Groupes

Marc SAGE (collab. Michel WIGNERON)

19 septembre 2017

Table des matières

1 Introduction

Structures et lois.

Une *loi*[1] est donnée par une *table de composition*, telle nos tables de multiplication, qui dicte comment deux éléments doivent être *composés*.

↱	△	□	#
△	□	△	#
□	△	□	#
#	#	#	#

exemple de loi sur un trio $\{\triangle, \square, \#\}$

Selon les contraintes de la loi, l'ensemble régi sera différemment *structuré*. Sans aucune contrainte, il est *amorphe* – sans structure : on parlera de ***magma***[2].

Les noms des structures *groupes-anneaux-corps* au programme des classes préparatoires furent forgés principalement dans les tomes de *Moderne Algebra* de VAN DER WAERDEN, ouvrage qui a fortement inspiré le collectif BOURBAKI – partant, une bonne partie des mathématiciens postérieurs. Revenir à la langue allemande éclaire en quoi ces termes français décrivent la complexification croissante de ces structures :

1. simple regroupement (*Grup*, groupe) ;
2. cartel d'entreprises (*Ring*, anneau) ;
3. corps d'armée (*Körper*, corps).

Morphismes.

Connaître, c'est relier. Connaître une structure passe donc par la compréhension des applications depuis et vers cette structure qui, si possible, "préservent" cette dernière : respecter la structure, c'est conserver la forme, c'est rendre la *même forme*, d'où l'importance de l'étude des *homomorphismes*[3] – souvent abrégé en "*morphismes*". Par exemple, les morphismes d'espaces vectoriels sont les applications linéaires.

Chaque type de structure amène son lot de morphismes, lesquels nous définirons en temps voulu. Cependant, les définitions suivantes s'appliquent *indépendamment du type considéré* et c'est pourquoi nous les donnons dès cette introduction :

Un ***isomorphisme***[4] *est un morphisme bijectif.*

Un ***endomorphisme***[5] *est un morphisme dont source et but coïncident.*

Un ***automorphisme***[6] *est un endomorphisme bijectif.*

La notion la plus discriminante est celle d'isomorphisme : on ne voudra pas distinguer deux structures *isomorphes* – c'est-à-dire qui ont littéralement la même forme ! Par exemple, deux espaces vectoriels de même dimension sont indistinguables au sens suivant : ayant fixé une base de l'un et une base de l'autre, chaque propriété vectorielle portant sur l'un se transporte immédiatement sur l'autre. Et réciproquement. Le choix

[1] *Rappel* : une ***loi de composition interne*** (***l. c. i.***) sur un ensemble E est une application $E^2 \longrightarrow E$.

[2] Un magma est donc simplement un ensemble muni d'une l. c. i., *i. e.* un couple $(M, *)$ où $*$ est une l. c. i. sur M.

[3] *homo* = même, *morphe* = forme

[4] *iso* = égal

[5] *endo* = à l'intérieur de

[6] *auto* = soi-même (retenir AUTO = ISO + ENDO)

des bases est précisément celui d'un isomorphisme : la variété de choix pour les espaces vectoriels reflète leur *automorphie*, décrite par les groupes linéaires $GL(E) = \operatorname{Aut} E$.

À l'instar des morphismes, plusieurs définitions ou propositions pourraient être formulées dans un cadre général où, par « truc », il faudrait entendre l'un des types de structure suivants :

monoïde, groupe, anneau, corps, espace vectoriel, algèbre.

Dans ce chapitre, nous aborderons les groupes et les monoïdes.

Exercice d'application

Proposer un magma dont la table de composition est donnée en introduction.

Cette table était

↱	△	□	#
△	□	△	#
□	△	□	#
#	#	#	#

. Le dièse # est absorbant et le carré □ est neutre : imposons donc $\binom{\#}{\square} = \binom{0}{1}$ pour la multiplication complexe. Le triangle △ est alors une racine carrée de □ autre que □, donc vaut -1. Réciproquement, on vérifie que le monoïde $\{-1, 0, 1\}$ multiplicatif convient :

× ↱	-1	1	0
-1	1	-1	0
1	-1	1	0
0	0	0	0

.

---

2 Monoïdes, inversibles, groupes

Les groupes décrivent nos *actions composables* et *réversibles*. Voyons déjà les actions composables tout court, étant plus naturel d'avancer avant de chercher à reculer.

Quitte à anticiper, signalons que les monoïdes seront aux groupes ce que les anneaux sont aux corps. Le langage monoïdal, bien que hors programme, permettra donc d'éclairer la présentation des anneaux.

2.1 Monoïdes, exemples

Définition (monoïde, ordre, abélien)

On appelle ***monoïde*** *tout magma associatif*[7] *unifère,* i. e. *tout triplet* $(M, *, \varepsilon)$ *tel que*

[7] On pourra alors dans chaque (multi-)composé retirer toutes les parenthèses sans ambigüité, *i. e. associer* les composants comme l'on désirera.

1. $*$ *est une l. c. i. sur* M *;*
2. *chaques éléments* $m, \mu, \mathfrak{m}$ *de* M *vérifient* $m * (\mu * \mathfrak{m}) = (m * \mu) * \mathfrak{m}$ *;*
3. ε *est un élément de* M *vérifiant* $\forall m \in M, \begin{cases} m * \varepsilon = m \\ \varepsilon * m = m \end{cases}$ *, alors unique (***exercice !***)*
   et appelé son ***neutre***[8] *.*

Le cardinal d'un monoïde est aussi appelé son ***ordre****.*
Un monoïde M *est dit* ***abélien***[9] *(ou* ***commutatif****) si* $\forall m, \mu \in M,\ m * \mu = \mu * m$*.*

Conventions (multiplicatives et additives)

On renvoie au cours de première année pour les vocabulaire et notations multiplicatifs et additifs[10] :

monoïde M qualifié de	loi notée	loi appelée	neutre noté	neutre appelé
multiplicatif	$\times$ ou $\cdot$ ou	multiplication	1_M voire 1	***un***
additif	$+$	addition	0_M voire 0	***zéro***

Comme il est d'usage avec la multiplication usuelle, souvent la loi d'un monoïde multiplicatif est abrégée en $\cdot$ voire disparaît complètement[11].

L'usage est de réserver la notation additive *exclusivement* aux monoïdes *abéliens*.

Sauf contre-indication, nous utiliserons
dans ce cours la notation *multiplicative*.

Exemples (monoïdes)

1. Soit A un ensemble. L'ensemble $A^A = \mathrm{Fonc}\,(A, A)$ est un monoïde pour la composition. Son neutre est l'application identité Id_A dont l'action ne change rien. C'est l'exemple typique de monoïde qui "transcrit" en mathématique notre action sur un ensemble donné.
2. Soit S une structure. Les endomorphismes de S forment un monoïde $\mathrm{End}\, S$ pour la composition. Cela a déjà été montré pour les espaces vectoriels, ce le sera pour les autres structures[12].
3. $\mathbb{N}$ est un monoïde additif (pour l'addition usuelle). Il permet d'itérer des endomorphismes (*cf.* § 2.2).

FIG 1 : $0 \curvearrowright 1 \curvearrowright 2 \curvearrowright 3 \curvearrowright \cdots$

[8] Un neutre est parfois appelé une unité, d'où la terminologie *unifère* (= qui porte une unité).

[9] Dans ses travaux de 1824 sur la résolution des équations polynomiales de degré 5, Niels Abel a mis en évidence l'importance de la *commutativité* d'un certain groupe de permutations, d'où la terminologie.

[10] Le symbole + vient simplement du t abrégeant le latin *et*. Il apparaît en 1489 avec Johannes Widmann dans son ouvrage *Behende und hubsche Rechenung auff allen Kauffmanschafft*, puis en 1544 avec Michael Stifel dans son *Arithmetica Integra*.

[11] Le premier usage de la croix de saint André $\times$ apparaît en 1631 dans le *Clavis mathematicae* de William Oughtred. Thomas Harriot utilisait un point et René Descartes simplement la juxtaposition. Les imprimeurs cependant eurent sans doute leur part de responsabilité.

[12] Remarque – En voyant un ensemble comme une structure "sans structure", *i. e.* où les morphismes entre ensembles sont juste des applications sans contrainte aucune, on retrouve le monoïde $\mathrm{End}\, A = A^A$ du premier exemple.

4. Pour chaque ensemble A, est un monoïde l'ensemble $A^* := \coprod_{n\in\mathbb{N}} A^n$ des mots sur A muni de la concaténation

$$((a,b,c,...,z),(\alpha,\beta,\gamma,...,\omega)) \mapsto (a,b,c,...,z,\alpha,\beta,\gamma,...,\omega).$$

   Son neutre est le ***mot vide*** ( ), unique élément de $A^0 = A^{\emptyset}$.
5. Sont des monoïdes additifs[13] $\overline{\mathbb{N}}$, $\mathbb{Z}$, $\mathbb{Q}$, $\overline{\mathbb{Q}_+}$, $\mathbb{R}$ et $\overline{\mathbb{R}_+}$ (mais pas $\mathbb{N}^*$, faute de neutre) ou encore $18\mathbb{N}$, $\mathbb{N}\backslash\{1\}$ et $\overline{\mathbb{N}}\backslash\{1,2,5\}$.
6. Sont des monoïdes multiplicatifs $\{42^n\}_{n\in\mathbb{N}}$, $\{-1,0,1\}$, $\mathbb{Z}$, $\mathbb{Z}^*$, $\overline{\mathbb{Z}^*}$, $\mathbb{Q}$, $\mathbb{Q}^*$, $\overline{\mathbb{Q}^*}$, $\mathbb{R}$, $\mathbb{R}^*$, $\overline{\mathbb{R}^*}$, $\overline{\mathbb{R}^*_+}$, $\mathbb{C}$ et $\mathbb{C}^*$.
7. Le segment $[0,1]$ est un monoïde pour min et pour max. Plus généralement, une partie de $\overline{\mathbb{R}}$ est un monoïde pour min (resp. max) ssi elle admet un *maximum* (resp. un *minimum*).
8. Chaque singleton muni de la seule loi possible (constante) est un monoïde, appelé un ***monoïde trivial***.

REMARQUE – Le monoïde $[0,\infty]$ servira de cadre pour les familles sommables – *cf.* chapitre 8 ? ? ?.

Exercices d'application

1. *Déterminer les parties de $\overline{\mathbb{R}}$ qui sont des monoïdes pour la soustraction, resp. la division.*
2. *L'espace $\mathbb{R}^3$ est-il un monoïde pour le produit vectoriel ?*
3. *Soit E un ensemble. L'ensemble $\mathfrak{P}(E)$ est-il un monoïde pour resp. la réunion, l'intersection, la privation, la différence symétrique*[14] *?*
4. *Soit A un ensemble. L'ensemble A^* des mots sur A est-il un monoïde pour le mélange faro*

$$((a_1,a_2,a_3,...,a_p),(b_1,b_2,b_3,...,b_q)) \mapsto \begin{cases} (a_1,b_1,a_2,b_2,a_3,b_3,...,a_p,b_p,b_{p+1},b_{p+2},...,b_q) & si\ p \le q \\ (a_1,b_1,a_2,b_2,a_3,b_3,...,a_q,b_q,a_{q+1},a_{q+2},...,a_p) & si\ p > q \end{cases} \quad ?$$

---

1. Soit $A \subset \overline{\mathbb{R}}$ un monoïde "soustractif". Notons n son neutre. La différence $n-n$ vaut alors 0 (calcul usuel) mais vaut aussi n (puisque n est neutre), d'où $n = 0$. La neutralité de 0 implique pour chaque $a \in A$ les égalités $a - 0 = a = 0 - a$, *i. e.* $a = -a$, d'où $a = 0$ et $A = \{0\}$. Réciproquement, ce singleton est un monoïde (trivial) pour $-$.

   On montrerait de même que les monoïdes "divisifs" inclus dans $\overline{\mathbb{R}}$ sont $\{1\}$ et $\{-1,1\}$.

[13] La barre coiffante signifie l'achèvement de l'ordre, c'est-à-dire que l'on a rajouté au besoin des *maximum* et *minimum*. Par exemple $\overline{\mathbb{N}} := \mathbb{N} \amalg \{\infty\}$ et $\overline{\mathbb{R}} := \mathbb{R} \amalg \{\pm\infty\}$.

[14] La ***différence symétrique*** de deux ensembles A et B est l'ensemble $A\Delta B := A\backslash B \amalg A\backslash B = (A \cup B)\backslash(A \cap B)$.

2. Le produit vectoriel $\wedge$ fait bien sens sur tout $\mathbb{R}^3$. Soit par l'absurde n un neutre pour $\wedge$. On a alors pour chaque vecteur a l'orthogonalité $a = a \wedge n \perp a$, d'où $a \perp a$ et la nullité de a, ce qui montre l'inclusion $\mathbb{R}^3 \subset \{0\}$: contradiction.

   On aurait également pu nier l'associativité en invoquant un trièdre direct (u, v, w) et en constatant la différence des composés $\left\{ \begin{array}{c} (u \wedge u) \wedge v = 0 \wedge v = 0 \\ u \wedge (u \wedge v) = u \wedge w = -v \end{array} \right.$.

3. Les lois $\cup$ et $\cap$ sont associatives et admettent pour neutres respectifs $\emptyset$ et E (*cf.* cours de première année). De même, Δ est associative et commutative (exercice de première année) et admet pour neutre le vide vu pour chaque partie $P \subset E$ les égalités

$$P \Delta \emptyset = (P \cup \emptyset) \setminus (P \cap \emptyset) = P \setminus \emptyset = P.$$

   En revanche, vu les égalités $\left\{ \begin{array}{c} E \setminus (E \setminus E) = E \setminus \emptyset = E \\ (E \setminus E) \setminus E = \emptyset \setminus E = \emptyset \end{array} \right.$, la privation n'est jamais associative (sauf si E est vide, auquel cas $\mathfrak{P}(E)$ est un monoïde trivial).

4. Le mot vide est un neutre pour le faro $*$ (remplacer dans la définition p ou q par 0). Si A est un singleton, le faro est clairement associatif (et, quand A est vide, $A^* = A^0$ est un monoïde trivial). En revanche, si l'on peut invoquer dans A deux éléments *distincts* $a \neq b$, on constatera la différence des mélanges $\left\{ \begin{array}{c} [ab] * ([a] * [b]) = [ab] * [ab] = [aabb] \\ ([ab] * [a]) * [b] = [aab] * [b] = [abab] \end{array} \right.$. Finalement, A^* est un monoïde pour le faro ssi $\operatorname{Card} A \leq 1$.

2.2 Itérés

Le monoïde $\mathbb{N}$ vérifie (admis) le **théorème fondamental de définition de suites par itération** dans chaque ensemble, étant donnés un point de départ dans cet ensemble et une application stabilisant ce dernier :

$$\forall A,\ \left\{ \begin{array}{l} \forall @ \in A \\ \forall f \in A^A \end{array} \right.\ ,\ \exists! a \in A^{\mathbb{N}},\ \left\{ \begin{array}{l} a_0 = @ \\ \forall n \in \mathbb{N},\ a_{n+1} = f(a_n) \end{array} \right.\ .$$

Ce théorème est très fréquemment utilisé en analyse. Il permet également (hors programme) de construire l'addition, la multiplication et l'exponentiation dans $\mathbb{N}$. Restant dans le programme, il permet de définir proprement les *itérés* d'un élément.

Proposition – Définition (suite des itérés, idempotent, involutif, involution)

Soit $(M, *)$ un monoïde et soit $a \in M$.

La composition par a (à droite ou à gauche[15]) détermine une unique suite $(a^{*n})_{n \in \mathbb{N}}$ ayant pour terme initial le neutre de M, appelée ***suite des itérés*** *de a :*

$$1 \longmapsto a \longmapsto a^2 \longmapsto a^3 \longmapsto \cdots$$

(en additif : $0 \longmapsto a \longmapsto 2a \longmapsto 3a \longmapsto \cdots$*).*

[15] La lectrice scrupuleuse montrera en exercice que les deux suites ainsi définies coïncident.

L'élément a est dit ***idempotent***[16] *quand* $a^2 = a$ (i. e. *quand ses puissances sont égales) :*

$$1 \longmapsto a \longmapsto a \longmapsto a \longmapsto \cdots .\ \textit{FIG 2}$$

L'élément a est dit ***involutif***[17] *quand* $a^2 = 1$ (i. e. *quand ses puissances bouclent dès le début) :*

$$1 \longmapsto a \longmapsto 1 \longmapsto a \longmapsto \cdots .\ \textit{FIG 3}$$

Une ***involution*** *d'un ensemble A est un involutif du monoïde A^A,* i. e. *une application $f : A \longrightarrow A$ telle que $f \circ f = \mathrm{Id}_A$.*

Les involutions permettant de "revenir en arrière", nous les retrouverons avec les groupes. Elles font partie de la faune des classes préparatoires.

Exemples (involutions)

1. Les symétries dans un espace vectoriel (dont les réflexions planes et symétries centrales),
2. la complémentation $A \mapsto {}^cA$ dans un $\mathfrak{P}(E)$,
3. la complémentation $x \mapsto a - x$ dans un segment $[0, a]$,
4. la complémentation $d \mapsto \frac{n}{d}$ dans l'ensemble des diviseurs d'un naturel n,
5. l'opposition $r \mapsto -r$ dans $\mathbb{R}$, l'inversion $q \mapsto \frac{1}{q}$ dans $\mathbb{Q}^*$,
6. la conjugaison complexe $c \mapsto \overline{c}$.

Exercices d'application

1. *Déterminer les idempotents de $\mathfrak{P}(E)$ muni de Δ ainsi que les involutifs de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ muni de $+$ ou $\times$.*
2. *On définit la* ***moyenne géométrique*** *de chaque famille $(a_1, a_2, ..., a_N)$ de réels positifs par $\sqrt[N]{a_1 a_2 \cdots a_N}$. Soit $n \geq 1$ un naturel. Montrer que la moyenne géométrique des diviseurs de n vaut $\sqrt{n}$.*

---

1. Soit $A \subset E$. Puisque $A \Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$, le seul idempotent de $\mathfrak{P}(E)$ muni de Δ est $\emptyset$.

   Pour chaque complexe a, l'égalité $2a = 0$ équivaut à la nullité de a et celle $a^2 = 1$ équivaut à $a = \pm 1$. Ainsi, le seul involutif de $\mathbb{C}$ (*a fortiori* de $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$) pour $+$ est 0 et les deux involutifs pour $\times$ sont ± 1.
2. Calculons le produit des diviseurs de d, reparamétré par l'involution $d \mapsto \frac{n}{d}$ ci-dessus :

$$\left(\prod_{d|n} d\right)^2 = \prod_{d|n} d \prod_{\delta|n} \delta \overset{\substack{\text{reparamétrage} \\ d := \frac{n}{\delta}}}{=} \prod_{d|n} d \prod_{d|n} \frac{n}{d} = \prod_{d|n} d \frac{n}{d} = n^{\#\,\mathrm{Div}(n)}.$$

   Prendre la racine carrée conclut.

---

[16] *idem* = même, *potent* = puissance

[17] *in-évolutif* : qui n'évolue pas (au sens des itérés), qui revient en arrière.

2.3 Inversibles, groupes

Définition (élément régulier, inversible, groupe)

Soit M un monoïde.

Un élement $a \in M$ est dit ***régulier*** *(ou* ***simplifiable****) si l'on peut simplifier par a des deux côtés,* i. e. *si*[18]

$$\forall m, \mu \in M, \ \begin{cases} am = a\mu \Longrightarrow m = \mu \\ ma = \mu a \Longrightarrow m = \mu \end{cases} .$$

Deux éléments a et b sont dits ***symétriques l'un de l'autre*** *si $ab = 1 = ba$. À a fixé, quand il y a un tel b, l'élément a est dit* ***symétrisable****. Un tel b est alors unique (***exercice !****), est appelé le* ***symétrique*** *de a.*

Lorsque la loi est notée multiplicativement (resp. additivement), un élément symétrisable s'appelle un ***inversible*** *(resp.* ***opposable****), son symétrique s'appelle son* ***inverse*** *(resp.* ***opposé****) et est noté a^{-1} (resp. $-a$) quand le symétrisable est noté a.*

L'ensemble des symétrisables de M est appelé son ***groupe des inversibles***[19] *et est noté $M^\times$ (lire « M croix*[20] *»). Lorsque $M^\times = M$, on dit que M est un* ***groupe****.*

Un ***groupe*** est ainsi un magma associatif unifère où chaque élément est inversible, *i. e.* un quadruplet $(G, \cdot, 1, i)$ où :

1. $\cdot$ est une application $G^2 \longrightarrow G$ (sa ***loi***) telle que $\forall g, \gamma, \mathfrak{g} \in G, \ g\,(\gamma\mathfrak{g}) = (g\gamma)\,\mathfrak{g}$;
2. 1 est un élément de G (son ***neutre***) tel que $\forall g \in G, \ \begin{cases} g\ 1 = g \\ 1\ g = g \end{cases}$;
3. i est une application $G \longrightarrow G$ (son ***inversion***) telle que $\forall g \in G, \ \begin{cases} g\ i\,(g) = 1 \\ i\,(g)\ \ g = 1 \end{cases}$.

Avant de voir des exemples de groupes, étudions un peu leurs constituants : les inversibles.

Propriétés (inversibles)

Soit M un monoïde.

1. *Chaque inversible est régulier. Dans un groupe, chaque élément est régulier.*
2. *Chaque involutif est inversible et vaut son propre inverse (ainsi $1^{-1} = 1$).*
3. *L'application $m \mapsto m^{-1}$ est une involution de $M^\times$ qui "inverse" la loi*[21] *:*

$$\forall m, \mu \in M^\times, \qquad \left(m^{-1}\right)^{-1} = m \qquad et \qquad (m\mu)^{-1} = \mu^{-1} m^{-1}.$$

Démonstration

[18] Cela revient à l'injectivité des deux compositions par a.

[19] En pratique, plus personne ne dit « symétrique » et la majorité se comprend lorsqu'elle parle multiplicativement. Il n'est donc pas rare d'entendre « inversible pour + », ce qui ne manquera pas de choquer l'oreille avertie.

[20] Ne pas confondre $M^\times$ (groupe des inversibles) avec M^* (notation déconseillée car ambigüe) qui peut désigner l'ensemble des mots sur l'alphabet M tout comme le monoïde M privé de son neutre.

[21] On dit que l'application $m \mapsto m^{-1}$ est un ***anti-morphisme*** ; les ***morphismes*** (tout court) vont quant à eux *préserver* la loi.

1. Composer par l'inverse d'un inversible va permettre de simplifier par ce dernier, d'un côté comme de l'autre. Montrons-le par exemple pour le côté gauche. Soit $a \in M^\times$, soient $m, \mu \in M$ tels que $am = a\mu$. Composer à gauche par a^{-1} donne $a^{-1}(am) = a^{-1}(a\mu)$, *i. e.* $\left(a^{-1}a\right)m = \left(a^{-1}a\right)\mu$, *i. e.* $1m = 1\mu$, *i. e.* $m = \mu$, *c. q. f. d.*

   Dans un groupe, chaque élément est inversible, donc régulier.

2. Soit $i \in M$ involutif. On a donc $i^2 = 1$, *i. e.* $ii = 1 = ii$, ce qui montre que i est inversible d'inverse i.

3. Soit $m \in M^\times$. Notons $\mu := m^{-1}$. On a alors $m\mu = 1 = \mu m$, *i. e.* $\mu m = 1 = m\mu$, ce qui montre que μ est inversible d'inverse m ; ainsi l'inverse $\left(m^{-1}\right)^{-1}$ fait-il sens et vaut-il m.

   Soit de plus $\mu \in M^\times$. On a alors les égalités

$$\begin{cases} (m\mu)\left(\mu^{-1}m^{-1}\right) = m\left(\mu\mu^{-1}\right)m^{-1} = m1m^{-1} = mm^{-1} = 1 \\ \left(\mu^{-1}m^{-1}\right)(m\mu) = \mu^{-1}\left(m^{-1}m\right)\mu = \mu^{-1}1\mu = \mu^{-1}\mu = 1 \end{cases},$$

   ce qui montre que $m\mu$ et $\mu^{-1}m^{-1}$ sont inverses l'un de l'autre.

Remarques

• Le point 1 légitime la simplification dans chaque groupe sans autre forme de procès.

• Le point 2 est particulièrement utilisé dans les monoïdes fonctionnels :

chaque involution est bijective de réciproque elle-même.

• *Mnémonique* (point 3) : on met ses chaussettes *avant* ses chaussures mais, pour se mettre pieds nus, on retirer *d'abord* ses chaussures avant ses chaussettes.

• Demander si un monoïde donné est un groupe cache une question plus fine, à savoir *quel est son groupe des inversibles*. C'est comme demander si un naturel est premier, resp. si une application est surjective, resp. si un polynôme est scindé, resp. si une application linéaire est injective : il est alors plus précis de trouver ses facteurs premiers, resp. son image, resp. ses racines (avec multiplicité), resp. son noyau.

Exemples (groupes des inversibles)

1. On a $M_n(\mathbb{R})^\times = GL_n(\mathbb{R})$ pour chaque naturel n et on a $\left(E^E\right)^\times = \mathfrak{S}_E$ pour chaque ensemble E. Plus généralement, on démontrera en § 4.3 l'égalité

$$(\operatorname{End} S)^\times = \operatorname{Aut} S \text{ pour chaque structure } S.$$

2. Chez les polynômes, on a $\mathbb{C}[X]^\times = \begin{cases} \mathbb{C}[X] \text{ pour } + \\ \mathbb{C}^* \text{ pour } \times \end{cases}$ et plus généralement

$$A[X]^\times = A^\times \text{ pour chaque anneau } A \text{ intègre.}$$

3. Chez les entiers, on a $\mathbb{Z}^\times = \begin{cases} \mathbb{Z} \text{ pour } + \\ \{\pm 1\} \text{ pour } \times \end{cases}$ et $\mathbb{N}^\times = \begin{cases} \{0\} \text{ pour } + \\ \{1\} \text{ pour } \times \end{cases}$.

Exercices d'application

1. *Montrons qu'est abélien chaque groupe dont chaque élément est involutif.*
2. *Soit M un monoïde. Montrer l'égalité $M^{\times\times} = M^{\times}$,* i. e. *que le groupe des inversibles de M est un groupe.*

---

1. Soit G un groupe où $\forall g \in G,\ g^2 = 1$. On a alors pour chaques $a, b \in G$ les égalités
$$ab = a1b = a\,(ab)^2\,b = a\,(abab)\,b = a^2\,(ba)\,b^2 = ba.$$
Autre rédaction : chaque élément de G est involutif, donc vaut son propre inverse, d'où pour chaques $a, b \in G$ les égalités $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$.
2. Montrons que le "magma" $M^{\times}$ muni de la loi induite par celle de M est un groupe. Il s'agit bien d'un magma car le composé de deux inversibles est inversible (*cf.* propriété précédente, point (3)). Il est associatif car sa loi découle d'une loi associative (celle du monoïde M). Il est unifère car 1 est inversible (*cf.* point (2)). Soit enfin $m \in M^{\times\times}$. Notons n l'inverse de m dans le monoïde $M^{\times}$ On a donc dans $M^{\times}$ l'égalité $mn = 1 = nm$; or, la loi de $M^{\times}$ étant celle de M, cette dernière égalité se lit également dans M, montrant que m est inversible dans M (d'inverse n), d'où $m \in M^{\times}$, *c. q. f. d.*

2.4 Groupes symétriques

Action fonctionnelle, permutations, groupes symétriques

Soit A un ensemble. Le groupe des inversibles de A^A est formé des bijections de A dans lui-même, appelées ***permutations*** de A. Il est noté $\mathfrak{S}_A$ ou $\mathfrak{S}(A)$ et s'appelle le ***groupe symétrique***[22] de A.

Pour chaque naturel n, on note $\mathfrak{S}_n$ le groupe symétrique du segment $[|1, n]$. Ces groupes ont été abordés en première année[23]. Donnons-en une vision géométrique pour les petits n, afin de ne pas se noyer dans la définition axiomatique[24].

Soit $[AB]$ un segment. Alors les transformations géométriques de la droite (AB) qui préservent le segment $[AB]$ sont : la réflexion d'axe la médiatrice de $[AB]$... et[25] l'identité de (AB). La réflexion "correspond à" la permutation de $\mathfrak{S}_2$ échangeant les extrémités 1 et 2, à savoir la transposition (1 2).

[22] L'expression $ab + ba$ est dite *symétrique* en un sens naturel : échanger les lettres a et b n'affecte pas la somme. Plus généralement, une expression littérale est *symétrique* lorsque son évaluation est inchangée par permutations de ses lettres. Un groupe *symétrique* est ainsi l'ensemble des transformations préservant une expression symétrique – d'où son nom.

