Action, monoïdes & groupes (16h)

Marc SAGE

mercredi 10, jeudi 11, vendredi 12, mercredi 17, vendredi 19, lundi 22, vendredi 26 septembre 2014

Table des matières

Ce cours présente une introduction aux groupes par une approche *action*. Nous espérons y montrer que c'est *en pensant l'action* qu'émergent naturellement les groupes – ainsi que d'autres structures moins populaires (bien que foisonnant chez les anneaux).

1 Introduction : agir

Comment modéliser en mathématique notre *action* ? Une idée est de *répéter un acte* élémentaire (comme faire un pas) à partir d'un point de départ : en mathématique, cela revient à *itérer* une application sur un objet donné. Afin de pouvoir itérer *aussi loin que voulu*, il est agréable de disposer d'un ensemble de référence permettant

1. de commencer ;
2. de faire le pas suivant ;
3. de ne pas revenir en arrière.

Un tel référent, nécessairement infini (par le point 3), sera l'ensemble $\mathbf{N}$ formé des entiers naturels.

1.1 Itérer une action

Question (ensemble des itérés). *Soient o un objet et f une fonctionnelle*[1]*. Existe-t-il un ensemble contenant o et stable par f ?*

(intuitivement, on veut former l'ensemble $\{o, f(o), f(f(o)), f(f(f(o))), ...\}$ des itérés de o par f).

Remarque (minimalité). Si un tel ensemble existe, alors il en existe un plus petit (au sens de l'inclusion). Soit en effet I un tel ensemble : alors l'intersection des parties de I contenant o et stables par f convient (**exercice !**).

Problème (boucles). Même si l'on se donne un tel ensemble, rien n'empêche les boucles itératives : retour en o ou bien plus loin dans les itérés. Le second point peut être éviter en imposant l'injectivité de f, le premier en empêchant cette dernière d'atteindre o.

Réponse (N et l'axiome de l'infini). Lorsque o est l'ensemble vide $\emptyset$ et lorsque f est le ***successeur*** $a \mapsto a \cup \{a\}$, les deux points ci-dessus sont vérifiés (**exercice !**) et une réponse positive à la question ci-dessus est donnée par l'***axiome de l'infini*** :

$$\exists I,\ \emptyset \in I \text{ et } \forall i \in I,\ i \cup \{i\} \in I.$$

On définit alors $\mathbf{N}$ comme le plus petit ensemble contenant $\emptyset$ et stable par s. On appelle ensuite les premiers itérés de $\emptyset$ suivant la liste usuelle des noms des entiers : $0 := \emptyset$, $1 := s(0)$, $2 = s(s(0))$, $3 = s(s(s(0)))$...

Une fois $\mathbf{N}$ construit, on dispose d'un puissant théorème[2] d'itération.

Théorème (suite des itérés) (admis). *Soient f une application stabilisant un ensemble A et α un élément de A. Il y a alors une unique suite $(a_n) \in A^{\mathbf{N}}$ telle que $a_0 = \alpha$ et $\forall n \in \mathbf{N},\ a_{n+1} = f(a_n)$:*

$$\alpha = a_0 \overset{f}{\longmapsto} a_1 \overset{f}{\longmapsto} a_2 \overset{f}{\longmapsto} a_3 \overset{f}{\longmapsto} \cdots.$$

(idée de démonstration : définir les segments $[0, n] \subset \mathbf{N}$, construire ensuite par récurrence la restriction u^n de la suite cherchée à $[0, n]$, définir enfin une "diagonale" $a_n := u^n_n$)

Explicitement, pour tout naturel n on a

$$a_n = f^{\circ n}(\alpha)$$

où $(f^{\circ n})$ désigne la suite du théorème lorsque A est remplacé par A^A, α par Id_A et f par $F \mapsto f \circ F$:

$$\mathrm{Id} \longmapsto f \longmapsto f \circ f \longmapsto f \circ f \circ f \longmapsto \cdots.$$

Exemples (lois sur N). Les lois usuelles des entiers sont toutes définies à partir d'*actions* : itérer s donne l'addition, itérer $+$ donne la multiplication, itérer $\times$ donne l'exponentiation, itérer $\wedge$ donne une tour

[1] On entend ici une "fonction" dont le "domaine" de définition est la classe de tous les ensembles, par exemple $a \mapsto a$, $a \mapsto \{a\}$, $a \mapsto \mathsf{P}(a)$, $a \mapsto \emptyset$, $a \mapsto \cup a$... (Formellement, il s'agit d'un prédicat P binaire tel que $\forall a,\ \exists! b,\ P(a, b)$.)

[2] Ce théorème est en fait *équivalent* à l'axiome de l'infini, au sens où : si son énoncé fait sens et est vrai pour un certain triplet $(\mathbf{N}, 0, s)$ où l'on a abrégé $s : a \mapsto a + 1$, alors l'application s évitera 0 et sera injective. L'arithmétique est donc essentiellement une histoire d'*itération*.

d'exposants... Plus précisément, pour tous naturels[3] a et n, on a :

$$\begin{aligned}
a+n &= s^{\circ n}(a) = a + \underbrace{1+1+1+\cdots+1}_{n \text{ symboles } 1} \quad \begin{array}{l}(\text{appliquer } s \text{ revient donc à ajouter 1,}\\ \textit{i. e.} \text{ le successeur est l'incrémentation})\end{array} ;\\
a\times n &= [\mathrm{Id}+a]^{\circ n}(0) = 0 + \underbrace{a+a+a+\cdots+a}_{n \text{ symboles } a};\\
a^n &= [\mathrm{Id}\times a]^{\circ n}(1) = 1 \times \underbrace{a\times a\times a\times\cdots\times a}_{n \text{ symboles } a};\\
a\uparrow n &= \left[a^{\mathrm{Id}}\right]^{\circ n}(a) = \underbrace{a^{\left(a^{\left(a^{\cdots^{(\cdots a)}}\right)}\right)}}_{n \text{ symboles } a} \text{ (par exemple } a\uparrow 3 = a^{a^a}\text{, la notation } \uparrow \text{ est inventée).}
\end{aligned}$$

Remarque culturelle. La question posée en tout début de section possède une réponse positive pour toute fonctionnelle f et pour tout objet o dès que l'on dispose de l'axiome de l'infini et des axiomes de remplacement[4]. L'ensemble des itérés de o par f sera alors noté $\{f^{\circ n}(o)\ ;\ n\in\mathbf{N}\}$ sans plus de cérémonie.

1.2 Itérer dans un monoïde

Les itérés d'une application modélisent d'une part une *action neutre* (l'action immobile de $f^0 = \mathrm{Id}$) d'autre part une *succession d'actions* sans se poser de question d'association (vu l'égalité $f^{p+q} = f^p \circ f^q$ pour tous naturels p et q). En ce sens, l'ensemble référent $\mathbf{N}$ muni de l'addition est l'exemple même de "monoïde".

Définition (monoïde).
*Une **loi de composition interne** sur un ensemble A est une application $A^2 \longrightarrow A$.*
*Un **magma** est un ensemble muni d'une l. c. i..*
*Un **monoïde** est un magma unifère associatif.* (**exercice** : *le neutre est alors unique*)

Exemples (monoïdes). $\binom{\mathbf{N}}{+}$, $\binom{18\mathbf{N}}{+}$, $\binom{\mathbf{N}^*}{\times}$, $\{42^n\ ;\ n\in\mathbf{N}\}$, $\binom{A^A}{\circ}$, $\{f^{\circ n}\ ;\ n\in\mathbf{N}\}$, $\binom{\mathfrak{P}(E)}{\cup}$, $\binom{\mathfrak{P}(E)}{\cap}$, $\binom{\mathfrak{P}(E)}{\Delta}$, l'ensemble $A^* := \coprod_{n\in\mathbf{N}} A^n$ des mots sur A muni de la concaténation (le neutre est le mot vide[5], unique élément de A^0). Si M est un monoïde, alors $\mathfrak{P}(M)$ en est aussi un pour la loi $AB := \{ab\}_{b\in B}^{a\in A}$.

Contre-exemples (non-monoïdes). $\binom{\mathbf{Z}}{-}$, $\binom{\mathbf{N}^*}{+}$, $\binom{\mathbf{Q}^*}{\div}$, $\binom{\mathbf{R}^3}{\wedge}$, A^* muni du mélange faro.

Définition (itérés, idempotent, involution). Soit $(M,*)$ un monoïde. Soit $a\in M$.
La composition par a (à droite ou à gauche) détermine une unique suite (a^{*n}) ayant pour terme initial le neutre de M :

$$\begin{array}{rl} & 1 \longmapsto a \longmapsto a^2 \longmapsto a^3 \longmapsto \cdots\\ (\text{en additif :} & 0 \longmapsto a \longmapsto 2a \longmapsto 3a \longmapsto \cdots).\end{array}$$

*On dit que a est **idempotent** quand $a^2 = a$ (*i. e. *quand toutes ses puissances sont égales) :*

$$1 \longmapsto a \longmapsto a \longmapsto a \longmapsto \cdots$$

*On dit que a est **involutif** quand $a^2 = 1$ (*i. e. *quand ses puissances bouclent dès le début) :*

$$1 \longmapsto a \longmapsto 1 \longmapsto a \longmapsto \cdots$$

[3] Dans ce suit, écrire "n symboles" n'a de sens que lorsque n est identifié à un entier "usuel" (*i. e.* dont le nom appartient à la liste usuelle de nos nombres), condition *sine qua non* permettant d'expliciter les $\cdots$. Par exemple, l'entier usuel "sept" sera identifié à $s(s(s(s(s(s(s(\emptyset)))))))$.

[4] En fait, si l'on note $Infini(o,f)$ l'axiome de l'infini où l'on a remplacé $\emptyset$ par o et s par f, alors tous les $Infini(o,f)$ sont équivalents pour les couples (o,f) tes que f est injective et évite o. Cela montre que, du point de vue de l'*action*, le couple $(\emptyset, s)$ ne joue aucun rôle particulier (il sera cependant commode en vue de la théorie ordinale). On gagnera à faire le lien avec les axiomes de Peano.

[5] formellement, le mot vide est l'application vide de $\emptyset$ vers A, unique élément de $A^\emptyset$

Exemples (idempotents). Les projecteurs dans un espace vectoriel, tout élément d'un $\mathfrak{P}(E)$ pour la loi $\cup$ ou $\cap$, toute fonction de $\{0,1\}^E$ pour la loi $\times$ (**exercice** : *idempotents de* $\mathfrak{P}(E)$ *muni de* Δ *?*).

Exemples (involutions). Les symétries dans un espace vectoriel, la complémentation dans un $\mathfrak{P}(E)$ $(A \mapsto {}^cA)$ ou dans un segment $[0,a]$ $(x \mapsto a-x)$ ou dans l'ensemble des diviseurs d'un naturel $(d \mapsto \frac{n}{d})$, l'opposition dans $\mathbf{R}$ $(r \mapsto -r)$, l'inversion dans $\mathbf{Q}^*$ $(q \mapsto \frac{1}{q})$, la conjugaison complexe $z \mapsto \overline{z}$ (**exercice** : *involutions de* $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ *ou* $\mathbf{C}$ *muni de* $+$ *ou* $\times$ *?)*

Définition (action). *On dit qu'un ensemble* Ω ***opère*** *ou* ***agit*** *sur un ensemble* A *si l'on s'est donné une application* $\left\{\begin{array}{ccc}\Omega\times A & \longrightarrow & A\\ (\omega,a) & \longmapsto & \omega\cdot a\end{array}\right.$. *On parle aussi de* ***loi de composition externe****. Les éléments de* Ω *sont appelés* ***opérateurs*** *ou* ***agents****.*

Exemples (actions).

1. Lorsque $\Omega = A^A$, on a une action ***fonctionnelle***[6] $f\cdot a := f(a)$.
2. Lorsque $\Omega = \mathbf{N}$ et A est un monoïde, on a une action ***itérative*** $n\cdot a := a^{*n}$.
3. Lorsque A est un magma, n'importe quel $\omega \in A$ agit sur A par *composition* (à gauche ou à droite) $\omega\cdot a := \omega a$ (ou $a\omega$). Plus généralement, lorsque $\Omega = A$ est un magma, la l. c. i. de A en est une l. c. e..
4. De même, si M dénote un magma, alors M et $\mathfrak{P}(M)$ agissent l'un sur l'autre par *composition* (d'un côté comme de l'autre) $\omega\cdot A := \{\omega a\}_{a\in A}$ et $A\cdot\omega := \{a\omega\}_{a\in A}$.
5. Lorsque A est un espace vectoriel, le corps de base agit sur A par *homothétie*.
6. On peut également définit une action ***constante*** $\omega\cdot a := a_0$ et un action ***neutre*** $\omega\cdot a := a$.

1.3 Action à rebours : itérer dans les *deux* sens

Question (groupes géométriques). *Quelles transformations géométriques (disons isométriques) laissent invariant un carré ?*

Numérotons ses quatre sommets A,B,C,D dans l'ordre trigonométriques. On trouve deux réflexions d'axes passant par deux sommets opposés (A,C) et (B,D), deux réflexions d'axes passant par deux milieux opposés $(A,B)(C,D)$ et $(B,C)(A,D)$, deux rotations d'un quart de tour (centrées en le centre de ABCD) de sens contraires (A,B,C,D) et (A,D,C,B), une symétrie centrale $(A,C)(B,D)$. Observer que ce "groupe" de transformations est stable par composition et que chacun de ses éléments admet une transformation réciproque (on avait oublié l'identité !). Les réflexions sont leurs propres inverses (*i. e.* sont des involutions), l'inverse d'une rotation s'obtient en opposant son angle.

Même question avec un triangle équilatéral. On trouve (outre l'identité) trois réflexions d'axes les médiatrices et deux réflexions d'un tiers de tour (centrées en le centre du triangle). Même constatation : ce "groupe" de transformations est un monoïde (pour la composition) dont tous les éléments possèdent un inverse.

Idem pour un segment : on obtient l'identité et une réflexion.

Regardons enfin un cercle. Toute rotation centrée en le centre du cercle le préserve – de même pour toute réflexion d'axe un diamètre. La composée de deux réflexions d'axes sécants étant une réflexions centrée en l'intersection des axes, on dispose encore d'un monoïde où tout le monde est inversible. On observera par ailleurs, si r désigne une rotation et Δ une droite, l'identité dite ***de conjugaison*** :

$$r\circ \underset{\Delta}{\mathrm{ref}} \circ r^{-1} = \underset{r(\Delta)}{\mathrm{ref}}\ .$$

Le "groupe" obtenu n'est donc trivialement pas commutatif.

Question (groupes algébriques). *Dans* $\mathbf{R}+i\mathbf{R}$*, quelles transformations algébriques préservent les lois ainsi que* $\mathbf{R}$ *?*

Soit σ un candidat. On doit avoir d'une part $\sigma(a+ib) = \sigma(a)+\sigma(i)\sigma(b) = a+b\sigma(i)$ (pour tous réels a et b), d'autre part $\sigma(i)^2 = \sigma\left(i^2\right) = \sigma(-1) = -1$, d'où $\sigma(i) = \pm i$. On trouve finalement deux candidats : l'identité et la conjugaison, qui marchent. On retrouve le groupe du segment !

[6] On gagnera plus généralement à penser que B^A agit sur A pour tout ensemble B (même si les valeurs tombent dans B au lieu de A).

Même question pour $\mathbf{Q}+\mathbf{Q}j+\mathbf{Q}j^2$ *(en préservant* $\mathbf{Q}$ *de façon bijective).* On trouve l'identité et la permutation de j et j^2 : encore le même groupe.

Questions (groupes lumineux). *On se donne une table de diodes lumineuses, pouvant chacune être allumée ou bien éteinte. On dispose d'une série d'interrupteurs changeant chacun l'état des lampes d'une partie donnée de la table (la partie dépendant de l'interrupteur). On se demande si, à partir d'une configuration de départ, on peut en actionnant les interrupteurs obtenir n'importe quelle autre configuration lumineuse.*

Codons une configuration lumineuse par un mot en base 2 (de longueur le nombre de lampes). Alors les interrupteurs agissent sur l'ensemble de ce mots de manière involutive (donc réversible) : le "groupe engendré" par les interrupteurs est encore un monoïde avec inverses.

Questions (groupe ludique). *Résoudre un Rubik's cube.*

Les transformations de l'espace (des rotations d'un quart de tour) sont toutes composables à la suite et sont inversibles : le "groupe" qu'elles engendrent est à élucider.

Définition (élément régulier, inversible, groupe). Soit M un monoïde.

On dit qu'un $a \in M$ *est* ***régulier*** *(ou* ***simplifiable****) si l'on peut simplifier par* a *des deux côtés,* i. e. *si les deux compositions par* a *sont injectives.*

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*, on dit que* a *est* ***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***[7] *et est noté* $M^\times$*. Lorsque* $M^\times = M$*, on dit que* M *est un* ***groupe****.*

Exercice (inversibilité). *Montrer qu'un élément* a *dans un monoïde est inversible ssi les deux compositions par* a *sont bijectives. Même question en remplaçant "bijectives" par "surjectives".*

Exercice (régularité en cardinalité finie). *Montrer que, dans un monoïde fini, la régularité et l'inversibilité (d'un élément donné) coïncident.*

Exercice (régularité dans A^A**).** *Montrer que, dans un monoïde* A^A*, la régularité et l'inversibilité coïncident. On pourra montrer plus précisément*[8] *les équivalences*

$$\begin{aligned} f \text{ inversible à gauche} &\iff f \text{ régulier à gauche} \iff f \text{ injectif,} \\ f \text{ inversible à droite} &\iff f \text{ régulier à droite} \iff f \text{ surjectif.} \end{aligned}$$

Remarque (action). Le fait de rapporter un élément à son action multiplicative 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 !

Propriétés (inversibles).

Les inversibles sont réguliers. Un groupe est régulier. Le groupe des inversibles est un groupe ($M^{\times\times} = M^\times$*).*

Les involutifs sont inversibles et valent leur propres inverses (ainsi $1^{-1} = 1$*)*

L'application $m \mapsto m^{-1}$ *est une involution de* $M^\times$ *qui inverse*[9] *la loi :*

$$\left(a^{-1}\right)^{-1} = a \qquad et \qquad (ab)^{-1} = b^{-1}a^{-1}$$

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

Soient a *et* b *deux inversibles qui commutent. On a alors pour tous relatifs* n, p, q *:*

$$\begin{aligned} a^p a^q &= a^{p+q} \qquad \text{(en additif : } pa + qa = (p+q)\,a\text{),} \\ (ab)^n &= a^n b^n \qquad \text{(en additif : } n\,(a+b) = na + nb\text{).} \end{aligned}$$

Remarque culturelle (régularité et groupes). Le monoïde $(\mathbf{N}, +)$ est régulier : on peut le "symétriser" et ainsi construire le groupe $(\mathbf{Z}, +)$. De même, le monoïde $(\mathbf{Z}^*, \times)$ est régulier et on peut le "symétriser"

[7] 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.

[8] de la surjectivité à l'inversibilité à droite il pourra servir d'utiliser l'axiome du choix

[9] on dit qu'il s'agit d'un ***anti-morphisme*** ; les ***morphismes*** (tout court) vont quant à eux *préserver* la loi

pour construire le groupe $(\mathbf{Q}^*, \times)$. On pourrait montrer qu'un monoïde peut se "prolonger" en un groupe ssi il est régulier.

