ définit une action transitive $G \curvearrowright \mathfrak{C}$.
(ii) Montrer que $G_H = N_G(H)$ (le normalisateur de H).
(iii) En déduire que $|\mathfrak{C}| = \big[G : N_G(H)\big]$.
(iv) Montrer que $|H| \mid |N_G(H)|$.
(v) En déduire que $|\mathfrak{C}| \mid [G : H]$.

Exercice IV.18. Pour chaque G fini il existe des sous-groupes propres H_i, $i < k$, tels que

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : H_i].$$

Indication : ce n'est qu'une généralisation de la preuve du Lemme IV.3.2, avec moins d'hypothèses.

Chapitre V

Le produit direct et semi-direct

Le quotient de groupe, dont nous avons discuté dans le chapitre précédent, permet de « décomposer » (d'une manière) un groupe G en deux groupes plus simples (d'une manière, encore), les groupes N et G/N (sous l'hypothèse que $N \trianglelefteq G$). Dans ce chapitre nous discuterons de la question inverse : peut-on reconstruire G à partir de ces deux « blocs » ? Bien évidemment, cette dernière question suppose que G est connu. Lorsque G n'est pas connu, on peut encore se demander quels sont les groupes que l'on peut construire à partir de deux groupes donnés (qui joueront les rôles de N et de G/N, respectivement).

1. Le produit direct : externe, puis interne

Commençons avec la version la plus facile de cette question : on nous donne deux groupes H et K, et c'est tout. Que pouvons-nous construire avec ?

Définition V.1.1. Soit H et K deux groupes. Nous munissons le produit cartésien

$$H \times K = \{(x, y) : x \in H,\, y \in K\}$$

de la loi

$$(x, y) \cdot (u, v) = (xu, yv).$$

On appelle $H \times K$, muni de cette loi, le **produit direct (externe)** de H et K.

Comme c'est un produit cartésien, il est muni également de deux **projections canoniques**

$$\pi_1 \colon H \times K \to H, \qquad \pi_1(x, y) = x,$$
$$\pi_2 \colon H \times K \to K, \qquad \pi_2(x, y) = y.$$

Proposition V.1.2. *L'ensemble $G = H \times K$, muni de cette loi, est un groupe, dans lequel le neutre est (e, e) (c'est à dire, (e_H, e_K)), et l'inverse est*

$$(x, y)^{-1} = (x^{-1}, y^{-1}).$$

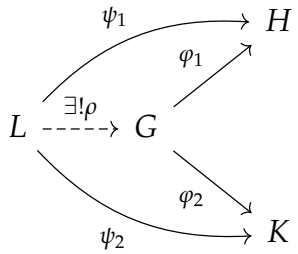
Les projections canoniques π_1 et π_2 sont des épimorphismes (morphismes surjectifs).

Remarque V.1.3. Nous pouvons construire $G = H_1 \times H_2 \times \cdots \times H_n = \prod_{i=1}^{n} H_i$ de la même manière, avec projections canoniques $\pi_i \colon G \to H_i$ pour chaque $1 \leq i \leq n$.

Exemple V.1.4. $(\mathbf{R}^2, +) = (\mathbf{R}, +) \times (\mathbf{R}, +)$, et plus généralement, $(\mathbf{R}^{n+m}, +) = (\mathbf{R}^n, +) \times (\mathbf{R}^m, +)$

Voici une manière alternative de définir le produit direct $H \times K$. Elle peut sembler être bien trop compliquée, mais elle a ses avantages.

Définition V.1.5. Soit H, K et G des groupes, et soit $\varphi_1 \colon G \colon \to H$ et $\varphi_2 \colon G \to K$ des morphismes. On dit que le triplet $(G, \varphi_1, \varphi_2)$ vérifie la **propriété universelle du produit direct** $H \times K$ si pour tout autre triplet (L, ψ_1, ψ_2), où $\psi_1 \colon L \to H$ et $\psi_2 \colon L \to K$ sont des morphismes, il existe un unique morphisme $\rho \colon L \to G$ qui rend le diagramme suivant commutatif :



Autrement dit, il existe un unique $\rho\colon L \to G$ qui vérifie $\psi_i = \varphi_i \circ \rho$ pour $i = 1, 2$.

Dans l'Exercice V.2 on montre que $(H \times K, \pi_1, \pi_2)$ vérifie cette propriété universelle, et de surcroît, ce triplet est caractérisé, à isomorphisme unique près, par la propriété universelle. Dans le contexte des **catégories**, que nous ne définirons pas ici, une caractérisation à isomorphisme unique près est le mieux que l'on peut espérer, et la propriété universelle est la **définition** du produit direct – qui n'est plus juste le groupe $H \times K$, mais le triplet $(H \times K, \pi_1, \pi_2)$.

Étudions un peu plus ce triplet $(H \times K, \pi_1, \pi_2)$. Que peut-on dire de $\pi_1\colon H \times K \to H$, par exemple ? Calculons sont image et sont noyau :

— $\operatorname{img} \pi_1 = H$. Autrement dit, π_1 est surjectif. Bon, on le savait déjà, rien de nouveau ici.

— $\ker \pi_1 = \{e\} \times K$. Ça c'est plus intéressant – le noyau est isomorphe à K, et de surcroît par un isomorphisme canonique, qui est juste la restriction de π_2 :

$$\pi_2(e, y) = y.$$

L'application inverse de cet isomorphisme est le **plongement canonique** de K dans $H \times K$:

$$\iota_2\colon K \to H \times K, \qquad \iota_2(y) = (e, y).$$

— De la même manière, $\ker \pi_2 = H \times \{e\}$ est canoniquement isomorphe à H : dans un sens par la restriction de π_2, et dans le sens inverse par le plongement canonique

$$\iota_1\colon H \to H \times K, \qquad \iota_1(x) = (x, e).$$

Puisque H est canoniquement isomorphe au sous-groupe $H \times \{e\} \leq H \times K$, nous aurons tendance à faire abstraction de la distinction. Autrement dit, nous allons prétendre que $x \in H$ est le même que $(x, e) \in H \times K$, de sorte que $H \leq H \times K$, et même $H \trianglelefteq H \times K$, puisque c'est le noyau de π_2. De la même manière, nous allons prétendre que $y \in K$ est le même que $(e, y) \in H \times K$, de sorte que $K \trianglelefteq H \times K$.