[23] Ce sont *ces* groupes finis qui apparaissent dans les travaux d'Évariste Galois (début du XIX$^{\text{e}}$ siècle) portant sur la résolution des équations polynomiales. Galois parlait alors de « *groupes* de substitution », signifiant sans doute que ces substitutions étaient *unies* de quelque manière remarquable.

[24] due à Arthur Cayley en 1854, plusieurs dizaines d'années après Galois

[25] Ne pas oublier l'identité !

FIG 4 : les 2 symétries du segment

Soit ABC un triangle équilatéral. Alors les transformations planes préservant le triangle ABC sont de trois types : les trois réflexions d'axes les médiatrices des segments de ABC (auxquelles correspondent les trois transpositions de $\mathfrak{S}_3$), les deux rotations d'angles $\pm\frac{2\pi}{3}$ de centre celui de T (auxquelles correspondent les deux 3-cycles (1 2 3) et (1 3 2)) – sans oublier l'identité.

FIG 5 : les 6 symétries du triangle

Le lecteur pourra également chercher à réaliser $\mathfrak{S}_4$ à l'aide d'un tétraèdre régulier.

Proposition (translations, "petit" théorème de Lagrange)

Soit G un groupe.

1. *Ses **translations** $\left\{\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & ag \end{array}\right.$ et $\left\{\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & ga \end{array}\right.$ (lorsque a décrit G) en sont des permutations*[26].
2. *Lorsque G est abélien et fini, on l'égalité $g^{|G|}=1$ pour chaque $g\in G$ (**"petit" théorème de Lagrange***[27]*).*

Démonstration

1. Soit $a\in G$ et notons $\gamma_a : g\mapsto ag$ la translation à **g**auche par a, élément du monoïde G^G. On y vérifie aisément les égalités $\gamma_1=\mathrm{Id}$ et $\gamma_a\gamma_b=\gamma_{ab}$ (pour chaque $b\in G$), d'où le fait que γ_a et $\gamma_{a^{-1}}$ soient réciproques l'une de l'autre. On procéderait de même pour les translations à droite.
2. Soit $g\in G$. Rédigeons additivement (juste pour changer). La translation par g étant surjective par le point précédent, on peut écrire $G=g+G$. Travaillons alors la somme des éléments du groupe[28] :

$$\sum_{\gamma\in G}\gamma \overset{G=g+G}{=} \sum_{\gamma\in g+G}\gamma \overset{\text{reparamétrage}}{\underset{\mathfrak{g}:=\gamma-g}{=}} \sum_{\mathfrak{g}\in G}(g+\mathfrak{g}) = \sum_{\mathfrak{g}\in G} g+\sum_{\mathfrak{g}\in G}\mathfrak{g} \overset{\text{reparamétrage}}{\underset{\gamma:=\mathfrak{g}}{=}} |G|\,g+\sum_{\gamma\in G}\gamma,$$

d'où le résultat $|G|\,g=0$ en simplifiant par $\sum_{\gamma\in G}\gamma$.

Remarques

• Le fait de rapporter un élément à son action multiplicative (*via* les translations) n'est pas anodin : essayez d'expliquer à un enfant pourquoi $\frac{1}{a}\frac{1}{b}=\frac{1}{ab}$ sans parler de l'effet de la multiplication par une fraction ! Cette remarque est à la base d'un théorème de Cayley (*cf.* § 4.4) affirmant que les groupes symétriques sont en un certain sens les plus généraux.

• L'hypothèse d'abélianité pour le "petit" théorème de Lagrange est en fait superflue (*cf.* § 4.7).

[26] Par exemple, si G est le plan (identifié aux translations planes), on pourra visualiser que faire glisser suivant un vecteur donné "ne change rien globalement" ; si G est le cercle $\mathbb{U}$, faire tourner d'un angle donné "ne change rien globalement".

[27] Joseph-Louis Lagrange a prouvé dès 1771 un cas particulier de ce théorème dans ses *Réflexions sur la résolution algébrique des équations, II* publiées dans les *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin.*

[28] idée très fructueuse = démonstration exigible !

Exercice d'application

Soit A un ensemble. Montrer que $\mathfrak{S}_A$ n'est jamais abélien, sauf si $|A| \leq 2$.

Il est clair que sont abéliens les groupes $\mathfrak{S}_0 = \{\mathrm{Id}_\emptyset\}$, $\mathfrak{S}_1 = \{\mathrm{Id}\}$ et $\mathfrak{S}_2 = \{\mathrm{Id}, (1\ 2)\}$.

Soit E de cardinal au moins 3. Soient a, x, y distincts dans E. Alors les deux transpositions $(a\ x)$ et $(a\ y)$ ne commutent pas vu que les composées $\begin{cases} (a\ x) \circ (a\ y) = (a\ y\ x) \\ (a\ y) \circ (a\ x) = (a\ x\ y) \end{cases}$ diffèrent (elles n'agissent pas pareil sur a par exemple).

2.5 Autres exemples de groupes

Automorphismes

Soit S une structure. Les automorphismes de S forment un groupe $\mathrm{Aut}\, S$ pour la composition. Cela a déjà été montré pour les espaces vectoriels, ce le sera pour les autres structures[29].

Groupe référent, itération bilatère[30]

$\mathbb{Z}$ est un groupe additif (*est-il un groupe multiplicatif ?*). Il permet d'itérer "en arrière", donc dans les deux sens. On renvoie au cours de première année pour les définitions et propriétés des itérés d'un inversible.

Groupes numériques

Sont des groupes additifs $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (pas $\mathbb{N}$).

FIG 6 : $\cdots \underset{\leftarrow}{\ } -3 \underset{\leftarrow}{\ } -2 \underset{\leftarrow}{\overset{\curvearrowright}{\ }} -1 \underset{\leftarrow}{\overset{\curvearrowright}{\ }} 0 \underset{\leftarrow}{\overset{\curvearrowright}{\ }} 1 \underset{\leftarrow}{\overset{\curvearrowright}{\ }} 2 \overset{\curvearrowright}{\ } 3 \overset{\curvearrowright}{\ } \cdots$

Sont des groupes multiplicatifs $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ (pas $\mathbb{Z}^*$).
Tous abéliens.

Sous-groupes complexes

Les complexes unitaires forment un groupe[31] (multiplicatif) noté $\mathbb{U}$.

FIG 7 : cercle unité

Pour chaque naturel n, les racines n-ièmes de l'unité également, leur groupe[32] est noté $\mathbb{U}_n$.

[29] Sans contrainte aucune (structure "sans structure"), on retrouve le groupe $\mathrm{Aut}\, A = \mathsf{S}_A$ du premier exemple.

[30] *bi-latère* : deux côtés

[31] À visualiser comme le cercle unité.

[32] À visualiser comme un n-gone régulier.

FIG 8 : n-gone régulier (selon parité n)

De même pour la réunion $\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ (**exercice !**).
Tous abéliens.

Quaternions (hors programme)

Tout comme $\mathbb{C}$ peut être vu comme un espace vectoriel de la forme $\mathbb{R}\oplus\mathbb{R}i$ muni d'une multiplication vérifiant $i^2=-1$, on admettra l'existence d'un $\mathbb{R}$-espace vectoriel[33] $\mathbb{H}$ de la forme $\mathbb{R}\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k$ muni d'une multiplication (associative) vérifiant $i^2=j^2=k^2=ijk=-1$. Alors la partie $\{\pm1,\pm i,\pm j,\pm k\}$ est un groupe d'ordre 8 appelé ***groupe des quaternions*** et noté $\mathbb{H}_8$.

Groupes géométriques.

Forment un groupe (infini) pour la composition respectivement[34] :

1. les translations du plan ;
2. les rotations de même centre ;
3. les homothéties de même centre ;
4. les composées de rotations et homothéties de même centre (similitudes directes de même centre) ;
5. les rotations/translations (déplacements) ;
6. les homothéties/translations ;
7. les composées de réflexions (isométries : rotations, translations, réflexions glissées).

Plus généralement, les isométries qui laissent invariante une figure donnée dans un espace euclidien (*i. e.*, à $\mathcal{F}$ partie fixée d'un certain $\mathbb{R}^n$, les isométries σ telles que $\sigma(\mathcal{F})=\mathcal{F}$) forment le ***groupe des symétries*** de la figure considérée. Ainsi avons-nous réalisé les groupes $\mathfrak{S}_2$, $\mathfrak{S}_3$ et $\mathfrak{S}_4$.

Groupe ludique

Considérons un Rubik's cube. Chacune de ses six faces comportant neuf cases, il possède $6\times9=54$ cases. Les coups autorisés sont des rotations d'un quart de tour, chacune réversible et toutes composables entre elles. Le "groupe ludique" associé est ainsi un groupe inclus dans $\mathfrak{S}_{54}$ (on parlera plus tard de *sous-groupe*).

Groupes triviaux

Chaque singleton muni de la seule loi possible (constante) est un groupe, appelé un ***groupe trivial***.

Exercices d'application

[33] La lettre "H" abrège au choix « **h**yper-complexe » ou leur créateur « **H**amilton ».

[34] Montrer que ces groupes sont stables par composition est le plus délicat, c'est de la géométrie classique de lycée qui n'est plus dans l'esprit des concours. Le prouver à l'aide des expressions complexes des transformations est cependant bien plus aisé (et éclairant).

1. *Parmi les groupes géométriques donnés, lesquels sont abéliens ?*
2. *Déterminer le groupe des symétries du carré. Est-il abélien ?*
3. *Le groupe $\mathbb{H}_8$ est-il abélien ? Préciser la probabilité (pour la loi uniforme sur $\mathbb{H}_8^2$) que deux quaternions commutent. (On pourra établir la table de multiplication de $\mathbb{H}_8$.)*

---

1. Forment des groupes abéliens : les translations, les rotations (resp. homothéties, resp. similitudes directes) de même centre. (En termes complexes, ces groupes correspondent à $\mathbb{C}$, $\mathbb{U}$, $\mathbb{R}^*$ et $\mathbb{C}^*$). En revanche, vu que la composée de deux symétries centrales distinctes est une translation dont le sens du vecteur change selon l'ordre de composition, les trois autres groupes ne sont pas abéliens (déplacements, homothéties/translations, isométries).
2. On trouve d'une part les réflexions par rapport aux deux médiatrices et par rapport aux deux diagonales, d'autre part les quatre rotations d'angle multiple d'un quart de tour (dont la symétrie centrale de centre celui du carré... et l'identité). Ce groupe d'ordre 8 est un cas particulier de ***groupe diédral*** (hors programme) – groupe des symétries d'un polygone régulier.

FIG 9 : les 8 symétries du carré

3. Multiplier l'égalité $ijk = -1$ à $\begin{matrix}\text{droite}\\ \text{gauche}\end{matrix}$ par $\begin{matrix}-k\\ -i\end{matrix}$ donne $\begin{matrix}ij\left(-k^2\right) = k\\ \left(-i^2\right)jk = i\end{matrix}$, *i. e.* $\begin{matrix}ij = k\\ jk = i\end{matrix}$. Multiplier ces deux égalités donne alors $ijjk = ki$, d'où $-ik = ki$. Par ailleurs, multiplier l'égalité $ij = k$ à gauche par i donne $i^2j = ik$, *i. e.* $ik = -j$. On en déduit le produit $ki = -ik = j$. Puisque j est non nul (son carré vaut -1), son double non plus, *i. e.* $-j \neq j$, *i. e.* $ik \neq ki$, ce qui montre que i et k ne commutent pas. Ainsi $\mathbb{H}_8$ n'est-il pas abélien.

   Les éléments ± 1 commutent clairement avec tous les autres. Il nous reste à évaluer les produits mettant en jeu i, j, k autres que ij, jk, ik (déjà connus). Pour ce faire, observons que la validité de nos quatre hypothèses de calcul est conservée si l'on remplace[35] $\begin{cases} i \text{ par } j\\ j \text{ par } k\\ k \text{ par } i\end{cases}$: d'une part c'est clair pour les égalités $i^2 = j^2 = k^2 = -1$, d'autre part multiplier $ijk = -1$ à droite i et à gauche par $-i$ donne $\left(i^2\right)jki = -i^2$, *i. e.* $jki = -1$, ce qui est l'égalité $ijk = -1$ obtenue après action du cycle $(i\ j\ k)$. Par conséquent, la validité des résultats du paragraphe précédent est conservée par permutation cyclique de i, j, k : les égalités déjà connues $\begin{cases} ij = k\\ jk = i\\ ik = -j\end{cases}$ deviennent ainsi $\begin{cases} jk = i\\ ki = j\\ ji = -k\end{cases}$ puis $\begin{cases} ki = j\\ ij = k\\ kj = -i\end{cases}$.

[35] Elle est dite ***invariante par permutation cyclique*** de i, j, k.

Nous en déduisons le reste de la table de $\mathbb{H}_8$:

$\times$ ↱	i	$-i$	j	$-j$	k	$-k$
i	-1	1	k	$-k$	$-j$	j
$-i$	1	-1	$-k$	k	j	$-j$
j	$-k$	k	-1	1	i	$-i$
$-j$	k	$-k$	1	-1	$-i$	i
k	j	$-j$	$-i$	i	-1	1
$-k$	$-j$	j	i	$-i$	1	-1

.

On voit alors que les seuls gros carrés contenant des couples qui commutent sont les trois de la diagonales (et les sept contenant les produits de ± 1). Comme chaque gros carré contient quatre couples, la probabilité cherchée vaut $\frac{(3+7)\cdot 4}{16\cdot 4} = \frac{5}{8} = 62,5\%$.

Remarque – Un exercice jadis classique affirme que la probabilité que deux éléments d'un groupe non abélien commutent est inférieure à $62,5\%$. Nous venons d'établir que le groupe des quaternions réalise le cas d'égalité.

---

3 Création de structures

Lors de la création de nouvelles structures, la philosophie est la même que pour les espaces vectoriels : à l'aide de briques de base (exemples du cours), on construit des gros trucs de référence (souvent par puissances, cas particuliers de produits cartésiens), puis on en exhibe des sous-trucs et on y engendre d'autres sous-trucs.

3.1 Loi "parties"

Soit $(M, *)$ un magma. Alors $\mathfrak{P}(M)$ est un magma pour la loi

$$A * B := \{a * b\}_{b\in B}^{a\in A} \qquad \text{(pour chaques parties } A, B \subset M\text{)}.$$

On utilise beaucoup cette loi dans les groupes, par exemple quand on parle de sommes de sous-espaces vectoriels, à l'instar de $\mathbb{C} = \mathbb{R} + i\mathbb{R}$ ou de $\mathbb{Q}\left[\sqrt{5}\right] = \mathbb{Q} + \mathbb{Q}\sqrt{5}$. Elle constitue surtout une commodité d'écriture, un utile raccourci calculatoire, en particulier pour l'étude des groupes quotient. Dans cette optique utilitariste, on utilisera volontiers le fait que

les caractères associatif, abélien et unifère
"passent" de la loi sur M à celle sur $\mathfrak{P}(M)$.

Lorsqu'une partie est donnée par extension, on oubliera volontiers les accolades afin d'alléger les notations.

Propriétés ("opposé parties")

On a pour chaques parties A et B d'un groupe additif les égalités

$$-(-A) = A, \qquad A - A = A + (-A), \qquad -(A+B) = -A - B$$
$$\text{et l'implication } A \subset B \Longrightarrow -A \subset -B.$$

Démonstration

Il suffit d'écrire tranquillement :

$$\begin{aligned} -(-A) &= \{-o\}_{o\in -A} = \{-(-a)\}_{a\in A} = \{a\}_{a\in A} = A, \\ A - A &= \{a-\alpha\}_{\alpha\in A}^{a\in A} = \{a+(-\alpha)\}_{\alpha\in A}^{a\in A} = A + \{-\alpha\}_{\alpha\in A} = A + (-A), \\ -(A+B) &= -\{a+b\}_{b\in B}^{a\in A} = \{-(a+b)\}_{b\in B}^{a\in A} = \{-a-b\}_{b\in B}^{a\in A} = -A - B \text{ et,} \\ \text{supposant } A &\subset B,\ -A = \{-a\}_{a\in A} \subset \{-b\}_{b\in B} = -B. \end{aligned}$$

Remarques – **Gare aux confusions**

• La notation $A \times B$ désignera en priorité un produit *cartésien* : dans un monoïde multiplicatif, le produit "parties" sera noté AB.

• Tout comme l'opposition ou l'inversion complexes, la "loi" $A \mapsto -A$ n'est pas une *l. c. i.* car elle n'a qu'un seul argument (elle est dite *singulaire*) au lieu de deux (ce n'est pas une loi binaire).

• L'"opposé" $-A$ n'est pas le symétrique[36] "parties" de A mais simplement l'image directe de A par l'opposition $a \mapsto -a$, ou encore l'image de A par la loi "partie" associé à la loi singulaire "opposer".

• De même, la "différence" $A - A$ ne dénote pas le composé "parties" de A et de son opposé "parties" (ce qui devrait donner le neutre "parties") mais simplement le composé "parties" des parties A et $-A$.

Exercice d'application

a. *Que vaut la somme $\mathbb{Z} + \mathbb{Z}$? L'opposé $-\mathbb{Z}$?*

b. *Soient λ et μ deux réels. Montrer que la partie $\lambda\mathbb{Z} + \mu\mathbb{Z}$ est stable par addition et par opposition.*

c. *Soit $n \in \mathbb{N}$. Pour chaque relatif z, on note $\overline{z} := z + n\mathbb{Z}$. Montrer pour chaques $a, b \in \mathbb{Z}$ l'égalité*

$$\overline{a} + \overline{b} = \overline{a+b}.$$

---

[36] On montrerait aisément qu'un tel symétrique ne fait sens que si A est un singleton.

a. La présence d'un zéro permet d'écrire

$$\mathbb{Z}+\mathbb{Z}\supset\mathbb{Z}+0=\{z+0\}_{z\in\mathbb{Z}}=\{z\}_{z\in\mathbb{Z}}=\mathbb{Z},$$

les stabilités de $\mathbb{Z}$ par addition et par opposition s'explicitent en les inclusions

$$\begin{array}{rcl}\mathbb{Z}+\mathbb{Z} & = & \{z+\zeta\}_{z\in\mathbb{Z}}^{\zeta\in\mathbb{Z}}\subset\{s\ ;\ s\in\mathbb{Z}\}=\mathbb{Z}\\ \text{et } -\mathbb{Z} & = & \{-z\}_{z\in\mathbb{Z}}\subset\{o\ ;\ o\in\mathbb{Z}\}=\mathbb{Z},\end{array}$$

enfin l'inclusion $-\mathbb{Z}\subset\mathbb{Z}$ donne (par croissance de l'opposition "parties") l'inclusion $-(-\mathbb{Z})\subset-\mathbb{Z}$, *i. e.* (par idempotence de l'opposition "parties") l'inclusion réciproque $\mathbb{Z}\subset-\mathbb{Z}$.

Finalement, les deux double-inclusions sus-montrées aboutissent à

$$\mathbb{Z}+\mathbb{Z}=\mathbb{Z}=-\mathbb{Z}.$$

REMARQUE – Il est immédiat de généraliser et d'obtenir *pour chaque monoïde M et pour chaque groupe G les égalités*

$$\begin{array}{rcl} & & MM=M\ et\ GG=G=G^{-1}\\ \textit{(en additif} & : & M+M=M\ et\ G+G=G=-G\textit{)}.\end{array}$$

b. Utilisons ce qui précède. On a d'une part les égalités

$$\begin{array}{rcl}(\lambda\mathbb{Z}+\mu\mathbb{Z})+(\lambda\mathbb{Z}+\mu\mathbb{Z}) & = & \lambda\mathbb{Z}+(\mu\mathbb{Z}+\lambda\mathbb{Z})+\mu\mathbb{Z}\\ & = & \lambda\mathbb{Z}+(\lambda\mathbb{Z}+\mu\mathbb{Z})+\mu\mathbb{Z}\\ & = & (\lambda\mathbb{Z}+\lambda\mathbb{Z})+(\mu\mathbb{Z}+\mu\mathbb{Z})\\ & = & \lambda(\mathbb{Z}+\mathbb{Z})+\mu(\mathbb{Z}+\mathbb{Z})\\ & = & \lambda\mathbb{Z}+\mu\mathbb{Z}\end{array}$$

d'autre part les inclusions

$$-(\lambda\mathbb{Z}+\mu\mathbb{Z})\subset-\lambda\mathbb{Z}-\mu\mathbb{Z}=\lambda(-\mathbb{Z})+\mu(-\mathbb{Z})=\lambda\mathbb{Z}+\mu\mathbb{Z}.$$

c. Soient $a,b\in\mathbb{Z}$. Le calcul précédent permet d'écrire

$$\overline{a}+\overline{b}=a+n\mathbb{Z}+b+n\mathbb{Z}=a+b+n\underbrace{(\mathbb{Z}+\mathbb{Z})}_{=\mathbb{Z}}=\overline{a+b}.$$

3.2 Groupes quotients $^{\mathbb{Z}}\!/_{n}$

On fixe pour toute cette section un naturel $n\in\mathbb{N}$.

Proposition – Définition (groupe $^{\mathbb{Z}}\!/_{n}$)

1. *Les parties* $\overline{z} := z + n\mathbb{Z}$ *pour* z *décrivant* $\mathbb{Z}$ *forment, pour l'addition "parties" de* $\mathfrak{P}(\mathbb{Z})$*, un groupe abélien où*[37]

$$\forall a, b \in \mathbb{Z},\ \begin{cases} \overline{a} + \overline{0} = \overline{a} = \overline{0} + \overline{a} \\ \overline{a} + \overline{b} = \overline{a+b} \\ -\overline{a} = \overline{-a} \end{cases}.$$

Ce groupe est noté[38] *indifféremment* ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, ${}^{\mathbb{Z}}\!/_{(n)}$ *ou*

$${}^{\mathbb{Z}}\!/_{n} := \{\overline{z}\ ;\ z \in \mathbb{Z}\} = \{z + n\mathbb{Z}\}_{z\in\mathbb{Z}}$$

2. *On impose* $n > 0$*. Le groupe* ${}^{\mathbb{Z}}\!/_{n}$ *est alors d'ordre*

$$\text{Card } {}^{\mathbb{Z}}\!/_{n} = n$$

et constitué des classes des entiers de chaque suite de n *entiers consécutifs, par exemple*

$${}^{\mathbb{Z}}\!/_{n} = \begin{matrix} \left\{\overline{1}, \overline{2}, \overline{3}, ..., \overline{n}\right\} \\ \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\} \\ \left\{\overline{-n}, \overline{-(n-1)}, ..., \overline{-2}, \overline{-1}\right\} \end{matrix}.$$

Démonstration

1. L'égalité $\overline{a} + \overline{b} = \overline{a+b}$ a déjà été établie et c'est grâce à elle que de nombreuses propriétés du magma $\mathbb{Z}$ vont se transférer à ${}^{\mathbb{Z}}\!/_{n}$ simplement en "passant tout sous la barre" : la commutativité en écrivant $\overline{a}+\overline{b} = \overline{a+b} = \overline{b+a} = \overline{b}+\overline{a}$, l'associativité vu (à $c \in \mathbb{Z}$ fixé) les égalités $\begin{cases} \left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{a+b} + \overline{c} = \overline{(a+b)+c} \\ \overline{a} + \left(\overline{b} + \overline{c}\right) = \overline{a} + \overline{b+c} = \overline{a+(b+c)} \end{cases}$, le caractère unifère d'après les égalités $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$, enfin l'inversibilité suivant $\overline{a} + \overline{-a} = \overline{a+(-a)} = \overline{0}$.

2. Montrons l'inclusion ${}^{\mathbb{Z}}\!/_{n} \subset \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\}$. Soit $g \in {}^{\mathbb{Z}}\!/_{n}$, soit $z \in \mathbb{Z}$ tel que $g = \overline{z}$. La division euclidienne[39] de z par n s'écrit $z = nq + r$, d'où (q étant relatif) $\overline{z} = \overline{r}$, ce qui conclut (puisque $r \in [|0, n|[$).

   Montrons que les n classes $\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}$ sont distinctes, ce qui transformera l'inclusion précédente en égalité. Soient $u, v \in [|0, n|[$ tels que $\overline{u} = \overline{v}$. Soit $\lambda \in \mathbb{Z}$ tel que $v - u = \lambda n$. Vu les appartenances $u, v \in [|0, n|[$, la différence $v-u$ tombe dans $]|-n, n|[$, d'où la comparaison $|\lambda n| < n$. Puisque $n \neq 0$, on peut récupérer $|\lambda| < 1$; or λ est entier, donc nul, d'où la nullité de $n\lambda = v-u$ et l'égalité $u = v$.

   Enfin, vu la surjectivité des translations dans un groupe, on a pour chaque relatif a les égalités

$$\begin{aligned} {}^{\mathbb{Z}}\!/_{n} &= \overline{a} + {}^{\mathbb{Z}}\!/_{n} = \overline{a} + \{\overline{u}\}_{u\in[|0,n|[} = \{\overline{a} + \overline{u}\}_{u\in[|0,n|[} \\ &= \{\overline{a+u}\}_{u\in[|0,n|[} \overset{\text{reparamétrage}}{\underset{v:=u+a}{=}} \{\overline{v}\}_{v\in[|a,a+n|[}. \end{aligned}$$

---

[37] Ces égalités traduisent le fait que la surjection $\begin{cases} \mathbb{Z} & \twoheadrightarrow & {}^{\mathbb{Z}}\!/_{n} \\ z & \mapsto & \overline{z} \end{cases}$ est un *morphisme de groupes*. La flèche multiple $\twoheadrightarrow$ indique une *surjectivité* : on pourra visualiser de multiples flèches terminant au même endroit, tels autant d'antécédents envoyés sur une même image.

[38] Prononcer « $\mathbb{Z}$ sur $n\mathbb{Z}$ » ou « $\mathbb{Z}$ sur n ».

[39] La division euclidienne est légitime car n est ici non nul.

Remarques

• Lorsque l'on calculera *modulo* n, on gagnera à travailler avec des entiers de norme *minimale*. Il sera ainsi utile d'utiliser des descriptions comme

$$\mathbb{Z}/_4 = \left\{\overline{-1}, \overline{0}, \overline{1}, \overline{2}\right\} \qquad \text{ou} \qquad \mathbb{Z}/_7 = \left\{\overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}.$$

• Lorsque $n = 0$, chaque classe est un singleton $\overline{z} = \{z\}$ et la surjection $z \mapsto \overline{z}$ devient injective, donc le groupe

$$\mathbb{Z}/_0 = \{\{z\} \ ; \ z \in \mathbb{Z}\}$$

est d'ordre infini (dénombrable[40]). Il ressemble à s'y méprendre à $\mathbb{Z}$: on dira qu'il sont *isomorphes*. Quotienter par 0 ne présente donc aucun intérêt conceptuel.

Définition (égalité *modulo* n)

On appelle ***égalité modulo*** n *la relation sur* $\mathbb{Z}$ *formée des couples* (a, b) *tels que*

$$a = b \ [n] \overset{\text{déf.}}{\iff} b \in a + n\mathbb{Z} \iff \exists \lambda \in \mathbb{Z}, \ b - a = \lambda n.$$

Remarque – Karl Gauss a introduit ce vocabulaire dans ses *Disquisitiones arithmeticae* de 1801. Il y remplaçait l'égalité $=$ par le symbole de ***congruence*** $\equiv$ mais ce n'est pas indispensable : l'essentiel est de signaler quelque part que l'on calcule *modulo* (« à la mesure de ») quelque chose et de préciser ce quelque chose[41], le ***module***, la mesure à l'aune de laquelle on calcule.

Proposition – Définition (classes *modulo* n)

1. *On a pour chaques relatifs* a *et* b *l'équivalence* $a = b \ [n] \iff \overline{a} = \overline{b}$.
2. *L'égalité* modulo n *est une relation d'équivalence sur* $\mathbb{Z}$.
3. *Pour l'égalité* modulo n*, la classe d'équivalence d'un* $z \in \mathbb{Z}$ *fixé est ce que nous avons noté*

$$\overline{z} = z + n\mathbb{Z}, \text{ appelée simplement } \textbf{\textit{classe de}} \ z \ \textbf{\textit{modulo}} \ n.$$

4. *L'égalité* modulo n *est compatible*[42] *avec l'addition et la multiplication de* $\mathbb{Z}$.