Groupe référents (droite Z et boucles $\mathbf{Z}/_n$). Tout comme $\mathbf{N}$ est le monoïde référent pour agir à partir d'un point de départ, le groupe additif $\mathbf{Z}$ sera le groupe référent pour agir *dans les deux sens* à partir d'un point de départ à l'aide d'une bijection :

$$\cdots \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} f^{-3}(o) \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} f^{-2}(o) \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} f^{-1}(o) \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} o \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} f(o) \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} f^2(o) \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} f^3(o) \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} \cdots.$$

On retrouve le théorème d'itération cette fois indexée par $\mathbf{Z}$: *si une application f inversible stabilise un ensemble A (autrement dit si on se donne un $f \in \mathfrak{S}_A$), alors pour tout $\alpha \in A$ il y a une unique suite $(a_k) \in A^{\mathbf{Z}}$ telle que* $\left\{ \begin{array}{c} a_0 = \alpha \\ \forall k \in \mathbf{Z},\ a_{k+1} = f(a_k) \end{array} \right.$. Avec des flèches d'action :

$$\cdots \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} a_{-3} \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} a_{-2} \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} a_{-1} \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} \alpha = a_0 \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} a_1 \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} a_2 \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} a_3 \underset{f^{-1}}{\overset{f}{\longleftrightarrow}} \cdots.$$

Dans le cas de la suite des itérés d'un inversible a, cela devient

$$\cdots \rightleftarrows a^{-3} \rightleftarrows a^{-2} \rightleftarrows a^{-1} \rightleftarrows 1 \rightleftarrows a \rightleftarrows a^2 \rightleftarrows a^3 \rightleftarrows \cdots \text{ (multiplicatif)}$$

$$\text{ou} \qquad \cdots \rightleftarrows -3a \rightleftarrows -2a \rightleftarrows -a \rightleftarrows 0 \rightleftarrows a \rightleftarrows 2a^2 \rightleftarrows 3a \rightleftarrows \cdots \text{ (additif)}$$

Il se peut que les itérés bouclent : [dessin]. C'est le cas par exemples des itérés de $e^{\frac{2\pi i}{n}}$ dans $\mathbf{C}^*$: on obtient le groupe $\mathbf{U}_n := \left\{ e^{\frac{2\pi i k}{n}} \right\}_{0 \leq k < n}$ des racines n-ièmes de l'unité, dit ***cyclique*** d'ordre n (visualiser un n-gone régulier inscrit dans le cercle unité dont 1 est un sommet). En version additive (définie plus tard), ce groupe sera également noté $\mathbf{Z}/_n$: on "tord"[10] la droite $\mathbf{Z}$ et on la "boucle" en égalant n à 0.

Contre-exemples (boucles avortées).

Les tapis-roulant $(a, b, c, ...) \mapsto \left\{ \begin{array}{c} \text{ou} \\ \end{array} \begin{array}{c} (0, a, b, c, ...) \\ (b, c, d, ...) \end{array} \right.$ n'ont rien d'inversible (penser à la dérivation polynomiale ou à la multiplication par X). Leurs itérés stationnent quand les coordonnées sont en nombre fini (cas nilpotent), à l'instar de $\left\{ \begin{array}{c} \mathrm{Im} : a + ib \mapsto b \mapsto 0 \\ i\,\mathrm{Re} : a + ib \mapsto ia \mapsto 0 \end{array} \right.$. [dessin : boucle avortée]

De même pour des projecteurs $(a, b, c, ...) \mapsto \left\{ \begin{array}{c} \text{ou} \\ \end{array} \begin{array}{c} (0, b, c, ...) \\ (a, 0, c, ...) \end{array} \right.$, à l'instar de $\left\{ \begin{array}{c} \mathrm{Re} : a + ib \mapsto a \mapsto a \mapsto \cdots \\ i\,\mathrm{Im} : a + ib \mapsto ib \mapsto ib \mapsto \cdots \end{array} \right.$. [dessin : boucle avortée]

2 Groupes

2.1 Définitions & exemples

Définitions (groupes, ordre, abélien). *Un **groupe** est un ensemble muni d'une loi vérifiant :*

1. *associativité ;*
2. *présence d'un neutre ;*
3. *inversibilité de tous les éléments.*

*Le cardinal d'un groupe est aussi appelé son **ordre**.*
*Un groupe commutatif sera dit **abélien**.*

Exemples (groupes numériques). Sont des groupes additifs $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ (pas $\mathbf{N}$). Sont des groupes multiplicatifs $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ (pas $\mathbf{Z}^*$). Tous abéliens.

[10] Dans les deux cas, on parle de ***torsion*** d'ordre n.

Exemples (sous-groupes complexes). Les complexes unitaires forment un groupe (multiplicatif) noté $\mathbf{U}$, les racines n-ièmes de l'unité également (on a déjà rencontré $\mathbf{U}_n$), de même pour la réunion $\bigcup_{n\in\mathbf{N}^*}\mathbf{U}_n$ (**exercice !**). Tous abéliens.

Exemples (groupes symétriques). Le groupe des inversibles du monoïde E^E, formé des bijections de E sur E, est noté $\mathfrak{S}(E)$ ou $\mathfrak{S}_E$ et est appelé le ***groupe symétrique*** de E. Il n'est jamais abélien (sauf si $|E|\leq 2$: **exercice !**). Pour tout naturel n, on note $\mathfrak{S}_n$ le groupe symétrique du segment $[1,n]$. On a déjà rencontré $\mathfrak{S}_2$ et $\mathfrak{S}_3$ (certes maquillés) comme groupes de transformations laissant invariant un segment, resp. un triangle. On peut aussi (**exercice !**) réaliser $\mathfrak{S}_4$ comme groupe laissant invariant un tétraèdre régulier.

Exemples (groupes géométriques). Les translations du plan forment un groupe pour la composition, de même pour les rotations de même centre ou les homothéties de même centre (tous abéliens). En "mélangeant" ces groupes, on obtient le groupe des rotations/homothéties (similitudes) de même centre (abélien), celui des rotations/translations (non abélien), celui des homothéties/translations, celui des rotations/translations/réflexions (isométries) (non abélien).

Exemples exotique (quaternions). Tout comme $\mathbf{C}$ peut être vu comme un espace vectoriel de la forme $\mathbf{R}\oplus\mathbf{R}i$ muni d'une multiplication vérifiant $i^2=-1$, on admettra l'existence d'un espace vectoriel $\mathbf{H}$ de la forme $\mathbf{R}\oplus\mathbf{R}i\oplus\mathbf{R}j\oplus\mathbf{R}k$ muni d'une multiplication vérifiant $i^2=j^2=k^2=ijk=-1$. Alors la partie $\{\pm 1,\pm i,\pm j,\pm k\}$ est un groupe d'ordre 8 appelé ***groupe des quaternions***[11] et noté $\mathbf{H}_8$. (**exercice** : *est-il abélien ?*)

Voyons un premier moyen de construire des groupes à l'aide d'autres.

Définition-proposition (produits de groupes). *Soit (G_i) une famille de groupes. La loi $(g_i)(h_i):=(g_ih_i)$ munit le produit cartésien $\prod G_i$ d'une structure de groupe, appelé* ***groupe produit*** *des G_i.*

Ainsi, tout se passe coordonnée par coordonnée. (**exercice** : *montrer que $\prod G_i$ est abélien ssi $\forall i$, G_i est abélien)*

Dans le cas d'une famille finie, on gagnera à présenter les -uplets de manière verticale, à l'instar de

$$\begin{pmatrix}a\\b\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}\begin{pmatrix}A\\B\end{pmatrix}=\begin{pmatrix}a\alpha A\\b\beta B\end{pmatrix}.$$

Par exemple, l'addition de $\mathbf{C}$ est celle du groupe produit $\mathbf{R}\times\mathbf{R}$.

Lorsque tous les groupes sont égaux, le produit cartésien devient une puissance G^X et l'on retrouve des fonctions :

$$fg : x\mapsto f(x)\,g(x).$$

2.2 Le problème des chapeaux : vers les groupes cycliques

L'université PSL envisage un nouveau test d'entrée. Elle se donne des couleurs – appelons n leur nombre. Chaque candidat se voit attribuer un chapeau, portant l'une des n couleurs, dont il ignore la couleur. Les candidats se mettent un file indienne, chacun voyant les chapeaux des candidats devant lui et pouvant entendre la voix tous ceux derrière. À tout de rôle, en commençant par la queue de la file, les candidats doivent deviner la couleur de leurs chapeaux.

Idée (ajouter et soustraire de l'information). Notons V_i l'information **v**isible par le i-ième candidat (à savoir les couleurs des chapeaux des k-ièmes candidats pour $k>i$) et C_i l'information voulue (la **c**ouleur du i-ième chapeau). Alors l'information V_i s'obtient en "additionnant" les $C_{k>i}$; en d'autres termes, l'information C_i s'obtient en soustrayant V_i de V_{i-1}. Ainsi, si l'on pouvait mettre sur l'ensemble des couleurs une structure additive avec soustraction (par exemple un groupe), on pourrait adopter la stratégie suivante :

1. le premier candidat annonce V_1 ;
2. le deuxième candidat voit V_2 et a entendu V_1, donc il peut calculer $V_1-V_2=C_2$ et énoncer sa couleur (après cela, les candidats suivants, ayant entendu V_1 et C_2, connaissent $V_1-C_2=V_2$) ;
3. le troisième candidat voit V_3 et connaît V_2, donc il peut calculer $V_2-V_3=C_3$ et énoncer sa couleur (de laquelle les candidats suivants déduisent $V_2-C_3=V_3$)... Et ainsi de suite.

[11] la lettre "H" abrège au choix "hyper-complexe" ou leur créateur "Hamilton"

Mise en œuvre. On code chaque couleur par un entier de $[0, n[$. L'addition des entiers nous tend les bras mais elle ne stabilise pas $[0, n[$: on s'y ramène en soustrayant un bon multiple de n. On définit donc une somme $a \oplus b$ comme le reste de la division de $a + b$ par n. Mais il devient alors pénible de vérifier les axiomes d'un groupe[12] et l'on devra toujours bricoler pour retomber dans $[0, n[$. Pour pallier ces difficultés, au lieu de choisir un bon multiple de n pour retomber dans $[0, n[$, on va *tous* les choisir. Pour tout entier a, définissons la ***classe*** de a *modulo*[13] n par

$$\overline{a} := a + n\mathbf{Z}.$$

Par exemple :

1. modulo 2, la classe de 0 est $0 + 2\mathbf{Z} = 2\mathbf{Z}$, elle est formée des entiers pairs ;
2. modulo 2, la classe de 1 est formée des entiers impairs ;
3. modulo n, la classe de 0 est formée des multiples de n, tout comme la classe de n et celle de $42n$.

On vérifiera en **exercice** l'équivalence (valide pour tous entiers a et b) $\overline{a} = \overline{b} \iff b - a \in n\mathbf{Z}$. Usuellement, on préfère s'exprimer sans classes et l'écrira plutôt "$a = b$" en disant quelque part "*modulo*[14] n", ce qui peut s'abréger "$a = b \ [n]$" (voire "$a \equiv b \ [n]$") :

$$a = b \ [n] \overset{\text{déf.}}{\iff} b - a \in n\mathbf{Z} \iff \overline{a} = \overline{b}.$$

On définit à présent la ***somme*** de deux classes A et B modulo n par

$$A + B := \overline{a + b} \text{ où } \begin{cases} a \in A \\ b \in B \end{cases}.$$

On vérifiera *soigneusement* que le classe $\overline{a + b}$ ne dépend pas des a et b choisis[15]. En particulier, on pourra toujours utiliser

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

Grâce à ces identités, les axiomes de l'addition usuelle "passent sous la barre", d'où il découle aisément que l'ensemble ${}^{\mathbf{Z}}\!/_{n} := \{\overline{a} \ ; \ a \in \mathbf{Z}\}$ des classes *modulo* n est un groupe. Ce dernier possède n éléments, par exemple

$${}^{\mathbf{Z}}\!/_{n} = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\} = \left\{\overline{-1}, \overline{-2}, ..., \overline{-n}\right\}.$$

On l'appelle le ***groupe cyclique*** d'ordre n. [dessin : n-gone régulier]

2.3 Le principe de conjugaison

Définition (conjugués). *Étant donnés dans un groupe deux éléments a et g, l'élément gag^{-1} est appelé le **conjugué** de a par g.*

Remarque (conjuguer et commuter). Deux éléments commutent ssi conjuguer l'un par l'autre ne change rien :

$$ab = ba \iff \begin{array}{ccc} a = bab^{-1} & \iff & b^{-1}ab = a \\ b = a^{-1}ba & \iff & aba^{-1} = b \end{array}. \text{ Ainsi :}$$

étudier la conjugaison revient à mesurer le défaut de commutativité.

L'exemple des isométries stabilisant un cercle permet de visualiser l'effet d'une conjugaison :

$$r \circ \underset{\Delta}{\text{ref}} \circ r^{-1} = \underset{r(\Delta)}{\text{ref}}.$$

Le *type* de transformation est inchangé (ici une réflexion), seul est modifié le point de vue (ici l'axe par rapport auquel on réfléchit). [dessin]

[12] Vérifier tout par soi-même, sachant que $a \oplus b = (a + b) - \left\lfloor \frac{a+b}{n} \right\rfloor n$. Ce n'est pas difficile – juste pénible et peu éclairant.

[13] littéralement : « à la mesure de »

[14] ainsi l'égalité "à la mesure de n" signifie-t-elle "à un multiple de n près"

[15] Soient $a' \in A$ et $b' \in B$. Puisque $\overline{a} = A = \overline{a'}$, il y a un $\lambda \in \mathbf{Z}$ tel que $a' = a + \lambda n$. De même, il y a un $\mu \in \mathbf{Z}$ tel que $b' = b + \mu n$. On a alors $a' + b' = (a + b) + (\lambda + \mu)\, n$, d'où l'égalité cherchée des classes.

De même, si φ désigne une bijection entre deux ensembles E et F, alors conjuguer par φ permet de "passer" d'une permutation de E à une permutation de F :

$$\left\{\begin{array}{ccc}\mathfrak{S}_E & \xrightarrow{\sim} & \mathfrak{S}_F \\ \sigma & \longmapsto & \varphi\circ\sigma\circ\varphi^{-1}\end{array}\right. \qquad \left(\begin{array}{ccc}\text{observer le} & & y\in F \quad \overset{?}{\dashrightarrow} \quad \left[\varphi\sigma\varphi^{-1}\right](y)\in E \\ \text{parcours à } \sigma & : & \simeq\downarrow \varphi^{-1} \qquad\qquad \simeq\uparrow \varphi \\ \text{fixé d'un } y\in F & & \varphi^{-1}(y) \quad \xrightarrow{\sigma} \quad \sigma\left(\varphi^{-1}(y)\right)\end{array}\right)$$

La permutation σ *agit comme* chacune de ses conjuguées, seul est modifié le point de vue (ici le nom des éléments permutés). [dessin avec $\{1,2,3,4,5\}$ et $\{A,B,C,D,E\}$]

Chez les matrices carrées, on connaît l'effet de la conjugaison : un changement de base. Les conjuguées d'une même matrices *agissent* toutes *de la même manière* (l'endomorphisme représenté est le même), seul change le point de vue (ici la base choisie).

Enfin, si l'on demande de comprendre la loi $*$ de $[0,1[$ définie par $(a,b)\mapsto\frac{a+b}{1+ab}$, il sera éclairant d'observer que $a*b=\operatorname{th}(\operatorname{ath}a+\operatorname{ath}b)$, de sorte que la loi étudiée n'est autre que la conjuguée de l'addition de $\mathbf{R}_+$ par th :

$$\begin{array}{ccccc}[0,1[^2 & \longrightarrow & [0,1[& \qquad (a,b) & \longrightarrow & \frac{a+b}{1+ab} \\ \simeq\downarrow (\operatorname{ath},\operatorname{ath}) & & \simeq\uparrow \operatorname{th} & \simeq\downarrow & & \simeq\uparrow \operatorname{th} \\ \mathbf{R}_+^2 & \xrightarrow{+} & \mathbf{R}_+ & (\operatorname{ath}a,\operatorname{ath}b) & \xrightarrow{+} & \operatorname{ath}a+\operatorname{ath}b\end{array}.$$

On retiendra de tout cela le **principe de conjugaison** :

$$\textit{conjuguer revient à } \left\{\begin{array}{c}\textit{changer de point de vue tout} \\ \textit{en conservant la même action}\end{array}\right. .$$

Exercice. *Soient $f:E\longrightarrow E$ et $\varphi:E\xrightarrow{\sim}F$. Déterminer* $\operatorname{Fix}\left(\varphi f\varphi^{-1}\right)$ *en fonction de* $\operatorname{Fix}f$. *En déduire une détermination des conjugués d'une réflexion plane par une rotation.*

2.4 Sous-groupes

Le lecteur gagnera à faire le parallèle durant toute cette section avec la notion de *sous-espace vectoriel* (laquelle n'est qu'un cas particulier additif de celle de sous-groupe).

2.4.1 Définition, intersections, centralisateurs

Les exemples de groupes géométriques montrent que des parties de groupes peuvent être des groupes, ce qui motive la définition suivante.

Soit G un groupe. Soit A une partie de G.

Définition (sous-groupes). *On dit que A est un* ***sous-groupe*** *de G si A est un groupe pour la loi de G induite sur A (i. e. restreinte à $A\times A$).*

★ Des parties peuvent être des groupes pour d'autres lois sans pour autant être des sous-groupes. Par exemple, la partie $\mathbf{R}\times\{18\}$ du groupe additif $\mathbf{C}$ est un groupe pour l'addition réelle sur la première coordonnée et la loi constante sur la seconde mais ne peut être un sous-groupe de $\mathbf{C}$ car ne contient pas son neutre $(0,0)$.

Proposition (critère pour déterminer un sous-groupe). *A est un sous-groupe de G si et seulement si les conditions suivantes sont vérifiées :*

1. *A contient le neutre de G (*i. e. $1_G\in A$*) ;*
2. *A est stable par composition (*i. e. $\forall a,a'\in A,\ aa'\in A$*) ;*
3. *A est stable par inversion (*i. e. $\forall a\in A,\ a^{-1}\in A$*).*

Démonstration.
$\boxed{\Longrightarrow}$ Supposons que A est un sous-groupe de G. Il 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 la condition 1. La condition 2 signifie précisément que la loi induite est bien définie (*i. e.* est à valeurs dans A). Enfin, si $a \in A$, il admet un inverse a' dans A, ce qui s'écrit $aa' = \mathtt{1} = a'a$, *i. e.* $aa' = 1 = a'a$, d'où $a^{-1} = a' \in A$ et la condition 3.
$\boxed{\Longleftarrow}$ Supposons les trois conditions de l'énoncé. La condition 2 énonce que la loi induite est bien définie. L'associativité portant sur tous les éléments de G, elle est en particulier valide pour ceux de A. La condition 1 fournit un neutre pour A. Enfin, tout élément de A est inversible dans G et la condition 3 nous dit que son inverse reste dans A.

En pratique, c'est le sens $\boxed{\Longleftarrow}$ qui sert le plus souvent : il est plus agréable de montrer une appartenance et deux stabilités plutôt que de se farcir à vérifier les axiomes d'un groupe (surtout l'associativité).

En application, reprendre les exemples de groupes complexes et géométriques.
On s'exercera également sur la propriété suivante.