Et voici une autre manière (tentative, pour l'instant) de présenter un produit direct $H \times K$, comme un groupe G dont H et K sont des sous-groupes. Que peut-on en dire ?

Définition V.1.6. Soit G et groupe et H et K deux sous-groupes. Alors on dit que G est un **produit direct interne** de H et K, que l'on notera provisoirement par $G = H \times_i K$, si :

— $H \cap K = \{e\}$.

— $G = HK$.

— Let sous-groupes H et K **commutent** : si $x \in H$ et $y \in K$, alors $xy = yx$.

Proposition V.1.7. *Soit H et K deux groupes, et $G = H \times K$ leur produit directe (externe). Identifions H avec $H \times \{e\}$ et K avec $\{e\} \times K$ comme plus haut. Sous cette identification, H et K sont des sous-groupes de G, et $G = H \times_i K$ est leur produit direct interne.*

Réciproquement, soit G un groupe, et $H, K \leq G$ des sous-groupes de sorte que $G = H \times_i K$ est le produit direct interne. Alors tout membre de G s'écrit d'une manière unique comme xy avec $x \in H$

et $y \in K$, et si $x, u \in H$ et $y, v \in K$, alors :

$$(xy)(uv) = (xu)(yv), \qquad (xy)^{-1} = x^{-1}y^{-1}$$

(où $xu, x^{-1} \in H$ et $yv, y^{-1} \in K$). Autrement dit, l'application

$$\rho\colon H \times K \to G, \qquad \rho(x,y) = xy = \pi_1(x,y)\pi_2(x,y)$$

est un isomorphisme $H \times K \cong G$.

Démonstration. .... ■

Autrement dit, le produit direct externe est aussi un produit direct interne, et tout produit direct interne est canoniquement isomorphe au produit direct externe. Dans la suite, nous ferons abstraction de la distinction, notant les deux par $G = H \times K$.

Remarque V.1.8. Soit G un groupe, $H, K \leq G$ des sous-groupes, et supposons que les deux premières conditions de la définitions d'un produit directe interne sont vérifiées :
— $H \cap K = \{e\}$.
— $G = HK$.
Alors H et K commutent si et seulement si les deux sont des sous-groupes distingués.

Démonstration. Dans un sens, supposons que H et K commutent. Soient $x \in H$, $u \in K$, et $w \in G$. Puisque $G = HK$, on a $w = yv$ avec $y \in H$ et $v \in K$. Ainsi,

$$wxw^{-1} = yvxv^{-1}y^{-1} = yxy^{-1}vv^{-1} = yxy^{-1} \in H,$$
$$wuw^{-1} = yvuv^{-1}y^{-1} = vuv^{-1}yy^{-1} = vuv^{-1} \in K.$$

Autrement dit, $wHw^{-1} \subseteq H$ et $wKw^{-1} \subseteq K$ pour tout $w \in G$, d'où $H, K \trianglelefteq G$.

Pour la réciproque, supposons que $H, K \trianglelefteq G$. Soit $x \in H$ et $u \in K$, et étudions $[x,u] = xux^{-1}u^{-1}$ (cet élément s'appelle le **commutateur** de x et u). Puisque $H \trianglelefteq G$, on a $ux^{-1}u^{-1} \in uHu^{-1} = H$, donc $[x,u] \in H$. D'une manière similaire, $xux^{-1} \in xKx^{-1} = K$, donc $[x,u] \in K$. Donc $[x,u] \in H \cap K = \{e\}$, c'est à dire $[x,u] = e$. Autrement dit, $xu = ux$, et nous avons montré que H et K commutent. ■

Par conséquent, $G = H \times_i K$ si et seulement si :
— $H \cap K = \{e\}$.
— $G = HK$.
— $H, K \trianglelefteq G$.

2. Le produit semi-direct : interne, puis externe

Le produit direct interne nous permet de dire que un groupe G est obtenu de deux sous-groupes $H, K \leq G$ d'une manière particulièrement simple. Il s'avère être très utile d'affaiblir la définition en prenant que « la moitié » de la dernière condition :

Définition V.2.1. Soit G un groupe et $H, K \leq G$ deux sous-groupes. Nous disons que $G = H \rtimes K$, ou que G est le **produit semi-direct interne** de H avec K (l'ordre est important) si
— $H \cap K = \{e\}$.
— $G = HK$.
— $H \trianglelefteq G$.

Notez bien que dans $H \rtimes K$ et dans $H \trianglelefteq G$, le triangle pointe vers H !
On pourrait également définir $G = H \ltimes K$, en replaçant $H \trianglelefteq G$ par $K \trianglelefteq G$: le triangle pointe alors toujours vers K.

Remarque V.2.2. Soit G un groupe, et $H, K \leq G$. Si $H \trianglelefteq G$, alors $N_G(H) = G$, et en particulier, $K \leq N_G(H)$. Réciproquement, d'après le 2e théorème d'isomorphie (Théorème III.3.3), si $K \leq N_G(H)$, alors $H \trianglelefteq HK = KH$. Si on sait d'ailleurs que $HK = G$ (ou que $KH = G$), alors $H \trianglelefteq G$.