[40] On verra au chap8 ? ? ? que $\mathbb{Z}$ est dénombrable, par exemple *via* la bijection

$$\left\{\begin{array}{ccc} \mathbb{N} & \xrightarrow{\sim} & \mathbb{Z} \\ n & \longmapsto & (-1)^n \left\lceil \frac{n}{2} \right\rceil \\ 2|z| + \mathbf{1}_{\mathbb{Z}^*_-}(z) & \longleftarrow | & z \end{array}\right. .$$

[41] Par exemple, les crochets « $[n]$ » peuvent s'expliciter en « $\bmod n$ » voire en « *modulo* n ».

[42] Une relation $\overset{\circ}{=}$ sur un magma M est dit ***compatible*** avec la loi de ce dernier si

$$\forall m, m', \mu, \mu' \in M, \ \left\{\begin{array}{c} m \overset{\circ}{=} m' \\ \mu \overset{\circ}{=} \mu' \end{array}\right. \implies m\mu \overset{\circ}{=} m'\mu'.$$

L'archétype de la relation compatible est l'égalité $=$, d'où la notation semblable $\overset{\circ}{=}$ que nous avons utilisée et celle similaire $\equiv$ souvent rencontrée pour les relations *d'équivalence* compatibles (appelées ***congruences***).

Démonstration Soient $a, b \in \mathbb{Z}$.

1. On a toujours l'appartenance $b = b + 0n \in \overline{b}$. Si $\overline{a} = \overline{b}$, on en déduit $b \in \overline{b} = \overline{a} = a + \mathbb{Z}n$, d'où $a = b \ [n]$.

   Supposons réciproquement $a = b \ [n]$. Soit $\lambda \in \mathbb{Z}$ tel que $b = a + \lambda n$. En se souvenant que les translations d'un groupe sont surjectives, d'où l'on tire $\mathbb{Z} + \lambda = \mathbb{Z}$, on a alors les égalités

$$\overline{b} = b + \mathbb{Z}n = a + \lambda n + \mathbb{Z}n = a + (\mathbb{Z} + \lambda)\, n = a + \mathbb{Z}n = \overline{a}.$$

2. Puisque l'égalité ensembliste est une relation d'équivalence, on a l'égalité $\overline{a} = \overline{a}$, l'équivalence $\overline{a} = \overline{b} \iff \overline{b} = \overline{a}$ et (à $c \in \mathbb{Z}$ fixé) l'implication $\left\{ \begin{array}{l} \overline{a} = \overline{b} \\ \overline{b} = \overline{c} \end{array} \right. \implies \overline{a} = \overline{c}$. Le point précédent permet alors de transformer ces trois affirmations en termes d'égalités *modulo* n, exprimant précisément ce qu'il fallait démontrer.

3. À $z \in \mathbb{Z}$ fixé, les éléments de la classe d'équivalence[43] de z sont par définition les relatifs a tels que $a = z \ [n]$, *i. e.* ceux tels que $a \in z + n\mathbb{Z}$, d'où l'égalité annoncée.

4. Soient $a', b' \in \mathbb{Z}$ tels que $\left\{ \begin{array}{l} a = a' \ [n] \\ b = b' \ [n] \end{array} \right.$, *i. e.* tels que $\left\{ \begin{array}{l} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{array} \right.$. Additionner donne alors $\overline{a} + \overline{b} = \overline{b} + \overline{b'}$, *i. e.* $\overline{a' + b'} = \overline{a + b}$, ou encore $a + b = a' + b' \ [n]$.

   Pour la multiplication, il va falloir[44] travailler "à la main". Soient $\lambda, \mu \in \mathbb{Z}$ tels que $\left\{ \begin{array}{l} a' = a + \lambda n \\ b' = a + \lambda n \end{array} \right.$. On a alors

$$a'b' = (a + \lambda n)\,(b + \mu n) = ab + n\,(a\mu + b\lambda + \lambda\mu n) \in \overline{ab}, \text{ d'où } a'b' = ab \ [n]\,.$$

Remarque – **Calcul *modulo* n.** Le point (4) doit guider l'intuition : on additionnera "comme d'habitude" avec des vraies égalités dans $\mathbb{Z}$ en précisant quelque part « *modulo* n »[45]. Les égalités $\left\{ \begin{array}{c} \overline{a} + \overline{0} = \overline{a} = \overline{0} + \overline{a} \\ \overline{a} + \overline{b} = \overline{a + b} \\ -\overline{a} = \overline{-a} \end{array} \right.$ légitiment ce guide : on peut écrire de vraies égalités dans ${}^{\mathbb{Z}}\!/_{n}$ en mettant des barres partout et en additionnant "comme dans $\mathbb{Z}$".

Remarques – **Quotient ${}^{\mathbb{Z}}\!/_{n}$.**

• **Quotient & relation d'équivalence.** L'ensemble ${}^{\mathbb{Z}}\!/_{n}$ est le quotient de $\mathbb{Z}$ par l'égalité *modulo* n, d'où la notation et l'appellation de ***groupe quotient***[46].

• **Quotienter & diviser.** Une relation d'équivalence correspondant à une partition, « *quotienter* $\mathbb{Z}$ par l'égalité *modulo* n » (au sens du quotient ${}^{\mathbb{Z}}\!/_{= [n]}$) signifie également « *diviser* le bloc $\mathbb{Z}$ en parties chacune un translaté de $n\mathbb{Z}$ », « le *partitionner* suivant les classes *modulo* n ».

[43] Il serait insensé de parler de la classe d'équivalence de z sans avoir établi le point précédent.

[44] La raison est simple : si l'on pouvait toujours écrire $\overline{a}\overline{b} = \overline{ab}$ pour la multiplication "parties", on aurait en particulier l'égalité $\overline{0}\overline{0} = \overline{0}$, laquelle implique l'inclusion $n\mathbb{Z} \subset n^2\mathbb{Z}$, d'où le fait que n soit multiple de son carré, ce qui est impossible dès que l'on impose $n \geq 2$.

[45] Un tel calcul est qualifié de ***modulaire*** (adjectif relatif à *modulo*).

[46] Pour une histoire de la notion de groupe quotient (de Galois à Hölder en passant par Jordan), on pourra consulter l'article *The development and understanding of the concept of quotient group* de Julia Nicholson (disponible en ligne).

FIG 10 : $\mathbb{Z}$, ses éléments, ses classes mod n

• **Quotienter & tuer.** On observera l'égalité $\overline{n} = \overline{0}$ et plus généralement la nullité *modulo* n de chaque multiple de n. Dans cette optique, on pourra visualiser la barre de quotient $\diagup_n$ comme la trace d'un coup de sabre assassin. « Quotienter par » doit en effet être compris par « tuer », « annuler », « assassiner » :

quotienter par quelque chose,
c'est tuer tous ses éléments.

Il va de soi que cet assassinat porte des conséquences à assumer afin de ne pas se laisser surprendre. Par exemple, on peut évaluer la somme

$$\arctan 2 + \arctan 5 + \arctan 8 = \operatorname{Arg}(1+2i) + \operatorname{Arg}(1+5i) + \operatorname{Arg}(1+8i)$$

en l'identifiant à l'argument du produit $(1+2i)(1+5i)(1+8i) = -65-65i$, argument valant $-\frac{3\pi}{4}$; or la somme cherchée est clairement positive ! Comment lever cette contradiction ? En ne perdant pas de vue que l'identification précédente n'est valide que *modulo*[47] 2π... c'est-à-dire dans le groupe $\mathbb{R}\diagup_{2\pi}$ dont on devinera aisément le sens.

• **Quotienter & boucler (hors programme).** Lorsque l'on s'intéresse aux questions resp. de parité, de jours de la semaine, de demi-tons dans une octave, d'heures dans la journée ou de minutes dans une heure, on considère des nombres entiers (ce qui dénombre) tout en "tuant" le naturel resp. $2, 7, 12, 24, 60$. Cela revient à se placer dans le groupe $\mathbb{Z}\diagup_n$ pour le naturel n correspondant[48]. On pourra visualiser que l'on "tord", "boucle", "enroule" la droite $\mathbb{Z}$ pour forcer $n = 0$ et l'on retrouve en fait le groupe $\mathbb{U}_n$ (à un *isomorphisme* près, *cf.* § 4), à l'exception de $\mathbb{Z}\diagup_0$ qui s'identifie à $\mathbb{Z}$ ("tuer" 0 ne change pas grand chose !).

FIG 11 : "bouclage" de $\mathbb{Z}$ en $n = 0$, de $\mathbb{R}$ en $2\pi = 0$.

Exercice d'application

Soit u un nombre entier de six chiffres divisible par 13, mettons $u = abcdef$ écrit en base 10. Montrer que l'entier $bcdefa$ est aussi divisible par 13.

Notons $v := bcdefa$. Exprimons v en fonction de u *modulo* 13 (sachant que $u \equiv 0$ par hypothèse) :

$$v = 10u - 10^6 a + a \equiv \left(1 - 10^6\right) a.$$

Il suffit donc de montrer $10^6 \equiv 1$ *modulo* 13. C'est l'occasion d'utiliser la compatibilité de la multiplication ainsi que les classes des entiers de $[\![-6, 6]\!]$:

$$10^6 \equiv (-3)^6 = 3^{3\times 2} = \left(3^3\right)^2 = 27^2 \equiv 1^2 = 1, \text{ } c.\ q.\ f.\ d.$$

---

[47] Un bon encadrement fournirait $\frac{5\pi}{4} = 2\pi - \frac{3\pi}{4}$ comme réponse.
[48] Observer que tuer n revient à tuer chacun de ses multiples.

3.3 Produit cartésien

Rappelons que le produit cartésien[49] $M \times N$ de deux magmas est muni d'un loi (dite ***loi produit***)

$$\left(\begin{pmatrix} m \\ n \end{pmatrix}, \begin{pmatrix} \mu \\ \nu \end{pmatrix}\right) \mapsto \begin{pmatrix} m\mu \\ n\nu \end{pmatrix}.$$

De même, étant donnés un naturel ℓ et une suite $(M_1, M_2, ..., M_\ell)$ de magmas de longueur ℓ, la ***loi produit*** est définie sur le produit $\prod_{i=1}^{\ell} M_i$ par[50]

$$\left(\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_\ell \end{pmatrix}, \begin{pmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_\ell \end{pmatrix}\right) \mapsto \begin{pmatrix} m_1\mu_1 \\ m_2\mu_2 \\ \vdots \\ m_\ell\mu_\ell \end{pmatrix}.$$

Plus généralement, étant donnés un ensemble I et une famille (M_i) de magmas indexée par I, on définit sur le produit cartésien[51]

$$\prod_{i\in I} M_i := \left\{(m_i)_{i\in I} \ ; \ \forall i \in I, \ m_i \in M_i\right\}$$

une ***loi produit*** par

$$\left((m_i)_{i\in I}, (\mu_i)_{i\in I}\right) \mapsto (m_i\mu_i)_{i\in I}.$$

Lorsque les magmas coïncident – notons M leur valeur commune –, le produit devient une puissance

$$\prod_{i\in I} M_i = \prod_{i\in I} M = M^I, \text{ espaces des fonctions de } I \text{ vers } M$$

et l'on retrouve les lois fonctionnelles $(f, g) \mapsto \left\{\begin{array}{ccc} I & \longrightarrow & M \\ i & \longmapsto & f(i)\, g(i) \end{array}\right.$. Bien se convaincre que la signification est identique – nous sommes simplement passés de la notation indicielle à celle fonctionnelle.

Propriétés (ce qui "passe" au produit)

Chaque produit de magmas est resp. associatif, commutatif, unifère ssi chacun de ses facteurs l'est.

Chaque élément d'un tel produit est resp. neutre, inversible (quand cela fait sens) ssi chacune de ses coordonnées l'est

Démonstration

[49] Au cas où : *cartésien* vient de René *Descartes* et ne prend conséquemment *pas de "h"*.

[50] Tout se passe donc *coordonnée par coordonnée* (d'où le nom de ***loi terme à terme*** également utilisé), ce qui se voit bien mieux en présentant les familles *verticalement* plutôt qu'horizontalement.

[51] L'ensemble $\prod_{i\in I} M_i$ est défini par compréhension : mais *dans quel ensemble ?* La question est oiseuse en classes préparatoires ; voici toutefois une réponse pour les pointilleuses. La famille (M_i) est par définition une application de source I, notons $\mathcal{M}$ son but et définissons $M := \cup\mathcal{M}$. Alors chaque M_i est inclus dans M et le produit $\prod M_i$ sera défini comme partie de M^I.

Soit (M_i) une famille[52] de magmas. On a alors les équivalences

$$\begin{aligned}
\prod M_i \text{ commutatif} &\iff \forall m, \mu \in \prod M_i,\ m\mu = \mu m \\
&\iff \forall m, \mu \in \prod M_i,\ \forall i,\ m_i\mu_i = \mu_i m_i. \\
&\overset{?}{\iff} \forall i,\ \forall a, b \in M_i,\ ab = ba \\
&\iff \forall i,\ M_i \text{ commutatif}
\end{aligned}$$

(bien prendre le temps de décomposer l'équivalence $\overset{?}{\iff}$ en deux implications). L'associativité se traite de même. L'affirmation sur le caractère unifère découle de celle sur les neutres (montrée toujours de manière analogue), celle sur les inversibles de ce que deux éléments du produit sont inverses l'un de l'autre ssi leurs coordonnées le sont dans le magma unifère correspondant (démonstration toujours semblable).

Corollaire – Définition (groupe produit, monoïde produit)

Le produit cartésien de chaque famille de groupes, muni de la loi produit, reste un groupe, appelé ***groupe produit****. (*Idem *en remplaçant « groupe » par « monoïde ».)*

Démonstration

Le caractère associatif et unifère passe au produit, de même pour les inversibles – la proposition précédente montre au passage pour chaque famille (M_i) de monoïdes l'égalité

$$\left(\prod_{i\in I} M_i\right)^\times = \prod_{i\in I} M_i^\times.$$

Exercice d'application

Préciser l'équivalence $\overset{?}{\iff}$ dans la démonstration ci-dessus.

Supposons $\forall i,\ \forall a, b \in M_i,\ ab = ba$. Soient $m, \mu \in \prod M_i$, soit $i_0 \in I$. Remplacer dans l'hypothèse (i, a, b) par $\left(i_0, m_{i_0}, \mu_{i_0}\right)$ donne alors $m_{i_0}\mu_{i_0} = \mu_{i_0} m_{i_0}$.

Supposons $\forall m, \mu \in \prod M_i,\ \forall i,\ m_i\mu_i = \mu_i m_i$. Soit $i_0 \in I$, soient $a, b \in M_i$. On définit une famille $f \in \prod M_i$ en envoyant $i_0 \mapsto a$ et chaque autre indice sur le neutre du M_i correspondant : on a alors $f_{i_0} = a$. On définirait de même une famille $g \in \prod M_i$ telle que $g_{i_0} = b$. Remplacer dans l'hypothèse (m, μ, i) par (f, g, i_0) donne alors $f_{i_0} g_{i_0} = g_{i_0} f_{i_0}$.

3.4 Sous-structures

3.4.1 Introduction

Les structures en classes préparatoires (monoïdes, groupes, anneaux, corps, espaces vectoriels, algèbres) sont constituées

[52] On omet de préciser l'ensemble indexant lorsque le contexte est clair.

1. d'une part d'*éléments distingués* (les neutres) ;
2. d'autre part d'*opérations distinguées* (lois internes, externes, inversion) ;
3. les objets de ces deux classes étant soumis à certains *axiomes* (associativité, neutralité, distributivité...).

La philosophie est alors la suivante : un sous-truc sera une partie où ces axiomes seront vérifiés, ce qui présuppose *que chacun de ces objets distingués* (éléments[53] & opérations) *fasse sens dans la partie considérée*. Un sous-truc[54] sera alors naturellement muni d'une structure de truc.

Pour les éléments distingués, faire sens dans une partie revient à l'*appartenance* à cette partie.

Pour les opérations, faire sens reviendra à une certaine *stabilité* – voyons l'exemple des lois (de composition interne). Soit M un magma et soit A une partie de M. On dispose alors d'une application $\left\{\begin{array}{ccc} M^2 & \longrightarrow & M \\ (m,\mu) & \longmapsto & m\mu \end{array}\right.$ (la loi de M) ainsi que de sa restriction à A^2, abusivement appelée "loi induite sur A", à savoir $\left\{\begin{array}{ccc} A^2 & \longrightarrow & M \\ (a,\alpha) & \longmapsto & a\alpha \end{array}\right.$. Si on peut remplacer dans cette dernière l'ensemble but M par A, alors cette restriction sera une loi (*interne*) sur A – et réciproquement. Par conséquent :

la loi induite sur A fait sens ssi A est stable par la loi de M.

Par exemple, un sous-espace vectoriel[55] est une partie contenant le vecteur nul (élément distingué), stable par addition (loi interne), par opposition (inversion pour $+$) et par homothétie (l'action du corps de base, loi externe), les quatre axiomes – tous des énoncés universels – étant automatiquement vérifiés par restriction de ceux de l'espace vectoriel de base.

Précisons à présent cette philosophie pour les groupes et (en vue des anneaux) pour les monoïdes.

3.4.2 Sous-monoïdes

Définition – Proposition (sous-monoïde) (hors programme)

Une partie d'un monoïde en est un ***sous-monoïde*** *si :*

1. *elle contient le neutre*[56] *de ce monoïde ;*
2. *elle est stable par la loi de ce monoïde.*

Cette partie est alors un monoïde pour la loi induite par le monoïde de base.

Démonstration

Soit $(M,\cdot,1)$ un monoïde, soit S un sous-monoïde de M. Montrons que $\left(S,\cdot_{|S^2},1\right)$ est un monoïde. Avant toute chose, la loi $\cdot_{|S^2}$ fait bien sens puisque S est stable par $\cdot$ et

[53] Les neutres sont trop souvent oubliés !

[54] *sous* = sous-ensemble = partie, *truc* = truc, la terminologie est limpide

[55] *Rappel* : la stabilité par soustraction découle de celles par addition et par homothétie de rapport -1, d'où la caractérisation usuelle en terme de combinaisons linéaires.

[56] Ne pas oublier le neutre !

l'élément 1 appartient bien à S. Ensuite, spécialiser l'axiome $\forall m \in M,\ 1m = m = m1$ en chaque élément de S (on peut car S est une partie de M) montre que 1 est neutre pour S. Enfin, spécialiser l'axiome $\forall m, \mu, \mathfrak{m} \in M,\ m(\mu\mathfrak{m}) = (m\mu)\mathfrak{m}$ en trois éléments de S montre que $\cdot_{|S^2}$ est associative.

Exemples (sous-monoïdes) Abrégeons $M \Subset \mathcal{M}$ pour dire (uniquement dans ces exemples) « M est un sous-monoïde de $\mathcal{M}$ ».

1. Soit M un monoïde. La relation $\Subset$ est une relation d'ordre sur $\mathfrak{P}(M)$ admettant un minimum, le ***sous-monoïde neutre*** $\{1\}$, et un maximum[57], le ***sous-monoïde plein*** M :

$$\{\text{neutre}\} \Subset S \Subset M \qquad \text{(pour chaque sous-monoïde } S\text{)}.$$

   Les éléments réguliers forment un sous-monoïde, tout comme ceux inversibles (ainsi $M^\times \Subset M$) ou encore ceux ***centraux*** (*i. e.* qui commutent avec chaque élément de M).
2. Chez les nombres, on peut écrire $\{0\} \Subset 2\mathbb{N} \Subset \mathbb{N}$, $\sqrt{2}\mathbb{Q}_+ \Subset \mathbb{R}_+ \Subset (\mathbb{R}_+ + i\mathbb{R}_+)$ (pour $+$ mais pas pour $\times$). On peut s'amuser à compliquer : $\{0, 18, 23\} \amalg (\mathbb{N} + 36) \Subset \mathbb{N}$, $\{0\} \amalg [42, \infty] \Subset \overline{\mathbb{R}_+}$ et $\{0\} \amalg \left[2, \frac{15}{7}\right] \amalg \{3\} \amalg [4, \infty[\Subset \mathbb{R}_+$.
3. Les fonctions $\mathbb{R} \longrightarrow \mathbb{R}$ impaires constituent un sous-monoïde de $\left(\mathbb{R}^\mathbb{R}, \circ\right)$ (mais pas les paires – **pourquoi ?**).
4. Soit I un intervalle réel. Alors les fonctions $I \longrightarrow I$ croissantes forment un sous-monoïde de I^I, de même pour les monotones (mais pas pour les décroissantes). Par ailleurs, les fonctions croissantes de I vers $\mathbb{R}$ forment un monoïde additif.
5. Soit S une structure. Soit f un endomorphisme de S. Alors les itérés de f forment un sous-monoïde $\{f^{\circ n}\}_{n\in\mathbb{N}}$ de $\operatorname{End} S$.
6. Soit E un espace vectoriel réel, soit f un endomorphisme de E. Alors les polynômes en f constituent un sous-monoïde $\mathbb{R}[f]$ de $L(E)$, pour $+$ comme pour $\circ$. Par ailleurs, l'ensemble des sous-espaces vectoriels de E forment un sous-monoïde de $\mathfrak{P}(E)$ pour l'addition "parties".
7. Soient $A \subset B$ deux ensembles. On a alors $\mathfrak{P}(A) \Subset \mathfrak{P}(B)$ pour $\cup$ comme pour Δ mais pas (sauf cas trivial) pour $\cap$ (**pourquoi ?**). Prolongeons par ailleurs à chaque B les applications de source A en fixant chaque point de $B \setminus A$: on peut alors écrire $A^A \Subset B^B$ (pour $\circ$).
8. Soient $a \leq b$ deux naturels. Alors $\mathbb{Q}_a[X] \Subset \mathbb{Q}_b[X]$ pour l'addition. De même, en complètant les matrices de taille $a \times a$ en rajoutant[58] des 1 sur la diagonale de longueur $b - a$, on obtient $M_a(\mathbb{C}) \Subset M_b(\mathbb{C})$ pour $+$ et pour $\times$.
9. Soient M un monoïde et I un ensemble. Alors la partie $M^{(I)}$ du monoïde puissance M^I formée des familles ***presque nulles*** (*i. e.* prenant une valeur neutre en dehors d'un ensemble fini) en forment un sous-monoïde. En particulier, si $\mathbb{P}$ dénote l'ensemble des nombres premiers, on a une bijection $\left\{ \begin{array}{ccc} \mathbb{N}^{(\mathbb{P})} & \xrightarrow{\sim} & \mathbb{N}^* \\ (v_p) & \longmapsto & \prod_{p\in\mathbb{P}} p^{v_p} \end{array} \right.$ entre monoïdes qui préserve le produit et le neutre[59].

[57] Certains auteurs appellent ces *extrema* les sous-monoïdes ***triviaux*** mais tous ne sont pas d'accord pour nommer ainsi le monoïde plein. Un peu de souplesse est donc de rigueur quand on parle de sous-truc *trivial*.

[58] Cela revient comme au paragraphe précédent à prolonger à l'aide de l'identité.

[59] On parlera d'un ***isomorphisme*** de monoïdes (*cf.* § 4.2).

Remarque – **Sous-monoïdes et loi "parties".** L'utilisation de la loi "parties" permet une reformulation économe :

chaque partie S d'un monoïde en
est un sous-monoïde ssi $1 \in S \supset SS$
(version additive : ssi $0 \in S \supset S + S$*).*

Remarque – **Faux sous-monoïdes.** Une partie *peut être un monoïde* pour une autre opération (avec le même neutre) ou pour un autre neutre (avec la même loi) *sans pour autant être un sous-monoïde.*

Par exemple, la partie $\mathbb{R}_+ \times \{0, 18\}$ du monoïde additif $\mathbb{R}_+^2$ est un monoïde pour l'addition réelle sur la première coordonnée et la loi constante nulle sur la seconde, ce monoïde contient le neutre $(0, 0)$ du groupe $\mathbb{R}_+^2$ mais ne peut en être un sous-monoïde car n'est pas stable par l'addition de ce dernier (le double de $(0, 18)$ sort de $\mathbb{R} \times \{0, 18\}$).

De même, la partie $\mathbb{R} \times \{0\}$ du monoïde $\mathbb{R}^2$ muni de la multiplication sur chaque coordonnée est un monoïde pour la loi induite (de neutre $(1, 0)$) mais n'est pas un sous-monoïde de $\mathbb{R}^2$ car ne contient pas son neutre $(1, 1)$. Autre contre-exemple : étant donné un idempotent $i \neq 1$, la partie $\{i\}$ du monoïde $\{1, i\}$ est un monoïde pour la même loi mais ne possède pas le même neutre. Enfin, pour chaque naturel $n > 0$, l'ensemble $\mathbb{Z}/n$ est une partie du monoïde $\mathfrak{P}(\mathbb{Z})$ qui est un monoïde pour loi induite mais pas pour le même neutre ($n\mathbb{Z}$ contre $\{0\}$).

3.4.3 Sous-groupes

Proposition – Définition (sous-groupe)

Soit G un groupe. Une partie de G est un groupe pour la loi induite par celle de G ssi :

1. *elle contient*[60] *le neutre de G ;*
2. *elle est stable par la loi de G ;*
3. *elle est stable par l'inversion de G.*

Cette partie est alors appelée un ***sous-groupe***[61] *de G.*

Démonstration

Soit A une partie de G.

$\boxed{\Longrightarrow}$ Supposons que A est un groupe pour la loi induite par celle de G. La partie A contient un neutre $\mathtt{1}$: en composant l'égalité $\mathtt{1} \circ \mathtt{1} = \mathtt{1}$ par l'inverse $\mathtt{1}^{-1}$ (dans G), on obtient $\mathtt{1} = 1_G$, ce qui montre[62] la condition 1. La condition 2 signifie précisément que la loi induite est bien définie (*i. e.* est à valeurs dans A). Soit enfin $a \in A$: il admet un inverse a' dans A, ce qui s'écrit $aa' = \mathtt{1} = a'a$, *i. e.* $aa' = 1 = a'a$, d'où les égalité et appartenance $a^{-1} = a' \in A$ et la condition 3.

[60] Ne pas oublier le neutre !

[61] Un sous-groupe est en particulier un sous-monoïde.

[62] Notre démonstration du $\boxed{\Longrightarrow}$ semble ne pas conclure dans les monoïdes sans pouvoir inverser le neutre, d'où la recherche précédente de "faux sous-monoïdes" où le neutre fait défaut.

$\boxed{\Longleftarrow}$ Supposons les trois conditions de l'énoncé. La condition 2 énonce que la loi induite fait sens. L'associativité portant sur chaque élément de G^3, elle est en particulier valide pour ceux de A^3. La condition 1 fournit un neutre pour A. Enfin, chaque élément de A est inversible dans G et la condition 3 nous dit que son inverse reste dans A.

En pratique, on utilise surtout le sens $\boxed{\Longleftarrow}$ afin d'éviter à avoir à vérifier certains axiomes pénibles comme l'associativité.

Exemples (sous-groupes) On note encore $G \Subset \mathcal{G}$ pour dire (et uniquement dans ces exemples) « G est un sous-groupe de $\mathcal{G}$ ».

1. Soit G un groupe. La relation $\Subset$ est une relation d'ordre sur $\mathfrak{P}(G)$ admettant un minimum, le ***sous-groupe neutre*** $\{1\}$, et un maximum, le ***sous-groupe plein*** G :

$$\{\text{neutre}\} \Subset S \Subset G \qquad (\text{pour chaque sous-groupe } S).$$

   Est un sous-groupe de G son ***centre*** $Z(G)$ formé des éléments commutant avec chaque élément de G.
2. Les polynômes réels composent un sous-groupe additif $\mathbb{R}[X]$ de $\mathbb{R}^{\mathbb{N}}$. Plus généralement, étant donnée une famille (G_i) de groupes, les familles du groupe produit $\prod G_i$ presque nulles (*i. e.* prenant une valeur neutre en dehors d'un ensemble fini) en forment un sous-groupe (strict ssi l'ensemble indexant est infini).
3. Avant de reprendre les groupes du cours, signalons que chaque sous-espace vectoriel d'un espace vectoriel donné en est un sous-groupe additif.
4. Parmi les groupes numériques additifs, on peut écrire :

$$\{0\} \Subset \mathbb{Z} \Subset \mathbb{Q} \Subset \mathbb{R} \Subset \mathbb{C} \Subset \mathbb{H} \qquad \text{et même intercaler}$$
$$7\mathbb{Z} \Subset \mathbb{Z} \Subset \mathbb{Z}\left[\frac{1}{8}\right] \Subset \mathbb{Q} \Subset \mathbb{Q}\left[\sqrt{5}\right] \Subset \mathbb{R} \Subset \mathbb{R}\left[e^{\frac{2\pi i}{3}}\right] \Subset \mathbb{C}.$$

5. Parmi les multiplicatifs[63] :

$$\begin{aligned} \{\pm 1\} &= \mathbb{U}_2 \Subset \mathbb{Q}^* \Subset \mathbb{R}^* \Subset \mathbb{C}^* \Subset \mathbb{H}^*; \\ \mathbb{U}_n &\Subset \bigcup_{k\in\mathbb{N}^*} \mathbb{U}_k \Subset \mathbb{U} \Subset \mathbb{C}^*; \\ \{\pm 1, \pm i\} &= \mathbb{U}_4 \Subset \mathbb{H}_8 \Subset \mathbb{H}^*. \end{aligned}$$

6. Parmi les géométriques : tous ceux cités (les infinis comme les diédraux) sont des sous-groupes du groupe des isométries (affines) du plan, lui-même sous-groupe du groupe des permutations du plan.
7. En version complexe, on dirait que (toujours pour la composition) les groupes $\mathrm{Id}+\mathbb{C}$, $\mathbb{U}\,\mathrm{Id}$, $\mathbb{R}\,\mathrm{Id}$, $\mathbb{C}\,\mathrm{Id}$, $\mathbb{U}\,\mathrm{Id}+\mathbb{C}$ et $\mathbb{R}\,\mathrm{Id}+\mathbb{C}$ sont des sous-groupes de $(\mathbb{C}\,\mathrm{Id}+\mathbb{C}) \cup \left(\mathbb{C}\overline{\mathrm{Id}}+\mathbb{C}\right)$, lui-même sous-groupe de $\mathfrak{S}(\mathbb{C})$ (**exercice** : mettre tous ces sous-groupes sur un même schéma en précisant toutes les relations $\Subset$).