Propriété (intersection de sous-groupes). *La famille des sous-groupes de G est stable par intersection (non nécessairement finie).*

Démonstration. Soit (G_i) une famille de sous-groupes de G. Le neutre de G appartient à chaque G_i, donc à leur intersection. Soient a et b dans $\bigcap G_i$. Alors chaque G_i contient a, *a fortiori* son inverse, donc ce dernier tombe dans $\bigcap G_i$. De plus chaque G_i contient a et b, *a fortiori* leur produit, donc ce dernier tombe dans $\bigcap G_i$.

★ Le résultat est toujours faux pour le complémentaire (**pourquoi ?**) et est en général faux pour une réunion : on montrera en effet qu'*une réunion de deux sous-groupes en est un ssi l'un est inclus dans l'autre* (**exercice !**).

Donnons un dernier exemple générique de sous-groupes.

Définition (commutant, centre, centralisateur). *Le **commutant** de A ou **centralisateur** de A est la partie formée des éléments (de G) qui commutent à tous ceux de A :*

$$\operatorname{Comm} A := \{g \in G \ ; \ \forall a \in A, \ ag = ga\} =: Z_G(A) .$$

*Le commutant de G s'appelle son **centre** :*

$$Z(G) := \{g \in G \ ; \ \forall x \in G, \ xg = gx\} = Z_G(G) .$$

Le centre d'un groupe mesure son degré de commutativité : en particulier, G est abélien ssi $Z(G) = G$.
On vérifiera (**exercice !**) que *les centralisateurs sont tous des sous-groupes.*
Exercice. *Déterminer $Z(\mathbf{H}_8)$ ainsi que tous les commutants de $\mathbf{H}_8$.*
Exercice. *Dans un groupe produit, les produits de sous-groupes sont-ils des sous-groupes ? Y en a-t-il d'autres ?*

2.4.2 Sous-groupes additifs de Z et de R

Observer que les $n\mathbf{Z}$ sont pour tout naturel $n \geq 0$ des sous-groupes (additifs) de $\mathbf{Z}$. Montrons que ce sont en fait les seuls.

Soit G un sous-groupe additif de $\mathbf{Z}$. [Micro-analyse : si G est de la forme cherchée, disons $G = n\mathbf{Z}$, alors n est le plus petit élément strictement positif de G (à moins que G soit nul). Fin de la micro-analyse.] Si G est nul, il s'écrit $0\mathbf{Z}$ et on a fini. On supposera donc G non nul. Soit $g \neq 0$ dedans : quitte à l'opposer, on peut supposer $g > 0$. Il fait alors sens de définir $m := \min(G \cap \mathbf{N}^*)$. Montrons l'égalité $G = m\mathbf{Z}$. L'inclusion $\supset$ est immédiate puisque les itérés de m restent dans G. Réciproquement, soit par l'absurde un $g \in G \setminus m\mathbf{Z}$. Une division euclidienne de g par m (on peut car $m \neq 0$) donne $g = mq + r$ avec $0 \leq r < m$. Le reste r est non nul (sinon $g \in m\mathbf{Z}$) et doit rester dans G (il s'écrit $g - mq \in G - mG \subset G$), donc tombe dans $G \cap \mathbf{N}^*$, d'où $r \geq \min(G \cap \mathbf{N}^*)$, ce qui est absurde.

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

Proposition (sous-groupes additifs[16] de R). *Soit G un sous-groupe (additif) de $\mathbf{R}$. Alors :*

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

Démonstration. On suit la même démonstration que pour $\mathbf{Z}$. Notons $G' := G \cap \mathbf{R}_+^*$. 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 supposer $a > 0$, d'où la non-vacuité de G' ; le réel $i := \inf G'$ fait alors sens[17].

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 le $\left(\left\lfloor \frac{g}{\varepsilon} \right\rfloor + 1\right)$-ième[18]), *c. q. f. d.*.

Supposons $i > 0$. Montrons $i \in G$ puis $G = i\mathbf{Z}$. Supposons par l'absurde $i \notin G$. Par définition de i, il y a un des $g, h \in G'$ tels que[19] $i < g < h < 2i$: 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 $\mathbf{Z}i \subset G$. Enfin, soit par l'absurde un g dans $G \setminus i\mathbf{Z}$. Effectuons une division euclidienne $g = qi + r$ où $q \in \mathbf{Z}$ et $0 \leq r < i$. Alors l'élément $r = g - qi$ tombe dans G' et est $< \inf G'$, d'où la contradiction.

Application (périodes). Soit $f : \mathbf{R} \longrightarrow \mathbf{R}$. Une ***période*** de f est un réel T tel que $f\,(\mathrm{Id} + T) = f$. Les périodes forment un sous-groupe. Lorsqu'il est discret, ***la période*** de f est la plus petite période strictement positive. (Dans le cas dense, f est constante si on la suppose de plus continue).

Exercice. *Soient a et b deux réels > 0. Montrer que $a\mathbf{Z} + b\mathbf{Z}$ est un sous-groupe[20] et qu'il est dense ssi $\frac{a}{b}$ est irrationnel.*

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

2.4.3 Sous-groupes engendrés

On vient de voir que, lorsqu'un groupe contient un élément, il contient tous ses itérés. Que peut-on dire de ce sous-groupe lorsqu'il contient *plusieurs* éléments ?

Soit A une partie d'un groupe G.

"Définition" (sous-groupe engendré). *On appelle **sous-groupe engendré** par A le plus petit sous-groupe de G contenant A. On le note[21] $\langle A \rangle$.*

Description interne. *$\langle A \rangle$ est formé des produits d'éléments de A et d'inverses d'éléments de A :*

$$\langle A \rangle = \left\{ a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \ ; \quad \begin{array}{c} \overrightarrow{\varepsilon} \in \{\pm 1\}^n \\ \overrightarrow{a} \in A^n \end{array} \right\}_{n \in \mathbf{N}}$$

Description externe. *$\langle A \rangle$ est l'intersection de tous les sous-groupes contenant A :*

$$\langle A \rangle = \bigcap_{H \supset A}^{H \text{ s. g.}} H.$$

[16] La démonstration montre en fait qu'un sous-monoïde de $\mathbf{R}_+$ est ou bien discret ou bien dense ; l'inversibilité n'intervient nullement au niveau conceptuel.

[17] 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 $\mathbf{R}$ 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*.

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

[19] insérer d'abord un h entre i et $2i$, puis un g entre i et h

[20] Il n'est pas toujours vrai que le composé de deux sous-groupes reste un sous-groupe. On verra en T. G. une caractérisation simple de cela.

[21] en algèbre, les chevrons signifient très souvent "sous-structure engendrée par" : sous-monoïde, sous-groupe, sous-anneau, sous-espace vectoriel, sous-algèbre...

La description externe est souvent "théorique" : elle permet de montrer l'existence de la sous-structure engendrée mais ne l'éclaire pas contrairement à la description interne.

Démonstration. La définition ci-dessus pourrait être vide ! Montrons que $\bigcap_{H \supset A}^{H \text{ sg}} H$ tombe dessous. Cette intersection est l'infimum (pour $\subset$) de la famille des sous-groupes de G contenant A. Or les deux conditions "être un sous-groupe" et "contenir A" passent à l'intersection, donc cet *infimum* est un minimum.

Notons A' la partie décrite "depuis l'intérieur" et montrons qu'elle vaut $\langle A \rangle$. Un sous-groupe contenant A doit contenir les éléments de A et leurs inverses, *a fortiori* les produits de tels éléments, donc finalement doit contenir tout A'. Il est par ailleurs clair que A' contient le neutre (prendre $n = 0$) et est stable par produit et inverse.

Pour revenir à la question posée, si un groupe G contient une partie A, alors il est un sous-groupe contenant A, donc contient le plus petit tel sous-groupe $\langle A \rangle$. On retiendra plus généralement :

1. l'implication $A \subset B \Longrightarrow \langle A \rangle \subset \langle B \rangle$ (visible sur la description interne)
2. l'inclusion $A \subset \langle A \rangle = \langle \langle A \rangle \rangle$ avec égalité ssi A est un sous-groupe.

Exemples.
Nous avons rencontré plus haut les sous-groupes engendrés par un seul élément, dits ***monogènes***. La description interne devient

$$\langle a \rangle = \left\{ a^k \ ; \ k \in \mathbf{Z} \right\} \qquad \text{(en additif, on retrouve } \langle a \rangle = \mathbf{Z}a\text{)}.$$

Deux cas apparaissent :

1. ou bien tous les itérés se distinguent les uns des autres (on reconnaît alors le groupe référent $\mathbf{Z}$) ;
2. ou bien une égalité $a^k = a^l$ montre qu'un itéré a^{k-l} non trivial est neutre, ce qui fait boucler les itérés (on reconnait alors un groupe cyclique $\mathbf{Z}/n$)

★ Par conséquent, *les groupes monogènes sont les deux groupes référents* : $\mathbf{Z}$ (infini) et les $\mathbf{Z}/n$ (cycliques).
Dans le cas abélien, des éléments $a_1, a_2, ..., a_n$ en nombre fini engendrent un sous-groupe de la forme

$$\begin{array}{rcl} \langle a_1, a_2, ..., a_n \rangle & = & \left\{ a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \ ; \ \overrightarrow{k} \in \mathbf{Z}^n \right\} \\ \text{(en additif)} & = & \mathbf{Z}a_1 + \mathbf{Z}a_2 + \cdots + \mathbf{Z}a_n. \end{array}$$

En non commutatif, tout peut se compliquer, même avec deux générateurs.

2.4.4 Ordre d'un élément

Soit G un groupe. On en étudie les sous-groupes *monogènes*.

Définition (ordre d'un élément). *Soit $g \in G$. On appelle **ordre** de g le plus petit exposant non nul à laquelle puissance g donne le neutre ; s'il n'y a pas de tel exposant, on définit*[22] *∞ pour l'ordre de g :*

$$\omega(g) := \inf_{\overline{\mathbf{N}}} \left\{ n \in \mathbf{N}^* \ ; \ g^n = 1 \right\}.$$

Exemple (ordre d'un sous-groupe cyclique). Soit $g \in G$. Alors ses itérés sont distincts jusqu'au $\omega(g)$-ième[23] qui boucle à 1 :

$$\langle g \rangle = \left\{ g^k \ ; \ 0 \leq k < \omega(g) \right\} = \begin{array}{l} \left\{ 1, g, g^2, ..., g^{\omega(g)-1} \right\} \text{ (ordre fini)} \\ \left\{ ..., g^{-2}, g^{-1}, 1, g, g^2, ... \right\} \text{ (ordre infini)} \end{array}.$$

Par conséquent, *l'ordre de g vaut l'ordre du sous-groupe qu'il engendre* :

$$\omega(g) = \# \langle g \rangle.$$

[22] La définition ci-dessous de $\omega(g)$ regroupe les deux cas – fini et infini. Pour le cas infini, la partie de $\overline{\mathbf{N}}$ considéré est vide ; or la partie vide est tautologiquement minorée par tout le monde, donc son plus grand minorant est $\max \overline{\mathbf{N}} = \infty$.

[23] Soient en effet a et b deux entiers vérifiant $g^a = g^b$ tels que $0 \leq a \leq b < \omega(g)$. On a alors $g^{b-a} = 1$ avec $0 \leq b - a < \omega(g)$, d'où $b - a = 0$ par minimalité de $\omega(g)$.

★ **Proposition (ordre et diviseurs).** *Soit $g \in G$. On a pour tout relatif k l'équivalence*

$$g^k = 1 \iff \omega(g) \text{ divise } k.$$

Démonstration. Le sens $\Longleftarrow$ est immédiat. Soit $k \in \mathbf{Z}$ tel que $g^k = 1$. Effectuons une division euclidienne $k = q\omega(g) + r$ où $0 \leq r < \omega(g)$. On a alors $1 = g^k = \left(g^{\omega(g)}\right)^q g^r = g^r$, ce qui force $r = 0$ par minimalité de $\omega(g)$.

Théorème (Lagrange soft). *Dans un groupe fini, tous les éléments sont d'ordre fini divisant celui du groupe :*

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

Démonstration (cas abélien). Soit $g \in G$. Puisque $G = gG$ (**pourquoi ?**) on a les égalités

$$\prod_{a\in G} a = \prod_{a\in gG} a = \prod_{b\in G} gb = \prod_{b\in G} g \prod_{b\in G} b = g^{|G|} \prod_{a\in G} a, \quad \begin{array}{c}\text{d'où le résultat en}\\ \text{simplifiant par } \prod_G\end{array}.$$

(On verra plus tard – et plus généralement – que l'ordre de tout *sous-groupe* divise celui de G.)

Corollaire (groupes d'ordre premier). *Tout groupe d'ordre premier est cyclique.*

Démonstration. Soit G un tel groupe. Soit $g \neq 1$ dedans (on peut car un premier est > 1). Alors l'ordre de g n'est pas 1 et doit diviser $|G|$, donc vaut $|G|$, ce qui montre que l'inclusion $\langle g\rangle \subset G$ est une égalité.

Question. *Comment l'ordre se comporte vis-à-vis du produit ?*

Regardons le cas de deux réflexions planes. Chacune est d'ordre 2. Notons θ l'angle entre leurs axes. Leurs deux composées sont des rotations d'angles $\pm 2\theta$, lesquelles sont d'ordre fini ssi $\theta \in \mathbf{Q}\pi$. Ainsi le produit de deux élément de petit ordre peut-il être d'ordre infini !

Regardons le cas abélien. Soient a et b deux éléments d'ordre fini *qui commutent*. Abrégeons $\binom{\alpha}{\beta} := \binom{\omega(a)}{\omega(b)}$. Vu les égalités $(ab)^{\alpha\beta} = (a^\alpha)^\beta \left(b^\beta\right)^\alpha = 1$, l'ordre de ab doit diviser le produit $\alpha\beta$. On peut même affiner ce qui précède et remplacer le produit de α et β par leur p. p. c. m.. Montrons alors

$$\frac{\alpha \vee \beta}{\alpha \wedge \beta} \mid \omega(ab) \mid \alpha \vee \beta.$$

Abrégeons $\omega := \omega(ab)$. De $1 = (ab)^\omega = a^\omega b^\omega$, on déduit $a^\omega = b^{-\omega} \in \langle b\rangle$, donc $1 = (a^\omega)^{\#\langle b\rangle} = a^{\omega\beta}$, d'où $\alpha \mid \omega\beta$. En écrivant $\binom{\alpha}{\beta} = \binom{\alpha'\delta}{\beta'\delta}$, il vient $\alpha' \mid \omega\beta'$, d'où $\alpha' \mid \omega$, et (par symétrie) $\alpha'\beta' \mid \omega$, *i. e.* $\frac{\alpha\beta}{\delta^2} = \frac{\mu}{\delta} \mid \omega$.

Mais on ne peut rien dire de plus en général : si $a = b$ est d'ordre 2, alors $\omega = 1$ (égalité à droite) ; si $\alpha\wedge\beta = 1$, alors $\omega = \alpha\beta$ (égalité à gauche). On pourra si le dénominateur $\alpha \wedge \beta$ vaut 1, cas particulier remarquable.

★ **Cas particulier (ordres étrangers).** *L'ordre du produit de deux éléments qui commutent et d'ordres finis étrangers vaut le produit de leurs ordres :*

$$\left\{\begin{array}{c}\omega(a)\wedge\omega(b) = 1\\ ab = ba\end{array}\right. \Longrightarrow \omega(ab) = \omega(a)\,\omega(b).$$

2.5 Morphismes

Pour tout réel θ, notons $\left\{\begin{array}{l}\overline{\theta} \text{ le complexe } e^{i\theta}, \text{ élément du groupe } (\mathbf{U}, \times),\\ \widetilde{\theta} \text{ la rotation d'angle } \theta, \text{ élément du groupe } (\mathrm{Rot}, \circ),\\ \widehat{\theta} \text{ l'angle de mesure } \theta, \text{ élément du groupe } \left(\mathbf{R}/_{2\pi\mathbf{Z}}, +\right).\end{array}\right.$. Au lieu de symboles coiffants, on gagnera à utiliser des *couleurs*. Il équivaut alors, pour tous réels α, β, γ, d'écrire

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

Ainsi, le calcul effectué dans l'un de trois groupes $(\mathbf{U}, \times)$, $(\mathrm{Rot}, \circ)$ ou $\left(\mathbf{R}/_{2\pi\mathbf{Z}}, +\right)$ 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*.

2.5.1 Définitions & exemples

Pour comprendre des objets, un grand principe est le suivant : *étudier les applications entre ces objets qui "préservent" leur "forme"*. La forme des groupes est donnée par leur langage, à savoir :

1. une loi binaire (la *l. c. i.*) ;
2. un objet distingué (le neutre) ;
3. une loi singulaire (l'inversion).

Définition (morphisme, endo-, iso-, auto-). *On appelle* ***(homo)morphisme de groupes*** *toute application $f : G \longrightarrow H$ dont les source et but sont des groupes qui préserve (on quantifie universellement sur G) :*

1. *le produit $f(ab) = f(a) f(b)$;*
2. *le neutre $f(1) = 1$;*
3. *l'inverse $f\left(a^{-1}\right) = f(a)$.*

Un ***endomorphisme*** *est un morphisme dont source et but coïncident.*
Un ***isomorphisme*** *est un morphisme bijectif.*
Un ***automorphisme*** *est un endomorphisme bijectif. (AUTO = ENDO + ISO)*
On note[24] $\mathrm{End}\, G$ *(resp.* $\mathrm{Aut}\, G$*) l'ensemble des endomorphismes (resp. automorphismes) de G.*

Exercice (monoïde des endomorphismes). *Montrer que* $\mathrm{End}\, G$ *est un monoïde d'inversibles* $\mathrm{Aut}\, G$ *:*

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

On en déduit en particulier que la "relation"[25] « 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[26] – on *ne veut pas* distinguer deux groupes isomorphes. (La même remarque tiendrait en remplaçant "groupe" par n'importe quelle autre structure.)

Culture sagittale. Les trois propriétés définitoires d'un morphisme peuvent d'interpréter en termes de diagrammes commutatifs :

$$\begin{array}{ccc} G \times G & \xrightarrow{(f,f)} & H \times H \\ \downarrow *_G & & \downarrow *_H \\ G & \xrightarrow{f} & H \end{array} \qquad \begin{array}{ccc} \{1_G\} & \longrightarrow & \{1_H\} \\ \downarrow \cap & & \downarrow \cap \\ G & \xrightarrow{f} & H \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow^{-1} & & \downarrow^{-1} \\ G & \xrightarrow{f} & H \end{array} .$$

Pour s'en assurer, regarder l'image d'un objet en haut à gauche par les deux composées allant vers en bas à droite. Par exemple, dans le premier diagramme, un $(a, b) \in G^2$ sera envoyé selon $\downarrow\longrightarrow$ sur $f(ab)$ et selon $\longrightarrow\downarrow$ sur $f(a) f(b)$. On aurait également pu court-circuiter le deuxième diagramme en remplaçant les flèches $\longrightarrow\downarrow$ par une seule flèche $\searrow$.

[24] On pourra trouver la notation $\mathrm{Hom}(F, G)$ pour désigner l'ensemble des morphismes de F vers G. Ainsi aura-t-on l'égalité $\mathrm{End}\, G = \mathrm{Hom}(G, G)$.

[25] Attention, la classe-domaine de cette "relation" n'est pas forcément un ensemble (tout comme l'inclusion, l'équipotence, la subpotence...).