Il en découle que dans Définition V.2.1 :

— La condition $G = HK$ peut être remplacée par $G = KH$.

— La condition $H \trianglelefteq G$ peut être remplacée par $K \leq N_G(H)$ (qui est, superficiellement, plus faible).

Lemme V.2.3. *Soit G un groupe, et $H, K \leq G$ des sous-groupes de sorte que $G = H \rtimes K$ est le produit semi-direct interne. Pour $x \in H$ et $y \in K$, posons*

$$\varphi_y(x) = yxy^{-1}$$

(c'est la conjugaison par y). Alors

— *L'application $y \mapsto \varphi_y$ est un morphisme $K \to \mathrm{Aut}(H)$ (en particulier, chaque φ_y est un automorphisme de H).*

— *Tout membre de G s'écrit d'une manière unique comme xy avec $x \in H$ et $y \in K$, et si $x, u \in H$ et $y, v \in K$, alors :*

$$(xy)(uv) = \big(x\varphi_y(u)\big)(yv), \qquad (xy)^{-1} = \varphi_{y^{-1}}(x^{-1})y^{-1}$$

(où $x\varphi_y(u), \varphi_{y^{-1}}(x^{-1}) \in H$ et $yv, y^{-1} \in K$).

(Donc $(x, y) \mapsto xy$ est une bijection entre pe produit cartésien $H \times K$ et G, bien que ce ne soit pas forcément un isomorphisme de groupes.)

Ainsi, si $G = H \rtimes K$, alors nous pouvons reconstruire G avec sa loi de H et K – à conditions de connaître également l'application $y \mapsto \varphi_y$. Essayons de faire pareil mais sans connaître G à l'avance.

Définition V.2.4. Soit H et K deux groupes, et soit $\alpha \colon K \to \mathrm{Aut}(H)$ un morphisme. Pour $y \in K$, notons $\alpha(y) \in \mathrm{Aut}(H)$ plutôt par α_y, de sorte que l'on puisse écrire $\alpha_y(x)$ pour $x \in H$.

Le produit **semi-direct externe** de H et de K **selon** α, noté $H \rtimes_\alpha K$, consiste de l'ensemble $H \times K$ (le produit cartésien), muni de la loi suivante :

$$(x, y) \cdot_\alpha (u, v) = \big(x\alpha_y(u), yv\big).$$

Ainsi, tout produit semi-direct interne est aussi un produit direct externe. La réciproque est vraie également :

Proposition V.2.5. *Soit H et K deux groupes, et soit $\alpha \colon K \to \mathrm{Aut}(H)$ un morphisme.*

(i) *Le produit semi-direct externe $H \rtimes_\alpha K = (H \times K, \cdot_\alpha)$ est un groupe.*

(ii) *Les applications*

$$\iota_1 \colon H \to H \times K, \qquad \iota_1(x) = (x, e),$$
$$\iota_2 \colon K \to H \times K, \qquad \iota_2(y) = (e, y),$$

sont des plongements de H et K dans $H \rtimes_\alpha K$. Ainsi, identifiant $x \in H$ avec (x, e) et $y \in K$ avec (e, y), nous pouvons considérer que H et K sont des sous-groupes de $H \rtimes_\alpha K$.

(iii) *Avec ces identifications, $H \rtimes_\alpha K$ est un produit semi-direct interne de $H \rtimes K$. En particulier, pour $x \in H$ et $y \in K$:*

$$\varphi_y(x) = yxy^{-1} = \alpha_y(x),$$

et α est l'application $y \mapsto \varphi_y$.

Exemple V.2.6. Soit G le groupe diédral D_n, pour $n \geq 3$. Soit $H \subseteq D_n$ les rotations, et soit $s \in D_n$ une réflexion. Posons $K = \langle s \rangle = \{e, s\}$. Alors H et K sont des sous-groupes, $H \cap K = \{e\}$ et $HK = D_n$. De surcroît, $H \trianglelefteq D_n$ (car tout sous-groupe d'indice 2 est distingué).

Ainsi, $D_n = H \rtimes K$, en tant que produit directe interne. Nous pouvons calculer $\varphi_y(x)$ explicitement pour une rotation $x \in H$ et pour $y \in \{e, s\}$:

$$\varphi_e(x) = x, \qquad \varphi_s(x) = x^{-1}.$$

En particulier, H et K ne commutent pas, donc $D_n \ncong H \times K$.

Lemme V.2.7. *Soit $(G, +)$ un groupe additif (donc abélien). Définissons $\alpha_i \colon G \to G$ pour $i \in \mathbf{Z}/2\mathbf{Z}$ par :*

$$\alpha_{\overline{0}}(x) = x, \qquad \alpha_{\overline{1}}(x) = -x.$$

Alors $\alpha_i \in \mathrm{Aut}(G)$, et $\alpha \colon \mathbf{Z}/2\mathbf{Z} \to \mathrm{Aut}(G)$ est un morphisme.

Ceci nous permet de construire D_n comme produit semi-direct externe : $D_n \cong \mathbf{Z}/n\mathbf{Z} \rtimes_\alpha \mathbf{Z}/2\mathbf{Z}$, selon le α du Lemme V.2.7.

Exercices

Exercice V.1. Montrer que si $H \cong H'$ et $K \cong K'$ alors $H \times K \cong H' \times K'$.

Montrer que $(H \times K) \times L \cong H \times (K \times L)$.

Exercice V.2. Soit H et K deux groupe, $H \times K$ leur produit direct, et π_1 et π_2 les projection canoniques. Montrer que :

— $(H \times K, \pi_1, \pi_2)$ vérifie la propriété universelle du produit direct (Définition V.1.5).