[63] L'exemple de $\bigcup_{k\in\mathbb{N}^*} \mathbb{U}_k$ ne doit pas laisser penser qu'une réunion de sous-groupes est toujours un sous-groupe. En effet, pour la réunion de *deux* sous-groupes, ce n'est jamais le cas (sauf situation triviale : *cf.* exercice d'application 2).

8. De chaque groupe symétrique $\mathfrak{S}_n$ le groupe alterné $\mathfrak{A}_n$ est un sous-groupe (strict si $n \geq 2$).
9. On peut également adapter les exemples de sous-monoïdes précédents :
$$\begin{array}{rcl} 7\mathbb{Z} & \Subset & \mathbb{Z}, \quad \mathbb{Q}\pi \Subset \mathbb{R}, \\ \mathfrak{S}_A & \Subset & \mathfrak{S}_B \text{ (si } A \subset B), \\ GL_a(\mathbb{C}) & \Subset & GL_b(\mathbb{C}) \text{ (si } a \leq b), \\ \{f^{\circ z}\}_{z\in\mathbb{Z}} & \Subset & \operatorname{Aut} S \text{ (si } f \in \operatorname{Aut} S). \end{array}$$
10. Soit I un intervalle réel : alors les homéomorphismes $I \longrightarrow I$ forment un sous-groupe de $\mathfrak{S}_I$, duquel les homéomorphismes croissants constituent un sous-groupe (mais pas les décroissants).

REMARQUE – **Faux sous-groupes.** Une partie *peut être un groupe* pour une autre opération (avec le même neutre) *sans pour autant être un sous-groupe.*

Par exemple, la partie $\mathbb{R}\times\{0,42\}$ du groupe additif $\mathbb{C}$ est un groupe pour l'addition réelle sur la première coordonnée et la loi constante nulle sur la seconde, ce groupe contient le neutre $(0,0)$ du groupe $\mathbb{C}$ mais ne peut en être un sous-groupe car n'est pas stable par l'addition de ce dernier (le double de $(0,42)$ sort de $\mathbb{R}\times\{0,42\}$).

REMARQUE – **Sous-groupes et loi "parties".** L'utilisation de la loi "parties" permet une reformulation économe :
$$\begin{array}{c} \textit{chaque partie } S \textit{ d'un groupe en} \\ \textit{est un sous-groupe } \textit{ssi}^{64} \left\{ \begin{array}{l} 1 \in S \supset SS \\ S^{-1} \subset S \end{array} \right. \\ \textit{(version additive : ssi } \left\{ \begin{array}{l} 0 \in S \supset S+S \\ -S \subset S \end{array} \right. . \end{array}$$

Proposition (théorème de Lagrange) (hors programme)

Dans chaque groupe fini, l'ordre de chaque sous-groupe divise celui du groupe plein.

Démonstration

Soit G un groupe, soit S un sous-groupe de G. Soit $g \in G$. La translation à gauche par g induit une bijection $S \xrightarrow{\sim} gS$, ce qui montre que les classes *modulo* S sont équipotentes. Par ailleurs, l'appartenance $g = g1 \in gS$ montre que ces classes recouvrent G et les implications (à $\gamma \in G$ et $s, \sigma \in S$ fixés)
$$gs = \gamma\sigma \Longrightarrow \left\{ \begin{array}{l} g = \gamma\sigma s^{-1} \in \gamma S \\ \gamma = \gamma s\sigma^{-1} \in gS \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} gS \subset \gamma SS = \gamma S \\ \gamma S \subset gSS = gS \end{array} \right. \Longrightarrow gS = \gamma S$$
que ce recouvrement est une *partition* (remarquer que l'on a utilisé toute l'hypothèse $1 \in S = S^{-1} = SS$). En notant $\mathcal{Q}$ l'ensemble (quotient) de ces classes, on peut alors conclure quand G est fini[65] :
$$|G| = \left| \biguplus_{C\in\mathcal{Q}} C \right| = \sum_{C\in\mathcal{Q}} |C| = \sum_{C\in\mathcal{Q}} |S| = |\mathcal{Q}|\ |S| .$$

[64] On peut même remplacer les inclusions $\subset$ par des égalités $=$ d'après l'exercice d'application § 3.1).

[65] La notation $\uplus$ pour l'union disjointe rappelle l'aspect *additif* du langage vernaculaire (« Dans mon sac, j'ai une pomme *plus* un portefeuille *plus* un livre, *plus*...») et ainsi que le cardinal de chaque union disjointe vaut la *somme* des cardinaux des réunis.

Exercices d'application

1. *Soit A une partie d'un monoïde (resp. groupe). Montrer qu'est un sous-monoïde (resp. sous-groupe) le* ***commutant*** *de A,* i. e. *l'ensemble des éléments qui commutent avec chaque élément de A.*
2. *Montrer que la réunion de deux sous-groupes (d'un même groupe) demeure un sous-groupe ssi l'un est l'inclus dans l'autre. Que dire si l'on remplace "deux" par un entier plus grand ?*

---

1. Abrégeons C le commutant de A. Soit $a \in A$. Puisque $1a = a = a1$, on a l'appartenance $1 \in C$. Soient $c, c' \in C$: leur composé reste alors dans C vu les égalités

$$a\,(cc') = (ac)\,c' \overset{c\in C}{=} (ca)\,c' = c\,(ac') \overset{c'\in C}{=} c\,(c'a) = (cc')\,a.$$

   Lorsque le monoïde de contexte est un groupe, l'énoncé $ac^{-1} = c^{-1}a$ fait sens et équivaut (translater par c des deux côtés) à $ca = ac$, ce qu'on a puisque $(a, c) \in A \times C$, d'où l'on conclut $c^{-1} \in C$.

   Remarque – Quand A vaut tout le monoïde (resp. groupe), son commutant est le centre de ce dernier et l'on retrouve le fait que les éléments centraux forment un sous-monoïde (resp. -groupe).

2. Soient G et H deux sous-groupes. Le sens $\boxed{\Longleftarrow}$ est immédiat vu qu'alors la réunion $G \cup H$ se réduit à G ou H. Supposons donc $G \cup H$ sous-groupe. Supposons que G n'est pas inclus dans H et soit $g \in G \setminus H$; montrons alors $H \subset G$. Soit $h \in H$. Le composé gh reste dans $G \cup H$: s'il tombe dans H, alors $g \in Hh^{-1} \subset H$, ce qu'on n'a pas ; il tombe donc dans G, d'où $h \in g^{-1}G \subset G$, ce qui conclut.

   Dans le plan $\mathbb{F}_2^2$, les trois droites engendrées par resp. $\binom{1}{0}$, $\binom{0}{1}$ et $\binom{1}{1}$ sont des sous-espaces vectoriels, donc des sous-groupes additifs. Leur réunion vaut le plan tout entier, lequel est un sous-espace vectoriel, *a fortiori* un sous-groupe. On pourrait généraliser en changeant de corps de base (fini) ou en modifiant la dimension (finie).

   Remarque – Pour une réunion infinie, nous avons déjà signalé le contre-exemple $\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ (exemple 5 ci-dessus). Sa version "plate" (et additive) serait la réunion $\bigcup_{n\in\mathbb{N}^*} \mathbb{Z}\left[\frac{1}{n}\right] = \mathbb{Q}$.

3.4.4 Sous-groupes de $\mathbb{Z}$ et de $\mathbb{R}$, périodes

Proposition (sous-groupes de $\mathbb{Z}$)

Chaque sous-groupe additif de $\mathbb{Z}$ est monogène[66]*,* i. e. *de la forme $a\mathbb{Z}$ pour un certain naturel a.*

[66] *mono* = un, *gène* = générateur, donc *monogène* = engendré par un élément

Démonstration

Soit G un sous-groupe additif de $\mathbb{Z}$.

FIG 12 : un sous-groupe[67] $n\mathbb{Z}$

Si G est nul, il s'écrit $0\mathbb{Z}$ et on a fini. On supposera donc G non nul. Soit $g \neq 0$ dedans : quitte à l'opposer, on peut imposer $g > 0$. La partie $G' := G \cap \mathbb{N}^*$ est alors non vide et il fait sens de définir

$$m := \min G'.$$

Montrons l'égalité $G = m\mathbb{Z}$. L'inclusion $\supset$ est immédiate puisque les itérés de m restent dans G. Soit réciproquement $g \in G$. Une division euclidienne de g par m (on peut car $m \neq 0$) donne $g = qm + r$ où $\begin{cases} q \in \mathbb{Z} \\ r \in [|0, m[\end{cases}$. Le reste $r \in \mathbb{N}$ tombe alors hors de G' (puisque $r < \inf G'$) mais reste dans G (puisque $r = g - qm$ où $\begin{cases} g, m \in G \\ q \in \mathbb{Z} \end{cases}$), donc appartient à $(\mathbb{N} \cap G) \setminus G' = \{0\}$, d'où l'appartenance $g = qi \in \mathbb{Z}i$.

Ces sous-groupes, dits ***discrets*** (car chaque élément est "isolé" des autres), se généralisent à $\mathbb{R}$ (les multiples entiers d'un même réel forment un sous-groupe). Mais nous connaissons d'autres sous-groupes non discrets – l'ensemble des rationnels, qui sont denses. En un certain sens (la proposition suivante), on a décrit chaque sous-groupe additif de $\mathbb{R}$.

Proposition (sous-groupes additifs de $\mathbb{R}$) (hors programme)

Soit G un sous-groupe (additif) de $\mathbb{R}$. Alors :

1. *ou bien G est de la forme $g\mathbb{Z}$ pour un certain réel $g \geq 0$;*
2. *ou bien G est dense dans $\mathbb{R}$.*

Démonstration

On suit la même démonstration[68] que pour $\mathbb{Z}$. Notons $G' := G \cap \mathbb{R}_+^*$. Si G est nul, on est dans le premier cas avec $g = 0$. On supposera désormais G non nul. Soit $a \neq 0$ dedans. Quitte à l'opposer, on peut imposer $a > 0$, d'où la non-vacuité de G' ; le réel $i := \inf G'$ fait alors sens.

Supposons $i = 0$. Soient $g < h$ dans G. La différence $h - g$ est alors dans G'. Par définition d'un *infimum*, il y a un $\varepsilon \in G'$ tel que $i \leq \varepsilon < h - g$: l'un des itérés de ε tombe alors dans $]g, h[$ (par exemple[69] le $\left(\left\lfloor \frac{g}{\varepsilon} \right\rfloor + 1\right)$-ième), *c. q. f. d.*

FIG 13

[67] Micro-analyse : si G est de la forme cherchée, disons $G = n\mathbb{Z}$, alors n est le plus petit élément strictement positif de G (à moins que G soit nul). Fin de la micro-analyse.

[68] La démonstration va bloquer quand on va essayer de diviser g par i : non pas que la division euclidienne n'ait pas d'analogue dans $\mathbb{R}$ mais diviser par 0 reste impossible, ce qui nous forcer à envisager le cas $i = 0$. Par ailleurs, dans le cas $i > 0$, il faudra montrer en outre que l'*infimum* est un *minimum*.

[69] On a d'une part $\left(\left\lfloor \frac{g}{\varepsilon} \right\rfloor + 1\right)\varepsilon > \frac{g}{\varepsilon}\varepsilon = g$, d'autre part $\left(\left\lfloor \frac{g}{\varepsilon} \right\rfloor + 1\right)\varepsilon \leq \left(\frac{g}{\varepsilon} + 1\right)\varepsilon = g + \varepsilon < h$.

Supposons $i > 0$. Montrons $i \in G$ puis $G = i\mathbb{Z}$.

Supposons par l'absurde $i \notin G$. Par définition de i, il y a[70] des $g, h \in G'$ tels que $i < g < h < 2i$: alors la différence $h - g$ reste dans G' (comme différence positive d'éléments de G) mais est $< i$ (vu la comparaison $h - g < 2i - g$ et l'équivalence $2i - g < i \iff g < i$), ce qui est absurde.

De l'appartenance $i \in G$ on déduit par itération l'inclusion $\mathbb{Z}i \subset G$.

Soit enfin $g \in G$. Effectuons une division euclidienne $g = qi + r$ où $\begin{cases} q \in \mathbb{Z} \\ r \in [0, i[\end{cases}$. Le reste tombe alors dans $\mathbb{R}_+$ (puisque $r \geq 0$) et dans G (puisque $r = g - qi$ où $\begin{cases} g, i \in G \\ q \in \mathbb{Z} \end{cases}$) mais hors de G' (puisque $r < \inf G'$), donc appartient à $(\mathbb{R}_+ \cap G) \setminus G' = \{0\}$, d'où l'appartenance $g = qi \in \mathbb{Z}i$.

Définition – Proposition (périodes)

*Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$. Une **période**[71] de f est un réel T tel que $f(\mathrm{Id} + T) = f$,* i. e. *tel que*

$$\forall t \in \mathbb{R},\ f(t + T) = f(t).$$

Les périodes de f forment un sous-groupe de $\mathbb{R}$.
*Lorsqu'il est discret, **la période** de f est la plus petite période strictement positive.*
Dans le cas dense, f est constante si on l'impose de plus continue.

Démonstration

Puisque $f \circ (\mathrm{Id} + 0) = f \circ \mathrm{Id} = f$, le réel 0 est une période de f. On a par ailleurs pour chaques périodes T et U de f les égalités

$$f \circ (\mathrm{Id} - T) \overset{\substack{T \text{ est une} \\ \text{période de } f}}{=} [f \circ (\mathrm{Id} + T)] \circ (\mathrm{Id} - T) = f \circ \underbrace{[(\mathrm{Id} + T) \circ (\mathrm{Id} - T)]}_{=(\mathrm{Id}-T)+T=\mathrm{Id}} = f \text{ et}$$

$$f \circ (\mathrm{Id} + (T + U)) = f \circ (\mathrm{Id} + T) \circ (\mathrm{Id} + U) \overset{\substack{T \text{ est une} \\ \text{période de } f}}{=} f \circ (\mathrm{Id} + U) \overset{\substack{U \text{ est une} \\ \text{période de } f}}{=} f.$$

Imposons que f soit continue et ait un groupe de périodes dense. Soit a un réel, soit $\varepsilon > 0$, soit par continuité $\delta > 0$ tel que $|t| < \delta \implies |f(t) - f(0)| < \varepsilon$, soit par densité $T \in]0, \delta[$ une période de f et soit $z \in \mathbb{Z}$ tel que $|a + zT| < \delta$. On a alors $|f(a + zT) - f(0)| < \varepsilon$, *i. e.* $|f(a) - f(0)| < \varepsilon$. Ceci tenant pour chaque $\varepsilon > 0$, ce dernier module est nul, d'où l'égalité $f(a) = f(0)$ et la constance de f.

Exercice d'application

a. *Soient a et b deux réels non nuls. Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe et qu'il est dense ssi $\frac{a}{b}$ est irrationnel.*

b. *Soient f et g deux fonctions $\mathbb{R} \longrightarrow \mathbb{C}$ continues périodiques. Notons a et b leurs périodes respectives. Donner une CNS simple sur a et b pour que $f + g$ soit périodique.*

[70] Insérer d'abord un h entre i et $2i$, puis un g entre i et h.
[71] L'application f est dite ***périodique*** si elle admet une période non nulle.

a. La somme $a\mathbb{Z} + b\mathbb{Z}$ contient le neutre $0 = a0 + b0$ et on a déjà vu (*cf.* calculs § 3.1) qu'elle était stable par addition et par opposition.

Supposons $a\mathbb{Z}+b\mathbb{Z}$ discret, mettons $= c\mathbb{Z}$ pour un réel c. Alors $a \in a\mathbb{Z}+b\mathbb{Z} = c\mathbb{Z}$, d'où ($a$ étant par ailleurs non nul) un $k \in \mathbb{Z}^*$ teℓ que $a = ck$; on dispose de même d'un $\ell \in \mathbb{Z}^*$ teℓ que $b = c\ell$. On en déduit $\frac{a}{b} = \frac{ck}{c\ell} = \frac{k}{\ell} \in \mathbb{Q}$.

Supposons $\frac{a}{b}$ rationnel, mettons $= \frac{k}{\ell}$ avec $k, \ell \in \mathbb{Z}$. On a alors les inclusions

$$a\mathbb{Z} + b\mathbb{Z} = \frac{kb}{\ell}\mathbb{Z} + \frac{b\ell}{\ell}\mathbb{Z} \subset \frac{b}{\ell}\left(k\mathbb{Z} + \ell\mathbb{Z}\right) \subset \frac{b}{\ell}\mathbb{Z},$$

ce qui montre que $a\mathbb{Z}+b\mathbb{Z}$ est inclus dans un sous-groupe discret, donc ne saurait être dense, donc est discret.

Remarque – Il n'est pas toujours vrai que le composé de deux sous-groupes reste un sous-groupe, *cf.* tome de première année pour une caractérisation.

b. Regardons les cas simples : si b est un multiple de a, il est clair que $f + g$ sera b-périodique. Plus généralement, dans le cas où $\frac{a}{b} \in \mathbb{Q}$, mettons $\frac{a}{b} = \frac{p}{q}$ avec $p, q \in \mathbb{Z}$, alors le réel $aq = bp$ est clairement une période de $f+g$. Montrons que la condition $\frac{a}{b} \in \mathbb{Q}$ est nécessaire.

Supposons $f + g$ périodique et notons c sa période. On a donc $f\left(\mathrm{Id} + c\right) + g\left(\mathrm{Id} + c\right) = f + g$, ce qui se réécrit mieux en séparant f et g :

$$f\left(\mathrm{Id} + c\right) - f = g - g\left(\mathrm{Id} + c\right) \ ;$$

notons δ cette fonction commune. En regardant le membre de gauche, on voit que δ est a-périodique et elle est également b-périodique d'après l'expression de droite, ce qui montre que tout réel de $a\mathbb{Z} + b\mathbb{Z}$ est période de δ. Or, supposant par l'absurde $\frac{a}{b} \notin \mathbb{Q}$, la partie $a\mathbb{Z} + b\mathbb{Z}$ est dense dans $\mathbb{R}$, donc la fonction δ est ε-périodique pour chaque $\varepsilon > 0$; étant plus continue, δ est constante. Une récurrence immédiate montre alors les égalités

$$\forall n \in \mathbb{N},\ f\left(nc\right) = f\left(0\right) + n\delta$$

et le caractère borné de f (continue périodique) force la nullité de δ. Revenant à la définition de δ, on voit que la période c est une période commune à f et g, donc doit être dans $a\mathbb{N}^* \cap b\mathbb{N}^*$; mais ce dernier est vide puisque $\frac{a}{b} \notin \mathbb{Q}$, d'où la contradiction voulue.

3.5 Intersection, structures engendrées

Dorénavant, le mot « truc » désignera
au choix « groupe » ou « monoïde ».

Proposition (intersection de sous-trucs)

Soit une structure de type truc. Alors la classe de ses sous-trucs est stable par intersection quelconque (non nécessairement finie).

Démonstration

La même que pour une intersection de sous-espaces vectoriels. Le cas monoïdal va découler du cas pour les groupes. Soient donc G un groupe, I un ensemble et (G_i) une famille de sous-groupes de G indexée par I. Le neutre appartenant à chaque sous-groupe, il appartient à chaque G_i, donc à leur intersection. Soient par ailleurs a, b dans cette dernière. Soit $i \in I$: puisque G_i contient a et b et est stable par composition et inversion, le composé ab et l'inverse a^{-1} tombent dedans.

Remarque – Cette propriété est fausse si l'on remplace « intersection » par « réunion », par exemple pour les espaces vectoriels où réunir deux droites distinctes n'a jamais donné de sous-espace vectoriel (pour les groupes, *cf.* exercice 2 § 3.4.3).

Comme pour les sous-espaces vectoriels, cette propriété permet de décrire de façon *externe* le sous-truc engendré par une partie, en partant du grand truc (l'"extérieur" de la partie) et en rétrécissant petit à petit.

Proposition – Définition (sous-truc engendré : description externe)

Soit A une partie d'une structure de type truc. Le ***sous-truc engendré*** *par A est le plus petit*[72] *sous-truc contenant A, à savoir*[73]

$$\langle A \rangle := \bigcap_{S \supset A}^{S \text{ sous-truc}} A.$$

On a d'une part les inclusion et égalité

$$A \subset \langle A \rangle = \langle \langle A \rangle \rangle \text{ , avec égalité } A = \langle A \rangle \text{ ssi } A \text{ est un sous-truc,}$$

d'autre part pour chaque partie B l'implication

$$A \subset B \Longrightarrow \langle A \rangle \subset \langle B \rangle, \text{ avec équivalence si } B \text{ est un sous-truc.}$$

Démonstration[74]

La partie $\langle A \rangle$ ci-dessus fait déjà sens car l'intersection est non vide (le truc dont A est une partie est un sous-truc contenant A) ; elle est un sous-truc d'après la proposition précédente ; puisque chaque intersecté contient A, leur intersection aussi. Ainsi $\langle A \rangle$ est-il un sous-truc contenant A. Soit par ailleurs S un sous-truc contenant A : il apparaît dans l'intersection ci-dessus, donc contient cette dernière. Finalement, $\langle A \rangle$ est bien le plus petit sous-truc contenant A.

A étant la plus petite partie contenant A, il suffit qu'elle soit un sous-truc pour valoir le plus petit sous-truc contenant A ; puisque $\langle A \rangle$ est un sous-truc, d'une part

[72] plus petit au sens de l'*inclusion* $\subset$

[73] Les symboles $\langle . \rangle$ s'appellent des *chevrons* (en anglais : *pointed brackets*).

[74] Aviez-vous pensé à vérifier que les symboles écrits faisaient sens ?

on obtient l'égalité $\langle\langle A\rangle\rangle = \langle A\rangle$, d'autre part l'égalité $A = \langle A\rangle$ implique que A soit un sous-truc.

Supposons $A \subset B$. L'engendré $\langle B\rangle$ est un sous-truc, il contient B, *a fortiori* A, donc est un sous-truc contenant A, donc contient $\langle A\rangle$, *c. q. f. d.* Si de plus B est un sous-truc, le conséquent $\langle A\rangle \subset \langle B\rangle$ devient $\langle A\rangle \subset B$, ce qui avec l'inclusion $A \subset \langle A\rangle$ implique $A \subset B$.

Remarques

- Demander si une partie donnée est un sous-truc cache une question plus fine, à savoir *quel est le truc qu'elle engendre*.
- Le cas d'équivalence s'utilise en pratique sous la forme

chaque sous-truc en contient un autre
dès qu'il en contient une partie génératrice.

Comme pour les sous-espaces vectoriels, on a une description *interne* de l'engendré : *rajouter ce qu'il manque*. Pour les monoïdes, on rajoutera les composés[75] d'éléments de A, pour les groupes on rajoutera en outre dans les composés les *inverses* d'éléments de A.

Proposition (sous-truc engendré : description interne)

Soit A une partie d'un monoïde, resp. d'un groupe. On a alors l'égalité

$$\langle A\rangle = \left\{ \prod_{i=1}^{n} a_i \ ; \quad \begin{array}{c} n \in \mathbb{N} \\ a \in A^n \end{array} \right\}, \qquad \textit{resp.} \qquad \langle A\rangle = \left\{ \prod_{i=1}^{n} a_i^{\varepsilon_i} \ ; \quad \begin{array}{c} n \in \mathbb{N} \\ a \in A^n \\ \varepsilon \in \{\pm 1\}^n \end{array} \right\}.$$

Démonstration

Démontrons formellement (et uniquement à but technique) le cas monoïdal, qui *doit* paraître immédiat au niveau du sens. Le cas des groupes est analogue (reste seulement à tenir compte de l'inversion) et laissé à la lectrice.

Soit M un sous-monoïde contenant A. Étant stable par composition, M contient (par une récurrence immédiate) les composés $\prod_{i=1}^{n} a_i$ pour n parcourant $\mathbb{N}^*$ (et a décrivant A^n) ; contenant le neutre, composé de la famille vide, M contient le composé $\prod_{i=1}^{0} a_i$. Finalement, M contient tout $\langle A\rangle$.

Il reste à montrer que $\langle A\rangle$ est un sous-monoïde contenant A. La famille vide (prendre $n = 0$) a pour composé le neutre, ce qui montre $1 \in \langle A\rangle$. Pour chaque $a \in A$, la famille à un élément $1 \mapsto a$ a pour composé a, ce qui montre que $\langle A\rangle$ contient A. Soient enfin $x, \xi \in \langle A\rangle$. Soient $n, \nu \in \mathbb{N}$ et $(a, \alpha) \in A^n \times A^\nu$ tels que $x = \prod_{i=1}^{n} a_i$ et $\xi = \prod_{i=1}^{\nu} \alpha_i$. Alors la famille $\left\{ \begin{array}{c} [|1,n|] \ni i \mapsto a_i \\ ]|n,n+\nu|] \ni \iota \mapsto \alpha_{\iota-n} \end{array} \right.$ de $A^{n+\nu}$ a pour composé $\prod_{i=1}^{n} a_i \prod_{\iota=n+1}^{n+\nu} \alpha_{\iota-n} = x\xi$, ce qui montre que $\langle A\rangle$ est stable par composition.

Exemples (sous-trucs engendrés) Lorsque la partie génératrice est décrite en extension, on retirera volontiers les accolades.

[75] Sans oublier le composé vide – le neutre !