[26] Attention : les objets dont parlent les axiomes de la théorie des groupes ne sont pas des groupes ! Ce sont des transformations, des permutations. Aussi devrait-on plutôt parler de *théorie des transformations*, tout comme on parle de théorie des ensembles, théorie des vecteurs ou de théorie des nombres. C'est seulement quand on jongle entre les différents modèles et que l'on étudie les morphismes les reliant que l'on devrait parler de *théorie des groupes*, théories des univers, théories des espaces vectoriels, théories des modèles des entiers...

Remarque (magmas, monoïde groupes). Reprenons les trois propriétés définitoires d'un morphisme de groupes.

Le point (1) définit un ***morphisme de magmas*** (la loi est préservée)

Les points (1) et (2) définissent un ***morphisme de monoïdes*** (la loi et le neutre sont préservés).

Les points (1) et (2) et (3) définissent un ***morphisme de groupes*** (la loi, le neutre et l'inversion sont préservés).

Ainsi, plus la structure d'enrichit, plus les morphismes sont contraints. Cependant, on montrera (**exercice !**) que[27] :

entre groupes, le point (1) implique tous les points (1), (2) et (3).

Définition - exercices (noyau, image). Soit $f : G \longrightarrow H$. *On définit son* ***noyau***

$$\operatorname{Ker} f := \{a \in G \ ; \ f(a) = 1_H\}.$$

Alors $\operatorname{Ker} f$ *est un sous-groupe de* G *et* $\operatorname{Im} f$ *un sous-groupe de* H. *De plus,* f *est injectif ssi* $\operatorname{Ker} f = \{1\}$. (Tout se passe comme pour les espaces vectoriels.)

Application (définition de π). Le morphisme $\left\{ \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{C}^* \\ t & \longmapsto & e^{it} \end{array} \right.$ est continu et non trivial, donc son noyau ne peut être dense, il est par conséquent discret (*cf.* section 2.4.2), donc de la forme $2\pi\mathbf{Z}$ pour un certain réel $\pi > 0$.

Automorphismes intérieurs. Soit M un monoïde. La conjugaison $x \mapsto mxm^{-1}$ par un inversible donné m définit un automorphisme de M. Un tel automorphisme est dit ***intérieur***[28] et leur ensemble sera noté $\operatorname{Int} M$. **Exercice** : *montrer qu'est un morphisme de groupes* $\left\{ \begin{array}{ccc} M^\times & \longrightarrow & \operatorname{Aut} M \\ m & \longmapsto & x \mapsto mxm^{-1} \end{array} \right.$ *; quelle est son image ? son noyau ?*

Projection *modulo*. Pour tout naturel n, la projection canonique $\mathbf{Z} \twoheadrightarrow {}^{\mathbf{Z}}\!/_{n}$ est un morphisme de groupes (généralisé en T. G.).

Produits de groupes. Soient A et B deux groupes. Sont alors des morphismes de groupes les deux projections canoniques $\left\{ \begin{array}{ccc} A \times B & \twoheadrightarrow & A \\ (a,b) & \longmapsto & a \end{array} \right.$ et $\left\{ \begin{array}{ccc} A \times B & \twoheadrightarrow & B \\ (a,b) & \longmapsto & b \end{array} \right.$. De même, sont des morphismes de groupes les deux injections canoniques $\left\{ \begin{array}{ccc} A & \hookrightarrow & A \times B \\ a & \longmapsto & (a,1) \end{array} \right.$ et $\left\{ \begin{array}{ccc} B & \hookrightarrow & A \times B \\ b & \longmapsto & (1,b) \end{array} \right.$. **Bonus sagittal (exercice !)** : *montrer que ces deux dernières sont les seuls morphismes* (i,j) *faisant commuter le diagramme* $\begin{array}{ccccc} & \overset{(i,j)}{\hookrightarrow} & & \overset{\text{produit}}{\twoheadrightarrow} & \\ A \times B & \longrightarrow\!\!\!\!\!\rightarrow\!\!\!\!\!\rightarrow & (A \times B)^2 & \longrightarrow & A \times B \\ & & = & & \end{array}$.

Plongements. Soit G un sous-groupe d'un groupe H. Est alors un morphisme de groupes l'injection canonique $\left\{ \begin{array}{ccc} G & \hookrightarrow & H \\ a & \longmapsto & a \end{array} \right.$ induite par l'inclusion $G \subset H$ (en anglais : *inclusive mapping*). Réciproquement, l'image d'un morphisme de groupes injectif étant isomorphe au groupe source (**pourquoi ?**),

★ *tout morphisme injectif* doit *être vu* ★ *(on parle alors*
★★ *comme l'*inclusion *d'un sous-groupe* ★★ *de* ***plongement****).*

Par exemple, dans un produit de groupes, on *doit* penser chacun des facteurs comme autant de sous-groupes grâce aux isomorphismes induits par les injections canoniques (à l'instar de $\left\{ \begin{array}{ccc} A & \xrightarrow{\sim} & A \times \{1\} \\ a & \longmapsto & (a,1) \end{array} \right.$), on doit penser chaque facteur *plongé dans* le produit[29]. **Exercice** : *montrer que tous les groupes* ${}^{\mathbf{Z}}\!/_{n}$ *se plongent dans* $\mathbf{U}$.

[27] C'est pourquoi l'on définit souvent dans la littérature un morphisme de groupes comme un morphismes de magmas entre deux groupes. Nous pensons que cela ne met pas en lumière le fait qu'un homomorphisme doit *par étymologie* préserver la structure, d'où notre présentation.

[28] **Culture** : les automorphismes intérieurs sont *génériques*, au sens où à G groupe fixé il y a un sur-groupe $G^\Diamond$ tel que $\operatorname{Int} G^\Diamond$ "contienne" $\operatorname{Aut} G$ (*cf.* T. G.).

[29] Cela servira en fin du D. M. étudiant les sous-groupes de ${}^{\mathbf{Q}}\!/_{\mathbf{Z}}$.

2.5.2 Isomorphismes & invariants d'isomorphie

L'introduction a exhibé des isomorphismes entre trois groupes :

$$\left\{\begin{array}{ccccccc} \mathbf{R} & \twoheadrightarrow & \mathbf{R}/\mathbf{Z} & \xrightarrow{\sim} & \mathbf{U} & \xrightarrow{\sim} & \{\text{rotations de centre } 0\} \\ 2\pi\theta & \longmapsto & \overline{\theta} & \longmapsto & e^{i\theta} & \longmapsto & \text{la rotation d'angle } \theta \end{array}\right. .$$

En restreignant à $n \in \mathbf{N}^*$ fixé la projection $\twoheadrightarrow$ à $\mathbf{Z}\frac{2\pi}{n}$, on obtient[30] des isomorphismes entre des groupes cycliques d'ordre n :

$$\left\{\begin{array}{ccccc} \mathbf{Z}/n & \xrightarrow{\sim} & \mathbf{U}_n & \xrightarrow{\sim} & \{\text{rotation du } n\text{-gone régulier}\} \\ \overline{k} & \longmapsto & e^{2\pi i\frac{k}{n}} & \longmapsto & \text{la rotation d'angle } k\frac{2\pi}{n} \end{array}\right. .$$

Nous allons voir qu'en fait tous les groupes cycliques d'ordre fixés sont isomorphes.

Itération. Soit a dans un monoïde. L'itération fournit un morphisme de monoïdes $\left\{\begin{array}{ccc} \mathbf{N} & \twoheadrightarrow & \langle g\rangle \\ n & \longmapsto & a^n \end{array}\right.$ (**pourquoi** est-il surjectif ?) qui se prolonge lorsque a est inversible en un morphisme de groupes $\left\{\begin{array}{ccc} \mathbf{Z} & \twoheadrightarrow & \langle g\rangle \\ k & \longmapsto & a^k \end{array}\right.$. Le noyau de ce dernier est un sous-groupe de $\mathbf{Z}$, donc est de la forme $\mathbf{Z}\omega$ pour un certain naturel ω : lorsque a est d'ordre infini, on a $\omega = 0$ et le morphisme est un *iso*morphisme, sinon ω vaut l'ordre[31] de a et le morphisme d'itération induit (**exercice !**) un isomorphisme $\left\{\begin{array}{ccc} \mathbf{Z}/\omega & \twoheadrightarrow & \langle g\rangle \\ \overline{k} & \longmapsto & a^k \end{array}\right.$. On en conclut :

$$\textit{tous les groupes cycliques d'ordre fixé sont isomorphes :} \left\{\begin{array}{l} \textit{à } \mathbf{Z} \textit{ (si ordre infini)} \\ \textit{à } \mathbf{Z}/\omega \textit{ (si ordre fini } \omega\textit{)} \end{array}\right. .$$

Intéressons-nous à présent à la question de déterminer si des groupes donnés sont isomorphes.

Question. *Est-ce les groupes* $\mathbf{U}_4$ *et* $\mathbf{U}_2 \times \mathbf{U}_2$ *sont isomorphes ?* On serait tenté de répondre "oui" vu les cardinaux...

Regardons plus généralement tous les morphismes de $\mathbf{U}_4$ vers $\mathbf{U}_2^2$. Soit φ un tel morphisme. Observer que φ est déterminé par $\varphi(i)$ vu que $\mathbf{U}_4$ est engendré par i : on a $\forall k \in \mathbf{Z},\ \varphi\left(i^k\right) = \varphi(i)^k$. Par ailleurs, les éléments de $\mathbf{U}_2$ étant tués après itération, il est de même dans toute puissance de $\mathbf{U}_2$, en particulier dans $\operatorname{Im}\varphi$, d'où la nullité de $\varphi\left(i^2\right) = \varphi(i)^2$: ainsi tombe en défaut l'injectivité de φ (son noyau n'est pas trivial car contient ± 1) qui du coup ne peut être un isomorphisme.

Question. *Lesquels groupes sont isomorphes parmi* $\mathbf{Z}$, $\mathbf{U}_8$, $\mathbf{U}_4 \times \mathbf{U}_2$, $\mathbf{U}_2^3$, $\mathbf{H}_8$ *et* D_8 *(les symétries du carrés) ?*

Au lieu de bricoler "à la main" comme ci-dessus (ce qui serait fastidieux), on va chercher des *invariants* d'isomorphie afin d'éliminer des candidats.

Le premier invariant est bien sûr le *cardinal* (un isomorphisme est bijectif !). On peut donc éliminer $\mathbf{Z}$ de la liste ci-dessus (qui sera tout seul dans sa classe d'isomorphie).

Ensuite, un isomorphisme doit préserver tous les énoncés s'écrivant dans le langage des groupes, ce qui nous donne beaucoup d'invariants[32] :

1. le *caractère abélien* (et plus généralement les *centralisateurs*) ;
2. l'*ordre du centre* ;
3. les *classes de conjugaison* ;

[30] Proprement, la projection $\mathbf{R} \twoheadrightarrow \mathbf{R}/\mathbf{Z}$ induit une projection $\mathbf{Z}\frac{2\pi}{n} \twoheadrightarrow \frac{2\pi}{n}\mathbf{Z}/\mathbf{Z}$ et il n'est pas difficile de montrer que ce dernier groupe est isomorphe à $\mathbf{Z}/n$: $\left\{\begin{array}{ccccc} \mathbf{Z}\frac{2\pi}{n} & \twoheadrightarrow & \frac{2\pi}{n}\mathbf{Z}/\mathbf{Z} & \xrightarrow{\sim} & \mathbf{Z}/n \\ k\frac{2\pi}{n} & \longmapsto & \overline{\frac{k}{n}} & \longmapsto & \overline{k} \end{array}\right.$.

[31] On aurait ainsi pu définir l'ordre de a comme le générateur > 0 du noyau de son morphisme d'évaluation. Ce point de vue sera adopté dans les anneaux (où nous itérerons l'unité) car, contrairement aux éléments d'ordre infini, on n'aura alors pas à distinguer le cas du noyau nul.

[32] À notre connaissance, on ne peut pas remontrer de l'identité de tous ces invariants au caractère isomorphe de deux groupes. Nous donnons ici uniquement des moyens de *nier* l'existence d'isomorphismes, moyens que par ailleurs l'on ne doit pas s'empêcher d'utiliser pour investiguer la *construction* d'isomorphismes – bien au contraire.

4. le *nombre minimal de générateurs*[33] ;
5. les *caractères*[34] ;
6. la *torsion*[35] d'ordre fixé ;
7. les *ordres* des éléments...

Ainsi aurait-on pu dire, pour nier le caractère isomorphe des groupes $\mathbf{U}_4$ et $\mathbf{U}_2 \times \mathbf{U}_2$, que tous les éléments de $\mathbf{U}_2 \times \mathbf{U}_2$ sont tués après deux itération alors que ce n'est pas le cas de l'élément i de $\mathbf{U}_4$ (cet argument est noyé dans la preuve ci-dessus). Ce même argument permet d'isoler le candidat $\mathbf{U}_2^3$ des autres (qui contiennent tous des éléments d'ordre 4). Par ailleurs, sont tués après quatre itérations tous les groupes à l'exception de $\mathbf{U}_8$, ce qui isole ce dernier.

La caractère abélien permet par ailleurs de regrouper d'une part les groupes abéliens $\mathbf{U}_8$, $\mathbf{U}_4 \times \mathbf{U}_2$ et $\mathbf{U}_2^3$ (dont on vient de voir qu'aucun n'est isomorphe à l'autre), d'autre part ceux non abéliens $\mathbf{H}_8$ et D_8. Reste à statuer sur ces deux derniers. Listons pour cela précisément les ordres :

$\mathbf{H}_8$:

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

et D_8 :

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

.

On voit alors que $\mathbf{H}_8$ possède une seule involution alors que D_8 en possède cinq, ce qui ruine leur possible caractère isomorphe.

Exercice. *Dresser les tables des ordres des autres groupes et montrer que les listes ("ensembles" avec répétitions et sans ordre) des ordres sont toutes distinctes.* **Sanity check** : tous les ordres doivent diviser 8 (**pourquoi ?**).

Conclusion. Les groupes ci-dessus fournissent autant de classes d'isomorphie.

Culture (exo pénible). On a en fait décrit tous les groupes d'ordre 8.

Exercice (compatibilité du produit cartésien avec "être isomorphe à"). Soient $\alpha : A \xrightarrow{\sim} A'$ et $\beta : B \xrightarrow{\sim} B'$ deux isomorphismes de groupes. *Montrer que que les groupes produit $A \times B$ et $A' \times B'$ sont isomorphes.* **Bonus sagittal** *: montrer l'unicité de l'isomorphisme si l'on exige la commutativité du diagramme*

$$\begin{array}{ccccc} A & \hookrightarrow & A \times B & \hookleftarrow & B \\ \alpha \downarrow \simeq & & \downarrow ? & & \beta \downarrow \simeq \\ A' & \hookrightarrow & A' \times B' & \hookleftarrow & B' \end{array} .$$

Exercices (commutativité et associativité du produit de groupes). Soient trois groupes A, B, C.

Montrer que les produits $A \times B$ et $B \times A$ sont isomorphes. **Bonus sagittal** *: montrer l'unicité de l'isomorphisme si l'on exige la commutativité du diagramme*

$$\begin{array}{ccccc} & \hookrightarrow & A \times B & \hookleftarrow & \\ A & & \downarrow ? & & B \\ & \hookrightarrow & B \times A & \hookleftarrow & \end{array} .$$

Montrer que les produits $A \times (B \times C)$ et $(A \times B) \times C$ sont isomorphes. **Bonus sagittal** *: montrer l'unicité de l'isomorphisme si l'on exige la commutativité du diagramme*

$$\begin{array}{ccccccc} & \hookrightarrow & A \times (B \times C) & \hookleftarrow & A & \hookrightarrow & \\ & & \uparrow & & & & \downarrow \\ B \times C & & \hookleftarrow & & B & & A \times B \\ & & \uparrow & & & & \downarrow \\ & \hookleftarrow & C & \hookrightarrow & (A \times B) \times C & \hookleftarrow & \end{array}$$

(où le morphisme $A \times (B \times C) \xrightarrow{?} (A \times B) \times C$ n'a pas été précisé par commodité de lecture).

2.5.3 Transport de structure

Reprenons le problème des chapeaux. Notons C l'ensemble des couleurs et n son cardinal. On a donc une bijection $\varphi : \left\{ \begin{array}{ccc} C & \xrightarrow{\sim} & \mathbf{U}_n \\ c & \longmapsto & \mathbf{c} \end{array} \right.$. Pour définir le composé de deux couleurs de C, on va les "voir" dans $\mathbf{U}_n$, les y

[33] Cela s'appelle la *dimension* en théorie des espaces vectoriels. Cependant, prendre gare avec les groupes que toutes les familles génératrices minimales n'ont pas forcément même longueur : le groupe $\mathbf{Z}$ est engendré d'une part par 1, d'autre part par 2 et 3 mais n'est engendré ni par 2 ni par 3.

[34] Un ***caractère*** d'un groupe G est un morphisme de G vers $\mathbf{C}^*$. L'analogue vectoriel des caractères sont les formes linéaires.

[35] Un élément est dit de n-torsion (ou d'ordre au plus n) s'il est tué après n itérations. Ainsi un élément est-il d'ordre n ssi il est de n-torsion mais pas de k-torsion pour tout $k < n$.

composer, puis les "revoir" dans C :

$$\begin{array}{ccc} C^2 & \overset{?}{\dashrightarrow} & C \\ \simeq\downarrow (\varphi,\varphi) & & \simeq\uparrow \varphi^{-1} \\ \mathbf{U}_n^2 & \xrightarrow{\times} & \mathbf{U}_n \end{array} \qquad \begin{array}{ccc} (a,b) & \overset{?}{\dashrightarrow} & \varphi^{-1}(\mathbf{a}\times\mathbf{b}) \\ \simeq\downarrow (\varphi,\varphi) & & \simeq\uparrow \varphi^{-1} \\ (\mathbf{a},\mathbf{b}) & \xrightarrow{\times} & \mathbf{a}\times\mathbf{b} \end{array}.$$

On définit donc pour tous $a, b \in C$:

$$a * b := \varphi^{-1}(\mathbf{a}\times\mathbf{b}).$$

La bijection φ devient alors un isomorphisme de groupes : la définition même donne $\varphi(a*b) = \varphi(a)\times\varphi(b)$. Mais il faut avant cela montrer que C est un groupe pour $*$. Par exemple, l'associativité découle de (l'injectivité de φ et de)

$$\varphi(a*(b*c)) := \mathbf{a}\times\varphi(b*c) = \mathbf{a}\times(\mathbf{b}\times\mathbf{c}) = (\mathbf{a}\times\mathbf{b})\times\mathbf{c} = \varphi(a*b)*\mathbf{c} = \varphi((a*b)*c).$$

En fait, *toutes* les propriétés de la structure transportée vont ainsi se retrouver "greffées" sur l'ensemble au départ astructuré ! (**exercice** : *vérifier que le neutre et l'inversibilité sont bien transportés*).

Exemple 0. On a vu section 2.3 comment retrouver la loi $a*b := \frac{a+b}{1+ab}$ en conjuguant l'addition usuelle par th. La loi $*$ sera donc associative, unifère de neutre $\operatorname{th} 0 = 0$ et abélienne et tout élément admettra un inverse.