— Si $(G, \varphi_1, \varphi_2)$ vérifie la propriété universelle du produit direct, alors il existe un **unique isomorphisme** $\rho \colon G \to H \times K$ de sorte que $\varphi_i = \pi_i \circ \rho$ (et donc $\pi_i = \varphi_i \circ \rho^{-1}$).

Exercice V.3 (Théorème des restes chinois)**.** Soit m et n sont premiers entre eux. Alors l'application $a + mn\mathbf{Z} \mapsto (a + n\mathbf{Z}, a + m\mathbf{Z})$ est un isomorphisme $\mathbf{Z}/mn\mathbf{Z} \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.
Indication : montrer que c'est un morphisme (en particulier, que c'est bien défini), et calculer son noyau.

Exercice V.4. Supposons que $G = H \rtimes K$.

(i) L'application $\pi \colon G \to K$, $\pi(xy) = y$ (où $x \in H$ et $y \in K$) est un épimorphisme. On l'appelle la **projection canonique** sur K.

(ii) Le noyau de la projection canonique sur est H.

(iii) Soit $s \colon K \to G$ l'application identité. Alors c'est encore un morphisme (un plongement), et $\pi \circ s = \mathrm{id}_K$.

Exercice V.5. Montrer la réciproque de l'exercice précédent. Soit G un groupe, $\pi \colon G \to K$ un épimorphisme, et soit $H = \ker \pi$. Supposons en outre que $s \colon K \to G$ est un morphisme tel que $\pi \circ s = \mathrm{id}_K$ (on dit dans ce cas que s est une **section** de π). Alors s est un plongement, de sorte que $\mathrm{img}\, s \cong K$, et $G = H \rtimes (\mathrm{img}\, s)$.

Chapitre VI

Théorèmes de Sylow

1. Un exercice préliminaire de combinatoire

Avant de parler des Théorème de Sylow, faisons un petit calcul. Considérons $\mathbf{Z}[X]$, l'ensemble des polynômes à coefficients entiers en l'inconnu X. La somme et le produit de deux polynômes dans $\mathbf{Z}[X]$ appartient encore à $\mathbf{Z}[X]$ (au fait, $(\mathbf{Z}[X], +, \cdot)$ est un anneau, voir la Définition I.5.1).

Si $P, Q \in \mathbf{Z}[X]$, on dit que P est Q cont **congru modulo** p, en symboles $P \equiv Q \mod p$, si $P - Q$ est divisible par p. Autrement dit, s'il existe $R \in \mathbf{Z}[X]$ tel que $P - Q = pR$. Dans la suite, nous allons omettre le $\mod p$ et noter la congruence modulo p par le symbole $\equiv$ seul.

Lemme VI.1.1. *La relation de congruence modulo p est une relation d'équivalence. Si $P_i \equiv Q_i$ pour $i = 1, 2$ alors*

$$P_1 + P_2 \equiv Q_1 + Q_2 \qquad \text{et} \qquad P_1 P_2 \equiv Q_1 Q_2.$$

Démonstration. Montrons que c'est une relation d'équivalence :
— Réflexive : $P - P = p \cdot 0$.
— Symétrique : si $P - Q = pR$, alors $Q - P = p(-R)$.
— Transitive : si $P - Q = pR$ et $Q - S = pT$ alors $P - S = p(R + T)$.
Pour la deuxième affirmation, on suppose que $P_i - Q_i = pR_i$ pour $i = 1, 2$. Alors :

$$(P_1 + P_2) - (Q_1 + Q_2) = p(R_1 + R_2)$$

et

$$(P_1 P_2) - (Q_1 Q_2) = (P_1 - Q_1)P_2 + Q_1(P_2 - Q_2) = p(R_1 P_2 + Q_1 R_2). \qquad \blacksquare$$

Lemme VI.1.2. *Soit $P, Q \in \mathbf{Z}[X]$. Alors pour tout $n \in \mathbf{N}$:*

$$(P + Q)^{p^n} \equiv P^{p^n} + Q^{p^n}.$$

Démonstration. Montrons ça d'abord pour $n = 1$. Si $0 < k < p$, alors $p \mid \binom{p}{k}$. En effet, p divise le numérateur de $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ mais non le dénominateur (et p est premier). Par conséquent :

$$(P + Q)^p - P^p - Q^p = \sum_{0 \le k \le p} \binom{p}{k} P^k Q^{p-k} - P^p - Q^p = \sum_{0 < k < p} \binom{p}{k} P^k Q^{p-k}$$

est divisible par p. Maintenant, on prouve par récurrence sur n. Pour $n = 0$ il n'y a rien à démontrer, puisque $p^n = 1$. À l'étape n on sait déjà que

$$(P + Q)^{p^n} \equiv P^{p^n} + Q^{p^n}.$$

D'où, d'après Lemme VI.1.1 :

$$(P + Q)^{p^{n+1}} = \left((P + Q)^{p^n}\right)^p \equiv \left(P^{p^n} + Q^{p^n}\right)^p \equiv P^{p^{n+1}} + Q^{p^{n+1}}. \qquad \blacksquare$$

En particulier, avec $m, n \in \mathbf{N}$ quelconques :

$$(1+X)^{mp^n} = \left((1+X)^{p^n}\right)^m \equiv (1+X^{p^n})^m.$$

À gauche, le coefficient de X^{p^n} et $\binom{mp^n}{p^n}$, et à droite m, d'où :

$$\boxed{\binom{mp^n}{p^n} \equiv m \mod p.}$$

Pour un argument plus calculatoire démontrant le même énoncé, voir l'Exercice VI.1.

2. Les trois théorèmes de Sylow

Soit G un groupe fini, p premier, et $k \in \mathbf{N}$. Sous quelles conditions existe-t-il un sous-groupe $H \leq G$ tel que $|H| = p^k$? D'après Lagrange, on a une condition nécessaire : il faut que $p^k \mid |G|$. Nous allons montrer que c'est aussi une condition suffisante. Concentrons-nous d'abord sur le cas où k est maximal.