1. Les monoïdes monogènes sont de la forme
$$\langle m\rangle = \begin{array}{l}\{1, m, m^2, m^3, ...\} = \{m^n\}_{n\in\mathbb{N}} \\ \{0, m, 2m, 3m, ...\} = \mathbb{N}m \text{ (additif)}\end{array}.$$
2. Les groupes monogènes sont de la forme
$$\langle g\rangle = \begin{array}{l}\{..., g^{-2}, g^{-1}, 1, g, g^2, ...\} = \{g^z\}_{z\in\mathbb{Z}} \\ \{..., -2g, -g, 0, g, 2g, ...\} = \mathbb{Z}g \text{ (additif)}\end{array}.$$
3. Chaque groupe G est réunion de ses sous-groupes monogènes :
$$G = \bigcup_{g\in G} \langle g\rangle\,.$$
4. Dans un groupe *abélien*[76] (additif), chaque partie finie $\{g_1, g_2, ..., g_n\}$ engendre un sous-groupe
$$\langle g_1, g_2, ..., g_n\rangle = \mathbb{Z}g_1 + \mathbb{Z}g_2 + \cdots + \mathbb{Z}g_n.$$
5. Dans le monoïde $\mathbb{N}$, on a les égalités $\langle 1\rangle = \mathbb{N}$, $\langle 0\rangle = \{0\}$, $\langle 2\rangle = 2\mathbb{N}$, $\langle 15\rangle = 15\mathbb{N}$ et $\langle 2, 5\rangle = \mathbb{N}\setminus\{1, 3\}$.
6. Dans le groupe $\mathbb{Z}$, on a $\langle 2, 3\rangle = 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ et $\langle 15, 35\rangle = 15\mathbb{Z} + 35\mathbb{Z} = 5\mathbb{Z}$.
7. Dans le groupe $\mathbb{Q}$, on a $\left\langle \frac{1}{10^n}\right\rangle_{n\in\mathbb{N}} = \mathbb{Z}\left[\frac{1}{10}\right]$ (nombres décimaux) et $\left\langle \frac{1}{d}\ ;\ d\in\mathbb{N}^*\right\rangle = \mathbb{Q}$.
8. Dans le groupe $\mathbb{H}_8$, on a $\langle -1\rangle = \mathbb{U}_2$, $\langle i\rangle = \mathbb{U}_4$ et $\langle i, j\rangle = \langle j, k\rangle = \langle i, k\rangle = \langle i, j, k\rangle = \mathbb{H}_8$.
9. Soient a, b dans un espace vectoriel réel. En voyant ce dernier comme un monoïde additif, resp. un groupe additif, resp. un espace vectoriel, on obtiendra $\langle a, b\rangle = \mathbb{N}a + \mathbb{N}b$, resp. $\langle a, b\rangle = \mathbb{Z}a + \mathbb{Z}b$, resp. $\langle a, b\rangle = \mathbb{R}a + \mathbb{R}b$.
10. Chaque groupe symétrique *fini* est engendré resp. par ses transpositions, par une transposition et un cycle de longueur maximale.
11. En dimension finie, chaque groupe linéaire est engendré par ses transvections et ses dilatations.
12. Les isométries planes sont engendrées par les réflexions[77] au sens où
$$\langle\text{réflexions}\rangle = \langle\text{rotations, translations, réflexions}\rangle = \{\text{isométries}\}\,.$$
13. Levons une éventuelle peur : *qu'engendre la partie vide ?* Si la question n'a pas déjà été tranchée pour les espaces vectoriels, observer ou bien dans la description externe que le plus petit sous-truc {neutre} contient $\emptyset$, ou bien dans la description interne que chaque élément de $\langle\emptyset\rangle$ est un composé vide, à savoir le neutre. Par conséquent[78],
$$\textit{la partie vide engendre la sous-structure neutre} : \langle\emptyset\rangle = \{\text{neutre}\}\,.$$

[76] Sans commutativité, tout se complique très vite, même avec seulement deux générateurs (penser simplement à deux réflexions planes).

[77] *Rappel* : la composée de deux réflexions est une rotation (si les axes sont sécants) ou une translation (si les axes sont parallèles).

[78] Cela est valable pour les structures de monoïdes, groupes et espaces vectoriels mais ne saurait l'être pour celles *possédant au moins deux éléments distingués*, le sous-truc $\langle\emptyset\rangle$ devant contenir ces derniers. *À préciser* donc *pour les anneaux, corps et algèbres.*

Proposition (générateurs de $\mathbb{Z}/n$)

Soient $n \in \mathbb{N}$ et $z \in \mathbb{Z}$. Alors $\overline{z}$ engendre $\mathbb{Z}/n$ ssi z et n sont étrangers.

Démonstration

Le z-ième itéré de $\overline{1}$ valant $\overline{z}$, le groupe $\mathbb{Z}/n$ est engendré par $\overline{1}$. On en déduit les équivalences

$$\overline{z} \text{ engendre } \mathbb{Z}/n \iff \langle\overline{z}\rangle \text{ contient } \mathbb{Z}/n = \langle\overline{1}\rangle \overset{\langle\overline{z}\rangle \text{ est un sous-groupe}}{\iff} \langle\overline{z}\rangle \ni \overline{1} \iff \exists\lambda \in \mathbb{Z},\ \lambda\overline{z} = \overline{1}$$

$$\iff \exists\lambda \in \mathbb{Z},\ \overline{\lambda z} = \overline{1} \iff \exists\lambda \in \mathbb{Z},\ \exists\mu \in \mathbb{Z},\ \lambda z + \mu n = 1 \overset{\text{Bézout}}{\iff} z \text{ et } n \text{ sont étrangers.}$$

Exercices d'application

1. *Montrer que le groupe $\mathbb{Z}^2$ n'est pas monogène.*
2. *Montrer que le groupe $\mathbb{Q}$ ne peut être engendré par un nombre fini d'éléments*[79].
3. *Soit $n \geq 3$ un entier. Considérons un n-gone régulier dont on note O le centre. L'étoile régulière à $2n$ branches obtenue en reliant O aux n sommets du n-gone et aux n milieux de ses segments détermine n droites. Notons D le groupe (dit **diédral**) d'ordre $2n$ formé des n réflexions par rapport à ces n axes et par les n rotations de centre O et d'angles multiples de $\frac{2\pi}{n}$. Soit s une telle réflexion et notons r la rotation de centre O et d'angle $\frac{2\pi}{n}$. Montrer que r et s engendrent D*

---

1. Soit par l'absurde $\binom{a}{b}$ un générateur de $\mathbb{Z}^2$. La "droite" $\mathbb{Z}\binom{a}{b}$ contient alors le vecteur orthogonal $\binom{-b}{a}$, d'où un relatif λ tel que $\binom{-b}{a} = \lambda\binom{a}{b}$. On a alors les égalités $a^2 + b^2 = a(\lambda b) + (-\lambda a)b = 0$, d'où la nullité du générateur $\binom{a}{b}$ et celle de la droite $\mathbb{Z}\binom{a}{b} = \mathbb{Z}^2$: contradiction.
2. Soit F une partie finie de rationnels : en notant d un dénominateur commun aux éléments de F, le calcul fractionnaire montre que l'engendré $\langle F\rangle$ ne contient que des fractions de dénominateur réduit au plus d, donc ne saurait valoir $\mathbb{Q}$ tout entier.
3. Tout d'abord, la rotation r appartient bien à D et engendre les n rotations de D. Nous pouvons donc nous concentrer sur les réflexions, lesquelles illustrent bien le **principe de conjugaison** suivant[80] :

   conjuguer une réflexion d'axe Δ par une isométrie φ donne la réflexion d'axe $\varphi(\Delta)$.

   On en déduit que les n réflexions de D sont les n conjuguées de s par la rotation d'angle $\frac{\pi}{n}$. En notant ρ cette dernière (qui n'appartient pas à D !), on peut lister

$$D = \left\{r^a, \rho^a s\rho^{-a}\ ;\ a \in [|0, n[\right\}.$$

[79] Une structure finiment engendrée est dite ***de type fini***. Par exemple, chaque espace vectoriel est de type fini ssi il est de dimension finie.

[80] En effet, la composée d'isométries reste une isométrie et l'égalité $\text{Fix}\left(\varphi f\varphi^{-1}\right) = \varphi(\text{Fix}\, f)$ valide pour chaque application f montre par ailleurs que l'isométrie considérée fixe exactement une droite.

Pour nous débarrasser de ρ, remarquons que l'isométrie $\rho s \rho$ est négative et (le voir sur un dessin) qu'elle fixe au moins l'axe de s, donc[81] est la réflexion s, ce qui s'écrit $s\rho^{-1} = \rho s$, d'où l'on tire par une récurrence immédiate $s\rho^{-a} = \rho^a s$ pour chaque naturel a. Ainsi les n réflexions de D se réécrivent-elles $\rho^a s \rho^{-a} = \rho^a (\rho^a s) = r^a s$ pour a décrivant $[|0, n[$, ce qui conclut à l'inclusion $D \subset \langle r, s \rangle$.

FIG 9 : les 8 symétries du carré

REMARQUE. – On a obtenu une bijection $\left\{ \begin{array}{ccc} \mathbb{Z}/_n \times \mathbb{Z}/_2 & \xrightarrow{\sim} & D \\ \left(\overline{a}, \widetilde{b}\right) & \longmapsto & r^a s^b \end{array} \right.$ (bien définie vu les ordres de r et de s, surjective par ce qui précède, injective par l'égalité des cardinaux) qui n'est toutefois pas un isomorphisme (le groupe source est abélien mais pas celui but), à moins que l'on "torde" convenablement la loi du produit (ce qui nous mènerait vers le produit semi-direct – très hors programme).

---

4 Morphismes

4.1 Motivation : isomorphie

Le groupe des rotations planes sera ici noté Rot.

Pour chaque réel θ, notons $\left\{ \begin{array}{l} \overline{\theta} \text{ le complexe } e^{i\theta}, \text{ élément du groupe } (\mathbb{U}, \times), \\ \widetilde{\theta} \text{ la rotation d'angle } \theta, \text{ élément du groupe } (\mathrm{Rot}, \circ), \\ \widehat{\theta} \text{ l'angle de mesure } \theta, \text{ élément du groupe } \left(\mathbb{R}/_{2\pi}, +\right). \end{array} \right.$.

Au lieu de symboles coiffants, on gagnera à utiliser des *couleurs*. Il équivaut alors, pour chaques réels α, β, γ, d'écrire

$$\left\{ \begin{array}{l} \overline{\gamma} = \overline{\alpha}^3 \times \overline{\beta}^{-7} \\ \widetilde{\gamma} = \widetilde{\alpha}^{\circ 3} \circ \widetilde{\beta}^{\circ -7} \\ \widehat{\gamma} = 3\widehat{\alpha} - 7\widehat{\beta} \end{array} \right. \text{. En notant , } \left\{ \begin{array}{l} \overline{\star} \text{ la loi du groupe } (\mathbb{U}, \times) \\ \widetilde{\star} \text{ la loi du groupe } (\mathrm{Rot}, \circ) \\ \widehat{\star} \text{ la loi du groupe } \left(\mathbb{R}/_{2\pi}, +\right) \end{array} \right. \text{, cela se réécrit } \left\{ \begin{array}{l} \overline{\gamma} = \overline{\alpha}^3 \,\overline{\star}\, \overline{\beta}^{-7} \\ \widetilde{\gamma} = \widetilde{\alpha}^3 \,\widetilde{\star}\, \widetilde{\beta}^{-7} \\ \widehat{\gamma} = 3\widehat{\alpha}\,\widehat{\star}\, - 7\widehat{\beta} \end{array} \right. .$$

Ainsi, le calcul effectué dans l'un de trois groupes $(\mathbb{U}, \times)$, $(\mathrm{Rot}, \circ)$ ou $\left(\mathbb{R}/_{2\pi}, +\right)$ peut être transporté immédiatement dans les autres : aux conventions d'écriture près (concernant les itérés), les calculs effectués dans ces groupes sont *les mêmes* (on a simplement changé la couleur de l'ampoule éclairant nos énoncés). En corollaire, puisque le langage des groupes ne comporte aucun symbole de relation, les énoncés prouvables dans ces trois groupes sont *les mêmes* (à un changement de couleur près) : ils sont *indistinguables* du point de vue de leur structure. On dira qu'ils ont même structure, même forme, qu'ils sont *isomorphes*.

[81] En notant σ la réflexion d'axe celui de s "rotationné" de $\frac{\pi}{2n}$, la rotation ρ se décompose en ρs, d'où il sort $\rho s \rho = (\sigma s)\, s\, (\sigma s) = \sigma s^2 \sigma s = \sigma^2 s = s$.

Nous aurons besoin d'une notion un peu plus souple que l'isomorphie. Comme annoncé en introduction, un *(homo)morphisme* de trucs[82] sera une applications entre trucs qui respectera la structure considérée, c'est-à-dire d'une part les éléments distingués, d'autre part les opérations distinguées. Nous préciserons cette notion pour chaque structure, le formalisme général étant un peu lourd à présenter.

Dans toute cette section,
le mot « truc » désignera au choix
« groupe » ou « monoïde ».

4.2 Homomorphismes, exemples

Définition – Proposition (morphisme)

On appelle ***(homo)morphisme de groupes*** *toute application $\varphi : G \longrightarrow H$ dont les source et but sont des groupes telle que*[83]

$$\forall g, \gamma \in G,\ \varphi(g\gamma) = \varphi(g)\,\varphi(\gamma)\,.$$

On appelle ***morphisme de monoïdes*** *(hors programme) toute application $\varphi : M \longrightarrow N$ dont les source et but sont des monoïdes telle que*[84]

$$\forall m, \mu \in M,\ \varphi(m\mu) = \varphi(m)\,\varphi(\mu) \qquad et \qquad \boxed{\varphi(1) = 1}.$$

Soient G et H deux groupes, soit $\varphi : G \longrightarrow H$. Alors φ est morphisme de groupes ssi φ est un morphisme de monoïdes qui respecte l'inversion au sens où

$$\forall g \in G,\ \varphi\left(g^{-1}\right) = \varphi(g)^{-1}\,.$$

Démonstration

Le sens $\boxed{\Longleftarrow}$ est immédiat. Supposons donc que φ préserve la loi. Observer que le neutre de H est son unique idempotent (comme dans chaque monoïde régulier) ; or l'image de l'idempotent 1 par le morphisme φ est idempotente, donc neutre, *i. e.* $\varphi(1) = 1$. Soit par ailleurs $g \in G$: les égalités $gg^{-1} = 1 = g^{-1}g$ "passant" au morphisme φ, on voit que $\varphi(g)$ et $\varphi\left(g^{-1}\right)$ sont inverses l'un de l'autre, d'où $\varphi(g)^{-1} = \varphi\left(g^{-1}\right)$.

Notations (non-exigibles) : étant données deux structures S et T de même type, on abrégera[85]

$\mathrm{Hom}(S,T)$ et $\mathrm{Iso}(S,T)$ l'ensemble des homo- (resp. iso-) morphismes de S vers T ;

$\mathrm{End}\,S := \mathrm{Hom}(S,S)$ et $\mathrm{Aut}\,S := \mathrm{Iso}(S,S)$ l'ensemble des endo- (resp. auto-) morphismes de S.

[82] Noter le *pluriel* : il y a un truc source *et* un truc but – même s'ils peuvent coïncider.

[83] On dit aussi que φ ***respecte*** ou ***préserve*** la loi (même s'il y a *deux* lois, une au départ et une à l'arrivée), ***conserve*** ou ***préserve*** les composés ou encore que φ est un ***morphisme de magmas***.

[84] Ne pas oublier le neutre ! On dit alors que φ préserve le neutre, l'unité, ou encore que φ est ***unitaire***.

[85] On renvoie à l'introduction pour les définitions de iso-, endo- et auto-morphismes.

Remarque – Un homomorphisme doit *par étymologie* préserver la structure. Constatons : un morphisme de magmas préserve la loi, un morphisme de monoïdes préserve de plus le neutre, un morphisme de groupes préserve en outre l'inversion. Ainsi,

plus la structure s'enrichit, plus les morphismes sont contraints.

Exemples (morphismes de groupes)

1. L'exponentielle $\mathbb{C} \overset{\exp}{\twoheadrightarrow} \mathbb{C}^*$ est un morphisme de groupes (surjectif), tout comme l'exponentiation $z \mapsto b^z$ de base n'importe quel réel $b > 0$ autre que 1.
2. Les logarithmes $\lg_a = \frac{\ln}{\ln a}$ sont des isomorphismes de $\mathbb{R}_+^*$ sur $\mathbb{R}$ lorsque a décrit $\mathbb{R}_+^* \setminus \{1\}$.
3. Mettre à la puissance un complexe c donné est un morphisme de groupes $\left\{ \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{C}^* \\ t & \longmapsto & t^c \end{array} \right.$.
4. Le déterminant est un morphisme (surjectif) de $GL_n(K)$ sur $K^\times$ pour chaque corps K et chaque naturel n non nul (si $n = 0$, le groupe $GL_n(K)$ est trivial et le déterminant aussi).
5. La signature est un morphisme (surjectif) de $\mathfrak{S}_n$ sur $\mathbb{U}_2$ pour chaque naturel $n \geq 2$ (pour $n \leq 1$, le groupe $\mathfrak{S}_n$ est trivial et la signature aussi).
6. Pour chaque naturel n, la projection canonique *modulo* n est un morphisme de groupes[86] $\left\{ \begin{array}{ccc} \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/n \\ z & \mapsto & z + n\mathbb{Z} \end{array} \right.$.
7. Dans un monoïde M, les conjugaisons $m \mapsto imi^{-1}$ par un inversible i sont des automorphismes de M, appelés ***automorphismes intérieurs***. Ces derniers induisent (**exercice !**) un morphismes de groupes $\left\{ \begin{array}{ccc} M^\times & \longrightarrow & \mathrm{Aut}\, M \\ i & \longmapsto & m \mapsto imi^{-1} \end{array} \right.$.
8. Itérer un élément m dans un monoïde M fournit un morphisme $\left\{ \begin{array}{ccc} \mathbb{N} & \longrightarrow & M \\ n & \longmapsto & m^n \end{array} \right.$ d'image $\langle m \rangle$. Lorsque cet élément est inversible, ce dernier morphisme se prolonge en un morphisme de groupes $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & M^\times \\ z & \longmapsto & m^z \end{array} \right.$. Par exemple, les groupes $c\mathbb{Z}$ sont isomorphes (à $\mathbb{Z}$) lorsque c parcourt $\mathbb{C}^*$ *via* les correspondances[87] $\left\{ \begin{array}{ccc} \mathbb{Z} & \xrightarrow{\sim} & c\mathbb{Z} \\ z & \longmapsto & cz \end{array} \right.$.
9. Soit G un groupe, soit S un sous-groupe de G. Est alors un morphisme de groupes l'injection canonique[88] $\left\{ \begin{array}{ccc} S & \hookrightarrow & G \\ s & \mapsto & s \end{array} \right.$.

[86] C'est traduire (certes pompeusement) en termes de morphismes le fait que le calcul dans le quotient se passe "comme dans le groupe quotienté".

[87] On peut rencontrer plusieurs notations pour abréger "est isomorphe à" (aucune n'est exigible). Les plus lâches sont $\approx$ ou $\simeq$ (existence d'un isomorphisme sans précision aucune), on renforcera en $\cong$ lorsque l'isomorphisme est implicite (par exemple lorsqu'il est unique), mettre enfin un "tilde" sur une flèche d'application (on fusionne les notations $\to$ et $\simeq$, ce qui donne $\xrightarrow{\sim}$) signifie que l'application dénotée par la flèche est un isomorphisme.

[88] En anglais : *inclusive mapping*.

10. Soient G et H deux groupes. Sont alors des morphismes de groupes les deux injections[89] canoniques $\left\{\begin{array}{ccc} G & \hookrightarrow & G\times H \\ g & \mapsto & (g,1)\end{array}\right.$ et $\left\{\begin{array}{ccc} H & \hookrightarrow & G\times H \\ h & \mapsto & (1,h)\end{array}\right.$ ainsi que les projections canoniques $\left\{\begin{array}{ccc} G\times H & \twoheadrightarrow & G \\ (g,h) & \mapsto & g\end{array}\right.$ et $\left\{\begin{array}{ccc} G\times H & \twoheadrightarrow & H \\ (g,h) & \mapsto & h\end{array}\right.$. On généraliserait sans peine au produit d'une famille quelconque de groupes (et de monoïdes).

Exercice d'application

*Pour chaque monoïde $\mathcal{M}$, on note $\widehat{\mathcal{M}} := \mathrm{Hom}\left(\mathcal{M},\mathbb{C}^*\right)$ (appelé le **dual** de $\mathcal{M}$). Soit M un monoïde. Montrer que*

a. *$\widehat{M}$ est un sous-groupe de $\mathbb{C}^{*M}$;*

b. *l'application $m\mapsto \underset{m}{\mathrm{eval}}$ est un morphisme de monoïdes $M\longrightarrow \widehat{\widehat{M}}$.*

---

a. L'application partout égale à 1 est toujours un morphisme de monoïdes vers $\mathbb{C}^*$, donc $\widehat{M}$ contient le neutre de $\mathbb{C}^{*M}$. Soient par ailleurs $\varphi,\psi\in\widehat{M}$: montrons $\frac{\varphi}{\psi}\in\widehat{M}$. On a[90]

$$\text{d'une part } \frac{\varphi}{\psi}(1)=\frac{\varphi(1)}{\psi(1)}\overset{\varphi\text{ et }\psi\text{ sont}}{\underset{\text{unitaires}}{=}}\frac{1}{1}=1\text{, d'autre part à } m,\mu\in M \text{ fixés}$$

$$\frac{\varphi}{\psi}(m\mu)=\frac{\varphi(m\mu)}{\psi(m\mu)}\overset{\varphi\text{ et }\psi\text{ sont des}}{\underset{\text{morphismes}}{=}}\frac{\varphi(m)\varphi(\mu)}{\psi(m)\psi(\mu)}=\frac{\varphi(m)}{\psi(m)}\frac{\varphi(\mu)}{\psi(\mu)}=\frac{\varphi}{\psi}(m)\ \frac{\varphi}{\psi}(\mu).$$

b. Notons $\acute{e}$ l'application prétendue être un morphisme et $\mathbf{1}$ le neutre de $\widehat{\widehat{M}}$. Soit $\varphi\in\widehat{M}$. On a alors d'une part

$$[\acute{e}(1)](\varphi)=\underset{1}{\mathrm{eval}}\,\varphi=\varphi(1)\overset{\varphi\text{ est}}{\underset{\text{unitaire}}{=}}1=\mathbf{1}(\varphi)\text{, d'où } \acute{e}(1)=\mathbf{1},$$

d'autre part à $m,\mu\in M$ fixés

$$\begin{aligned}&[\acute{e}(m\mu)](\varphi)=\underset{m\mu}{\mathrm{eval}}\,\varphi=\varphi(m\mu)=\varphi(m)\varphi(\mu)=\underset{m}{\mathrm{eval}}\,\varphi\times\underset{\mu}{\mathrm{eval}}\,\varphi\\ =\ &[\acute{e}(m)](\varphi)\times[\acute{e}(\mu)](\varphi)=[\acute{e}(m)\times\acute{e}(\mu)](\varphi)\text{, d'où l'égalité } \acute{e}(m\mu)=\acute{e}(m)\acute{e}(\mu).\end{aligned}$$

---

[89] La flèche $\hookrightarrow$, fusion d'une flèche d'application $\longrightarrow$ et d'un symbole d'inclusion $\subset$, signale une *injectivité*. En effet, généralisant les injections canoniques, il est bon de penser une injection $A\hookrightarrow B$ entre ensembles comme une *inclusion* $A'\subset B$ où l'on a identifié A à son image directe A' par l'injection (on dit parfois qu'on a *plongé* A dans B).

[90] Voici une très rare occasion où l'on peut se payer le luxe de ne pas séparer les deux vérifications $\varphi\psi\in\widehat{M}$ et $\varphi^{-1}\in\widehat{M}$.

4.3 Création de morphismes

Propriétés (identité, composée et réciproque de morphismes)

1. *L'identité est un (auto)morphisme de trucs*[91].
2. *La réciproque de chaque isomorphisme de trucs est un (iso)morphisme de trucs.*
3. *Lorsqu'elle fait sens, la composée de chaques morphismes de trucs reste un morphisme de trucs.*

Démonstration

1. Dans les magmas, on a à m, μ fixés les égalités $\mathrm{Id}\,(m\mu) = m\mu = \mathrm{Id}\,(m)\,\mathrm{Id}\,(\mu)$, le caractère *unitaire* (*i. e.* le fait de préserver le neutre) découlant de ce que Id fixe chaque élément – neutre compris.

2. Soit $f : M \xrightarrow{f} N$ un isomorphisme. Supposant f morphisme *de magmas*, à $n, \nu \in N$ fixés, noter $\binom{m}{\mu} := \binom{f^{-1}(n)}{f^{-1}(\nu)}$ permet d'écrire

$$f^{-1}(n\nu) \overset{\substack{\text{définition}\\ \text{de } m \text{ et } \mu}}{=} f^{-1}(\,f(m)\,f(\mu)\,) \overset{\substack{f \text{ est un}\\ \text{morphisme}}}{=} f^{-1}(\,f(m\mu)\,) = m\mu \overset{\substack{\text{définition}\\ \text{de } m \text{ et } \mu}}{=} f^{-1}(n)\,f^{-1}(\nu)\,.$$

   Supposant f *unitaire*, appliquer f^{-1} à l'hypothèse $f(1) = 1$ fournit l'égalité $f^{-1}(1) = 1$.

3. Soient $M \xrightarrow{f} N \xrightarrow{g} O$ deux morphismes. Supposant ces morphismes *de magmas*, on a à $m, \mu \in M$ fixés les égalités

$$\begin{aligned}[g \circ f]\,(m\mu) &\overset{\substack{\text{définition}\\ \text{de } \circ}}{=} g(\,f(m\mu)\,) \overset{\substack{f \text{ est un}\\ \text{morphisme}}}{=} g(\,f(m)\,f(\mu)\,) \overset{\substack{g \text{ est un}\\ \text{morphisme}}}{=} g(f(m))\;g(f(\mu))\\ &\overset{\substack{\text{définition}\\ \text{de } \circ}}{=} [g \circ f]\,(m)\;[g \circ f]\,(\mu)\,.\end{aligned}$$

   Supposant ces morphismes *unitaires*, on aura

$$[g \circ f]\,(1) \overset{\substack{\text{définition}\\ \text{de } \circ}}{=} g(f(1)) \overset{\substack{f \text{ est}\\ \text{unitaire}}}{=} g(1) \overset{\substack{g \text{ est}\\ \text{unitaire}}}{=} 1.$$

Corollaire (monoïde des endomorphismes)

Soit S une structure de type truc. Alors $\mathrm{End}\,S$ *est un monoïde d'inversibles* $\mathrm{Aut}\,S$ *:*

$$(\mathrm{End}\,S)^\times = \mathrm{Aut}\,S.$$

Démonstration

Les première et troisième propriétés ci-dessus montrent que $\mathrm{End}\,S$ est stable par composition et contient le neutre Id_S de S^S, donc est un sous-monoïde de ce dernier.

Un inversible de $\mathrm{End}\,S$ étant en particulier un endomorphisme bijectif, *i. e.* un automorphisme, on a l'inclusion $(\mathrm{End}\,S)^\times \subset \mathrm{Aut}\,S$. Réciproquement, la deuxième

[91] *Rappel* : le mot « truc » désigne au choix « groupe » ou « monoïde ».

propriété ci-dessus montre que la réciproque d'un automorphisme est un morphisme, donc reste dans $\operatorname{End} S$, d'où l'inclusion réciproque.

Remarque – **Classes d'isomorphie**. On en déduit en particulier que la "relation[92]" « être isomorphe à » vérifie les axiomes d'une relation d'équivalence : ses classes d'équivalence constituent précisément les objets d'étude de la théorie des groupes – on *ne veut pas* distinguer deux groupes isomorphes. (La même remarque tiendrait en remplaçant « groupe » par n'importe quelle autre structure.)

Par exemple, le groupe de symétries d'un segment est isomorphe à $\mathbb{U}_2$, ${}^{\mathbb{Z}}\!/_2$ ou $\mathfrak{S}_2$ à travers les correspondances

$$\begin{array}{ccccccc} \left(\begin{array}{c}\text{symétries du}\\ \text{segment,}\circ\end{array}\right) & \cong & \begin{pmatrix}\mathbb{U}_2\\ \times\end{pmatrix} & \cong & \begin{pmatrix}{}^{\mathbb{Z}}\!/_2\\ +\end{pmatrix} & \cong & \begin{pmatrix}\mathfrak{S}_2\\ \circ\end{pmatrix} \\ \text{Id} & \leftrightarrow & 1 & \leftrightarrow & \overline{0} & \leftrightarrow & \text{Id} \\ \text{réflexion} & \leftrightarrow & -1 & \leftrightarrow & \overline{1} & \leftrightarrow & (1\ 2) \end{array}.$$

Proposition (produit de morphismes)

1. *Le produit de chaque famille*[93] *de morphismes de trucs reste un morphisme de trucs.*
2. *Chaque produit d'isomorphismes de trucs est un isomorphisme de trucs.*

Démonstration

Soit $(\varphi_i : M_i \longrightarrow N_i)$ une famille de morphismes de magmas. Notons-en φ l'application produit.