Exemple 1. *On écrit au tableau les nombres* $1, \frac{1}{2}, \frac{1}{3}, ..., \frac{1}{2014}$. *On en choisit au hasard deux, mettons* a *et* b*, et on les remplace par* $a+b+ab$. *Donner l'ensemble des valeurs prises par le nombre final obtenu au bout de* 2013 *étapes.*

Notons $*$ la loi $(a,b) \mapsto a+b+ab$. Il serait agréable de montrer que $*$ est associative et commutative : la seule valeur possible serait alors le composé des 2014 nombres de départs. On peut montrer l'associativité à la main mais il est plus judicieux de réécrire

$$a*b = (a+1)(b+1) - 1 = \varphi^{-1}(\varphi(a)\varphi(b))$$
où $\varphi : x \mapsto x+1$. En deux dimensions :
$$\begin{array}{ccc} (a,b) & \xrightarrow{*} & ab+a+b \\ \simeq\downarrow(\varphi,\varphi) & & \simeq\uparrow\varphi^{-1} \\ (a+1,b+1) & \xrightarrow{\times} & ab+a+b+1 \end{array}.$$

Les propriétés de la loi $\times$ se transportent donc à $*$: ainsi tombent les commutativité et associativité recherchées. Enfin, le calcul du composé cherché est facilité une fois comprise $*$ comme conjuguée de la multiplication réelle : il vaut

$$\varphi^{-1}\left(\varphi(1)\varphi\left(\frac{1}{2}\right)\varphi\left(\frac{1}{3}\right)\cdots\varphi\left(\frac{1}{2014}\right)\right) = \left(2\frac{3}{2}\frac{4}{3}\frac{5}{4}\cdots\frac{2015}{2014}\right) - 1 = 2014.$$

Exemple 2 (anneaux $\mathfrak{P}(A)$). Soit A un ensemble. Notons $\mathbf{F}_2$ le groupe additif $\mathbf{Z}/2$ muni de la multiplication $\overline{a}\overline{b} := \overline{ab}$ (**exercice** : *vérifier qu'elle est bien définie*). Rappelons que les parties de A sont codées par les applications de $\mathbf{F}_2^A$ *via* la bijection

$$\left\{\begin{array}{ccc} \mathfrak{P}(A) & \xrightarrow{\sim} & \mathbf{F}_2^A \\ P & \longmapsto & \chi_P : \left\{\begin{array}{ccc} A & \longrightarrow & \mathbf{F}_2 \\ a & \longmapsto & \left\{\begin{array}{l} 1 \text{ si } a\in P \\ 0 \text{ si } a\notin P \end{array}\right. \end{array}\right. \\ \{a\in A\ ;\ f(a)=1\} & \longleftarrow & f \end{array}\right.$$

(**exercice** : *vérifier que les deux applications données sont réciproques l'une de l'autre*)

On remarquera alors que les lois (produit) $\times$ et $+$ de $\mathbf{F}_2^A$ correspondent respectivement à $\cap$ et à Δ, au sens où

$$\chi_{P\cap Q} = \chi_P\chi_P \text{ et } \chi_{P\Delta Q} = \chi_P + \chi_Q \text{ pour toutes parties } P, Q \subset A.$$

[dessin : exemple $A = \{a,b,c,d\}$, deux parties, leurs codages binaires, les patates] On retrouve ainsi que $\cap$ est associative, commutative, idempotente et unifère de neutre $\chi^{-1}(1) = A$. On prouve par le même coup que Δ est associative, unifère de neutre $\chi^{-1}(0) = \emptyset$, involutive, et que $\cap$ est distributive sur Δ. Sans aucun effort.

Exemple 3 (groupes symétriques). Soit $\varphi : A \xrightarrow{\sim} B$ une bijection. Rappelons (*cf.* section 2.3) que les groupes symétriques $\mathfrak{S}_A$ et $\mathfrak{S}_B$ sont alors conjugués *via* la conjugaison $i_\varphi : \left\{ \begin{array}{ccc} \mathfrak{S}_A & \xrightarrow{\sim} & \mathfrak{S}_B \\ \sigma & \longmapsto & \varphi\sigma\varphi^{-1} \end{array} \right.$. Regardons comment se transporte la loi de $\mathfrak{S}_A$ *via* la bijection i_φ :

$$\begin{array}{ccc} (\sigma, \rho) \in \mathfrak{S}_B & \overset{?}{\dashrightarrow} & \sigma\rho \\ \simeq\downarrow (i_\varphi, i_\varphi) & & \simeq\uparrow i_\varphi^{-1} \\ \left(\varphi\sigma\varphi^{-1}, \varphi\rho\varphi^{-1}\right) & \xrightarrow{\circ} & \left(\varphi\sigma\rho\varphi^{-1}\right) \end{array} .$$

On retrouve la loi de $\mathfrak{S}_B$. Ainsi la structure transportée était-elle *déjà* présente. On retiendra tout simplement que

$$\textit{la conjugaison } \left\{ \begin{array}{ccc} \mathfrak{S}_A & \xrightarrow{\sim} & \mathfrak{S}_B \\ \sigma & \longmapsto & \varphi\sigma\varphi^{-1} \end{array} \right. \textit{ est un isomorphisme de groupes.}$$

2.5.4 Systèmes générateurs

[non traité en cours]

Comme remarqué lors de la brève étude de $\mathrm{Hom}\left(\mathbf{U}_4, \mathbf{U}_2^2\right)$,

un morphisme est entièrement déterminé par l'image de générateurs.

Ce fait rejoint celui bien connu qu'une application linéaire est entièrement déterminée par les images d'une famille génératrice.

Exemple (endomorphismes des rationnels). *Déterminer* $\mathrm{End}\,(\mathbf{Q}, +)$.
Soit f un endomorphisme de $(\mathbf{Q}, +)$. Ce dernier groupe étant engendré par les fractions positives de numérateur 1, on va regarder les images des $\frac{1}{d}$. Or, la multiplication par un entier étant l'itération de l'addition, une récurrence immédiate montre l'égalité $f(nq) = nf(q)$ pour tout entier n et pour tout rationnel q, d'où l'on déduit (à $d \in \mathbf{N}^*$ fixé) les égalités $df\left(\frac{1}{d}\right) = f\left(d\frac{1}{d}\right) = f(1)$. Il en résulte pour tout $(n, q) \in \mathbf{Z} \times \mathbf{N}^*$ les égalités $f\left(\frac{n}{d}\right) = nf\left(\frac{1}{d}\right) = n\frac{f(1)}{d}$, ce qui montre que f est une homothétie de rapport $f(1)$. Réciproquement, toute homothétie de rapport entier convient.

Exemple (morphismes depuis un groupe cyclique). *Déterminer* $\mathrm{End}\,\mathbf{Z}$ *et* $\mathrm{End}\,\mathbf{U}_n$.
Soit $n \in \mathbf{N}$. Alors le groupe $\mathbf{Z}/n$ est monogène (pour $n = 0$, on retrouve $\mathbf{Z}$), donc tout morphisme f de source $\mathbf{Z}/n$ est déterminé par l'image de $\overline{1}$, cette dernière devant par ailleurs être d'ordre au plus n vu les égalités $0 = f\left(\overline{0}\right) = f\left(\overline{n}\right) = f\left(n\overline{1}\right) = nf\left(\overline{1}\right)$. Réciproquement, en notant G le groupe but, tout élément t de $G_{\leq n} := \{g \in G \ ; \ g^n = 1\}$ fournit un morphisme $\overline{k} \mapsto t^k$. On a ainsi des bijections (pour tout groupe G)

$$\left\{ \begin{array}{ccc} \mathrm{Hom}\left(\mathbf{Z}/n, G\right) & \simeq & G_{\leq n} \\ f & \longmapsto & f\left(\overline{1}\right) \\ \overline{k} \mapsto t^k & \longleftarrow & t \end{array} \right. .$$

Ainsi peut-on décrire $\mathrm{End}\,\mathbf{Z} \simeq \mathbf{Z}$ et $\mathrm{End}\,\mathbf{U}_n \simeq \mathbf{U}_n$.

Exemple (groupes linéaires). Soient n et k dans $\mathbf{N}^*$. *Déterminer les morphismes de* $GL_n(\mathbf{C})$ *vers* $\mathfrak{S}_k$.
Soit f un tel morphisme. On rappelle que GL_n est engendré par (si $n \geq 2$) les transvections (toutes conjuguées à $1 + E_{1,2}$) et par les dilatations (de la forme $1 + \lambda E_{i,i}$ avec $\lambda \neq -1$).
Regardons l'image d'une transvection $P\left(1 + E_{1,2}\right)P^{-1}$. Puisque le groupe but $\mathfrak{S}_k$ est fini, toutes les images sont (par Lagrange) d'ordre au plus $|\mathfrak{S}_k|$, donc tous les éléments du groupe source s'écrivant comme puissance $k!$-ième seront d'image triviale. Or l'identité

$$\forall \lambda \in \mathbf{C}, \ \forall a \in \mathbf{Z}, \ (1 + \lambda E_{1,2})^a = 1 + a\lambda E_{1,2}$$

montre que $1 + E_{1,2} = \left(1 + \frac{1}{k!}E_{1,2}\right)^{k!}$ est d'image nulle, donc tous ses conjugués aussi : finalement f agit trivialement sur les transvections.
Regardons l'image d'une dilatation $1+(\lambda - 1)E_{i,i}$. Cette dernière matrice diagonale s'écrit aussi $\left(1 + (\mu - 1)E_{i,i}\right)^{k!}$ pour tout μ racine $k!$-ième de λ, ce qui montre que les dilatations sont (comme les transvections) tuées par f.

Finalement, f est le morphisme trivial.

Exercice. *Déterminer les morphismes de $GL_n(\mathbf{R})$ vers $\mathfrak{S}_k$.*

Exemple (dual d'un groupe symétrique). Soit $n \in \mathbf{N}^*$. *Décrire le* ***dual*** *de $\mathfrak{S}_n$, à savoir l'ensemble des morphismes de $\mathfrak{S}_n$ vers $\mathbf{C}^*$.*

Soit ε un tel morphisme. Rappelons que $\mathfrak{S}_n$ est engendré par les transpositions et que ces dernières sont toutes conjuguées. Le groupe but étant abélien, ε est constant sur chaque classe de conjugaison (écrire $\varepsilon\left(aga^{-1}\right) = \varepsilon(a)\varepsilon(g)\varepsilon(a)^{-1} = \varepsilon(a)\varepsilon(a)^{-1}\varepsilon(g) = \varepsilon(g)$). Les transpositions étant d'ordre au plus 2, leur image commune également, donc vaut ± 1. Finalement, ou bien ε est trivial ou bien ε envoie une permutation σ engendré par T transpositions sur $(-1)^T$. Réciproquement, on montrerait[36] que $\sigma \mapsto (-1)^{n-\#\operatorname{Orb}\sigma}$ est bien un caractère non trivial de $\mathfrak{S}_n$, appelé sa ***signature***.

Finalement, le dual de $\mathfrak{S}_n$ est isomorphe à $\mathbf{U}_2$, l'élément non trivial étant sa signature.

3 Actions de groupes

Soit A un ensemble. On rappelle (*cf.* section 1.2) qu'une *action* sur A est la donnée d'une application

$$\left\{\begin{array}{ccc} \Omega \times A & \longrightarrow & A \\ (\omega, a) & \longmapsto & \omega \cdot a \end{array}\right. .$$

Lorsque l'ensemble opérant Ω est muni d'une structure "taillée" pour agir (typiquement un monoïde ou un groupe, *cf.* section 1), voyons comment l'on peut alors "enrichir" l'action $(\omega, a) \mapsto \omega \cdot a$.

3.1 Action d'un monoïde

Soit M un monoïde.

Définitions-notations (action d'un monoïde). *On dit que le monoïde M* ***agit*** *(ou* ***opère****) sur A si l'on s'est donné un morphisme de monoïdes $M \longrightarrow A^A$.*

Ainsi, tout $m \in M$ peut (et doit !) être vu comme un "endomorphisme"[37] de A. L'image d'un $m \in M$ appliqué sur un $a \in A$ sera noté

$$m \cdot a.$$

Définition (action transitive). *On dira qu'une action du monoïde M sur A est* ***transitive*** *si*

$$\forall a, b \in A,\ \exists m \in M,\ b = m \cdot a$$

En d'autres termes, une action est transitive si on peut "transiter" de n'importe quel élément de A vers n'importe quel autre élément de A *via* un certain agent de M (dépendant des éléments considérés). [dessin]

Pour faire le lien avec la notion d'action définie à la section 1.2, on vérifiera (**exercice !**) qu'une action $\left\{\begin{array}{ccc} M \times A & \longrightarrow & A \\ (m, a) & \longmapsto & m \cdot a \end{array}\right.$ de l'ensemble M sur A (au sens de 1.2) est une "action de monoïde" (au sens ci-dessus) ssi on a (pour tous $m, n \in M$ et tout $a \in A$) les égalités

$$n \cdot (m \cdot a) = (nm) \cdot a \qquad \text{et} \qquad 1 \cdot a = a.$$

Exemples.

1. Lorsque $M = A^A$, on a une action *fonctionnelle* $m \cdot a := m(a)$.
2. Lorsque $A = M$, on a une action par *composition* $m \cdot a := ma$ (de même si A est un monoïde dont M est un sous-monoïde).
3. Lorsque A est l'ensemble des parties de M, on a une action par *composition* $m \cdot P := mP = \{mp\}_{p \in P}$.

[36] on le fera dans le cours sur les groupes symétriques

[37] L'ensemble A n'ayant *a priori* aucune structure, il ne faut chercher à donner plus de sens à "morphisme" que simplement "application". Un endomorphisme d'un ensemble est juste une application qui stabilise ce dernier.

4. Lorsque A est un monoïde et quand $M = A^\times$, on a une action par *conjugaison* $m \cdot a := mam^{-1}$ (par exemple quand $A = M_n(\mathbf{R})$ et $M = GL_n(\mathbf{R})$).
5. Lorsque A est un monoïde et quand $M = \mathbf{N}$, on a une action par *itération* $m \cdot a := a^m$ (de même si A est un groupe et si $M = \mathbf{Z}$).
6. Lorsque le morphisme est constant, il vaut constamment Id_A (**pourquoi ?**) et on a alors une action *triviale* $m \cdot a := a$.
7. Lorsque A est une puissance E^I (où E et I sont deux ensembles invoqués) et $G := \mathfrak{S}_I$, on a une action par *permutation* $\sigma \cdot (a_i) := \left(a_{\alpha(i)}\right)$. Ainsi, considérer à (a_i) fixé l'ensemble des $\left(a_{\alpha(i)}\right)$ permet de coder un ensemble $[a_i]_{i\in I}$ sans ordre mais avec répétition, ce qu'on appelle un ***multi***[38]***-ensemble***.

On suppose désormais que M agit sur A.

Définition (orbite, fixateur, quotient). Soit $a \in A$. *L'**orbite** et le **fixateur** (ou **stabilisateur**[39]) de a (sous l'action donnée) sont respectivement*

$$\begin{aligned} \mathrm{Orb}\, a &:= \quad \{m \cdot a \ ; \ m \in M\} =: M \cdot a \text{ et} \\ \mathrm{Fix}\, a &:= \quad \{m \in M \ ; \ m \cdot a = a\} =: M_a. \end{aligned}$$

*L'ensemble des orbites est appelé ensemble **quotient** de A par (l'action[40] de) M et est noté*[41]

$$ {}_M\backslash^A := \{M \cdot a\}_{a\in A} = \{\mathrm{Orb}\, a\}_{a\in A} \qquad \begin{array}{c}\textit{(le contexte devant clarifier}\\ \textit{l'action sous-entendue de } M\textit{)}\end{array}$$

Exemples-exercices. On reprend les exemples ci-dessus un par un. Soit $a \in A$

1. L'orbite d'un $a \in A$ contient les images par toutes les fonctions constantes, donc vaut tout A. Ainsi l'action fonctionnelle est-elle transitive et le quotient trivial : ${}_{A^A}\backslash^A = \{A\}$. On a par ailleurs une bijection $\left\{ \begin{array}{ccc} \mathrm{Fix}\, a & \xrightarrow{\sim} & A^{A\setminus\{a\}} \\ f & \longmapsto & f_{|A\setminus\{a\}} \end{array} \right.$ décrivant le fixateur.
2. L'orbite $\mathrm{Orb}\, a$ est la "droite" Ma engendrée par a. Par conséquent,

   $$\begin{array}{c} \textit{lorsque } M \textit{ est un sous-monoïde de } A \textit{ agissant par composition,} \\ \textit{les quotient s'écrivent } {}_M\backslash^A = \{Ma\}_{a\in A} \textit{ et } {}^A\!/_M = \{aM\}_{a\in A}\,. \end{array}$$

   Le fixateur est l'ensemble des neutres à gauche de a (dans M) ; si $a \in M^\times$ il n'y a que le neutre.
3. Pas grand chose d'intéressant à dire.
4. L'orbite s'appelle une ***classe de conjugaison***. Le fixateur est le centralisateur : $\mathrm{Fix}\, a = \mathrm{Comm}\, a$. On retiendra que

   $$\textit{commuter, c'est être fixé par conjugaison.}$$

   Le quotient est l'ensemble des classes de conjugaison.
5. L'orbite est le sous-monoïde/groupe engendré $\mathrm{Orb}\, a = \langle a \rangle$, donc le quotient est formé des sous-monoïdes/groupes *monogènes*. Le fixateur va dépendre du bouclage :
   (a) si a est neutre, alors on boucle immédiatement et $\mathrm{Fix}\, a = \langle 1 \rangle$. Supposons donc $a \neq 1_A$:
   (b) ou bien $\mathrm{Fix}\, a$ est réduit à $\{1\}$ (il n'y pas de bouclage (par exemple, dans le cas d'un groupe, quand a est d'ordre infini) ou bien il y un bouclage à partir de $a^2, a^3, ...$) ;

[38] *multi* car chacun de ses éléments possède une certaine *multi*plicité

[39] Une partie *stable* par une application n'ayant pas forcément tous ses points *fixés*, nous pensons le vocabulaire "stabilisateur" ne guidant pas assez finement l'intuition. De l'autre point de vue de ce vocabulaire actif-passif, le mot "*fixateur*" évoque l'ensemble des agents *fixant*. La terminologie permettra donc (par exemple lorsque $M = A^A$) de ne pas confondre un ensemble de points fixes $\mathrm{Fix}\, m$ avec un fixateur $\mathrm{Fix}\, a$.

[40] pour l'importance du contexte, $GL_n(\mathbf{R})$ peut agir *par conjugaison* sur $M_n(\mathbf{R})$ mais aussi *par composition*

[41] Remarquer que les M sont du même côté, celui depuis où il agit (ici à gauche). On pourrait tout aussi bien définir une action à *droite* par un *anti*morphisme $\left\{ \begin{array}{ccc} M & \longrightarrow & A^A \\ m & \longmapsto & a \mapsto a \cdot m \end{array} \right.$, ce qui donnerait les propriétés $a \cdot 1 = a$ et $(a \cdot m) \cdot n = a \cdot (mn)$. Les orbites seraient alors définies par les $a \cdot M$ et l'ensemble quotient noté ${}^A\!/_M$. On peut même combiner les deux quand A est agi des deux côtés de manière "associative" (par exemple par compositions), d'où des "orbites" $M \cdot a \cdot N$ et un "quotient" ${}_M\backslash^A\!/_N$. Mais on s'en retiendra dans ce cours.

(c) ou bien $\operatorname{Fix} a$ contient un $\omega + 1 \geq 2$. En imposant ω minimal, on obtient $\operatorname{Fix} a = 1 + \langle \omega \rangle$ (dans le cas d'un groupe, quand a est d'ordre fini, on obtient $\omega = \omega(a)$).