Définition VI.2.1. Soit G un groupe fini et p premier. Soit p^n la puissance maximale de p qui divise $|G|$. Un sous-groupe $H \leq G$ d'ordre p^n s'appelle un **p-sous-groupe de Sylow** de G, ou simplement un **p-Sylow** de G.

Fixons quelques conventions. Nous gardons l'hypothèse que G est un groupe fini et p un nombre premier. Nous fixons le n maximal tel que $p^n \mid |G|$, et $m = |G|/p^n$. Ainsi :

$$|G| = mp^n, \qquad p \nmid m.$$

Avant d'énoncer et de démontrer les trois théorème de Sylow, démontons un lemme. Posons $|G| = mp^n$, où $p \nmid m$, et $X = \{S \subseteq G : |S| = p^n\}$. Si $g \in G$ et $S \in X$, alors $gS = \{gh : h \in S\} \in X$ également. Ceci définit une action $G \curvearrowright X$, que nous proposons d'étudier.

Lemme VI.2.2. *Soit O une orbite de cette action $G \curvearrowright X$, et supposons que $p \nmid |O|$. Alors il existe un p-Sylow $H \leq G$ tel que*

$$O = \{gH : g \in G\} = G/H.$$

Démonstration. Si $S \in O$ et $g \in S$, alors $e \in g^{-1}S \in O$. Ainsi nous pouvons choisir $S \in O$ tel que $e \in S$.

Soit $H = G_S$ son stabilisateur. Si $h \in H$ alors $h = he \in hS = S$, donc $H \subseteq S$. En particulier $|H| \leq p^n$. Par contre,

$$|O||H| = [G : H]|H| = |G| = mp^n.$$

Puisque $p \nmid |O|$, forcément $p^n \mid |H|$. Il en suit que $|H| = p^n$, c'est donc un p-Sylow. Puisque $H \subseteq S$, on a forcément $H = S$, donc $O = O_H$ Donc H est un p-Sylow, $H = S$, et $O = O_H = \{gH : g \in G\} = G/H$. ∎

Théorème VI.2.3 (Premier théorème de Sylow)**.** *Soit G un groupe fini et p premier. Alors G admet un p-Sylow.*

Preuve du premier théorème de Sylow. On a $|X| = \binom{mp^n}{p^n} \equiv m \mod p$. Puisque $p \nmid m$, on a $p \nmid |X|$. En particulier, il existe une orbite O tel que $p \nmid |O|$. D'après le Lemme VI.2.2, il existe un p-Sylow $H \leq G$ tel que $O = G/H$. En particulier, un p-Sylow existe. ∎

Si $H \leq G$ est un p-Sylow, $g \in G$ et $K = gHg^{-1}$ alors, puisque la conjugaison par g est un automorphisme : $K \leq G$ et $|K| = |H|$. En particulier, K est aussi un p-Sylow. D'ailleurs, d'après Lagrange, l'ordre de tout sous-groupe de H est une puissance de p. La réciproque est aussi vraie :

Théorème VI.2.4 (Second théorème de Sylow)**.** *Soit G un groupe fini et p premier. Alors tous les p-Sylow de G sont conjugués. Autrement dit, si H et K sont des p-Sylow, alors il existe $g \in G$ tel que $gHg^{-1} = K$.*

De surcroît, tout sous-groupe de G dont l'ordre est une puissance de p est un sous-groupe d'un p-Sylow de G.

Démonstration. Soit $H \leq G$ un p-Sylow, et $K \leq G$ un sous-groupe d'ordre p^ℓ pour un certain ℓ. Considérons l'action $K \curvearrowright G/H$: c'est la restriction à K de l'action $G \curvearrowright G/H$, qui est elle-même une restriction de $G \curvearrowright X$ de tout à l'heure. On a $|G/H| = m$, et $p \nmid m$, donc cette action admet au moins une orbite O' telle que $p \nmid |O'|$.

Fixons $gH \in O' \subseteq G/H$. Alors $O' = K \cdot gH = \{kgH : k \in K\}$, et $|O'| = [K : K_{gH}] \mid p^\ell$. Puisque $p \nmid |O|'$, c'est que $|O'| = 1$. Autrement dit, $kgH = gH$ pour tout $k \in K$, donc $kg \in gH$ et $k \in gHg^{-1}$. Ainsi, $K \subseteq gHg^{-1}$, et gHg^{-1} est un p-Sylow.

Si K est un p-Sylow, c'est que $|K| = |H| = |gHg^{-1}| = p^n$, donc $K = gHg^{-1}$. Ceci prouve le deuxième théorème. ∎

Maintenant, que nous savons que les p-Sylow existent et qu'ils sont tous conjugués, on peut se demander, combien il en existe exactement. Il n'est pas toujours possible d'y donner une réponse complète, mais nous pouvons établir au moins quelques contraintes.

Théorème VI.2.5 (Troisième théorème de Sylow)**.** *Soit G un groupe fini et p premier. Soit $|G| = p^n m$, où $p \nmid m$, et soit N_p le nombre des p-Sylow de G. Alors*

— *$N_p \mid m$, et*

— *$N_p \equiv 1 \mod p$.*

Démonstration. Soit $\mathfrak{S}$ l'ensemble des p-Sylows, de sorte que $N_p = |\mathfrak{S}|$. Si $H \in \mathfrak{S}$, alors $\mathfrak{S}$ est l'ensemble des conjugués de H, d'après le second théorème. Rappelons la conclusion de l'Exercice IV.17 : $|\mathfrak{S}| = \big[G : N_G(H)\big]$, et ceci divise $[G : H]$. Autrement dit, $N_p \mid m$.