1. On a alors pour chaques familles $m, \mu \in \prod M_i$ les égalités

$$\varphi(m\mu) \quad = \quad \varphi\big(\,(m_i)\,(\mu_i)\,\big) \overset{\text{déf. de la}}{\underset{\text{loi produit}}{=}} \varphi\big(\,(m_i\mu_i)\,\big) \overset{\text{déf.}}{\underset{\text{de }\varphi}{=}} \big(\,\varphi_i(m_i\mu_i)\,\big) \text{ et}$$

$$\varphi(m)\,\varphi(\mu) \overset{\text{déf.}}{\underset{\text{de }\varphi}{=}} (\varphi_i(m_i))\ (\varphi_i(\mu_i)) \overset{\text{déf. de la}}{\underset{\text{loi produit}}{=}} (\varphi_i(m_i)\ \ \varphi_i(\mu_i)) \overset{\text{chaque } \varphi_i \text{ est}}{\underset{\text{un morphisme}}{=}} (\varphi_i(m_i\mu_i))\,.$$

Imposant les morphismes φ_i *unitaires*, on a alors les égalités

$$\varphi\left(1_{\prod M_i}\right) \overset{\text{neutre}}{\underset{\text{produit}}{=}} \varphi\big(\,(1_{M_i})\,\big) \overset{\text{déf.}}{\underset{\text{de }\varphi}{=}} \big(\,\varphi_i(1_{M_i})\,\big) \overset{\text{chaque } \varphi_i}{\underset{\text{est unitiare}}{=}} (1_{N_i}) \overset{\text{neutre}}{\underset{\text{produit}}{=}} 1_{\prod N_i}.$$

2. Imposons de plus chaque φ_i bijectif. Alors le produit des morphismes φ_i^{-1} est clairement une réciproque de φ.

On peut par exemple affirmer pour chaque ensemble E que les groupes produits $\left(\left({}^{\mathbb{Z}}\!/_2\right)^E, +\right)$ et $\left(\mathbb{U}_2^E, \times\right)$ sont isomorphes *via* la puissance E-ième de l'isomorphisme ${}^{\mathbb{Z}}\!/_2 \xrightarrow{\sim} \mathbb{U}_2$ ci-dessus.

Autre corollaire de ce deuxième point :

[92] La classe-domaine de la "relation" d'isomorphie n'est pas forcément un *ensemble* (tout comme pour les relations d'appartenance, d'inclusion, d'équipotence, de subpotence...), d'où les guillemets.

[93] *Rappel* : chaque famille d'applications $\left(A_i \xrightarrow{f_i} B_i\right)$ induit une application "produit" définie par $\left\{\begin{array}{ccc} \prod A_i & \longrightarrow & \prod B_i \\ (a_i) & \longmapsto & (\,f_i(a_i)\,) \end{array}\right.$.

la "relation" d'isomorphie est compatible avec la multiplication cartésienne.

Par exemple, les deux isomorphismes $\begin{smallmatrix}\mathbb{Z}/_{18}\xrightarrow{\sim}\mathbb{U}_{18}\\ \mathbb{R}/_{2\pi}\xrightarrow{\sim}\mathbb{U}\end{smallmatrix}$ induisent un isomorphisme $\mathbb{Z}/_{18}\times \mathbb{R}/_{2\pi}\xrightarrow{\sim}\mathbb{U}_{18}\times\mathbb{U}$, ce qui peut alléger certaines écritures.

Exercice d'application

Soit E un ensemble. Parmi les monoïdes $\begin{pmatrix}\mathfrak{P}(E)\\ \cup\end{pmatrix}$, $\begin{pmatrix}\mathfrak{P}(E)\\ \cap\end{pmatrix}$, $\begin{pmatrix}\mathfrak{P}(E)\\ \Delta\end{pmatrix}$, $\begin{pmatrix}\mathbb{U}_2^E\\ \times\end{pmatrix}$ et $\begin{pmatrix}\left(\mathbb{Z}/_2\right)^E\\ \times\end{pmatrix}$, lesquels sont isomorphes ? Expliciter le cas échéant des isomorphismes. On rappelle au besoin l'équipotence $\mathfrak{P}(E)\xrightarrow{\sim}\left(\mathbb{Z}/_2\right)^E$ via les fonctions caractéristiques[94]*.*

Les deux premiers monoïdes sont isomorphes *via* la complémentation $A\mapsto {}^cA$. Les deux premiers et le dernier ne sont pas des groupes, contrairement aux troisième et quatrième, ce qui divise déjà les classes d'isomorphie en deux "groupes". La bijection rappelée est enfin un morphisme de $\times$ vers $\cap$ mais également de $+$ vers Δ ; or le groupe produit $\left(\mathbb{U}_2^E,\times\right)$ est isomorphe à $\left(\left(\mathbb{Z}/_2\right)^E,+\right)$. On a finalement deux classes d'isomorphie :

"le" groupe $\begin{pmatrix}\mathfrak{P}(E)\\ \Delta\end{pmatrix}\xrightarrow{\sim}\begin{pmatrix}\mathbb{U}_2^E\\ \times\end{pmatrix}$ et "le" monoïde $\begin{pmatrix}\mathfrak{P}(E)\\ \cup\end{pmatrix}\xrightarrow{A\mapsto {}^cA}{}_{\sim}\begin{pmatrix}\mathfrak{P}(E)\\ \cap\end{pmatrix}\xrightarrow{\sim}\begin{pmatrix}\left(\mathbb{Z}/_2\right)^E\\ \times\end{pmatrix}$.

4.4 Morphismes & images

Propriétés (image directe d'un sous-truc, image réciproque d'un sous-truc)

1. *L'image directe de chaque sous-truc (source) par un morphisme de trucs est un sous-truc (but).*
2. *L'image réciproque de chaque sous-truc (but) par un morphisme de trucs est un sous-truc (source).*

Démonstration

Soit $\varphi : M\longrightarrow N$ un morphisme de magmas.

[94] Rappelons que la fonction caractéristique d'une partie $A\subset E$ est l'application $\chi_A : E\longrightarrow \mathbb{Z}/_2$ définie par $e\mapsto\begin{cases}1 \text{ si } e\in A\\ 0 \text{ si } e\notin A\end{cases}$ ("χ" comme "**ch**aractéristique"). L'application $\chi : \mathsf{P}(E)\xrightarrow{\sim}\left(\mathbb{Z}/_2\right)^E$ est alors bijective de réciproque $f\mapsto\{e\in E\ ;\ f(e)=1\}$.

1. Soit S un sous-truc de M. La stabilité de $\varphi(S)$ par la loi de N découle des égalité et appartenance (à $s, \sigma \in S$ fixés)

$$\varphi(s)\varphi(\sigma) \underset{\text{morphisme}}{\overset{\varphi \text{ est un}}{=}} \varphi(s\sigma) \underset{\text{stable}}{\overset{S \text{ est}}{\in}} \varphi(S).$$

Si φ est de plus unitaire, puisque S contient 1, l'image $\varphi(S)$ contiendra alors $\varphi(1) = 1$.

2. Soit S un sous-truc de N. Pour chaques $m, \mu \in \varphi^{-1}(S)$, on a

$$\varphi(m\mu) \underset{\text{morphisme}}{\overset{\varphi \text{ est un}}{=}} \varphi(m)\varphi(\mu) \underset{\text{de } m \text{ et } \mu}{\overset{\text{invocation}}{\in}} S\ S \underset{\text{stable}}{\overset{S \text{ est}}{\subset}} S, \text{ d'où } m\mu \in \varphi^{-1}(S).$$

Si φ est de plus unitaire, l'appartenance $\varphi(1) = 1 \in S$ montre alors $1 \in \varphi^{-1}(S)$.

Corollaire (image d'un truc engendré)

Soient φ un morphisme de trucs et A une partie source. On a alors

$$\varphi(\langle A\rangle) = \langle \varphi(A)\rangle.$$

Démonstration.

Le lecteur doit tout d'abord se convaincre du résultat en utilisant la description interne d'un sous-groupe engendré et en écrivant des égalités comme $\varphi(\prod a_i^{\varepsilon_i}) = \prod \varphi(a_i)^{\varepsilon_i}$. Montrons le cas général sans description interne ni externe, de manière purement ensembliste.

Rappel : chaque application f induit des inclusions[95] $\begin{cases} P \subset f^{-1}(f(P)) \\ f\left(f^{-1}(Q)\right) \subset Q \end{cases}$ pour chaques parties P et Q incluses resp. dans la source et le but de f.

De l'inclusion $A \subset \langle A\rangle$, prendre les images directes par φ donne $\varphi(A) \subset \varphi(\langle A\rangle)$, puis prendre les engendrés donne $\langle \varphi(A)\rangle \subset \langle \varphi(\langle A\rangle)\rangle$; or, $\langle A\rangle$ étant un sous-truc source, son image $\varphi(\langle A\rangle)$ est un sous-truc but, donc vaut son engendré et l'inclusion précédente se réécrit $\langle \varphi(A)\rangle \subset \varphi(\langle A\rangle)$.

Notons $B := \varphi(A)$. De l'inclusion $\langle B\rangle \supset B$, prendre les images réciproques par φ donne $\varphi^{-1}(\langle B\rangle) \supset \varphi^{-1}(B) \supset A$, puis prendre les engendrés donne $\left\langle \varphi^{-1}(\langle B\rangle)\right\rangle \supset \langle A\rangle$; puisque $\langle B\rangle$ est un sous-truc but, son image réciproque $\varphi^{-1}(\langle B\rangle)$ est un sous-truc source, donc vaut son engendré et l'inclusion précédente se réécrit $\langle A\rangle \subset \varphi^{-1}(\langle B\rangle)$. Prendre les images directes donne alors $\varphi(\langle A\rangle) \subset \varphi\left(\varphi^{-1}(\langle B\rangle)\right) \subset \langle B\rangle$.

Exercice d'application

1. *Montrer que les translations à gauche de chaque groupe (resp. monoïde) constituent un groupe (resp. monoïde) isomorphe à ce dernier. En déduire un* **théorème de Cayley**[96] *:*

   chaque groupe est isomorphe à un sous-groupe d'un groupe symétrique.

[95] *Mméno* : la source venant avant le but, la partie P vient avant celle Q, donc P est avant et Q est après, ce qui s'écrit $\begin{matrix} P \subset ? \\ ? \subset Q \end{matrix}$; compléter ensuite chaque inclusion avec la *même* lettre (afin de faire sens !).

[96] Ce théorème fut publié en 1854 dans l'article *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$ de la revue *Philosophical Magazine*.

2. *Montrer que le groupe* $\mathbb{Z}$ *est* ***indécomposable****,* i. e. *n'est jamais isomorphe à un produit de deux groupes (sauf cas trivial à préciser).*
3. *Montrer que le groupe des symétries du carré n'est pas isomorphe au groupe des quaternions.*

---

1. Notons γ_a la translation à gauche par a. Les égalités[97] $\gamma_a\gamma_b = \gamma_{ab}$ (pour chaque b) et l'égalité $\gamma_1 = \mathrm{Id}$ montrent que γ est un morphisme de monoïdes d'image formée par les translations à gauche. Ce morphisme est injectif vu les implications[98] $\gamma_a = \gamma_b \implies \gamma_a(1) = \gamma_b(1) \implies a = b$, donc induit un isomorphisme du monoïde M (resp. groupe G) source sur son image, laquelle est un sous-monoïde de M^M (resp. un sous-groupe de $\mathfrak{S}_G$).
2. On a pour chaque groupe G deux isomorphismes $\left\{\begin{array}{ccccc} \{\blacklozenge\}\times G & \cong & G & \cong & G\times\{\blacklozenge\} \\ (\blacklozenge, g) & \leftrightarrow & g & \leftrightarrow & (g,\blacklozenge)\end{array}\right.$ pour chaque objet $\blacklozenge$: ainsi, *les groupes triviaux sont neutres (*modulo *isomorphie) pour la multiplication cartésienne.*

   Soient A et B deux groupes et soit un isomorphisme $\mathbb{Z} \overset{\varphi}{\cong} A\times B$. Nous allons montrer que A ou B est trivial (l'autre facteur étant alors isomorphe à $\mathbb{Z}$). D'une part, le groupe A est isomorphe à $A\times\{1_B\}$, donc (*via* l'isomorphisme φ^{-1}) à $\varphi^{-1}(A\times\{1\})$, d'autre part l'image réciproque du sous-groupe $A\times\{1_B\}$ de $A\times B$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$ pour un certain naturel a : il en sort une isomorphie $A \simeq a\mathbb{Z}$. Si a est nul, on a terminé (A est trivial), sinon $A \simeq a\mathbb{Z}$ est isomorphe à $\mathbb{Z}$. De même, si B n'est pas trivial, il est isomorphe à $\mathbb{Z}$, mais alors $\mathbb{Z} \simeq A\times B \simeq \mathbb{Z}\times\mathbb{Z}$ n'est pas monogène, contredisant l'exercice 1 § 3.5.

   On retiendra que *chaque groupe* ***décomposable*** *est isomorphe au produit de deux de ses sous-groupes stricts.*
3. Notons D le groupe diédral considéré, soit s une réflexion de D et appelons r la rotation d'angle $\frac{\pi}{2}$ (de centre celui du carré), de sorte à avoir (*cf.* exercice 3 § 3.5) l'égalité $D = \langle r, s\rangle$. Soit par l'absurde un isomorphisme $D \overset{\varphi}{\cong} \mathbb{H}_8$. On a alors les égalités $\mathbb{H}_8 = \varphi(D) = \varphi(\langle r,s\rangle) = \langle\varphi(r),\varphi(s)\rangle$. Puisque s est idempotent, son image $\varphi(s)$ est un idempotent de $\mathbb{H}_8$, donc vaut ±1, de sorte que $\mathbb{H}_8$ est engendré par ±1 et par un autre élément $q := \varphi(r)$. Le carré de ce dernier valant 1 ou -1, l'engendré $\mathbb{H}_8 = \langle\pm1, q\rangle$ sera toujours inclus dans $\langle -1,1,-q,q\rangle = \{-1,1,-q,q\}$, forçant en prenant les cardinaux l'absurde comparaison $|\mathbb{H}_8| \leq 4$.

4.5 Morphismes & noyaux

Définition (noyau d'un morphisme)

[97] *cf.* proposition § 2.4
[98] Entre groupes, on remplacera b par 1 pour montrer l'injectivité (*cf.* § 4.5).

On appelle ***noyau*** *d'un morphisme de trucs l'image réciproque du singleton neutre. Si* $\varphi : G \longrightarrow H$ *dénote un tel morphisme, son noyau est noté*[99]

$$\operatorname{Ker}\varphi := \{g \in G \ ; \ \varphi(g) = 1\}.$$

Propriétés (noyau, image, injectivité)

1. *Le noyau et l'image d'un morphisme de trucs sont des sous-trucs (resp. source et but).*
2. *Un morphisme de groupes est injectif ssi son noyau est trivial*[100]*.*

Démonstration

1. Vu les égalités $\begin{cases} \operatorname{Ker}\varphi = \varphi^{-1}(\{1\}) \\ \operatorname{Im}\varphi = \varphi(M) \end{cases}$, il suffit d'appliquer la propriété précédente aux sous-trucs resp. neutre et plein.
2. Supposons φ injectif. On a alors à $m \in M$ fixé les implications

$$m \in \operatorname{Ker}\varphi \overset{\text{déf. du noyau}}{\Longrightarrow} \varphi(m) = 1 \overset{\varphi \text{ est unitaire}}{\Longrightarrow} \varphi(m) = \varphi(1) \overset{\varphi \text{ est injectif}}{\Longrightarrow} m = 1,$$

d'où l'inclusion $\operatorname{Ker}\varphi \subset \{1\}$, la réciproque $\supset$ venant de l'unitarité de φ.

Supposons $\operatorname{Ker}\varphi = \{1\}$ et soient $m, \mu \in M$. On a alors les implications[101]

$$\varphi(m) = \varphi(\mu) \overset{N \text{ est un groupe}}{\Longrightarrow} \varphi(\mu)^{-1}\varphi(m) = 1 \overset{\varphi \text{ est un morphisme}}{\Longrightarrow} \varphi\left(\mu^{-1}m\right) = 1 \Longrightarrow \mu^{-1}m \in \operatorname{Ker}\varphi$$
$$\Longrightarrow \quad \mu^{-1}m = 1 \Longrightarrow m = \mu, \text{ d'où l'injectivité de } \varphi.$$

Remarques

• **Image et surjectivité.** On énonce souvent la propriété « *un morphisme de groupes est surjectif ssi son image vaut tout le groupe but* » en vis-à-vis de la propriété sur l'injectivité et le noyau. Nous ne l'avons pas fait car cette propriété est *purement ensembliste* et ne concerne donc absolument pas les structures.

• **Noyau et injectivité.** Le point 2 s'agit en tout et pour tout d'un raccourci de calcul dans les groupes. Ne pas y recourir dénote toutefois – outre une inclination pour le labeur inutile – une mécompréhension majeure, à savoir l'oubli qu'

à translation près, on peut toujours dans un groupe se ramener au neutre.

Exemples (noyaux de morphismes)

1. Le noyau de l'exponentielle $\mathbb{C} \twoheadrightarrow \mathbb{C}^*$ vaut $\operatorname{Ker}\exp = 2\pi i\mathbb{Z}$.

[99] *ker* abrège l'allemand *Kern* ou l'anglais *kernel* – rien à voir avec le terme breton signifiant "ville" ou "chez soi".

[100] On retrouve ainsi la proposition classique entre applications linéaires, ces dernières étant en particulier des morphismes de groupes additifs.

[101] Notre démonstration du sens $\Longleftarrow$ nécessite l'inversibilité : étant donné un idempotent $i \neq 1$ dans un monoïde, l'itération de i a pour noyau $\{1\}$ mais n'est pas injective. Le point (2) est donc *faux pour les monoïdes.*

2. Les noyaux des logarithmes $\mathbb{R}_+^* \longrightarrow \mathbb{R}$ sont triviaux : $\forall a \in \mathbb{R}_+^* \setminus \{1\}\ ,\ \operatorname{Ker} \lg_a = \{1\}$.
3. Soient A un anneau et n un naturel : le noyau $\operatorname{Ker} \det$ est le groupe spécial linéaire $SL_n(A)$.
4. Soit E un espace euclidien. Restreint au groupe $\mathcal{O}(E)$ des isométries de E, le déterminant a pour noyau le groupe spécial orthogonal $\mathcal{SO}(E) = \operatorname{Ker} \det_{|\mathcal{O}(E)}$ des déplacements (isométries préservant l'orientation).
5. Soit n un naturel. Dans $\mathfrak{S}_n$, le noyau de la signature est le groupe alterné : $\operatorname{Ker} \varepsilon = \mathfrak{A}_n$.
6. Pour chaque naturel n, le noyau de la projection canonique *modulo* n est formé des multiples de n :
$$\operatorname{Ker} \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n \\ z & \longmapsto & \overline{z} \end{array} \right. = n\mathbb{Z}.$$
7. Le noyau de l'injection canonique d'un sous-groupe dans un groupe est trivial.
8. Soient G et H deux groupes. Les noyaux des deux injections canoniques $\begin{array}{c} G \hookrightarrow G \times H \\ H \hookrightarrow G \times H \end{array}$ sont alors triviaux.
9. Soient G et H deux groupes. Les noyaux des deux projections canoniques $\begin{array}{c} G \times H \twoheadrightarrow G \\ G \times H \twoheadrightarrow H \end{array}$ valent alors respectivement $\begin{array}{c} \{1\} \times H \\ G \times \{1\} \end{array}$.

Proposition (quotienter un morphisme de source $\mathbb{Z}$) (hors programme)

Soit $\varphi : \mathbb{Z} \longrightarrow G$ un morphisme de groupes. Soit $n \in \mathbb{N}$ un générateur de $\operatorname{Ker} \varphi$. *Est alors un morphisme injectif de groupes*[102] *l'application* $\left\{ \begin{array}{ccc} \mathbb{Z}/n & \hookrightarrow & G \\ \overline{z} & \mapsto & \varphi(z) \end{array} \right.$.

Démonstration

Avant toute chose, le noyau de φ est un sous-groupe de $\mathbb{Z}$, donc est monogène, ce qui légitime l'invocation d'un naturel n comme dans l'énoncé.

Comme chaque application, φ induit[103] une injection $\Phi := \left\{ \begin{array}{ccc} \mathbb{Z}/\sim & \hookrightarrow & G \\ \overline{z} & \mapsto & \varphi(z) \end{array} \right.$ où $\sim$ dénote la relation d'équivalence "avoir même image par φ". Or les équivalences (à $a, b \in \mathbb{Z}$ fixés)

$$a \sim b \Longleftrightarrow \varphi(a) = \varphi(b) \overset{\text{comme au point (2)}}{\Longleftrightarrow} a - b \in \operatorname{Ker} \varphi \Longleftrightarrow a = b \ [n]$$

montrent que la relation $\sim$ est l'égalité *modulo* n. Enfin, Φ est un morphisme de groupes au vu des égalités à $a, b \in \mathbb{Z}$ fixés

$$\Phi\left(\overline{a} + \overline{b}\right) = \Phi\left(\overline{a+b}\right) = \varphi(a+b) \overset{\varphi \text{ est un morphisme}}{=} \varphi(a)\,\varphi(b) = \Phi(a)\,\Phi(b).$$

---

[102] Le morphisme φ induit donc un isomorphismes de groupes $\left\{ \begin{array}{ccc} \mathbb{Z}/n & \xrightarrow{\sim} & \operatorname{Im} \varphi \\ \overline{z} & \longmapsto & \varphi(z) \end{array} \right.$.

[103] L'image directe par φ d'une classe $\overline{z}$ étant le singleton $\{\varphi(z)\}$, dont l'union vaut $\varphi(z)$, on *définira* Φ explicitement en envoyant une classe sur l'union de son image directe, *i. e.* par $C \mapsto \cup\varphi(C)$, puis on en *déduira* la *propriété* $\Phi(\overline{z}) = \varphi(z)$.

Remarque – **Quotients (très hors programme)**. Le groupe source ne joue en fait aucun rôle : chaque morphisme de groupe $\varphi : G \longrightarrow H$ induit un isomorphisme $\left\{ \begin{array}{ccc} {}^{G}\!/_{\operatorname{Ker}\varphi} & \xrightarrow{\sim} & \operatorname{Im}\varphi \\ \overline{g} & \longmapsto & \varphi(g) \end{array} \right.$ où, en abrégeant $K := \operatorname{Ker}\varphi$, le groupe source ${}^{G}\!/_{K}$ est constitué des classes $\overline{g} := gK = Kg$ dites *modulo* K. Ces généralités ne sont plus dans l'esprit des concours[104] mais nous les utiliserons dans le cas particulier démontré afin d'alléger plusieurs démonstrations.

Corollaire (vers le lemme chinois)

Soient a et b deux naturels étrangers. Est alors un isomorphisme de groupes l'application[105]

$$\left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{ab} & \xrightarrow{\sim} & {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbb{Z}}\!/_{b} \\ \overline{z} & \longmapsto & (\widetilde{z}, \widehat{z}) \end{array} \right. .$$

Démonstration

L'application $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbb{Z}}\!/_{b} \\ z & \longmapsto & (\widetilde{z}, \widehat{z}) \end{array} \right.$ (inspirée du produit des projections canoniques *modulo* a et b resp.) est un morphisme de noyau $ab\mathbb{Z}$ vu à $z \in \mathbb{Z}$ fixé les équivalences

$$\begin{pmatrix} \widetilde{z} \\ \widehat{z} \end{pmatrix} = \begin{pmatrix} \widetilde{0} \\ \widehat{0} \end{pmatrix} \Longleftrightarrow \left\{ \begin{array}{l} a \mid z \\ b \mid z \end{array} \right. \overset{\text{Gauss}}{\Longleftrightarrow} ab \mid z,$$

donc induit un isomorphisme comme désiré.

Exercices d'application

1. *Soit M un monoïde. Déterminer le noyau de* $\left\{ \begin{array}{ccc} M^{\times} & \longrightarrow & \operatorname{Aut} M \\ i & \longmapsto & m \mapsto imi^{-1} \end{array} \right.$.
2. *Soit $c \in \mathbb{C}$. Donner une CNS simple décrivant l'injectivité de l'élévation à la puissance c.*

Remarque

1. Notons ι le morphisme ci-dessus et Z le centre de M. On a alors à $i \in M^{\times}$ fixé les équivalences

$$\begin{aligned} i \in \operatorname{Ker}\iota &\iff \left[m \mapsto imi^{-1}\right] = \underset{M}{\operatorname{Id}} \iff \forall m \in M,\ imi^{-1} = m \\ &\iff \forall m \in M,\ im = mi \iff i \in Z, \text{ d'où } \operatorname{Ker}\iota = Z \cap M^{\times}. \end{aligned}$$

[104] Si A dénote une partie non vide d'un groupe G, les classes *modulo* A forment alors un groupe pour la loi "parties" où $\overline{1}\,\overline{1} = \overline{1}$ ssi A est un sous-groupe de G tel que $\forall g \in G,\ gAg^{-1} = A$ (un tel sous-groupe est dit ***distingué***). L'application $g \mapsto \overline{g}$ est alors un morphisme de groupes.

[105] Il est entendu que les barres, tildes et circonflexes dénotent les classes *modulo* les entiers correspondants.

2. Notons $\binom{a}{b} := \binom{\operatorname{Re} c}{\operatorname{Im} c}$ et appelons ε le morphisme considéré $\left\{ \begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{C}^* \\ t & \longmapsto & t^c = t^a t^{ib \ln t} \end{array} \right.$.

Si a est non nul, on a alors pour chaque réel $t > 0$ les implications

$$t \in \operatorname{Ker} \varepsilon \Longrightarrow |\varepsilon(t)| = 1 \Longrightarrow t^a = 1 \Longrightarrow t = 1, \text{ d'où } \operatorname{Ker} \varepsilon = \{1\}.$$

Supposons $a = 0$. Si b est nul aussi, alors c est nul et ε est trivial : $\operatorname{Ker} \varepsilon = \mathbb{R}_+^*$. Sinon, on a pour chaque réel $t > 0$ les équivalences

$$t \in \operatorname{Ker} \varepsilon \Longleftrightarrow \varepsilon(t) = 1 \Longleftrightarrow t^{ib \ln t} = 1 \Longleftrightarrow b \ln t \in 2\pi\mathbb{Z} \Longleftrightarrow t \in \exp\left(\frac{2\pi}{b}\mathbb{Z}\right),$$

d'où $\operatorname{Ker} \varepsilon = \exp \frac{2\pi\mathbb{Z}}{\operatorname{Im} c}$. Dans les deux cas, le noyau n'est pas trivial.

Finalement, le morphisme ε est injectif ssi c n'est pas un imaginaire pur.

4.6 Morphismes et générateurs (hors programme)

Comme dans les espaces vectoriels, *un morphisme est entièrement déterminé sur une partie génératrice*. Voyons la puissance de cette affirmation.

Endomorphismes de $\mathbb{Q}$

Soit $\varphi \in \operatorname{End} \mathbb{Q}$. Puisque le groupe $\mathbb{Q}$ est engendré par les inverses des naturels non nuls, il suffit de déterminer les images de ces inverses. Soit donc $n \in \mathbb{N}^*$ et notons $g := \frac{1}{n}$. Les égalités $n\varphi(g) = \varphi(ng) = \varphi(1)$ donnent $\varphi(g) = \frac{\varphi(1)}{n} = \varphi(1)\, g$, ce qui montre que φ coïncide avec l'homothétie de rapport $\varphi(1)$ sur une partie génératrice de $\mathbb{Q}$, donc vaut cette homothétie sur tout $\mathbb{Q}$.

Réciproquement, les homothéties (de rapport rationnel) sont clairement des endomorphismes du groupe additif $\mathbb{Q}$ (et même des *auto*morphismes si le rapport est non nul).

Dual des groupes symétriques

Soit n un naturel. Déterminons les morphismes de $\mathfrak{S}_n$ vers $\mathbb{C}^*$.

Soit ε un tel morphisme, imposé non trivial. Le groupe symétrique étant engendré par les transpositions, il suffit de déterminer les images par ε des transpositions. Admettant que ces dernières soient conjuguées, le groupe but étant abélien, ces images sont identiques au vu des égalités (à τ et φ permutations fixées)

$$\varepsilon\left(\varphi\tau\varphi^{-1}\right) = \varepsilon(\varphi)\,\varepsilon(\tau)\,\varepsilon(\varphi)^{-1} \underset{\text{abélien}}{\overset{\mathbb{C}^* \text{ est}}{=}} \varepsilon(\varphi)\,\varepsilon(\varphi)^{-1}\,\varepsilon(\tau) = \varepsilon(\tau).$$

Une transposition étant par ailleurs involutive, cette image commune est un involutif de $\mathbb{C}^*$, à savoir ± 1, le cas $+1$ étant à rejeter car conduisant à l'absurde trivialité de ε. Réciproquement, la signature est bien un morphisme valant -1 sur les transpositions.