6. L'orbite est triviale $\operatorname{Orb} a = \{a\}$ et tout agent fxe : $\operatorname{Fix} a = M$. Le quotient est A vu à travers la bijection $\begin{cases} {}_M\backslash^A & \xrightarrow{\sim} & A \\ \{a\} & \longmapsto & a \end{cases}$.
7. L'orbite d'une famille (a_i) est le multi-ensemble $[a_i]$. Le fixateur est formé des ***symétries*** de la famille.

Exercices (actions quotients).

1. *Montrer que l'action de M induite sur $\mathfrak{P}(A)$ se restreint en une action triviale de $M^\times$ sur*[42] ${}_M\backslash^A$.
2. *Soit Ω agissant à droite sur A de façon compatible*[43] *avec l'action à gauche de M. Montrer que M agit sur*[44] ${}^A/_\Omega$.

On retiendra surtout le cas particulier où $M = A$ et un sous-monoïde $\Omega = N$ agissent par composition :

lorsque N est un sous-monoïde de M, en notant $\overline{a} := aN$ (pour tout a),
on a une action de M sur le quotient ${}^M/_N$ donnée par $m \cdot \overline{a} = \overline{ma}$.

Propriétés (fixateurs, orbites).

1. *L'action est transitive ssi il n'y a qu'une seule orbite,* i. e. *ssi* ${}_M\backslash^A = \{A\}$.
2. *Les fixateurs* $\operatorname{Fix} a$ *sont des sous-monoïdes de M.*
3. *Les orbites* $\operatorname{Orb} a$ *recouvrent tout A.*
4. *On a l'équivalence (pour tous a, b dans A)*

$$a \in \operatorname{Orb} b \iff \operatorname{Orb} a \subset \operatorname{Orb} b.$$

Démonstration.

1. On a les équivalences suivantes :

$$\begin{aligned} \text{l'action est transitive} &\iff \forall a, b \in A,\ \exists m \in M,\ b = m \cdot a \\ &\iff \forall a \in A,\ \forall b \in A,\ b \in \operatorname{Orb} a \\ &\iff \forall a \in A,\ A \subset \operatorname{Orb} a \\ &\iff \forall a \in A,\ \operatorname{Orb} a = A \\ &\iff {}_M\backslash^A = \{A\}\text{, ce qui conclut.} \end{aligned}$$

   Soit $a \in A$.
2. L'appartenance $1 \in \operatorname{Fix} a$ équivaut à l'axiome $1 \cdot a = a$. Soient par ailleurs s et t dans $\operatorname{Fix} a$: on a alors $(st) \cdot a = s \cdot (t \cdot a) = s \cdot a = a$, d'où $st \in \operatorname{Fix} a$.
3. On a $a = 1 \cdot a \in \operatorname{Orb} a \subset \bigcup_{x \in A} \operatorname{Orb} x$.
4. On vient de traiter le sens $\Longleftarrow$ (écrire $a \in \operatorname{Orb} a \subset \operatorname{Orb} b$). Pour le sens direct, écrire $a = m \cdot b$ montre que tout $n \cdot a$ de $\operatorname{Orb} a$ s'écrit $n \cdot (m \cdot b) = (nm) \cdot b$, lequel reste dans $\operatorname{Orb} b$.

Question ("partition" orbitale). Le dernier point montre que la relation "$a \in \operatorname{Orb} b$" (d'argument a, b) est réflexive et transitive. Est-elle en outre symétrique, *i .e.* est-ce une relation d'équivalence[45] ? En d'autres termes, le recouvrement par les orbites est-il une *partition*, *i. e.* deux orbites dis*tinctes* sont-elles toujours dis*jointes* ? Le cas de l'action itérative de $\mathbf{N}$ sur un $\langle a \rangle$ montre que *non* : l'orbite d'un $a^{n \geq 0}$ est $\left\{a^k\ ;\ k \geq n\right\}$, de sorte que les $\operatorname{Orb} a^n$ forment une suite décroissante.

[42] l'action de M sur A est quelconque, ce n'est pas forcément la composition

[43] comprendre $m \cdot (a \cdot \omega) = (m \cdot a) \cdot \omega$ pour tout $(m, a, \omega) \in M \times A \times \Omega$ (où l'on a abusivement utilisé le même $\cdot$ pour les deux actions)

[44] avec les notations évidentes ${}^A/_\Omega := \{a \cdot \Omega\}_{a \in A}$ et $a \cdot \Omega := \{a \cdot \omega\}_{\omega \in \Omega}$

[45] La réflexivité provient d'un neutre pour l'action, la symétrie viendra d'un inverse, la transitivité résulte de ce que l'action préserve le produit. Ainsi émerge naturellement la structure de *groupe* lorsque l'on vise le partitionnement par les orbites.

Essayons de voir le détail. Soit $m\cdot a = n\cdot b$ un point de rencontre de deux orbites $\mathrm{Orb}\, a$ et $\mathrm{Orb}\, b$. On voudrait montrer la double-inclusion $\mathrm{Orb}\, a = \mathrm{Orb}\, b$, *i. e.* la double-appartenance $\begin{cases} a \in M\cdot b \\ b \in M\cdot a \end{cases}$. Afin d'isoler a (ou b) à partir de l'égalité $m\cdot a = n\cdot b$, on aimerait bien pouvoir simplifier par m (ou n). Or, si m est inversible, on pourra bien écrire

$$a = 1\cdot a = \left(m^{-1}m\right)\cdot a = m^{-1}\cdot(m\cdot a) = m^{-1}\cdot(n\cdot b) = \left(m^{-1}n\right)\cdot b,$$ ce qui conclura.

Observons alors (**exercice !**) que le morphisme $M \longrightarrow A^A$ induit sur les inversibles un morphismes de groupes $M^\times \longrightarrow \mathfrak{S}_A$. Les orbites $M^\times\cdot a$ pour cette nouvelle action vont alors former une partition de A (d'après le calcul ci-dessus) dont la relation d'équivalence associée est "$a \in \mathrm{Orb}\, b$".

3.2 Action d'un groupe

Dorénavant, on supposera que $M = M^\times$ est un groupe, noté G.

Définition-propriétés (action d'un groupe). *On dit que le groupe G **agit** (ou **opère**) sur A si l'on s'est donné un morphisme de groupes $G \longrightarrow \mathfrak{S}_A$.*

Ainsi, tout $g \in G$ peut et doit être vu comme une *permutation*[46] $a \mapsto g\cdot a$ de l'ensemble agi.

★ Les orbites forment alors une partition de l'ensemble agi dont l'ensemble quotient est noté ${}_G\backslash^A = \{G\cdot a\}_{a\in A}$.

Les fixateurs sont des sous-groupes de G (**exercice** : *montrer la stabilité par inversion*).

Soit H est sous-groupe de G.

Exercice. *Décrire les orbites et les fixateurs de l'action de G sur ${}^G/_H$ par composition.*

Lemme (cardinal quotient). *Si G est fini, on a alors les égalités*

$$\left|{}^G/_H\right| = \frac{|G|}{|H|} = \left|{}_H\backslash^G\right|. \qquad \left(\text{mémento : } \begin{array}{c} \textit{le cardinal d'un quotient} \\ \textit{est le quotient des cardinaux} \end{array}\right)$$

Démonstration. Les éléments de ${}^G/_H$ sont des translatés de H ; or dans un groupe les translations[47] sont toujours injectives, ce qui montre que toutes les classes aH sont équipotentes – ainsi sont-elles toutes d'ordre $|H|$. Puisque ces classes sont au nombre de $\left|{}^G/_H\right|$ et partitionnent un ensemble de cardinal $|G|$, on en déduit l'égalité voulue :

$$|G| = \left|\biguplus_{C\in\, {}^G/_H} C\right| = \sum_{C\in\, {}^G/_H} |C| = \sum_{C\in\, {}^G/_H} |H| = |H| \sum_{C\in\, {}^G/_H} 1 = |H|\ \left|{}^G/_H\right|.$$

Corollaire (Lagrange). *L'ordre de tout sous-groupe divise l'ordre du groupe.*

On retrouve ainsi, lorsque H est cyclique (*i. e.* monogène fini), le "Lagrange soft" annoncé section 2.4.4.

Voyons à présent deux propositions très générales (la seconde cas particulier de la première), avec leurs corollaires respectifs. Ensemble, ils permettrons de montrer le premier théorème de Sylow, conclusion de ce cours. (Le deuxième théorème de Sylow est montré en T. G..)

Soit $a \in A$.

Proposition. *On a une équipotence* $\begin{cases} {}^G/_{\mathrm{Fix}\, a} & \xrightarrow{\sim} & \mathrm{Orb}\, a \\ \overline{g} & \longmapsto & g\cdot a \end{cases}$.

[46] Lorsque A est muni d'une structure (magma, monoïde, groupe, anneau, corps, espace vectoriel, algèbre...), une *action d'un monoïde M* est un morphisme de monoïdes $M \longrightarrow \mathrm{End}\, A$ et une *action d'un groupe G* est un morphisme de groupes $G \longrightarrow \mathrm{Aut}\, A$. Lorsque la structure est "nue", *i. e.* ensembliste, les endomorphismes de l'ensemble A sont les *fonctions* de A^A et les automorphismes de l'ensemble A sont les *permutations* de $\mathsf{S}(A)$ (*i. e.* les endomorphismes bijectifs).

[47] d'un côté comme de l'autre : le traitement des classes Ha et du quotient ${}_H\backslash^G$ est rigoureusement identique

Corollaire. *Lorsque G est fini, on a l'égalité*

$$\#\operatorname{Orb} a \ \times \ \#\operatorname{Fix} a = |G|\,, \qquad \textit{i. e.} \qquad |G| = |G \cdot a| \ \ |G_a|\,.$$

★ Sous-corollaire (équation aux classes). *Supposons A et G finis. Alors il y a une famille finie de sous-groupes (G_i) telle que*

$$|A| = \sum_i \frac{|G|}{|G_i|}.$$

Démonstration du sous-corollaire. On numérote les orbites Ω_i de A, on choisit[48] un représentant a_i dans chaque orbite Ω_i, on partitionne A selon ses orbites et on utilise le corollaire, ce qui donne (en posant $H_i := \operatorname{Fix} a_i$)

$$|A| = \sum_i |\Omega_i| = \sum_i |\operatorname{Orb} a_i| = \sum_i \frac{|G|}{|\operatorname{Fix} a_i|} = \sum_i \frac{|G|}{|H_i|}.$$

Démonstration du corollaire. L'équipotence donne l'égalité cardinale $|\operatorname{Orb} a| = \left|{}^{G}\!/_{\operatorname{Fix} a}\right|$ et le lemme $\left|{}^{G}\!/_{\operatorname{Fix} a}\right| = \frac{|G|}{|\operatorname{Fix} a|}$.

Démonstration de la proposition. Notons φ l'application de l'énoncé. La surjectivité de φ est immédiate. Montrons qu'elle est bien définie. Soit $(g, h, s) \in G^2 \times \operatorname{Fix} a$ tel que $h = gs$: on a alors $h \cdot a = (gs) \cdot a = g \cdot (s \cdot a) = g \cdot a$, comme voulu. Enfin, l'injectivité découle des équivalences (à $g, h \in G$ fixés)

$$\varphi(g) = \varphi(h) \iff g \cdot a = h \cdot a \iff h^{-1} g \cdot a = a \iff h^{-1} g \in \operatorname{Fix} a \iff g \in h \operatorname{Fix} a \iff \overline{g} = \overline{h}.$$

Exercice. *Que devient le corollaire quand G agit sur ${}^{G}\!/_{H}$ par composition ?*

On désinvoque désormais H.

★ Proposition (théorème du rang[49]). *Tout morphisme de groupes $f : G \longrightarrow H$ induit un isomorphisme de groupes* $\begin{cases} {}^{G}\!/_{\operatorname{Ker} f} & \xrightarrow{\sim} & \operatorname{Im} f \\ \overline{a} & \longmapsto & f(a) \end{cases}$.

Corollaire (formule du rang[50]). *Soit $f : G \longrightarrow H$ un morphisme de groupes finis. On a alors l'égalité*

$$|G| = \#\operatorname{Im} f \ \ \#\operatorname{Ker} f.$$

Sous-corollaire (lemme de Cauchy abélien). *Supposons G fini. Soit p un premier divisant $|G|$. Alors G possède un sous-groupe d'ordre p.*

Démonstration du corollaire. Comme ci-dessus : $|\operatorname{Im} f| = \left|{}^{G}\!/_{\operatorname{Ker} f}\right| = \frac{|G|}{|\operatorname{Ker} f|}$.

Démonstration (de Cauchy abélien). Puisque G est abélien, la surjection $s : \begin{cases} \prod_{g \in G} \langle g \rangle & \twoheadrightarrow & G \\ (a_g) & \longmapsto & \prod a_g \end{cases}$ est un morphisme de groupes, d'où les divisibilités

$$p \mid \#G = \#\operatorname{Im} s \underset{\text{du rang}}{\overset{\text{formule}}{\mid}} \#\operatorname{Dom} s = \#\prod_{g \in G} \langle g \rangle = \prod_{g \in G} \#\langle g \rangle = \prod_{g \in G} \omega(g)\ ;$$

le diviseur p étant premier, il doit diviser l'un des facteurs $\omega(g)$, mettons $p \mid \omega(\gamma)$ pour un $\gamma \in G$. Montrons pour conclure que $g := \gamma^{\frac{\omega(\gamma)}{p}}$ est d'ordre p (alors le groupe $\langle g \rangle$ répondra à la question) : d'une part l'égalité $g^p = \gamma^{\omega(\gamma)} = 1$ montre que $\omega(g)$ divise p, *i. e.* vaut 1 ou p, d'autre part le cas $\omega(g) = 1$ est exclu vu que minimalité de $\omega(g_0)$ empêche l'égalité $\gamma^{\frac{\omega(\gamma)}{p}} = 1$.

Démonstration de la proposition. On applique la proposition précédente à l'action de G sur H définie par $g \cdot h := \varphi(g)\, h$ et au cas particulier $a = 1$: le fixateur de 1 est alors $\operatorname{Ker} \varphi$ et son orbite est $\operatorname{Im} \varphi$.

[48] Pas besoin d'axiome du choix pour cela : tout ensemble fini admet un bon ordre et *a fortiori* une fonction de choix.

[49] Le théorème du rang dans les espaces vectoriel énonce que la restriction d'une application linéaire à tout supplémentaire de son noyau induit un isomorphisme sur son image. Or parler de supplémentaire est une façon déguisée (et moins abstraite) de parler de quotient, ce dernier pouvant être vu comme un supplémentaire "générique".

[50] Lorsque G est un espace vectoriel de dimension finie sur un corps K fini, prendre le logarithme de base $|K|$ fournit la formule du rang connue des applications linéaires.

Seul se rajoute le caractère "morphisme de groupes", ce qui tombe en écrivant (à $a, b \in G$ fixés) $\varphi(\overline{a})\,\varphi\left(\overline{b}\right) = f(a)\,f(b) = f(ab) = \varphi\left(\overline{ab}\right)$.

★ Même si la formule du rang pourrait s'énoncer "les groupes G et $\operatorname{Im} f \times \operatorname{Ker} f$ sont *équipotents*" (énoncé *combinatoire*), elle *ne dit pas* qu'ils sont *isomorphes* ! (énoncé *structurel* plus fort) (*cf.* D. M. pour voir des groupes indécomposables)

On verra une analogie avec la formule du rang vectorielle : même si elle énonce que les noyau et image d'un $f \in L(E)$ ont des *dimensions complémentaires* à celles de E (énoncé *combinatoire*), elle *ne dit pas* que $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont *supplémentaires* ! (énoncé *structurel* plus fort)

Théorème (Sylow). *Supposons G fini. Soient p un premier et v le plus grand naturel tel que $p^v \mid \#G$. Alors G possède un sous-groupe d'ordre p^v.*

Démonstration. On raisonne par récurrence à G *non* fixé sur la valuation v. Lorsqu'elle est nulle, il n'y rien à faire (le sous-groupe trivial est d'ordre p^0). Soit G un groupe tel que $v \geq 1$. Faisons agir G sur lui-même par conjugaison. Les éléments du centre ont tous une orbite réduite à un élément – et réciproquement. L'équation aux classes s'écrit donc

$$|G| = \sum_{g \in Z(G)} 1 + \sum_i \frac{|G|}{|G_i|} = |Z(G)| + \sum_i \frac{|G|}{|G_i|} \quad \begin{array}{c}\text{pour certains sous-groupes } G_i \textit{ stricts} \\ \text{(des commutants d'éléments hors de } Z(G)\text{)}\end{array}.$$

Si l'un des $|G_i|$ est multiple de p^v, on conclut en utilisant l'hypothèse de récurrence. Dans le cas contraire, p divise tous les $\frac{|G|}{|G_i|}$, donc divise leur somme, donc divise $|G| - \sum_i \frac{|G|}{|G_i|} = |Z(G)|$; le centre $Z(G)$ étant abélien, le lemme de Cauchy nous donne alors un sous-groupe Z de $Z(G)$ (donc de G) d'ordre p. Le groupe[51] ${}^{G}\!/_{Z}$ étant de cardinal $\frac{|G|}{p}$, l'hypothèse de récurrence nous en donne un sous-groupe $\mathcal{S}$ d'ordre p^{v-1}. On montre alors [dessin quotient] que la réunion $S := \cup \mathrm{S}$ des éléments de S est un sous-groupe[52] de G tel que $\mathcal{S} = {}^{S}\!/_{Z}$, d'où l'égalité $|S| = |\mathcal{S}|\,|Z| = p^v$.

4 Développements des exercices

Section 1.1.

★ Soit I contenant o et stable par f. L'ensemble $\{P \subset I\ ;\ o \in P \text{ et } \sigma(P) \subset P\}$ est alors non vide, donc admet un *infimum* – son intersection. Les deux conditions $\begin{cases} o \in P \\ \sigma(P) \in P \end{cases}$ passant à l'intersection, cet infimum est un *minimum*.

★ Tout successeur contient au moins l'élément rajouté ($\forall a,\ a \in s(a)$), donc ne peut valoir $\emptyset$.

Soient a et b tels que $s(a) = s(b)$. On a alors l'appartenance $a \in s(a) = s(b) = b \cup \{b\}$, d'où $\begin{cases} \text{ou} & a \in b \\ & a \in \{b\} \end{cases}$. De manière symétrique, on a $\begin{cases} \text{ou} & b \in a \\ & b \in \{a\} \end{cases}$. Si a différait de b, il resterait la conjonction $\begin{cases} a \in b \\ b \in a \end{cases}$, ce qu'exclut l'axiome de fondation (pas de "boucles" pour $\in$).

Section 1.2.

★ Soient u et v deux neutres dans un monoïde. Le composé uv vaut alors d'une part u (car v est neutre) d'autre part v (car u est neutre), d'où l'égalité $u = v$.

★ 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 $\emptyset$.

---

[51] Z commutant avec G, la loi de groupe $(aZ)(bZ) := abZ$ est bien définie

[52] Puisque $1 \in 1Z = \overline{1} \in \mathcal{S}$, on a $1 \in S$. Soit $a \in S$, soit $g \in G$ tel que $a \in gZ$: on alors $a^{-1} \in Z^{-1}g^{-1} \underset{\text{sous-groupe}}{\overset{Z \text{ est un}}{=}} Zg^{-1} \overset{Z \in Z(G)}{=} g^{-1}Z \in \mathcal{S}$, d'où $a^{-1} \in S$. Soit de plus $b \in S$, disons $b \in gZ$: on a alors $ab \in \overline{a}\overline{b} = \overline{ab} \in \mathcal{S}$, d'où $ab \in S$.