Revenons maintenant à l'action $G \curvearrowright X$, et soit Ω l'ensemble de ses orbites. Nous pouvons le partitionner en :

$$\Omega_1 = \{O \in \Omega : p \nmid |O|\}, \qquad \Omega_2 = \Omega \smallsetminus \Omega_1 = \{O \in \Omega : p \mid |O|\}.$$

Si $H \in \mathfrak{S}$, alors $H \in X$, et $O_H = G/H$ est de cardinal m, donc $G/H \in \Omega_1$. Ceci nous définit donc une application $\mathfrak{S} \to \Omega_1$, $H \mapsto G/H$.

Cette application est injective, car on peut retrouver H à partir de la famille $G/H = \{gH : g \in G\}$ (comment ?) D'après le Lemme VI.2.2, cette application est également surjective. Donc :

$$|X| = \sum_{O \in \Omega} |O| = \sum_{O \in \Omega_1} |O| + \sum_{O \in \Omega_2} |O| \equiv \sum_{H \in \mathfrak{S}} |G/H| = mN_p,$$

où $\equiv$ est la congruence modulo p. Nous avons aussi démontré plus tôt que

$$|X| = \binom{mp^n}{p^n} \equiv m.$$

Donc $mN_p \equiv m$, et puisque m est inversible modulo p, on a $N_p \equiv 1$, le tout modulo p. ∎

3. Applications

Corollaire VI.3.1. *Soit G un groupe fini et p un diviseur premier de $|G|$. Alors il existe $x \in G$ tel que* $\mathrm{ord}(x) = p$.

Démonstration. D'après le premier théorème, G admet au moins un p-Sylow, notons le par H. Par définition, $|H| = p^k$, où p^k est la plus grande puissance de p divisant $|G|$. Par hypothèse, $k \geq 1$, donc il existe $x \in H \smallsetminus \{e\}$. D'après Lagrange, $\mathrm{ord}(x) \mid |H|$, donc $\mathrm{ord}(x) = p^\ell$.

Puisque $x \neq e : \ell \geq 1$. Soit $y = x^{p^{\ell-1}}$. Alors $y \in H \leq G$ et $\mathrm{ord}(y) = p$. ■

Corollaire VI.3.2. *Soit $p < q$ premiers, et G un groupe d'ordre pq. Alors*

(i) *Le groupe G admet un unique q-Sylow.*

(ii) *S'il est aussi vrai que G admet un unique p-Sylow, alors G est cyclique : $G \cong C_{pq}$.*

Démonstration. D'après le troisième théorème, $N_q \equiv 1 \mod q$ et $N_q \mid p$. En particulier, $N_q \leq p < q$, donc forcément $N_q = 1$.

Soit H l'unique q-Sylow, et supposons également que G admet un unique p-Sylow, appelons-le K. On a $|H \cup K| \leq p + q - 1 < pq$ (l'identité appartient au deux). Il existe donc $x \in G \smallsetminus (H \cup K)$. D'après Lagrange :

$$\mathrm{ord}(x) \mid pq.$$

Quelles sont les possibilités pour $\mathrm{ord}(x)$?

— $\mathrm{ord}(x) = 1$: non, car $x \neq e$.

— $\mathrm{ord}(x) = p$: dans ce cas, $\langle x \rangle$ serait un p-Sylow, donc égal à K, or $x \neq K$, donc impossible.

— $\mathrm{ord}(x) = q$: impossible pour la même raison avec q et H au lieu de p et K.

— $\mathrm{ord}(x) = pq$: c'est l'unique possibilité qui reste !

Donc $\mathrm{ord}(x) = |G|$, d'où $G = \langle x \rangle$ est cyclique.

(On pourrait aussi appliquer l'Exercice VI.8 pour déduire que G est cyclique – mais dans notre cas la preuve directe est aussi facile.) ■

Corollaire VI.3.3. *Soit $p < q$ premiers, et G un groupe tel que $|G| = pq$. Si G est abélien, ou si $p \nmid (q-1)$, alors G est cyclique.*

Démonstration. Si G est abélien alors il admet un unique p-Sylow (car tous les p-Sylow sont conjugués). Supposons maintenant que $p \nmid q - 1$. Autrement dit, $q \not\equiv 1 \mod p$. D'après le troisième théorème, on a $N_p \mid q$, donc $N_p \in \{1, q\}$, et $N_p \equiv 1 \mod p$, donc $N_p \neq q$. On en déduit que $N_p = 1$, il existe donc un unique p-Sylow. D'après le Corollaire VI.3.2, G est cyclique. ■

Exercices

Exercice VI.1. Soit p premier et $m, n \in \mathbf{N}$. Montrons que $m \equiv \binom{mp^n}{p^n} \mod p$ d'une autre manière.

(i) Montrer que si $0 < k < p^n$, alors $p \mid \binom{p^n}{k}$.

(ii) Montrer que

$$\binom{mp^n}{p^n} = \sum_{k_1 + \cdots + k_m = p^n} \binom{p^n}{k_1} \cdots \binom{p^n}{k_m}.$$

(iii) En déduire que

$$\binom{mp^n}{p^n} \equiv m \mod p.$$

Exercice VI.2. On dit que G est un **p-groupe** si l'ordre de chaque élément de G est une puissance de p.

Montrer qu'un groupe fini est un p-groupe si et seulement si son ordre est une puissance de p.

Exercice VI.3. Soit G un groupe d'ordre p^n.

(i) Montrer que si $n > 1$, alors G admet un sous-groupe distingué d'ordre p^k avec $0 < k < n$.
Indication : il y a plusieurs cas à considérer, mais on pourrait commencer en regardant le Lemme IV.3.2.

(ii) Déduire que pour tout $0 \leq k \leq n$, G admet au moins un sous-groupe d'ordre p^k.