Montrons le fait admis : pour chaque longueur $\ell \in [|1,n|]$, *les ℓ-cycles sont conjugués*. Soient deux suites de ℓ entiers distincts $\begin{matrix} a_1, a_2, ...a_\ell \\ b_1, b_2, ..., b_\ell \end{matrix}$ dans $[|1,n|]$. Les parties $\begin{matrix} [|1,n|] \setminus \{a_1, a_2, ..., a_\ell\} \\ [|1,n|] \setminus \{b_1, b_2, ..., b_\ell\} \end{matrix}$ ayant même cardinal $n - \ell$, on peut invoquer une application les bijectant puis prolonger cette dernière en définissant $a_i \mapsto b_i$ pour chaque $i \in [|1,\ell|]$. Le prolongement φ obtenu injecte alors $[|1,n|]$ dans lui-même (discuter selon que l'argument est un a_i ou non), donc est une permutation de $\mathfrak{S}_n$ et l'on peut conclure aux égalités[106]

$$\varphi\,(a_1\ a_2\ ...\ a_\ell)\,\varphi^{-1} = (\varphi\,(a_1)\ \ \varphi\,(a_2)\ \ ...\ \varphi\,(a_\ell)) = (b_1\ b_2\ ...\ b_\ell)\,.$$

Utiliser des générateurs du groupe linéaire

Soit n un naturel. Décrivons les morphismes de $GL_n(\mathbb{C})$ vers un groupe fini.

Soit un tel morphisme et notons g l'ordre du groupe but. Le groupe linéaire étant engendré par les transvections et les dilatations, on s'intéresse aux images de ces dernières. Le groupe but étant d'ordre g, l'image du g-ième itéré de n'importe qui à la source sera neutre (par le "petit" théorème de Lagrange). Vu les égalités $I_n + \lambda E_{i,j} = \left(I_n + \frac{\lambda}{g} E_{i,j}\right)^g$ pour chaque scalaire λ et pour chaques indices $i \neq j$, chaque transvection est envoyée sur le neutre. De même, chaque complexe admettant une racine g-ième, chaque dilatation est une puissance g-ième, donc est également envoyée sur le neutre. Finalement, notre morphisme est trivial.

Le principe ci-dessus est particulièrement efficace lorsque l'on dispose d'une partie génératrice simple, par exemple finie, voire réduite à un seul élément – cas des structures *monogènes*. L'exercice qui suit permet de déterminer les endomorphismes des groupes monogènes, à l'instar de $\mathbb{Z}$ et des $\mathbb{U}_n$ cycliques.

Exercice d'application

Soient n un naturel et G un groupe abélien. *Montrer que :*

a. *les morphismes de $\mathbb{Z}/n$ vers G forment un sous-groupe de $G^{\mathbb{Z}/n}$;*

b. *la partie $G_n := \{g \in G\ ;\ g^n = 1\}$ est un sous-groupe de G ;*

c. *ces deux sous-groupes sont isomorphes.*

En déduire $\mathrm{End}\left(\mathbb{Z}/n\right)$ *et* $\mathrm{End}\,\mathbb{Z}$.

---

a. Nous l'avons déjà fait dans l'exercice § 4.2 (*dual d'un monoïde*), la seule hypothèse que nous eussions utilisée étant que le groupe but $\mathbb{C}^*$ était abélien.

b. G étant abélien, l'élévation à la puissance n est un endomorphisme de G. Son noyau G_n en est donc un sous-groupe.

[106] On a utilisé l'identité $\varphi\,(a\ b\ c\ ...\ z)\,\varphi^{-1} = (\varphi\,(a)\ \ \varphi\,(b)\ \ \varphi\,(c)\ \ ...\ \varphi\,(z))$ valide dans chaque ensemble E pour chaque permutation $\varphi \in \mathsf{S}_E$ et pour chaques éléments distincts $a, b, c, ..., z \in E$.

c. Le groupe $\mathbb{Z}/n$ étant engendré par $\overline{1}$, un morphisme de source $\mathbb{Z}/n$ est entièrement déterminé par l'image de ce générateur. Or ce dernier devient le neutre (de $\mathbb{Z}/n$) après n itérations, donc son image devient le neutre (de G) après n itérations, *i. e.* appartient à G_n.

Réciproquement, étant donné un $g \in G_n$, le morphisme $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ z & \longmapsto & g^z \end{array} \right.$ a un noyau contenant $n\mathbb{Z}$, donc induit un morphisme $\left\{ \begin{array}{ccc} \mathbb{Z}/n & \longrightarrow & G \\ \overline{z} & \longmapsto & g^z \end{array} \right.$.

Il est alors aisé de montrer que la correspondance sus-établie est bijective et est un morphisme de groupes :

$$\left\{ \begin{array}{ccc} \mathrm{Hom}\left(\mathbb{Z}/n, G\right) & \cong & G_n \\ \varphi & \longmapsto & \varphi\left(\overline{1}\right) \\ \overline{z} \mapsto g^z & \longleftarrow | & g \end{array} \right. .$$

Lorsque $G = \mathbb{Z}/n$, on a alors $G_n = G$ et l'isomorphisme ci-dessus se réécrit $\left\{ \begin{array}{ccc} \mathbb{Z}/n & \cong & \mathrm{End}\left(\mathbb{Z}/n\right) \\ g & \mapsto & \overline{z} \mapsto zg = g\overline{z} \end{array} \right.$, ce qui montre (comme pour $\mathbb{Q}$) que les endomorphismes de $\mathbb{Z}/n$ sont ses homothéties. (Pour $n = 0$, on retrouve le cas de $\mathbb{Z}$.)

4.7 Groupes monogènes

Regardons la suite des itérés d'un élément a d'un monoïde : $\begin{array}{c} 1, a, a^2, a^3 ... \\ 0, a, 2a, 3a ... \end{array}$. Se poursuit-elle indéfiniment[107] ? S'arrête-elle ? Boucle-t-elle et, si oui, où ? Le cas des idempotents et des nilpotents (par exemples dans les monoïdes matriciels) montre qu'elle peut stationner à partir de n'importe quel rang. Dans les groupes, ce ne sera pas possible.

On invoque pour toute cette section un groupe G et un élément $g \in G$.

4.7.1 Ordres : définitions & exemples

Définition (ordre d'un élément dans un groupe)

Si l'un des itérés de g vaut le neutre, on appelle ***ordre de*** *g le plus petit naturel*[108] *$n > 0$ tel que $g^n = 1$ (en additif : $ng = 0$). Sinon, ∞ est appelé l'****ordre de*** *g.*

[107] On parle bien sûr de la suite des *termes*, pas de celle des *indices* (qui est celle des naturels $0, 1, 2, 3...$).

[108] Bien observer la comparaison *stricte* $n > 0$: la définition forcerait sinon la nullité de chaque ordre ! Un ordre est donc toujours supérieur à 1.

Notation : dans ce cours, l'ordre d'un élément a sera noté

$$\omega(a) := \begin{cases} \infty \text{ si } \forall n \in \mathbb{N}^*,\ a^n \neq 1 \\ \min\{n \in \mathbb{N}^*\ ;\ a^n = 1\} \text{ sinon} \end{cases} = \inf_{\overline{\mathbb{N}}} \{n \in \mathbb{N}^*\ ;\ a^n = 1\}.$$

L'écriture en termes d'*infimum*[109] est inutile pour le calcul effectif mais pourra raccourcir certaines démonstrations.

Exemples (ordres)

1. Le neutre est l'unique élément d'ordre 1. Les idempotents sont les éléments d'ordre *au plus* 2. Les éléments d'ordre 2 sont donc les idempotents *autres que le neutre*[110].
2. Dans $\mathbb{C}$, chaque élément non nul est d'ordre infini. Dans $\mathbb{R}^*$, chaque réel autre que ± 1 est d'ordre infini. Dans $\mathbb{C}^*$, les ordres respectifs de $-1, j, i$ sont $2, 3, 4$ et les élément d'ordre fini forment la réunion $\bigcup_{k\in\mathbb{N}^*} \mathbb{U}_k$. Dans $\mathbb{H}_8$, les quaternions i, j, k sont chacun d'ordre 4.
3. Soit $n \geq 1$ un naturel. Dans $\mathbb{Z}/n$, la classe $\overline{1}$ est d'ordre n. Dans $\mathbb{U}$, l'ordre de $e^{\frac{2\pi i}{n}}$ vaut n. Dans $\mathfrak{S}_n$, l'ordre d'un cycle vaut sa longueur.
4. Chaque translation est d'ordre infini (sauf si son vecteur est nul). Chaque réflexion est d'ordre 2. Une homothétie est d'ordre ou bien 1 (identité), ou bien 2 (symétrie centrale), ou bien infini.
5. Une rotation plane est d'ordre fini ssi son angle est multiple rationnel de π. Dans ce cas, soient k et n deux relatifs étrangers tels que l'angle vaille $\frac{2k\pi}{n}$: l'ordre vaut alors $|n|$.
6. Pour chaque diviseur $d \mid \omega(g)$, l'élément $g^{\frac{\omega(g)}{d}}$ est d'ordre d.
7. Plus généralement, soit $z \in \mathbb{Z}$ et montrons $\omega(g^z) = \frac{\omega(g)}{\omega(g)\wedge z}$. Abrégeons $\omega := \omega(g)$, $\delta := \omega \wedge z$ et soient $\omega', z' \in \mathbb{Z}$ étrangers tels que $\begin{cases} \omega = \omega'\delta \\ z = z'\delta \end{cases}$. On a alors pour chaque naturel $n > 0$ les équivalences

$$(g^z)^n = 1 \iff g^{zn} = 1 \iff \omega \mid zn \iff \omega' \mid nz' \overset{\text{Gauss}}{\iff} \omega' \mid n,$$

ce qui montre (ω' étant non nul, sinon $\omega = \omega'\delta = 0$) que le plus petit tel n vaut ω'.

Propriétés (ordre d'un inverse, invariant d'isomorphie)

1. *L'ordre de chaque élément est le même que celui de son inverse.*
2. *L'ordre est préservé par isomorphisme.*

Démonstration

[109] *Rappel* : l'*infimum* de la partie vide est le *maximum* de l'ensemble ordonné sous-jacent.

[110] Plus généralement, on distinguera bien soigneusement pour chaque naturel n les propriétés « *être d'ordre n* » et « *avoir le neutre pour n-ième itéré* ».

1. On a pour chaque $n \in \mathbb{N}$ les équivalences $g^n = 1 \iff (g^n)^{-1} = 1^{-1} \iff \left(g^{-1}\right)^n = 1$, d'où l'égalité des parties $\{n \in \mathbb{N}^* \ ; \ g^n = 1\}$ et $\left\{n \in \mathbb{N}^* \ ; \ \left(g^{-1}\right)^n = 1\right\}$, *a fortiori* celle de leurs *infima* dans $\overline{\mathbb{N}}$.
2. Soit $a \mapsto \mathbf{a}$ un isomorphisme. On a alors pour chaque $n \in \mathbb{N}^*$ l'équivalence $g^n = 1 \iff \mathbf{g}^n = \mathbf{1}$, ce qui montre l'égalité des parties $\{n \in \mathbb{N}^* \ ; \ g^n = 1\}$ et $\{n \in \mathbb{N}^* \ ; \ \mathbf{g}^n = \mathbf{1}\}$, *a fortiori* celle de leurs *infima* dans $\overline{\mathbb{N}}$.

Application ($\mathbb{U}_{n^2} \not\simeq \mathbb{U}_n^2$)

Soit n un naturel et demandons : les groupes $\mathbb{U}_{n^2}$ et $\mathbb{U}_n^2$ sont-ils isomorphes ?

L'égalité des cardinaux ne doit pas nous induire en erreur. Remarquons plutôt que chaque élément de $\mathbb{U}_n^2$ devient le neutre après n itérations, donc est d'ordre au plus[111] n. Or le groupe $\mathbb{U}_{n^2}$ contient un élément d'ordre n^2. Une isomorphie $\mathbb{U}_{n^2} \overset{?}{\simeq} \mathbb{U}_n^2$ forcerait donc la comparaison $n^2 \leq n$, *i. e.* l'appartenance $n \in \{0, 1\}$.

Dans le cas $n = 1$, on obtient deux groupes triviaux – qui sont donc isomorphes.

Dans le cas $n = 0$, on demande si $\mathbb{C}^*$ est isomorphe à son carré : or $\mathbb{C}^*$ contient un seul élément d'ordre 2 (le complexe -1) tandis que son carré en contient trois (les couples $(\pm 1, \pm 1)$ privés du neutre), ce qui répond à la question par la négative.

Exercice d'application

Montrer que les groupes $\mathbb{U}_8$, $\mathbb{U}_4 \times \mathbb{U}_2$, $\mathbb{U}_2^3$, $\mathbb{H}_8$ et D_8 (symétries du carré) forment autant de classes d'isomorphie.

Solution méthodique (méticuleuse). Tous ces groupes étant d'ordre 8, on ne peut pas grossièrement éliminer des isomorphies à l'aide de différences cardinales. Comparons plutôt la liste des ordres de leurs éléments, comptés avec multiplicités. Procédons avec méthode :

$\mathbb{U}_8$:

a	1	-1	$\pm i$	$e^{\pm i\frac{\pi}{4}}, e^{\pm i\frac{3\pi}{4}}$
$\omega(a)$	1	2	$4\vert 4$	$8\vert 8\vert 8\vert 8$

,

$\mathbb{U}_4 \times \mathbb{U}_2$:

a	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}\pm 1\\\pm 1\end{pmatrix}$ sauf $\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}\pm i\\\pm 1\end{pmatrix}$
$\omega(a)$	1	$2\vert 2\vert 2$	$4\vert 4\vert 4\vert 4$

,

$\mathbb{U}_2^3$:

a	$(1,1,1)$	les autres
$\omega(a)$	1	$2\vert 2\vert 2\vert 2\vert 2\vert 2\vert 2$

,

$\mathbb{H}_8$:

a	1	-1	$\pm i$	$\pm j$	$\pm k$
$\omega(a)$	1	2	$4\vert 4$	$4\vert 4$	$4\vert 4$

,

D_8 :

a	Id	symétrie centrale	réflexions	rotations d'angle $\pm\frac{\pi}{2}$
$\omega(a)$	1	2	$2\vert 2\vert 2\vert 2$	$4\vert 4$

.

[111] *À ne pas confondre* : « être d'ordre n », « être d'ordre au plus n », « être d'ordre divisant n » et « devenir le neutre après n itérations » (*cf.* toutefois théorème suivant pour l'équivalence des deux derniers).

On obtient ainsi les listes d'ordres suivants (l'exposant marque la multiplicité) :

$\mathbb{U}_8$	$\mathbb{U}_4 \times \mathbb{U}_2$	$\mathbb{U}_2^3$	$\mathbb{H}_8$	D_8
$1\ 2\ 4^2\ 8^4$	$1\ 2^3\ 4^4$	$1\ 2^7$	$1\ 2\ 4^6$	$1\ 2^5\ 4^2$

.

Ces listes étant distinctes et l'ordre d'un élément étant préservé par isomorphisme, on a terminé.

Solution débrouillarde (expéditive). Les produits de $\mathbb{U}_?$ sont abéliens (contrairement à $\mathbb{H}_8$ et D_8), le groupe $\mathbb{U}_8$ contient un élément d'ordre 8 (et pas les autres), tous les éléments de $\mathbb{U}_2^3$ sont involutifs (le seul groupe dans ce cas), enfin D_8 est engendré par deux éléments d'ordres respectifs 2 et 4 (*cf.* exercice 3 § 3.5), ce qui impossible pour $\mathbb{H}_8$ (*cf.* exercice 3 § 4.4).

Remarque – On vient de décrire (à isomorphisme près, il s'entend – et sans preuve) les cinq groupes d'ordre 8.

4.7.2 Ordres & arithmétique

Théorème (ordre et divisibilité)

On a pour chaque relatif z les équivalences

$$g^z = 1 \iff \omega(g) \mid z.$$

Démonstration

Quand g est d'ordre infini, l'équivalence souhaitée est une tautologie de la forme "faux"$\iff$"faux". Supposons donc g d'ordre fini. Itérer g fournit un morphisme surjectif $i := \left\{ \begin{array}{ccc} \mathbb{Z} & \twoheadrightarrow & \langle g \rangle \\ z & \mapsto & g^z \end{array} \right.$ dont le noyau est un sous-groupe de $\mathbb{Z}$, donc vaut $\omega\mathbb{Z}$ pour un certain naturel $\omega > 0$ (le noyau est non nul puisqu'il contient $\omega(g) \geq 1$). On a pour chaque relatif z les équivalences

$$g^z = 1 \iff z \in \operatorname{Ker} i \iff z \in \omega\mathbb{Z} \iff \omega \mid z.$$

Il suffit pour conclure de montrer $\omega = \omega(g)$. Vu l'égalité $g^{\omega(g)} = 1$, on déduit des équivalences ci-dessus la divisibilité $\omega \mid \omega(g)$, d'où la comparaison $\omega \leq \omega(g)$, l'égalité voulue tombant alors en vertu de la minimalité de $\omega(g)$ et de l'égalité $g^\omega = 1$ (définition du noyau de i).

Théorème – Définition (groupes cycliques)

Chaque groupe monogène est :

1. *ou bien* ***cyclique*** *(*i. e. *isomorphe à $\mathbb{U}_n$ pour un certain $n \in \mathbb{N}^*$);*
2. *ou bien isomorphe à $\mathbb{Z}$.*

Explicitement, le caractère générateur de g induirait un isomorphisme[112]

$$\left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{\omega(g)} & \xrightarrow{\sim} & \langle g \rangle \\ \overline{z} & \longmapsto & g^z \end{array} \right. .$$

Démonstration

Imposons G monogène engendré par g. Reprenons le morphisme d'itération de g. Si les itérés de g sont deux à deux distincts (*i. e.* si g est d'ordre infini), alors ce morphisme (surjectif) est injectif, donc est un isomorphisme $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$. Sinon, il induit en quotientant par son noyau $\omega(g)\,\mathbb{Z}$ l'isomorphisme annoncé.

Remarque – En corollaire immédiat :

chaque groupe monogène est abélien.

Corollaire (ordre et ordre)

Dans chaque groupe, l'ordre de chaque élément vaut l'ordre du sous-groupe qu'il engendre :

$$\omega(g) = \operatorname{Card} \langle g \rangle .$$

Démonstration

L'isomorphisme précédent fournit une bijection $\langle g \rangle \xrightarrow{\sim} \mathbb{U}_{\omega(g)}$, d'où les égalités $\operatorname{Card} \langle g \rangle = \operatorname{Card} \mathbb{U}_{\omega(g)} = \omega(g)$.

Corollaire ("petit" théorème de Lagrange)

Lorsque G est fini, on a $g^{|G|} = 1$ (en additif : $|G|\, g = 0$). En d'autres termes,

l'ordre de chaque élément divise l'ordre du groupe.

Démonstration

Appliquer le théorème de Lagrange (*cf.* fin de § 3.4.3) au sous-groupe $\langle g \rangle$ donne $\operatorname{Card} \langle g \rangle \mid \operatorname{Card} G$, *i. e.* $\omega(g) \mid \operatorname{Card} G$, ou encore $g^{\operatorname{Card} G} = 1$. (Le cas abélien a été traité § 2.4).

Corollaire (groupes d'ordre premier)

Chaque groupe d'ordre premier est cyclique.

Démonstration

Soit p un premier, soit G un groupe d'ordre p. Puisque $p \geq 2$, on peut invoquer un élément g dans $G \setminus \{1\}$, qui n'est alors pas d'ordre 1. Or cet ordre divise $|G| = p$, donc vaut p. L'inclusion $\langle g \rangle \subset G$ devient alors une égalité vu les cardinaux.

Le théorème suivant permet d'élucider la structure d'un produit de groupes cycliques d'ordres *étrangers*.

[112] Observer pour la cohérence l'isomorphie ${}^{\mathbb{Z}}\!/_{0} \cong \mathbb{Z}$ (explicitement, un relatif z est en correspondance avec sa classe-singleton $\overline{z} = \{z\}$).

Théorème (lemme chinois)

Soient a et b deux naturels étrangers. Est alors un isomorphisme de groupes

$$\left\{\begin{array}{ccc} {}^{\mathbb{Z}}\!/_{ab} & \cong & {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbb{Z}}\!/_{b} \\ \overline{z} & \longmapsto & (\widetilde{z},\widehat{z}) \\ \overline{(b\mu)\,k+(a\lambda)\,\ell} & \longleftarrow\mid & \left(\widetilde{k},\widehat{\ell}\right) \end{array}\right.$$

où $\binom{\lambda}{\mu}$ *sont deux relatifs (donnés par* Bézout*) tels que* $\lambda a+\mu b=1$.

Démonstration

Notons C (comme "**c**hinois") l'isomorphisme $\overline{z}\mapsto(\widetilde{z},\widehat{z})$ établi § 4.5 et D l'application prétendue réciproque dans l'énoncé. Pour prouver les réciprocités relatives de C et D, on vérifie d'une part pour chaque relatif z les égalités

$$\overline{z}\overset{C}{\mapsto}(\widetilde{z},\widehat{z})\overset{D}{\mapsto}\overline{b\mu z+a\lambda z}=\overline{(a\lambda+b\mu)\,z}=\overline{1z}=\overline{z},$$

d'autre part pour chaques relatifs k,ℓ les égalités

$$\binom{\widetilde{k}}{\widehat{\ell}}\overset{D}{\mapsto}\overline{\underbrace{(b\mu)}_{=1-\lambda a}\,k+\underbrace{(a\lambda)}_{=1-\mu b}\,\ell}\overset{C}{\mapsto}\binom{\widetilde{k-(\lambda\widehat{k})\,a+(\lambda\ell)\,a}}{\widehat{(\mu k)\,b+\ell-(\mu\ell)\,b}}=\binom{\widetilde{k}}{\widehat{\ell}}.$$

Remarque – Le théorème est ainsi nommé car il permet de résoudre des conjonctions d'égalités modulaires (également appelées *systèmes de congruences arithmétiques*), à l'instar (si l'on cherche par exemple les vendredi treize sur une planète dont les mois feraient trente jours) de $\left\{\begin{array}{l} x=5 \mod 7 \\ x=13 \mod 30 \end{array}\right.$ d'inconnue x, dont on trouve des traces dans des manuscrits chinois[113] – évidemment dans un langage non moderne.

Exemple : dans la remarque précédente, il s'agit de trouver un antécédent de $\left(\widetilde{5},\widehat{13}\right)$. Vu l'identité de Bézout $13\cdot 7+(-3)\cdot 30=1$, un antécédent (*modulo* $7\cdot 30=210$) sera

$$30\cdot(-3)\cdot 5+7\cdot(13)\cdot 13=-450+1183=733=103\overset{\text{sanity}}{\underset{\text{check}}{=}}\begin{array}{l} 5\ (+14\cdot 7) \\ 13\ (+3\cdot 30) \end{array}.$$

Exercices d'application

1. *Déterminer les sous-groupes finis de* $\mathbb{C}^*$. *En déduire qu'est cyclique chaque sous-groupe de chaque groupe cyclique.*

[113] Un tel problème apparaît dans le *Classique mathématique de Maître Sun* écrit entre les III$^{\text{e}}$ et V$^{\text{e}}$ siècles. Une exposition méthodique de résolution devra attendre le XIII$^{\text{e}}$ siècle avec la publication en 1247 des *Neuf chapitres d'écrits sur le calcul* de Qin Jiushao.

2. *Montrer que l'ordre du produit de deux éléments commutant et d'ordres étrangers vaut le produit de ces ordres.*

---

1. Soit S un tel sous-groupe, notons $n := |S|$. Le petit Lagrange nous dit alors que chaque élément de S devient le neutre après n itérations, d'où l'inclusion $S \subset \mathbb{U}_n$ qui est une égalité vu les cardinaux. Réciproquement, on sait que les $\mathbb{U}_a$ pour a parcourant $\mathbb{N}^*$ sont des sous-groupes finis de $\mathbb{C}^*$.

   Soit C un groupe cyclique, soit S un sous-groupe de C. Soit φ un isomorphisme $C \simeq \mathbb{U}_c$ où $c := |C|$. Alors $\varphi(S)$ est un sous-groupe fini de $\varphi(C) = \mathbb{U}_c$, donc de $\mathbb{C}^*$, donc vaut $\mathbb{U}_s$ avec $s := |\varphi(S)| = |S|$, d'où la cyclicité de S (isomorphe à $\mathbb{U}_s$ *via* φ).

2. Soient a et b qui commutent et d'ordres respectifs α et β étrangers. Notons ω l'ordre de ab. Puisque a et b commutent, on peut développer la puissance $(ab)^{\alpha\beta} = (a^\alpha)^\beta \left(b^\beta\right)^\alpha = 1^\beta 1^\alpha = 1$, d'où la divisibilité $\omega \mid \alpha\beta$. Élever par ailleurs l'égalité $1 = (ab)^\omega$ à la puissance β donne $1 = a^{\omega\beta} \left(b^\beta\right)^\omega = a^{\omega\beta}$, d'où la divisibilité $\alpha \mid \omega\beta$; l'hypothèse d'extranétité et le théorème de Gauss donnent alors $\alpha \mid \omega$. On montrerait de même $\beta \mid \omega$, d'où (toujours par extranéité) la divisibilité $\alpha\beta \mid \omega$ et la conclusion $\omega = \alpha\beta$.

   Remarque – Sans les deux hypothèses, on se convaincra en composant deux réflexions d'axes sécants que l'ordre d'un produit peut prendre n'importe quelle valeur, finie comme infinie.

---

5 Le point des compétences

Formulaire

1. Généralités

• Un ***groupe*** est un quadruplet $(G, *, \varepsilon, i)$ où :

1. $*$ est une application $G^2 \longrightarrow G$ (sa ***loi***) telle que $\forall a, b, c \in G,\ a * (b * c) = (a * b) * c$;
2. ε est un élément de G (son ***neutre***) tel que $\forall g \in G,\ \begin{cases} g * \varepsilon = g \\ \varepsilon * g = g \end{cases}$;
3. i est une application $G \longrightarrow G$ (son ***inversion***) telle que $\forall g \in G,\ \begin{cases} g * i(g) = \varepsilon \\ i(g) * g = \varepsilon \end{cases}$.

• Un groupe est ***abélien*** (ou ***commutatif***) si deux quelconques de ses éléments commutent :

$$G \text{ abélien} \overset{\text{déf.}}{\iff} \forall a, b \in G,\ ab = ba.$$

• L'***ordre*** d'un groupe est son cardinal.

• *Exemples* : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (additifs), $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{U}$ et les $\mathbb{U}_n$ (multiplicatifs), les groupes symétriques $\mathfrak{S}_n$ (pour la composition), les groupes de symétries de figures géométriques, les groupes triviaux (singletons).

2. Création de groupes

• **Groupe produit** : chaque produit cartésien de groupes est un groupe pour la loi "coordonnée par coordonnée"

$$\begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_\ell \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_\ell \end{pmatrix} = \begin{pmatrix} g_1 h_1 \\ g_2 h_2 \\ \vdots \\ g_\ell h_\ell \end{pmatrix} \qquad \text{et} \qquad (g_i)_{i \in I} (h_i)_{i \in I} = (g_i h_i)_{i \in I}.$$

• Un ***sous-groupe*** est une partie qui est un groupe pour la loi induite. Une partie est un sous-groupe ssi elle contient le neutre, est stable par la loi et est stable par l'inversion :

$$S \text{ sous-groupe de } G \iff \begin{cases} \boxed{1 \in S} \text{ (à ne pas oublier !)} \\ \forall s, t \in S,\ \begin{cases} st \in S \\ s^{-1} \in S \end{cases} \end{cases} \implies S \text{ groupe pour la loi de } G.$$

• Chaque intersection de sous-groupes reste un sous-groupe :

$$(\forall i \in I,\ S_i \text{ sous-groupe de } G) \implies \bigcap_{i \in I} S_i \text{ sous-groupe de } G.$$

• Soit G un groupe et soit $A \subset G$. Le ***sous-groupe engendré*** par la partie A est le plus petit (pour l'ordre d'inclusion) sous-groupe de G contenant cette partie.

Explicitement, il est formé des produits d'éléments et d'inverses d'éléments de A – le produit vide étant le neutre.

$$\langle A\rangle = \bigcap_{S\supset A}^{S \text{ sous-groupe}} A = \left\{ \prod_{i=1}^{n} a_i^{\varepsilon_i} \ ; \quad \begin{array}{c} n\in\mathbb{N} \\ a\in A^n \\ \varepsilon\in\{\pm 1\}^n \end{array} \right\}.$$

- Un groupe est ***monogène*** s'il est engendré par un élément :

$$G \text{ monogène} \overset{\text{déf.}}{\iff} \exists g\in G,\ G=\langle g\rangle\,.$$

- Chaque sous-groupe de $\mathbb{Z}$ est monogène, ces sous-groupes sont les $n\mathbb{Z}$ pour n parcourant $\mathbb{N}$:

$$S \text{ sous-groupe de } \mathbb{Z} \iff \exists n\in\mathbb{N},\ S=n\mathbb{Z}.$$

3. Homorphismes de groupes

- Un ***morphisme de groupes*** est une application entres groupes qui préserve la loi (« l'image d'un composé est le composé des images »).

$$f: G\longrightarrow H \text{ morphisme de groupes} \iff \left\{ \begin{array}{l} G \text{ et } H \text{ groupes} \\ \forall a,b\in G,\ f(ab)=f(a)\,f(b) \end{array} \right. .$$

- Chaque morphisme de groupes préserve le neutre ainsi que l'inversion :

$$f: G\longrightarrow H \text{ morphisme de groupes} \Longrightarrow \left\{ \begin{array}{l} f(1_G)=1_H \\ \forall a\in G,\ f\left(a^{-1}\right)=f(a)^{-1} \end{array} \right.$$

- *Exemples* : la signature et le déterminant sont des morphismes de groupes.