★ Pour tout 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 $\mathbf{C}$ (*a fortiori* de $\mathbf{Z}$, $\mathbf{Q}$ et $\mathbf{R}$) pour $+$ est 0 et les deux involutifs pour $\times$ sont ± 1.

Section 1.3.

★ Soient b et β deux symétriques de a. On a alors les égalités $b = b1 = b(a\beta) = (ba)\beta = 1\beta = \beta$.
On a en fait montré qu'*un inverse à droite et un inverse à gauche coïncident.*

★ Soit a inversible. Les applications $a\,\mathrm{Id}$ et $a^{-1}\,\mathrm{Id}$ sont alors réciproques l'une de l'autre, donc bijectives, *a fortiori* surjectives (de même de l'autre sens).
Soit a tel que $a\,\mathrm{Id}$ et $\mathrm{Id}\,a$ soient surjectives. Des antécédents du neutre sont alors des inverses à droite et à gauche de a, donc (exo précédent) coïncident et a est inversible.

★ La régularité d'un a équivaut à l'injectivité des deux homothéties $a\,\mathrm{Id}$ et $\mathrm{Id}\,a$, *i. e.* (par finitude du monoïde de référence) à leur surjectivité, *i. e.* (par l'exercice précédent) à l'inversibiltié de a.

★ Soient $f, g \in A^A$ tels que $g \circ f = \mathrm{Id}$. Alors f est simplifiable à gauche (en composant à gauche par g), donc injective (simplifcations par des fonctions constantes). Par ailleurs, g est surjective (tout $a \in A$ admet $f(a)$ comme antécédent par g), donc régulière à droite (si $\alpha f = \beta f$, alors α et β coïndent sur $\mathrm{Im}\, f = A$).
Soit f injective. On définit une application g sur $\mathrm{Im}\, f$ par $f(a) \mapsto a$ (bien défini par injectivité) et par n'importe quoi ailleurs. On a alors clairement $g \circ f = \mathrm{Id}$.
Soit g régulière à droite. Alors g est surjective (sinon deux fonctions α et β différant uniquement en un point non atteint par g vérifieront $\alpha g = \beta g$) et l'on peut définir[53] une application f qui envoie un a sur l'un de ses antécédents. Il est alors immédiat que $g \circ f = \mathrm{Id}$.

Section 2.1.

★ L'ensemble $\bigcup_{n\in\mathbf{N}^*} \mathbf{U}_n = \bigcup_{n\in\mathbf{N}^*} \left\{e^{2\pi i \frac{k}{n}}\right\}^{k\in\mathbf{Z}} = \left\{e^{2\pi i \frac{k}{n}}\right\}_{n\in\mathbf{N}^*}^{k\in\mathbf{Z}}$ est formé des complexes d'argument multiple rationnel de 2π. Cet ensemble est stable par multiplication (d'une part car l'argument d'un produit est la somme des arguments, d'autre part car $2\pi\mathbf{Q}$ est stable par somme), il contient 1 (argument nul) et est stable par inversion (car $2\pi\mathbf{Q}$ est stable par opposition).

★ 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, b, c distincts dans E. Alors les deux transpositions (a,b) et (a,c) ne commutent pas : on a en effet $(a,b)(a,c) = (a,c,b) \neq (a,b,c) = (a,c)(a,b)$.

★ Nommons A, B, C, D les quatre sommet d'un tétraèdre régulier.
Les six réflexions par rapport aux plans médiateurs des six arêtes réalisent les $\binom{4}{2} = 6$ transpositions de $\mathfrak{S}_4$.
Les huit rotations (d'angle $\pm\frac{2\pi}{3}$) autour des quatre axes passant par un sommet et le centre du tétraèdre réalisent les huit 3-cycles $\mathfrak{S}_4$.
Les trois rotations (d'angle π) autour des quatre axes reliant deux milieux d'arêtes opposées réalisant les trois produit disjoints de transpositions.
Les six 4-cycles seront réalisés comme compositions d'une des six réflexions précédentes par une des trois rotations précédentes.
(**Remarque** : puisque les transpositions engendrent $\mathfrak{S}_4$, il a suffi de regarder les composées des premières réflexions mentionnées)

★ Multiplier $-1 = ijk$ à droite par $-k$ donne $k = ij\left(-k^2\right) = ij$, on a de même (par permutation cyclique) $j = ki$: multiplier à droite par i donne alors $ji = ki^2 = -k$. Par conséquent, les trois éléments i, j, k anticommutent deux à deux.

[53] à l'aide de l'axiome du choix

★ Notons $G := \prod G_i$. On a les équivalences

$$\begin{aligned}
G \text{ abélien} &\iff \forall \alpha, \beta \in G,\ \alpha\beta = \beta\alpha \\
&\iff \forall \alpha, \beta \in G,\ \forall i,\ [\alpha\beta]_i = [\beta\alpha]_i \\
&\iff \forall \alpha, \beta \in G,\ \forall i,\ \alpha_i\beta_i = \beta_i\alpha_i \\
&\iff \forall i,\ \forall \alpha, \beta \in G,\ \alpha_i\beta_i = \beta_i\alpha_i \\
&\overset{?}{\iff} \forall i,\ \forall a, b \in G_i,\ ab = ba \\
&\iff \forall i,\ G_i \text{ abélien}
\end{aligned}$$

(justifions la $\overset{?}{\iff}$: le sens $\Longleftarrow$ est immédiat (l'égalité $\alpha_i\beta_i = \beta_i\alpha_i$ ayant lieu dans G_i) ; pour $\Longrightarrow$, invoquer i, a, b puis définir deux familles α et β dans G telles que $\begin{pmatrix}\alpha_i \\ \beta i\end{pmatrix} = \begin{pmatrix}a_i \\ b_i\end{pmatrix}$, par exemple en prenant le neutre sur toutes les autres coordonnées)

Section 2.2.

★ Supposons $\overline{a} = \overline{b}$ modulo n. On a alors $a = a + 0n \in a + \mathbf{Z}n = \overline{a} = \overline{b}$, d'où

$$a - b \in \overline{b} - b = (b + \mathbf{Z}n) - b = \mathbf{Z}n.$$

Soit réciproquement $k \in \mathbf{Z}$ tel que $b - a = kn$. On a alors

$$\overline{b} = b + \mathbf{Z}n = (a + kn) + \mathbf{Z}n = a + (k + \mathbf{Z})\, n = a + \mathbf{Z}n = \overline{a}.$$

Section 2.3.

★ Soit $a \in E$. On a les équivalences

$$\begin{aligned}
a \in \operatorname{Fix}\left(\varphi f \varphi^{-1}\right) &\iff \left[\varphi f \varphi^{-1}\right](a) = a \\
&\iff \varphi\left(f\left(\varphi^{-1}(a)\right)\right) = a \\
&\iff f\left(\varphi^{-1}(a)\right) = \varphi^{-1}(a) \\
&\iff \varphi^{-1}(a) \in \operatorname{Fix} f \\
&\iff a \in \varphi\left(\operatorname{Fix} f\right),
\end{aligned}$$

d'où l'égalité $\operatorname{Fix}\left(\varphi f \varphi^{-1}\right) = \varphi\left(\operatorname{Fix} f\right)$.

Lorsque f est une réflexion plane et φ une rotation, le conjugué $\varphi f \varphi^{-1}$ est une isométrie positive (prendre le déterminant) fixant exactement un axe (l'image par φ de l'axe de f). Il s'agit donc de la rotation d'axe celui de f rotaté selon φ.

Section 2.4.1.

★ Soient G et H deux sous-groupes tels que $G \cup H$ est un sous-groupe. Supposons $G \not\subset H$ et montrons $H \subset G$. Soient $\begin{cases} g \in G \setminus H \\ h \in H \end{cases}$, tous deux dans $G \cup H$: le produit gh doit alors rester dans $G \cup H$. S'il tombe dans H, son composé avec h^{-1} reste dans H or $g \notin H$. Le produit gh tombe donc dans G, donc son composé avec g^{-1} reste dans G, *i. e.* $h \in G$, *c. q. f. d.*.

★ Le neutre étant central, il centralise tout le monde, *i. e.* il appartient à tous les centralisateurs.

Soit $g, h \in \operatorname{Comm} A$. Soit $a \in A$. On a alors $(gh)\, a = g\,(ha) = g\,(ah) = (ga)\, h = (ag)\, h = a\,(gh)$, d'où $gh \in \operatorname{Comm} A$. Par ailleurs, multiplier l'égalité $ag = ga$ par g^{-1} des deux côtés donne $g^{-1}a = ag^{-1}$, d'où $g^{-1} \in \operatorname{Comm} A$.

★ Vu que i, j, k anti-commutent, aucun d'eux (ni de leurs opposés) n'est central. Par ailleurs, ± 1 sont trivialement centraux. Finalement : $Z(\mathbf{H}_8) = \{\pm 1\}$.

Vu l'égalité $\operatorname{Comm} A = \bigcap_{a\in A} \operatorname{Comm} a$, il suffit de déterminer les centralisateurs des singletons.

± 1 sont centraux, donc $\operatorname{Comm}\{\pm 1\} = \mathbf{H}_8$.

i ne commute ni avec $\pm j$ ni avec $\pm k$, seulement avec ± 1 et $\pm i$, d'où $\operatorname{Comm}\{\pm i\} = \{\pm 1, \pm i\}$. Idem pour $\pm j$ et $\pm k$.

★ Soit (A_i) une famille de parties (chaque A_i de G_i). Montrons alors que $\prod A_i$ est un sous-groupe de $\prod G_i$ ssi chaque A_i est un sous-groupe de G_i :

• le neutre (1_i) est dans $\prod A_i$ ssi chaque A_i contient 1_i ;

• le composé $(a_i\alpha_i)$ de deux familles (a_i) et (α_i) reste dans $\prod A_i$ ssi pour chaque i le composé $a\alpha$ de deux éléments a et α de A_i reste dedans ;

• l'inverse $\left(a_i^{-1}\right)$ d'une famille (a_i) reste dans $\prod A_i$ ssi pour chaque i l'inverse a^{-1} d'un élément a de A_i reste dedans.

Lorsque tous les G_i sont égaux, dans G^I, la diagonale $\left\{(g)_{i\in I}\right\}_{g\in G}$ est un sous-groupe (isomorphe à G). Montrons lorsque $\begin{cases} |I| \geq 2 \\ |G| \geq 2 \end{cases}$ qu'elle ne peut être un produit de sous-groupes $\prod A_i$. Si c'est le cas, tout élément $a \in A_i$ donne en complétant avec des neutres (il y en a vu que $|I| > 1$) une famille de $\prod A_i$, donc de la diagonale, donc dont toutes les coordonnées sont égales, d'où $a = 1$, ce qui montre $A_i = \{1\}$ et ceci pour tout i, donc la diagonale $\prod A_i$ (qui est équipotente à G) se réduit à un singleton, contredisant $|G| > 1$.

(**Remarque** : nous *n'*avons *pas* montré que tout produit $\prod G_i$ contient un sous-groupe non produit de sous-groupes.)

Section 2.4.2.

★ $a\mathbf{Z} + b\mathbf{Z}$ contient le neutre $0 = a0 + b0$, on a les égalités

$$\begin{aligned}(a\mathbf{Z} + b\mathbf{Z}) + (a\mathbf{Z} + b\mathbf{Z}) &= a\mathbf{Z} + (b\mathbf{Z} + a\mathbf{Z}) + b\mathbf{Z} \\ &= a\mathbf{Z} + (a\mathbf{Z} + b\mathbf{Z}) + b\mathbf{Z} \\ &= (a\mathbf{Z} + a\mathbf{Z}) + (b\mathbf{Z} + b\mathbf{Z}) \\ &= a(\mathbf{Z} + \mathbf{Z}) + b(\mathbf{Z} + \mathbf{Z}) \\ &= a\mathbf{Z} + b\mathbf{Z}\end{aligned}$$

et on a les inclusions

$$\begin{aligned}-(a\mathbf{Z} + b\mathbf{Z}) &\subset -a\mathbf{Z} - b\mathbf{Z} \\ &= a(-\mathbf{Z}) + b(-\mathbf{Z}) \\ &= a\mathbf{Z} + b\mathbf{Z}.\end{aligned}$$

Supposons $a\mathbf{Z} + b\mathbf{Z}$ discret, mettons $= c\mathbf{Z}$ pour un réel c. Alors $a \in a\mathbf{Z} + b\mathbf{Z} = c\mathbf{Z}$, d'où un $k \in \mathbf{Z}$ tel que $a = ck$; on dispose de même d'un $l \in \mathbf{Z}$ tel que $b = cl$. On en déduit $\frac{a}{b} = \frac{ck}{cl} = \frac{k}{l} \in \mathbf{Q}$.

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

$$a\mathbf{Z} + b\mathbf{Z} = \frac{kb}{l}\mathbf{Z} + \frac{bl}{l}\mathbf{Z} \subset \frac{b}{l}(k\mathbf{Z} + l\mathbf{Z}) \subset \frac{b}{l}\mathbf{Z},$$

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

★ Supposons $\frac{a}{b}$ rationnel, mettons $= \frac{k}{l}$. Alors $al = kb$ est une période commune de f et g, donc une période de $f + g$.

Supposons par l'absurde $\frac{a}{b} \notin \mathbf{Q}$ et $f + g$ périodique de période c minimale. On a donc

$$f(\cdot + c) + g(\cdot + c) = f + g,$$

ce qui se réécrit mieux en séparant f et g :

$$f(\cdot + c) - f = g(\cdot + c) - g\,;$$

notons δ cette fonction commune. En regardant le membre de gauche, on voit que δ est a-périodique, mais également b-périodique d'après l'expression de droite, ce qui montre que tout réel de $a\mathbf{Z} + b\mathbf{Z}$ est période de δ.

Or, $a\mathbf{Z}+b\mathbf{Z}$ est dense dans $\mathbf{R}$ car $\frac{a}{b} \notin \mathbf{Q}$, donc δ est ε-périodique pour tout $\varepsilon > 0$; comme de plus δ est continue, δ est nécessairement constante :

$$\delta = \delta_0.$$

Mais on a en outre

$$f + g = f(\cdot + c) + g(\cdot + c) = f + \delta_0 + g + \delta_0,$$

ce qui force $\delta_0 = 0$. La période c est ainsi une période commune à f et g, donc doit être dans $a\mathbf{N}^* \cap b\mathbf{N}^*$; mais ce dernier est vide puisque $\frac{a}{b} \notin \mathbf{Q}$, d'où la contradiction voulue.

Section 2.5.1.

★ Montrons que $\operatorname{End} G$ est un sous-monoïde de G^G.
Id est bien un morphisme et est neutre dans $\operatorname{End} G$.
Soient f et g deux endomorphismes. Pour tous $a, b \in G$ on a alors

$$[g \circ f](ab) = g(f(ab)) = g(f(a) f(b)) = g(f(a))\ g(f(b)) = [g \circ f](a)\ [g \circ f](b),$$

ce qui montre $g \circ f \in \operatorname{End} G$.

Montrons $(\operatorname{End} G)^\times = \operatorname{Aut} G$.
Soit $f \in (\operatorname{End} G)^\times$. Notons g son inverse dans $\operatorname{End} G$. Alors f et g sont inverses l'un de l'autre dans G^G, donc sont réciproques l'un de l'autre, *a fortiori* bijectifs : f est donc un morphisme bijectif, d'où $f \in \operatorname{Aut} G$.

Soit $f \in \operatorname{Aut} G$. Il s'agit de montrer que $g := f^{-1}$ est un morphisme. Soient a et b dans G et notons $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} := \begin{pmatrix}g(a)\\ g(b)\end{pmatrix}$. On a alors

$$ab = \operatorname{Id}(a)\ \operatorname{Id}(b) = [f \circ g](a)\ [f \circ g](b) = f(g(a))\ f(g(b)) = f(\alpha) f(\beta) = f(\alpha\beta),$$

d'où (en appliquant g)

$$g(ab) = g(f(\alpha\beta)) = [g \circ f](\alpha\beta) = \operatorname{Id}(\alpha\beta) = \alpha\beta = g(a) g(b).$$

★ Soit $f : G \longrightarrow H$ une application entre groupes qui préserve la loi.
On a $f(1) = f\left(1^2\right) = f(1)^2$, d'où $1 = f(1)$.
Soit $a \in G$. On a $f(a) f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f(1) = 1$ et pareillement de l'autre côté, ce qui montre que $f(a)$ et $f\left(a^{-1}\right)$ sont inverses l'un de l'autre.

★ Soit $f : G \longrightarrow H$ un morphisme de groupes. Puisque f préserve le neutre, son noyau contient 1_G et son image contient 1_H.
Soient par ailleurs $a, b \in \operatorname{Ker} f$. On a alors $f\left(a^{-1}\right) = f(a)^{-1} = 1^{-1} = 1$ et $f(ab) = f(a) f(b) = 1 \cdot 1 = 1$, ce qui montre que $\operatorname{Ker} f$ est stable par composition et par inversion.
Soient enfin α et β dans $\operatorname{Im} f$. Soient $x, y \in H$ tels que $\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}f(x)\\ f(y)\end{pmatrix}$. On a alors $\alpha^{-1} = f(x)^{-1} = f\left(x^{-1}\right) \in \operatorname{Im} f$ et $\alpha\beta = f(x) f(y) = f(xy) \in \operatorname{Im} f$.
On a les équivalences

$$\begin{aligned}
f \text{ injectif} &\iff \forall a, b \in G,\ f(a) = f(b) \iff a = b \\
&\iff \forall a, b \in G,\ f(a) f\left(b^{-1}\right) = f(b) f\left(b^{-1}\right) \iff ab^{-1} = bb^{-1} \\
&\iff \forall a, b \in G,\ f\left(ab^{-1}\right) = f(b) f(b)^{-1} \iff ab^{-1} = 1 \\
&\iff \forall a, b \in G,\ f\left(ab^{-1}\right) = 1 \iff ab^{-1} = 1 \\
&\overset{?}{\iff} \forall c \in G,\ f(c) = 1 \iff c = 1 \qquad \left(\begin{array}{l} \implies \text{ prendre } (a, b) := (c, 1) \\ \impliedby \text{ prendre } c := ab^{-1} \end{array}\right) \\
&\iff \forall c \in G,\ c \in \operatorname{Ker} f \iff c \in \{1\} \\
&\iff \operatorname{Ker} f = \{1\}.
\end{aligned}$$

★ Notons $i : \left\{ \begin{array}{ccc} M^\times & \longrightarrow & \operatorname{Aut} M \\ m & \longmapsto & x \mapsto mxm^{-1} \end{array} \right.$ (comme "automorphisme **i**ntérieur"). L'image de i est formée des automorphismes intérieurs par définition de ces derniers.

Soient m et $n \in M^\times$. On a alors pour tout $x \in M$ les égalités

$$[i_n \circ i_m](x) = i_n(i_m(x)) = n\left(mxm^{-1}\right)n^{-1} = (nm)\,x\,(nm)^{-1} = i_{nm}(x),$$

ce qui montre l'égalité $i_n \circ i_m = i_{nm}$. On a par ailleurs les équivalences

$$\begin{array}{rcl} m \in \operatorname{Ker} i & \iff & i_m = \mathrm{Id} \\ & \iff & \forall x \in M,\ i_m(x) = \mathrm{Id}(x) \\ & \iff & \forall x \in M,\ mxm^{-1} = x \\ & \iff & \forall x \in M,\ mx = xm \\ & \iff & m \in Z(M), \end{array}$$

ce qui montre que le noyau de i est formé des éléments centraux inversibles ($\operatorname{Ker} i = Z(M) \cap M^\times$).