Exercice VI.4. Soit G un groupe d'ordre $p^n m$, où $p \nmid m$. Montrer que pour tout $0 \leq k \leq n$, G admet au moins un sous-groupe d'ordre p^k.

Exercice VI.5. Montrer, sans utiliser les théorèmes de Sylow, que le second théorème de Sylow est équivalent à l'affirmation suivante :

> Soit $H \leq G$ un p-Sylow, et $K \leq G$ un sous groupe dont l'ordre est une puissance de p. Alors il existe $g \in G$ tel que $gKg^{-1} \leq H$.

Exercice VI.6. Trouver les 2- et 3-Sylow des groupes symétriques S_3 et S_4. Vérifier les affirmations du second et du troisième théorème.

Exercice VI.7. Soit G un groupe d'ordre p^k avec p premier, admettant au plus un sous-groupe de chaque ordre. Montrer que G est monogène.
Indication : essayer de majorer le cardinal de $\{x \in G : \mathrm{ord}(x) < p^k\}$.

Exercice VI.8. Soit G un groupe d'ordre n (fini), admettant au plus un sous-groupe de chaque ordre. Soit $n = p_1^{k_1} \cdots p_m^{k_m}$ la factorisation de n en puissance de premiers.

(i) Montrer que pour chaque $1 \leq i \leq m$, G admet un sous-groupe H_i d'ordre $p_i^{k_i}$.

(ii) Montrer que chaque H_i est monogène (voir l'exercice précédent). Dans la suite, soit x_i un générateur de H_i.

(iii) Montrer que $H_i \trianglelefteq G$.

(iv) Montrer que $H_i \cap H_j = \varnothing$ pour $i \neq j$.

(v) Déduire que les x_i commutent entre eux (on pourrait s'inspirer de la preuve de la Remarque V.1.8).

(vi) Déduire que $y = x_1 x_2 \cdots x_m$ est un générateur de G, qui est par conséquent monogène.

Exercice VI.9. Soit G un groupe fini d'ordre n. À de l'Exercice II.23 et de l'Exercice VI.8, montrer que sont équivalents :

(i) G est cyclique.

(ii) G admet exactement un sous-groupe d'ordre d pour chaque $d \mid n$.

(iii) G admet au plus un sous-groupe de chaque ordre.

Chapitre VII

Groupes simples

1. Définition et exemples

On se rappelle que tout groupe G possède au moins deux sous-groupes distingués : le sous groupe trivial $\{e\}$, que nous noterons par la suite par 1, et G lui-même. Enfin, pour dire "deux", il faut encore que les deux soient distincts, c'est à dire que $G \neq 1$.

Définition VII.1.1. Un groupe G est dit **simple** s'il possède exactement deux sous-groupes distingués, le sous-groupe trivial $1 = \{e\}$ et G lui-même.

Autrement dit, G est simple si et seulement si :
— $G \neq 1$.
— Tout sous-groupe distingué de G est ou bien 1, ou bien G.

Exemple VII.1.2. Soit p premier. Alors le groupe cyclique d'ordre p (que nous notons des fois par C_p, des fois par $\mathbf{Z}/p\mathbf{Z}$) est simple.

Proposition VII.1.3. *Tout groupe simple abélien est cyclique d'ordre premier.*

Question VII.1.4. Existe-t-il d'autre groupes simples ? Non abéliens ?

La réponse est oui, mais malheureusement, on ne peut pas les construire à partir de groupes plus simples. . .car ils sont simples !

Exemple VII.1.5. Les groupes diédraux D_n (non abéliens) ne sont pas simples.

Rappel : la signature d'une permutation :

$$\operatorname{sgn} \colon S_n \to \{\pm 1\}.$$

Permutations **paires** et **impaires**.

Exemple VII.1.6. Le groupe S_n n'est pas simple pour $n \geq 3$ (par contre, $S_2 \cong C_2$ est simple). En effet, $A_n = \ker \operatorname{sgn}$ est un sous-groupe distingué qui n'est ni 1 ni S_n.
On appelle A_n le groupe **alterné**.

Dans les deux cas, D_n et S_n, on a trouvé un sous-groupe distingué d'indice deux (d'ailleurs, tout sous-groupe d'indice deux est distingué), d'où la non simplicité de D_n et de S_n.
Quid du sous-groupe distingué lui-même ?
— Dans le cas de D_n, c'est le groupe de rotations, qui est abélien – ça ne nous aide pas.
— Dans le cas de S_n, c'est le groupe alterné A_n, qui, au moins pour $n \geq 4$, n'est pas abélien.
Le groupe alterné serait-il éventuellement simple ?

Exemple VII.1.7.
— $A_2 = 1$ n'est pas simple.
— $A_3 \cong C_3$ est simple – mais abélien.
— A_4 n'est pas abélien, mais n'est pas simple non plus. En effet, posons

$$H = \big\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\big\}.$$

Alors $H < A_n$ – et c'est un sous-groupe distingué (rappel – conjugaison de cycles).

Ça commence mal, mais chaque fois c'est un peu plus compliqué – A_5 serait-il simple ?

Lemme VII.1.8. *Tout* 3*-cycle est pair, et toute permutation paire est produit de* 3*-cycles.*

Démonstration. Par récurrence sur le cardinal du support. ■

Lemme VII.1.9. *Soit $n \geq 5$, et $1 \neq H \trianglelefteq A_5$. Alors*

(i) *H continent au moins un* 3*-cycle.*

(ii) *H contient tous les* 3*-cycles.*

(iii) *$H = A_5$.*

Théorème VII.1.10. *Pour tout $n \geq 5$, A_n est un groupe simple (non abélien).*

2. Décomposition de Jordan-Hölder

On sait que si $G = H \rtimes K$ (produit semi-direct interne) alors $H \trianglelefteq G$ et $K \cong G/H$.