- L'image directe de chaque sous-groupe (resp. l'image réciproque de chaque sous-groupe) est un sous-groupe :

$$\text{si } f: G\longrightarrow H \text{ morphisme de groupes, } \left\{ \begin{array}{l} S \text{ sous-groupe de } G \\ T \text{ sous-groupe de } H \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} f(S) \text{ sous-groupe de } H \\ f^{-1}(T) \text{ sous-groupe de } G \end{array} \right. .$$

- Le ***noyau*** d'un morphisme de groupes est le sous-groupe formé des éléments envoyés sur le neutre. Chaque morphisme de groupes est injectif ssi son noyau vaut le singleton neutre :

$$\text{si } f: G\longrightarrow H \text{ morphisme de groupes, alors } \left\{ \begin{array}{l} \operatorname{Ker} f=\{a\in G\ ;\ f(a)=1\} \\ f \text{ injectif} \iff \operatorname{Ker} f=\{1\} \end{array} \right. .$$

- Un ***isomorphisme de groupes*** est un morphisme de groupes bijectif. La réciproque de chaque isomorphisme de groupes reste un isomorphisme de groupes :

$$f \text{ isomorphisme de groupes} \iff \left\{ \begin{array}{l} f \text{ morphisme de groupes} \\ f \text{ bijection} \end{array} \right. \Longrightarrow f^{-1} \text{ isomorphisme de groupes.}$$

4. Groupes cycliques, ordres

• Un groupe ***cyclique*** est un groupe isomorphe à $\mathbb{U}_n$ pour un certain naturel n non nul :

$$G \text{ cyclique} \Longleftrightarrow G \text{ isomorphe à } \mathbb{U}_{\operatorname{Card} G}.$$

• **Groupe quotient** : soit $n \in \mathbb{N}$.

L'ensemble des $\overline{a} := a + n\mathbb{Z}$ (***classes* modulo** n) pour a décrivant $\mathbb{Z}$ est un groupe pour la loi "parties". Ce groupe est noté ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ ou ${}^{\mathbb{Z}}\!/_{(n)}$ ou

$${}^{\mathbb{Z}}\!/_{n} := \left\{\overline{a}\ ;\ a \in \mathbb{Z}\right\}.$$

Il est d'ordre

$$\operatorname{Card}\left({}^{\mathbb{Z}}\!/_{n}\right) = \begin{cases} n \text{ si } n > 0 \\ \infty \text{ si } n = 0 \end{cases}.$$

Il est monogène, ses générateurs sont les classes d'entiers premiers avec n :

$$\forall z \in \mathbb{Z},\ {}^{\mathbb{Z}}\!/_{n} = \langle z \rangle \Longleftrightarrow z \wedge n = 1.$$

La projection canonique $a \mapsto \overline{a}$ est un morphisme de groupes :

$$\forall a, b \in \mathbb{Z},\ \overline{a} + \overline{b} = \overline{a + b}.$$

• Chaque groupe monogène est ou bien cyclique (s'il est fini) ou bien isomorphe à $\mathbb{Z}$ (s'il est infini) :

$$G \text{ monogène} \Longrightarrow G \text{ isomorphe à } \begin{cases} \mathbb{U}_{\operatorname{Card} G} \text{ si } G \text{ fini} \\ \mathbb{Z} \text{ sinon} \end{cases}.$$

• L'***ordre*** d'un élément g est ou bien le plus petit naturel n non nul tel que le n-itéré de g vaut le neutre (s'il existe un tel n) ou bien ∞ (s'il n'en existe pas) :

$$\text{ordre de } g = \begin{cases} \infty \text{ si } \forall n \in \mathbb{N}^*,\ g^n \neq 1 \\ \min\left\{n \in \mathbb{N}^*\ ;\ g^n = 1\right\} \text{ sinon} \end{cases}.$$

L'ordre de chaque élément vaut l'ordre du sous-groupe qu'il engendre :

$$\omega(g) = \operatorname{Card}\langle g \rangle.$$

• Pour chaque relatif z, le z-ième itéré d'un élément vaut le neutre ssi z est multiple de l'ordre de cet élément :

$$\forall g \in G,\ g^z = 1 \Longleftrightarrow \omega(g) \mid z.$$

• Dans chaque groupe fini, l'ordre de chaque élément divise l'ordre du groupe (à savoir démontrer dans un groupe abélien) :

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

Exercices d'entraînement

1. ★
   (a) *Montrer qu'un groupe est abélien ssi sa loi (resp. son inversion) est un morphisme de groupes.*
   (b) *Soit G un groupe. Montrer que les éléments d'ordre fini du centre $Z(G)$ forment un sous-groupe de $Z(G)$. Que dire si l'on remplace le centre $Z(G)$ par le groupe plein G ?*
   (c) *Le complémentaire d'un sous-groupe reste-t-il un sous-groupe ? Déterminer le sous-groupe qu'il engendre.*

2. ★
   (a) *Lesquels parmi les groupes additifs $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{Z}^2$ sont isomorphes ?*
   (b) *Montrer que $\mathbb{H}_8$ est indécomposable.*
   (c) *Regrouper selon leur classe d'isomorphie les groupes $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{R}_+^*$, $\mathbb{C}$, $\mathbb{C}^*$, $\mathbb{H}$ et $\mathbb{H}^*$ (on admettra l'isomorphie de groupes $\mathbb{R} \simeq \mathbb{C}$).*

3. ★*Soient a et b deux naturels.*
   (a) *Calculer le sous-groupe $\mathbb{U}_a \cap \mathbb{U}_b$.*
   (b) *Montrer que $\mathbb{U}_a$ est un sous-groupe de $\mathbb{U}_b$ ssi a divise b.*

4. ★*Soit G un sous-groupe fini d'un groupe linéaire. Soit $g \in G$. Montrer que g commute avec (chaque élément de) G ssi $g = \frac{1}{|G|}\sum_{\gamma\in G} \gamma g \gamma^{-1}$.*

5. ★★*Montrer que les sous-groupes de $\mathbb{U}$ autres que les $\mathbb{U}_n$ sont denses dans le cercle unité.*

6. ★★*Soit G un groupe. Montrer que les morphismes de G vers $\mathbb{C}^*$ forment une partie libre dans l'espace vectoriel $\mathbb{C}^G$.*

7. ★★*Soit G un groupe fini muni d'un automorphisme involutif ne fixant que le neutre. On invoque une telle involution et on la nomme i.*
   (a) *Montrer que l'application $\left\{ \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1}i(g) \end{array} \right.$ est injective, puis surjective.*
   (b) *En déduire que i est l'inversion de G.*
   (c) *Montrer que G est abélien puis que l'ordre de G est impair.*
   Soit réciproquement Γ un groupe fini abélien d'ordre impair.
   (d) *Exhiber un automorphisme involutif de Γ qui ne fixe que son neutre.*

8. ★★★*On appelle **exposant** d'un groupe le p. p. c. m. des ordres de ses éléments (qui peut être infini). Soit G un groupe abélien fini. Montrer que G contient un élément d'ordre l'exposant de G.*

9. ★★★*Caractériser les paires de groupes dont le produit est cyclique.*

10. ★★★*Soit G un groupe fini, soit A une partie non vide de G. Pour chaque naturel n, on note A^n le n-ième itéré de A pour la loi "parties". Montrer que $A^{|G|}$ est un sous-groupe de G. (On pourra étudier la suite des $|A^n|$.)*

Solutions des exercices d'entraînement

1.

(a) Notons m l'application $\left\{\begin{array}{ccc} G^2 & \longrightarrow & G \\ (a,b) & \longmapsto & ab \end{array}\right.$. On a alors les équivalences

$$\begin{array}{rcl} m \text{ est un morphisme} & \iff & \forall a,b,\alpha,\beta \in G^4,\ m\left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}\right) = m\begin{pmatrix} a \\ b \end{pmatrix} m\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ & \iff & \forall a,b,\alpha,\beta \in G^4,\ m\begin{pmatrix} a\alpha \\ b\beta \end{pmatrix} = ab\ \alpha\beta \\ & \iff & \forall a,b,\alpha,\beta \in G^4,\ a\alpha b\beta = ab\alpha\beta \\ & \overset{\text{simplification par } a \text{ et par } \beta}{\iff} & \forall a,b,\alpha,\beta \in G^4,\ \alpha b = b\alpha \\ & \iff & \forall b,\alpha \in G^2,\ \alpha b = b\alpha \\ & \iff & G \text{ est abélien, } \textit{c. q. f. d.}. \end{array}$$

L'inversion $i : g \mapsto g^{-1}$ est une involution, donc une bijection de G sur G. On demande donc de montrer qu'elle est un morphisme (de groupes) ssi G est abélien. Or, se rappelant (*cf.* cours) les égalités $i(g\gamma) = i(\gamma)\, i(g)$ (valides pour chaques $g, \gamma \in G$), on a les équivalences

$$\begin{array}{rcl} G \text{ est abélien} & \iff & \forall a,b \in G,\ ab = ba \\ & \overset{i \text{ injectif}}{\iff} & \forall a,b \in G,\ i(ab) = i(ba) \\ & \iff & \forall a,b \in G,\ i(b)\, i(a) = i(ba) \\ & \iff & i \text{ est un morphisme, } \textit{c. q. f. d.}. \end{array}$$

(b) Le neutre est d'ordre 1 et appartient au centre. Soient g et h d'ordre fini dans $Z(G)$. En notant $\begin{pmatrix} a \\ b \end{pmatrix} := \begin{pmatrix} \omega(g) \\ \omega(h) \end{pmatrix}$, la commutativité des itérés de a et b permet de réécrire $(gh)^{ab} = \left(g^a\right)^b \left(h^b\right)^a = 1^b 1^a = 1$, ce qui montre que gh est d'ordre fini. L'inverse g^{-1} a par ailleurs même ordre que g, donc est d'ordre fini.

Remarque – Nous retrouvons ainsi que $\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.

Sans la commutativité, la stabilité par composition tombe en défaut, comme nous l'avons déjà relevé dans le cours en composant deux réflexions.

(c) Un sous-groupe contenant toujours le neutre, son complémentaire ne peut être un sous-groupe.

Soit S un sous-groupe. L'intuition vectorielle où S est une droite dans un plan nous permet d'intuiter que ${}^cS$ engendre le groupe plein – sauf si S vaut déjà ce dernier, auquel cas son complémentaire, vide, engendre le sous-groupe neutre.

Puisque $\langle {}^cS \rangle$ contient déjà ${}^cS$, il suffit de montrer qu'il contient aussi S. Soit donc $s \in S$. Lorsque S n'est pas tout le groupe, on peut invoquer

un élément a hors de S : alors sa et a^{-1} tombent hors de S (sinon le composé $s^{-1}(sa)$ ou l'inverse $\left(a^{-1}\right)^{-1}$ resterait dedans puisque S est un sous-groupe), donc $\langle {}^{c}S\rangle$ contient le composé $(sa)\,a^{-1} = s$, ce qui conclut.

2.

(a) Le groupe $\mathbb{R}$ est indénombrable, contrairement aux autres. Le groupe $\mathbb{Q}$ est divisible par 2, au sens où chaque rationnel est un double, ce qui n'est pas le cas des puissances de $\mathbb{Z}$ (considérer un vecteur dont chaque coordonnée vaut 1). $\mathbb{Z}$ est monogène contrairement à son carré (*cf.* exercice 1 § 3.5). Les groupes donnés sont donc deux à deux non isomorphes.

(b) D'après l'exercice 2 § 4.4, un groupe décomposable est isomorphe à deux de ses sous-groupes stricts. Listons donc ces derniers pour $\mathbb{H}_8$: il y a $\mathbb{U}_1$, $\mathbb{U}_2$, $\mathbb{U}_4$ et ses analogues en remplaçant i par j ou k (si un sous-groupe contient deux éléments parmi i, j, k, il contiendra le troisième et donc l'engendré $\langle i, j, k\rangle = \mathbb{H}_8$). Tous sont abéliens, donc chaque produit de deux d'entre eux aussi, ce qui n'est pas le cas de $\mathbb{H}_8$.

(c) Les groupes $\mathbb{R}$ et $\mathbb{R}_+^*$ sont isomorphes *via* l'exponentielle (ou le logarithme naturel). Dans chaque groupe multiplicatif (sauf $\mathbb{R}_+^*$), l'élément -1 est d'ordre 2 mais aucun groupe additif ne contient de tel élément (chacun d'ordre 1 ou ∞). Les groupes rationnels sont dénombrables, contrairement aux autres. Les groupes quaternioniques ne sont pas abéliens, contrairement aux autres. Le groupe $\mathbb{C}^*$ contient des éléments de chaque ordre fini mais pas $\mathbb{R}^*$: pour chaque naturel $n \geq 1$, le complexe $e^{\frac{2\pi i}{n}}$ est d'ordre n mais le binôme $X^n - 1$ n'a qu'au plus deux racines réelles, 1 et -1, d'ordres respectifs 1 et 2. Finalement, à l'exception de $\mathbb{R}_+^* \overset{\ln}{\cong} \mathbb{R} \simeq \mathbb{C}$, chaque groupe est seul dans sa classe d'isomorphie.

REMARQUE (très hors programme) – Toutes les puissances (entières non nulles) du groupe additif $\mathbb{R}$ sont isomorphes. En effet, $\mathbb{R}$ étant indénombrable, sa $\mathbb{Q}$-dimension[114] est infinie, d'où pour chaque naturel $n \geq 1$ les égalités[115] $\dim_{\mathbb{Q}} \mathbb{R}^n = n \dim_{\mathbb{Q}} \mathbb{R} = \dim_{\mathbb{Q}} \mathbb{R}$, montrant l'isomorphie $\mathbb{R}^n \simeq \mathbb{R}$ en tant que $\mathbb{Q}$-espaces vectoriels (on retrouve $\mathbb{C}$ quand $n = 2$), *a fortiori* en tant que groupes additifs.

3. Une observation fort utile : pour chaque naturel $n \geq 1$ la description

$$\mathbb{U}_n = \{u \in \mathbb{U}\ ;\ u^n = 1\} = \{u \in \mathbb{U}\ ;\ \omega(u) \mid n\}.$$

(a) On a pour chaque $u \in \mathbb{U}$ les équivalences.

$$u \in \mathbb{U}_a \cap \mathbb{U}_b \iff \left\{ \begin{array}{l} u \in \mathbb{U}_a \\ u \in \mathbb{U}_b \end{array} \right. \iff \left\{ \begin{array}{l} \omega(u) \mid a \\ \omega(u) \mid b \end{array} \right. \iff \omega(u) \mid a \wedge b \iff u \in \mathbb{U}_{a \wedge b}.$$

(b) Puisque $\mathbb{U}_a$ est un sous-groupe de $\mathbb{U}$, il contient le même neutre que $\mathbb{U}_b$ (le complexe 1) et est stable par multiplication et par inversion, donc sera un sous-groupe de $\mathbb{U}_b$ ssi il en est une *partie*. Or un sous-groupe en contient

[114] L'axiome du choix – *cf.* annexe – est implicitement utilisé pour invoquer des $\mathbb{Q}$-bases et pour pouvoir parler de $\mathbb{Q}$-dimensions ; c'est pourquoi les isomorphismes trouvés demeurent "intangibles".
[115] On a utilisé l'arithmétique très simple et très hors programme des cardinaux infinis.

un autre ssi il en contient une partie génératrice. On peut alors conclure avec les équivalences

$$\mathbb{U}_a \subset \mathbb{U}_b \iff \left\langle e^{\frac{2\pi i}{a}} \right\rangle \subset \mathbb{U}_b \iff e^{\frac{2\pi i}{a}} \in \mathbb{U}_b \iff \omega\left(e^{\frac{2\pi i}{a}}\right) \mid b \iff a \mid b.$$

4. Une observation triviale et vitale : l'équivalence $g\gamma = \gamma g \iff g = \gamma g \gamma^{-1}$ pour chaque $\gamma \in G$. Ainsi tombe le sens direct où la sommande vaut constamment g. Supposons à présent que g vaut la moyenne de ses conjugués. On a alors, pour chaque $h \in G$, les égalités

$$|G|\, hgh^{-1} = h\left(\sum_{\gamma\in G} \gamma g \gamma^{-1}\right) h^{-1} = \sum_{\gamma\in G} (h\gamma)\, g\, (h\gamma)^{-1} \overset{\text{reparamétrage}}{\underset{c:=h\gamma}{=}} \sum_{c\in hG=G} cgc^{-1} = |G|\, g,$$

d'où l'on tire la conclusion $gh = hg$.

Remarque – Commuter avec quelqu'un, c'est être invariant par la conjugaison par ce dernier. En ce sens, l'égalité de l'énoncé "moyenne" les énoncés « g commute avec γ » et l'exercice montre qu'un élément commute avec chaque ssi il commute *en moyenne* avec tous.

5. Notons s le morphisme surjectif $\left\{ \begin{array}{ccc} \mathbb{R} & \twoheadrightarrow & \mathbb{U} \\ t & \mapsto & e^{it} \end{array} \right.$. Soit H un sous-groupe de $\mathbb{U}$. Notons $G := \varphi^{-1}(H)$. Puisque s est surjective, le groupe H est l'image directe $\varphi(G)$ de son image réciproque. Puisque s est un morphisme, l'image réciproque du sous-groupe H est un sous-groupe de $\mathbb{R}$, donc est ou bien dense dans $\mathbb{R}$, ou bien discrète. Dans le premier cas, l'image H par l'application continue s est dense dans $s(\mathbb{R}) = \mathbb{U}$. Supposons donc le second cas, mettons $G = a\mathbb{Z}$ pour un certain réel $a > 0$. On en déduit une description de $H = s(G) = s(\langle a\rangle) = \langle s(a)\rangle = \langle e^{ia}\rangle$. Si a est un multiple rationnel de π, en notant d le dénominateur réduit du rationnel $\frac{a}{2\pi}$, on aura $\langle e^{ia}\rangle = \left\langle e^{2\pi i \frac{1}{d}} \right\rangle = \mathbb{U}_d$. Dans le cas contraire, le sous-groupe $a\mathbb{Z} + 2\pi\mathbb{Z}$ sera dense dans $\mathbb{R}$, donc son image sera (toujours par continuité de s) dense dans $\mathbb{U}$; or cette image vaut $s(\langle a, 2\pi\rangle) = \langle s(a), s(2\pi)\rangle = \langle s(a)\rangle = H$, ce qui conclut.

6. La liaison de $\mathrm{Hom}(M, \mathbb{C}^*)$ dans $\mathbb{C}^M$ revient à la liaison d'une de ses parties *finies*, c'est-à-dire à la non-vacuité de l'ensemble des cardinaux de ces parties, ou encore à donner sens au *plus petit* tel cardinal. Raisonner par l'absurde permet donc (et on le fait) d'invoquer une telle partie finie de cardinal minimum : appelons-la Φ.

Soit alors $\lambda \in \mathbb{C}^{*\Phi}$ tel que $\sum_{\varphi\in\Phi} \lambda_\varphi \varphi = 0$ (on peut bien imposer chaque λ_φ non nul par minimalité de $\mathrm{Card}\,\Phi$). Soient $\psi \in \Phi$ et $m \in M$. On a alors dans $\mathbb{C}^M$

$$\begin{aligned} \text{d'une part } 0 &= \left[\sum_{\varphi\in\Phi} \lambda_\varphi \varphi\right] \circ (m\,\mathrm{Id}) \overset{\substack{\text{chaque } \varphi \text{ est} \\ \text{un morphisme}}}{=} \sum_{\varphi\in\Phi} \lambda_\varphi \varphi(m)\, \varphi, \\ \text{d'autre part } 0 &= \psi(m)\, 0 = \psi(m) \sum_{\varphi\in\Phi} \lambda_\varphi \varphi = \sum_{\varphi\in\Phi} \lambda_\varphi \psi(m)\, \varphi, \end{aligned}$$

d'où par différence la nullité de la combinaison linéaire $\sum_{\varphi\in\Phi} [\psi - \varphi](m)\, \lambda_\varphi \varphi$. Puisque le ψ-ième coefficient est nul, la minimalité de Φ impose la nullité de

chaque coefficient $[\psi - \varphi](m)\,\lambda_\varphi$, d'où (simplifiant par λ_φ) l'égalité $\psi(m) = \varphi(m)$ pour chaque φ. Cela tenant pour chaque m, la famille Φ est le singleton $\{\psi\}$ mais alors la relation de liaison initiale se réécrit $\lambda_\psi \psi = 0$, d'où la nullité de ψ qui, du coup, ne peut plus prendre ses valeurs dans $\mathbb{C}^*$.

7.

(a) Appelons f l'application donnée (elle est bien définie car, à $g \in G$ fixé, les éléments g^{-1} et $i(g)$ font sens et tombent dans G – *a fortiori* leur produit). On a alors pour chaques $a, b \in G$ les implications

$$\begin{aligned} f(a) = f(b) &\implies a^{-1} i(a) = b^{-1} i(b) \overset{\substack{i \text{ est un} \\ \text{morphisme}}}{\implies} i\left(ab^{-1}\right) = ab^{-1} \\ &\implies ab^{-1} \in \operatorname{Fix} i \implies ab^{-1} = 1 \implies a = b. \end{aligned}$$

Puisque les ensembles source et but de f sont de même cardinal fini, l'injectivité de f implique sa surjectivité.

(b) Soit $g \in G$. Soit a un antécédent de g par f. On a alors les égalités

$$i(g) = i(f(a)) = i\left(a^{-1} i(a)\right) = i(a)^{-1} \underbrace{i^2(a)}_{=\mathrm{Id}(a)=a} = \left(a^{-1} i(a)\right)^{-1} = f(a)^{-1} = g^{-1}.$$

(c) L'inversion i est un morphisme, donc (*cf.* exercice 1) G est abélien.

L'involution i partitionne G en paires de la forme $\{g, i(g)\}$, lesquelles sont de cardinal 1 ou 2, le cas du singleton ayant lieu ssi $g = i(g)$, *i. e.* ssi $g = \operatorname{Fix} i$ ou encore ssi $g = 1$. Il y a donc une seule paire réduite à un singleton, les autres étant chacune de cardinal 2. Additionner ces cardinaux donne un ordre impair pour G.

(d) Les questions précédentes montrent qu'un tel automorphisme vaut nécessairement l'inversion. Montrons que cette dernière, notée I, répond à la question. C'est clairement une involution et c'est un morphisme d'après l'exercice 1. Soit enfin $\gamma \in \operatorname{Fix} I$. Puisque $\gamma^2 = 1$, l'ordre de γ vaut 1 ou 2 ; or cet ordre divise celui de Γ, qui est impair, donc ne saurait être 2. On a par conséquent l'inclusion $\operatorname{Fix} I \subset \{1\}$, l'inclusion $\supset$ étant immédiate.

8. Comme dans tous les problèmes de groupes finis, c'est la décomposition du cardinal de notre groupe qui contient la « complexité » du groupe :

$$|G| = \prod p_i^{\alpha_i}.$$

L'énoncé demande de trouver un élément g_0 de G dont l'ordre est multiple de l'ordre de chaque autre élément. Puisque l'ordre de chaque élément de G divise l'ordre de G et est donc de la forme $\prod p_i^{\gamma_i}$, les puissances γ_i du g_0 que l'on cherche doivent être plus grandes que le γ_i de chaque élément de G. D'où l'idée de considérer, pour chaque i, parmi les éléments d'ordre une puissance de p_i (il y a toujours au moins le neutre), un élément g_i tel que cette puissance soit maximale, disons $\omega(g_i) = p^{\beta_i}$. Un exercice du cours (*cf.* § 4.7.2) assure alors que le produit $g_0 := \prod g_i$ est d'ordre $\prod p^{\beta_i}$.

Vérifions que tout ce passe comme on le souhaite. Soit $g \in G$ dont on note $\prod p_i^{\gamma_i}$ l'ordre. Alors, à i fixé, l'élément g puissance $\prod_{j \neq i} p_j^{\gamma_j}$ est d'ordre $p_i^{\gamma_i}$, d'où $\gamma_i \leq \beta_i$ par maximalité de β_i, et ce pour chaque i, ce qui conclut $\omega(g) \mid \omega(g_0)$.

9. Soient G et H deux groupes.

Supposons que $G \times H$ soit cyclique. Un groupe cyclique étant fini, G et H doivent être finis. Soient ensuite $\begin{matrix} G' \subset G \\ H' \subset H \end{matrix}$ deux sous-groupes : alors le produit $G' \times H'$ est un sous-groupe de $G \times H$, donc est cyclique. En particulier, si $H' = \{1_H\}$, le sous-groupe $G \times \{1_G\}$, qui est isomorphe à G, est cyclique. Bien sûr, par symétrie, l'on obtient la cyclicité de H.

On cherche donc une CNS sur deux entiers $u, v \geq 1$ pour que, en notant $C_n := {}^{\mathbb{Z}}\!/_{n}$ pour chaque entier $n \geq 1$, le produit $C_u \times C_v$ soit encore de la forme C_w. Lorsque u et v sont étrangers, c'est le cas d'après le lemme chinois. Montrons la réciproque.

Soit par l'absurde p un premier divisant u et v. Alors C_u et C_v ont tous deux un sous-groupe d'ordre p (prendre les multiples de $\frac{u}{p}$ et $\frac{v}{p}$), donc le groupe $C_p \times C_p$ sera cyclique comme sous-groupe d'un groupe cyclique. Mais cela est impossible car les éléments de $C_p \times C_p$ sont chacun d'ordre au plus p (raisonner sur chaque coordonnée) tandis que la cyclicité de $C_p \times C_p$ lui impose d'avoir un élément d'ordre $2p$, d'où la contradiction.

Finalement, $G \times H$ est cyclique ssi G et H sont cycliques d'ordres étrangers.

10. Notons ω l'ordre de G.

Déjà, le produit de ω fois un même élément de A donne le neutre de G d'après le théorème de Lagrange, donc A^ω contient 1. Par ailleurs, si l'on montre que A^ω est stable par multiplication, tout élément de A^ω admettra un inverse (son $(\omega - 1)$-ième itéré) toujours par Lagrange. Il nous suffit donc de montrer que $A^\omega A^\omega \subset A^\omega$; l'inclusion réciproque étant claire (on vient d'affirmer $1 \in A^\omega$, d'où $A^\omega = 1A^\omega \subset A^\omega A^\omega$), il suffit même de montrer l'égalité des cardinaux $\left|A^{2\omega}\right| \overset{?}{=} |A^\omega|$.

Il est bon d'observer que la translation par chaque élément de A (il en existe puisque A est non vide) injecte A^n dans $A^{n+1} = A^n A$ (pour chaque $n \geq 0$). Ainsi, la suite des cardinaux $|A^n|$ croît ; puisqu'elle ne peut dépasser l'ordre de G, elle stationne. Montrons que la croissance est *stricte* jusqu'au stationnement.

Soit $N \in \mathbb{N}$ tel que $\left|A^{N+1}\right| = \left|A^N\right|$. À $a \in A$ fixé, la translation $A^N \overset{a\times}{\hookrightarrow} A^{N+1}$ devient alors surjective (par égalité des cardinaux source et but), *i. e.* $A^{N+1} = aA^N$, ce qui permet d'écrire $A^{N+2} = A^{N+1}A = aA^N A = aA^{N+1}$, d'où $\left|A^{N+2}\right| = \left|A^{N+1}\right|$. Une récurrence immédiate montre alors le stationnement dès le rang N.

Pour conclure $\left|A^{2\omega}\right| \overset{?}{=} |A^\omega|$, il suffit donc d'avoir ω et 2ω au-delà de N, autrement dit $N \overset{?}{\leq} \omega$; or, en choisissant rétrospectivement N minimal, on aura $\left|A^{n+1}\right| > |A^n|$ pour chaque naturel $n < N$, ce qui permet d'obtenir

$$\omega = |G| \geq \left|A^N\right| \geq \left|A^{N-1}\right| + 1 \geq \left|A^{N-2}\right| + 2 \geq \cdots \geq \left|A^0\right| + N \geq N, \text{ } c.\ q.\ f.\ d.$$