★ Soient $\left\{ \begin{array}{l} i : A \longrightarrow A \times B \\ j : B \longrightarrow A \times B \end{array} \right.$ deux morphismes faisant commuter le diagramme $\begin{array}{ccccc} & \xrightarrow{(i,j)} & (A \times B)^2 & \overset{\text{produit}}{\twoheadrightarrow} & \\ A \times B & & & & A \times B \\ & \longrightarrow\!\!\underset{=}{\longrightarrow}\!\!\longrightarrow & & & \end{array}$.

On a alors pour tout $(a,b) \in A \times B$ l'égalité $\begin{pmatrix} a \\ b \end{pmatrix} = i(a)\,j(b)$, d'où (en imposant $b = 1$) les égalités $\begin{pmatrix} a \\ 1 \end{pmatrix} = i(a)\,j(1) = i(a)\,1 = i(a)$ et de même $\begin{pmatrix} 1 \\ b \end{pmatrix} = j(b)$.

Réciproquement, il est clair que de tels i et j sont des morphismes (injectifs).

★ Soit $n \in \mathbf{N}^*$. Définissons $\left\{ \begin{array}{ccc} \mathbf{Z}/n & \longrightarrow & \mathbf{U} \\ \overline{a} & \longmapsto & e^{2\pi i \frac{a}{n}} \end{array} \right.$. Montrons qu'elle est bien définie. Soient a et b dans $\mathbf{Z}$ tels que $\overline{a} = \overline{b}$. Soit $k \in \mathbf{Z}$ tel que $b = a + kn$. On a alors

$$e^{2\pi i \frac{b}{n}} = e^{2\pi i \frac{a+kn}{n}} = e^{2\pi i \frac{a}{n}} \left(e^{2\pi i}\right)^k = e^{2\pi i \frac{a}{n}}\, 1^k = e^{2\pi i \frac{a}{n}}.$$

Il est alors immédiat que c'est un morphisme. Pour son injectivité, un $a \in \mathbf{Z}$ tel que $e^{2\pi i \frac{a}{n}} = 1$ doit vérifier $2\pi i \frac{a}{n} \in 2\pi i \mathbf{Z}$, *i. e.* $a \in \mathbf{Z}n$, *i. e.* $\overline{a} = \overline{0}$.

(**Remarque** : en substance, on a dit qu'on disposait d'un isomorphisme et d'une inclusion $\mathbf{Z}/n \simeq \mathbf{U}_n \subset \mathbf{U}$ (explicitement : $\overline{a} \mapsto e^{2i\pi \frac{a}{n}}$)).

Section 2.5.2.

★ Soient k et $l \in \mathbf{Z}$ tels que $\overline{k} = \overline{l}$. Soit $z \in \mathbf{Z}$ tel que $l = k + z\omega$. On a alors

$$a^l = a^{k+z\omega} = a^k\,(a^\omega)^z = a^k 1^z = a^k 1 = a^k,$$

ce qui montre que l'application $\left\{ \begin{array}{ccc} \mathbf{Z}/\omega & \twoheadrightarrow & \langle g \rangle \\ \overline{k} & \longmapsto & a^k \end{array} \right.$ est bien définie. Il est alors immédiat que c'est un morphisme.

La surjectivité découle de la construction (avant de passer *modulo* ω). Quant à l'injectivité, on a pour tout $k \in \mathbf{Z}$ les équivalences $a^k = 1 \iff k \mid \omega(k) \iff \overline{k} = \overline{0}$.

★ Les tableaux des ordres sont les suivants :

$\mathbf{U}_8$:

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

$\mathbf{U}_2^3$:

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

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

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	$2\vert 2\vert 2$	$4\vert 4\vert 4\vert 4$

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

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

.

★ Soit $\varphi : A\times B \longrightarrow A'\times B'$ un morphisme faisant commuter le diagramme $\begin{array}{ccccc} A & \hookrightarrow & A\times B & \hookleftarrow & B \\ \downarrow \alpha & & \downarrow \varphi & & \beta \downarrow \\ A' & \hookrightarrow & A'\times B' & \hookleftarrow & B' \end{array}$.

En suivant le carré commutatif de droite, un $a \in A$ est envoyé d'une part sur $\varphi\begin{pmatrix} a \\ 1 \end{pmatrix}$, d'autre part sur $\begin{pmatrix} \alpha(a) \\ 1 \end{pmatrix}$. On aurait de même l'égalité $\varphi\begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ \beta(b) \end{pmatrix}$ pour tout $b \in B$, d'où (par multiplication)

$$\varphi\begin{pmatrix} a \\ b \end{pmatrix} = \varphi\left(\begin{pmatrix} a \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ b \end{pmatrix}\right) = \varphi\begin{pmatrix} a \\ 1 \end{pmatrix}\varphi\begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} \alpha(a) \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ \beta(b) \end{pmatrix} = \begin{pmatrix} \alpha(a) \\ \beta(b) \end{pmatrix}.$$

Réciproquement, montrons que le produit cartésien $\pi := (\alpha, \beta)$ de deux applications α et β défini par $\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} \alpha(a) \\ \beta(b) \end{pmatrix}$ est un isomorphisme ssi α et β en sont. On a d'une part les équivalences

$$\begin{aligned}
\pi \text{ est un morphisme} &\iff \forall \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} x \\ y \end{pmatrix} \in (A\times B)^2,\ \pi\left(\begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = \pi\begin{pmatrix} a \\ b \end{pmatrix}\pi\begin{pmatrix} x \\ y \end{pmatrix} \\
&\iff \forall a, x \in A,\ \forall b, y \in B,\ \pi\begin{pmatrix} ax \\ by \end{pmatrix} = \begin{pmatrix} \alpha(a) \\ \beta(b) \end{pmatrix}\begin{pmatrix} \alpha(x) \\ \beta(y) \end{pmatrix} \\
&\iff \begin{array}{l} \forall a, x \in A \\ \forall b, y \in B \end{array},\ \begin{pmatrix} \alpha(ax) \\ \beta(by) \end{pmatrix} = \begin{pmatrix} \alpha(a)\ \alpha(x) \\ \beta(b)\ \beta(y) \end{pmatrix} \\
&\iff \left\{ \begin{array}{l} \forall a, x \in A,\ \alpha(ax) = \alpha(a)\ \alpha(x) \\ \forall b, y \in B,\ \beta(by) = \beta(b)\ \beta(y) \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \alpha \text{ est un morphisme} \\ \beta \text{ est un morphisme} \end{array} \right. ,
\end{aligned}$$

d'autre part les équivalences

$$\begin{aligned}
\pi \text{ est bijectif} &\iff \forall \begin{pmatrix} a' \\ b' \end{pmatrix} \in A'\times B',\ \exists! \begin{pmatrix} a \\ b \end{pmatrix} \in A\times B,\ \pi\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a' \\ b' \end{pmatrix} \\
&\iff \begin{array}{l} \forall a' \in A' \\ \forall b' \in B' \end{array},\ \exists! \begin{pmatrix} a \\ b \end{pmatrix} \in A\times B,\ \left\{ \begin{array}{l} \alpha(a) = a' \\ \beta(b) = b' \end{array} \right. \\
&\iff \begin{array}{l} \forall a' \in A' \\ \forall b' \in B' \end{array},\ \left\{ \begin{array}{ll} \exists! a \in A,\ \alpha(a) = a' & \left(\begin{array}{c} \text{bien clarifier} \\ \text{cette équivalence} \end{array} \right) \\ \exists! b \in B,\ \beta(b) = b' & \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \forall a' \in A',\ \exists! a \in A,\ \alpha(a) = a' \\ \forall b' \in B',\ \exists! b \in B,\ \beta(b) = b' \end{array} \right. \\
&\iff \left\{ \begin{array}{l} \alpha \text{ est bijective} \\ \beta \text{ est bijective} \end{array} \right. .
\end{aligned}$$

★ Soit $\varphi : A\times B \longrightarrow B\times A$ faisant commuter le diagramme $\begin{array}{ccccc} & \hookrightarrow & A\times B & \hookleftarrow & \\ A & & \downarrow \varphi & & B \\ & \hookrightarrow & B\times A & \hookleftarrow & \end{array}$. Un $a \in A$ est alors envoyé, suivant le triangle de gauche, d'une part sur $\varphi\begin{pmatrix} a \\ 1 \end{pmatrix}$ d'autre part sur $\begin{pmatrix} 1 \\ a \end{pmatrix}$; on obtient de même l'égalité $\varphi\begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} b \\ 1 \end{pmatrix}$ pour tout $b \in B$, d'où (en multipliant) les égalités

$$\varphi\begin{pmatrix} a \\ b \end{pmatrix} = \varphi\begin{pmatrix} a \\ 1 \end{pmatrix}\varphi\begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix}\begin{pmatrix} b \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}.$$

Réciproquement, il est immédiat qu'un tel φ est un isomorphisme.

★ Supposons commuter le diagramme $\begin{array}{ccccc} \hookrightarrow & A\times(B\times C) & \hookleftarrow & A & \hookrightarrow \\ \uparrow & & & & \downarrow \\ B\times C & \hookleftarrow & B & \hookrightarrow & A\times B \\ \uparrow & & & & \downarrow \\ \hookleftarrow & C & \hookrightarrow & (A\times B)\times C & \hookleftarrow \end{array}$ muni en plus d'un morphisme $\varphi : A\times(B\times C) \longrightarrow (A\times B)\times C$ (non précisé par commodité de lecture). Suivre un $a\in A$ suivant les deux chemins de A vers $(A\times B)\times C)$ donne l'égalité $\varphi(a,(1,1)) = ((a,1),1)$, suivre un $b\in B$ donne $\varphi(1,(b,1)) = ((1,b),1)$ et suivre un $c\in C$ donne $\varphi(1,(1,c)) = ((1,1),c)$, d'où par multiplication

$$\varphi(a,(b,c)) = \varphi\begin{pmatrix} (a,(1,1)) \\ \times(1,(b,1)) \\ \times(1,(1,c)) \end{pmatrix} = \begin{pmatrix} \varphi(a,(1,1)) \\ \times\varphi(1,(b,1)) \\ \times\varphi(1,(1,c)) \end{pmatrix} = \begin{pmatrix} ((a,1),1) \\ \times((1,b),1) \\ \times((1,1),c) \end{pmatrix} = ((a,b),c).$$

Il est réciproquement clair qu'un tel φ est un isomorphisme.

Section 2.5.3.

★ Montrons que 1 est neutre : on a pour tout $a\in C$

$$a*1 := \varphi^{-1}(\mathbf{a}\times\mathbf{1}) = \varphi^{-1}(\mathbf{a}) = a \text{ et de même de l'autre côté.}$$

Soit $a\in C$. Montrons que a et $b := \varphi^{-1}\left(\mathbf{a}^{-1}\right)$ sont inverses l'un de l'autre. Noter que $\mathbf{b} = \varphi(b) = \mathbf{a}^{-1}$. On a alors

$$a*b := \varphi^{-1}(\mathbf{a}\times\mathbf{b}) = \varphi^{-1}(\mathbf{1}) = 1 \text{ et pareil de l'autre côté.}$$

★ Soient A et B dans $\mathbf{Z}/_2$. Soient $a,a',b,b'\in\mathbf{Z}$ tels que $\begin{pmatrix}\overline{a}\\ \overline{b}\end{pmatrix} = \begin{pmatrix}A\\ B\end{pmatrix} = \begin{pmatrix}\overline{a'}\\ \overline{b'}\end{pmatrix}$. Soient $k,l\in\mathbf{Z}^2$ tels que $\begin{cases} a' = a+2k \\ b' = b+2l \end{cases}$. On a alors les égalités

$$a'b' = (a+2k)(b+2l) = ab+2al+2bk+4kl \in ab+2\mathbf{Z}, \text{ d'où } \overline{a'b'} = \overline{ab}.$$

★ Notons χ et $\mathfrak{p}$ les deux applications. On a d'une part à $P\subset A$ fixé les égalités

$$\begin{aligned} [\mathfrak{p}\circ\chi](P) &= \mathfrak{p}(\chi_P) = \left\{ a\in A \ ; \ \underbrace{\chi_P(a)=1}_{\Longleftrightarrow a\in P} \right\} \\ &= \{a\in A \ ; \ a\in P\} = A\cap P = P, \end{aligned}$$

d'autre part à $f\in\mathbf{F}_2^A$ et $a\in A$ fixés les égalités

$$\begin{aligned} [\chi\circ\mathfrak{p}](f)(a) &= \chi_{\mathfrak{p}(f)}(a) = \begin{cases} 1 \text{ si } a\in\mathfrak{p}(f) \\ 0 \text{ si } a\notin\mathfrak{p}(f) \end{cases} \\ &= \begin{cases} 1 \text{ si } a\in\{x\in A \ ; \ f(x)=1\} \\ 0 \text{ si } a\notin\{x\in A \ ; \ f(x)=1\} \end{cases} \\ &= \begin{cases} 1 \text{ si } f(a)=1 \\ 0 \text{ si } f(a)\neq 1 \end{cases} \\ &= \begin{cases} 1 \text{ si } f(a)=1 \\ 0 \text{ si } f(a)=0 \end{cases} \quad \text{car } \operatorname{Im} f\subset\{0,1\} \\ &= f(a). \end{aligned}$$

Section 2.5.4.

★ On reprend la même démonstration. Les transvections sont tuées, également les dilatations de rapports *positifs*. Restent celles de rapport négatifs. Précisons alors que l'on peut imposer dans les générateurs choisis les dilatations agissant sur les *premières* rangées (*i. e.* dont le rapport est le *premier* coefficient sur la diagonale). Vu que chaque telle dilatation est produit de n'importe quelle autre (disons celle $Diag(-1,1,1,...,1)$ de rapport -1) par une dilatation positive, elles sont toutes même image. Le carré de cette dernière est l'image du carré d'une dilatation, donc est l'image d'une dilatation de rapport *positif*, donc est nul : l'image commune des dilatations négatives est donc est une racine carrée de Id, à savoir un produit disjoint de transpositions.

Réciproquement, soit σ un tel produit et définissons $\varphi : \left\{ \begin{array}{ccc} GL_n(\mathbf{R}) & \longrightarrow & \mathfrak{S}_k \\ A & \longmapsto & \left\{ \begin{array}{l} \mathrm{Id} \text{ si } |A|>0 \\ \sigma \text{ si } |A|<0 \end{array} \right. \end{array} \right.$. On a alors à $A, B \in GL_n(\mathbf{R})$ fixés les égalités.

$$\begin{array}{rcl} \varphi(A)\varphi(B) & = & \left\{ \begin{array}{l} \mathrm{Id} \text{ si } |A|>0 \\ \sigma \text{ si } |A|<0 \end{array} \right. \times \left\{ \begin{array}{l} \mathrm{Id} \text{ si } |B|>0 \\ \sigma \text{ si } |B|<0 \end{array} \right. \\ & \underset{\text{quatre cas}}{\overset{\text{distinguer les}}{=}} & \left\{ \begin{array}{ll} \mathrm{Id}=\sigma^2 & \text{si } |A||B|>0 \\ \sigma & \text{si } |A||B|<0 \end{array} \right. \\ & = & \left\{ \begin{array}{ll} \mathrm{Id} & \text{si } |AB|>0 \\ \sigma & \text{si } |AB|<0 \end{array} \right. = \varphi(AB). \end{array}$$

Section 3.1.

★ Soit $\left\{ \begin{array}{ccc} M \times A & \longrightarrow & A \\ (m,a) & \longmapsto & m \cdot a \end{array} \right.$ une loi externe et notons $\varphi : \left\{ \begin{array}{ccc} M & \longrightarrow & A^A \\ m & \longmapsto & \varphi_m : a \mapsto m \cdot a \end{array} \right.$. On a alors pour tous $m, n \in M$ les équivalences

$$\begin{array}{rl} & \forall a \in A,\ n \cdot (m \cdot a) = (nm) \cdot a \\ \iff & \forall a \in A,\ \varphi_n(\varphi_m(a)) = \varphi_{nm}(a) \\ \iff & \forall a \in A,\ [\varphi_n \circ \varphi_m](a) = \varphi_{nm}(a) \\ \iff & \varphi_n \circ \varphi_m = \varphi_{nm} \end{array}$$

et les équivalences $\begin{array}{l} \forall a \in A, \\ 1 \cdot a = a \end{array} \iff \begin{array}{c} \forall a \in A, \\ \varphi_1(a) = \mathrm{Id}(a) \end{array} \iff \varphi_1 = \mathrm{Id}.$

★ Soient $g \in M^\times$ et $a \in A$. Puisque g est inversible, on peut écrire $M = gM$, d'où il vient $g \cdot (M \cdot a) = (gM) \cdot a = M \cdot a$.

★ On considère l'action de M induite sur $\mathfrak{P}(A)$: montrons qu'elle est une action sur ${}^{A}\!/_{\Omega}$. Soit $a \in A$. On a alors d'une part $1 \cdot (a \cdot \Omega) = (1 \cdot a) \cdot \Omega = a \cdot \Omega$, d'autre part à $m, n \in M$ fixés

$$n \cdot (m \cdot (a \cdot \Omega)) = n \cdot ((m \cdot a) \cdot \Omega) = (n \cdot (m \cdot a)) \cdot \Omega = (nm \cdot a) \cdot \Omega = nm \cdot (a \cdot \Omega).$$

Tout découle donc de la compatibilité des deux actions et l'on pourra abandonner toutes les parenthèses.

★ La restriction $M^\times \longrightarrow A^A$ préserve la loi, donc sera un morphisme de *groupes* si l'on montre que son image est incluse dans $\mathfrak{S}_A$. Or l'image d'un inversible par un morphisme de monoïdes est inversible (établi au deuxième exercice de la section 2.5.1), ce qui conclut.

Section 3.2.

★ Soit $g \in \mathrm{Fix}\, a$. Faire agir g^{-1} sur $a = g \cdot a$ donne $g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = \left(g^{-1}g\right) \cdot a = 1 \cdot a = a$.

★ L'action (définie par $g \cdot \overline{\alpha} := \overline{g\alpha}$) est transitive vu l'égalité $\overline{\beta} = \beta\alpha^{-1} \cdot \overline{\alpha}$ pour tous $\alpha, \beta \in G$, donc chaque orbite vaut tout ${}^{G}\!/_{H}$.

Soit par ailleurs $\alpha \in G$: vu les équivalences (à $g \in G$ fixé)

$$g \in \mathrm{Fix}\,\overline{\alpha} \iff g \cdot \overline{\alpha} = \overline{\alpha} \iff \overline{g\alpha} = \overline{\alpha} \iff g\alpha \in \alpha H \iff g \in \alpha H \alpha^{-1},$$

on peut affirmer $\mathrm{Fix}\,\overline{\alpha} = \alpha H \alpha^{-1}$.

★ Grâce à l'exercice précédent, le corollaire s'écrit $|G| = \left|{}^{G}\!/_{H}\right| \left|\alpha H \alpha^{-1}\right| = \left|{}^{G}\!/_{H}\right| |H|$ et l'on retrouve le lemme exprimant le cardinal du quotient comme quotient des cardinaux.