Par contre, la réciproque est fausse : il se peut bien que $H \trianglelefteq G$ sans que G puisse s'exprimer comme $H \rtimes K$, pour un quelconque sous-groupe K de G. On aimerait dire que même dans ce cas, G est "composé" de deux "briques" H et G/K. Mais ceci a-t-il un sens ? La réponse est bien positive, si on passe aux "briques indécomposables" – c'est à dire, à des briques qui sont, eux, des groupes simples.

Définition VII.2.1. Sous groupe distingué **maximal**.

Lemme VII.2.2. *Soit $H \trianglelefteq G$. Alors H est distingué maximal dans G si et seulement si G/H est un groupe simple.*

Définition VII.2.3. — Suite de composition

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1.$$

— Raffinement d'une suite de composition.

— Suite de Jordan-Hölder : suite de composition qui n'admet pas de raffinement.

Lemme VII.2.4. *Une suite de composition est une suite de Jordan-Hölder si et seulement si tous les quotients G_i/G_{i+1} sont simples (ce qui est équivalent à : G_{i+1} est distingué maximal dans G_i).*

Lemme VII.2.5. *Soit G un groupe fini. Alors toute suite de composition peut être raffinée en en suite de Jordan-Hölder.*

En particulier, G admet au moins une suite de Jordan-Hölder.

Théorème VII.2.6 (Théorème de Jordan-Hölder)**.** *Soit G un groupe fini admettant deux suites de Jordan-Hölder :*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1,$$
$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_s = 1.$$

Alors $r = s$ et les suites de quotients $(G_i/G_{i+1} : 0 \leq i < r)$ et $(H_i/H_{i+1} : 0 \leq i < r)$ sont l'un une permutation de l'autre.

Démonstration. Par récurrence sur $\min(r, s)$. Si le minimum est zéro : ...

Sinon :

Si $G_1 = H_1$, l'hypothèse de récurrence s'applique directement.

Si $G_1 \neq H_1$, on pose $K = G_1 \cap H_1$. On montre que $G_1H_1 \trianglelefteq G$ d'où $G_1H_1 = G$, et $G_1/K \cong G/H_1$, $H_1/K \cong G/K_1$. On choisit une suite de Jordan-Hölder pour K :

$$K = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_t = 1.$$

Cela nous fournit des suites de Jordan-Hölder pour G_1 et H_1 :

$$G_1 \triangleright K \triangleright K_1 \triangleright \cdots \triangleright K_t = 1,$$
$$H_1 \triangleright K \triangleright K_1 \triangleright \cdots \triangleright K_t = 1.$$

Maintenant on peut appliquer l'hypothèse de récurrence. ■

Exemple VII.2.7. Quotients de Jordan-Hölder :

(i) Un groupe abélien d'ordre $n = p_1^{k_1} p_2^{k^2} \cdots$

(ii) D_n.

(iii) S_n, selon les valeurs de n.

3. Groupes résolubles

Rappel : le commutateur de $x, y \in G$ est

$$[x, y] = xyx^{-1}y^{-1}.$$

On a

$$[x, y] = e \qquad \Longleftrightarrow \qquad xy = yx.$$

Définition VII.3.1. Le groupe dérivé

$$G' = [G, G] = \big\langle [x, y] : x, y \in G \big\rangle$$

Exemple VII.3.2. Si G est abélien, alors $G' = 1$.

Exemple VII.3.3. Soit D_n le groupe diédral et $R \subseteq D_n$ l'ensemble des rotations. On se rappelle que :

— R est un sous-groupe cyclique d'ordre n.

— Si $s \in D_n$ est n'importe quelle réflexion, alors $s^2 = e$ et $D_n = R \rtimes \langle s \rangle$. En particulier $R \trianglelefteq D_n$.

Soit r un générateur de R : $R = \langle r \rangle$. Alors $D_n' = \langle r^2 \rangle$. Ceci pourrait-il être égal à R ? Distinct de R ?

Lemme VII.3.4. *Le groupe dérivé est un sous-groupe distingué, $G' \trianglelefteq G$, et le quotient G/G' est abélien.*

Proposition VII.3.5. *Soit G un groupe et $H \trianglelefteq G$. Alors G/H est abélien si et seulement si $H \geq G'$.*

Définition VII.3.6. Un groupe G est **résoluble** s'il admet une suite de composition

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$$

telle que chaque quotient G_i/G_{i+1} est abélien.

Exemple VII.3.7. Le groupe diédral $D_n = C_n \rtimes C_2$ est résoluble pour tout n.

Proposition VII.3.8. *Posons $G^{(0)} = G$, $G^{(1)} = G'$, $G^{(2)} = G''$, …, $G^{(n+1)} = (G^{(n)})'$. Alors G est résoluble si et seulement s'il existe n tel que $G^{(n)} = 1$.*

Proposition VII.3.9. *Soit G un groupe fini et*

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$$

une suite de Jordan-Hölder. Alors sont équivalents :

(i) *G est résoluble.*

(ii) *Tous les quotients G/G_i sont abéliens.*

(iii) *Tous les indices $[G_i : G_{i+1}]$ sont premiers.*

Exemple VII.3.10. Soit $n \in \mathbf{N}$. Alors S_n est résoluble si et seulement si $n \leq 4$.

Exercices

Exercice VII.1. Montrer que si $G' \leq H \leq G$ alors $H \trianglelefteq G$.

Exercice VII.2. Montrer que $S_n' = A_n$.
Indication : montrer que pour toute deux transpositions σ_1 et σ_2 on peut écrire le produit $\sigma_1\sigma_2$ sous la forme $[\sigma_1, \tau]$, pour une permutation τ bien choisie.