Moïse Malinge

Les Maths intuitives

COURS MP MPSI

Cours commenté et expliqué
MPSI – MP/MP*
MP2I – MPI/MPI*

ellipses

Chapitre 1

Structures algébriques

Objectifs du chapitre

La nature profonde de l'algèbre est de s'intéresser uniquement aux relations entre les éléments d'un ensemble puis de réaliser des analogies abstraites avec d'autres ensembles, qui peuvent être complètement différents. Ces éléments et les relations qui les relient sont qualifiés d'*ensembles structurés*, la *structure*, ou *loi*, étant l'ensemble des relations entre les éléments[a]. On constate alors en pratique qu'un certain nombre de ces structures sont assez fréquentes et « superposables », ce qui conduit à les définir de façon générale, indépendamment des ensembles qui les sous-tendent. Pour une première vue générale de ces structures usuelles, voici une synthèse vulgarisatrice[b] :

- Ensemble muni d'une loi interne « additive » ou « multiplicative » : *groupe*. Souvent noté $(G,+)$ ou $(G,\times)$.
- Ensemble muni de deux lois internes, l'une « additive » et l'autre « multiplicative » : *anneau*. Souvent noté $(A,+,\times)$.

Si la loi « multiplicative » induit une loi de « division », alors l'anneau est appelé *corps*. Souvent noté $(K,+,\times)$.

- Ensemble muni d'une loi interne « additive » et d'une loi externe « multiplicative » : *espace vectoriel*. Souvent noté $(E,+,.)$.
- Ensemble muni de trois lois, qui en font un anneau et un espace vectoriel : *algèbre*. Souvent noté $(E,+,\times,.)$.

La structure qui est de loin la plus utilisée aux concours est celle d'espace vectoriel (avec ses variantes, les espaces vectoriels normés, préhilbertiens ou euclidiens) mais elle n'est pas étudiée ici, car plusieurs chapitres ultérieurs lui sont consacrés. Ce chapitre contient donc trois sections : groupes, anneaux, algèbres.

Sommaire

[a] Par exemple, si un certain arbre généalogique se dessine de la même manière que l'organigramme d'une certaine entreprise, l'algébriste dira que ces deux ensembles de personnes ont une même structure.

[b] Des définitions rigoureuses viendront bien sûr ultérieurement, cette première description permet de ne pas tout confondre au début.

A Groupes

1 Généralités

Définition : groupe ○○○

Un ensemble G muni d'une loi de composition interne $*$ est appelé *groupe* si :

- La loi admet un *élément neutre* : $\exists e \in G \quad \forall a \in G \quad e * a = a * e = a.$
- La loi est *associative* : $\forall (a,b,c) \in G^3 \quad a * (b * c) = (a * b) * c.$
- Tout élément admet un *symétrique* : e neutre $\implies \quad \forall a \in G \quad \exists b \in G \quad a * b = b * a = e.$

Si, de plus, cette loi est commutative, alors ce groupe est dit *commutatif* ou *abélien*.
Enfin, le cardinal de l'ensemble est appelé *ordre* du groupe.

Remarques.

• *Unicités des neutres et symétriques.* Un neutre de groupe est unique ; en effet, si e et f sont deux neutres, alors $e * f = e$ et $e * f = f$. On parle donc *du* neutre du groupe. De même, tout élément a un unique symétrique (si y et z sont deux symétriques de x, alors $x * y = e$ puis en composant à gauche par z et par associativité de $*$, on aboutit à $y = z$).

• *Un groupe n'est jamais vide.* Un groupe ne peut pas être vide, car il contient au moins son élément neutre.

• *Abus usuel.* On fait souvent référence à un groupe par le seul nom de l'ensemble, sa loi étant sous-entendue. Ainsi, dire que G est un groupe constitue un léger abus de langage (on devrait dire $(G,*)$). Cet abus, usuel pour les structures algébriques, ne doit pas faire oublier que les lois font partie intégrante de ces structures.

• *Conséquences de l'associativité.* L'associativité de la loi permet d'omettre les parenthèses lors de compositions multiples. En outre, plus subtilement, si $a \in G$ admet un symétrique à gauche x, et un symétrique à droite y, alors, par associativité :

$$\begin{aligned} \underbrace{(xa)}_{=e} y &= x \underbrace{(ay)}_{=e} \\ y &= x \end{aligned}$$

Il n'y a donc pas lieu de distinguer, dans un groupe, les symétriques à droite des symétriques à gauche.

• *Notations usuelles pour les lois et les neutres.* Si la loi est commutative, on la note souvent $+$, l'élément neutre est noté 0 et on utilise le symbole $-$ pour les symétriques, qui sont appelés *opposés*. Si la loi n'est pas commutative ou dans le cas général, on la note plutôt $\times$, ou bien le symbole est même omis comme pour la multiplication des nombres ; l'élément neutre est noté 1 et on utilise le symbole $^{-1}$ pour les symétriques, qui sont appelés *inverses*. Ces notations, qui sont abusives, car elles n'ont rien à voir avec les $+$ et $\times$ traditionnels, sont utilisées dans le but de « recycler » nos réflexes de calculs acquis depuis longtemps avec les nombres entiers et réels. Ces abus permettent de largement accélérer et fiabiliser les calculs sur les groupes. Dans le cas commutatif, on introduit également la notation $\sum_{i \in I} a_i$ pour $(a_i)_{i \in I}$ une famille finie, qui vaut 0 par convention si I est vide, ou qui vaut $\sum_{i=a}^{b} a_i$ si $I = [\![a,b]\!]$ et $(a,b) \in \mathbb{N}^2$ avec $a \leqslant b$. On fait de même pour $\prod_{i=a}^{b} a_i$ et une loi notée multiplicativement, en prenant beaucoup de précautions en cas de non commutativité. La notation $\prod_{i \in I} a_i$, quant à elle, n'a de sens que si la multiplication est commutative. Ces notations ne sont pas obligatoires, car le programme indique qu'on est libre de présenter les calculs avec des points de suspension.

• *Notation usuelle pour les itérés.* Pour $n \in \mathbb{Z}$ et x un élément d'un groupe de neutre e on peut introduire les notations x^n et nx. Dans le cas de la notation générale ou multiplicative :

$$x^n = \begin{cases} \underbrace{x \times \ldots \times x}_{n \text{ fois}} & \text{si } n \text{ positif} \\ \underbrace{x^{-1} \times \ldots \times x^{-1}}_{-n \text{ fois}} & \text{si } n \text{ négatif} \\ e = 1 & \text{si } n = 0 \end{cases}$$

De même, dans le cas de la notation additive :

$$n\,x = \begin{cases} \underbrace{x + \ldots + x}_{n \text{ fois}} & \text{si } n \text{ positif} \\ \underbrace{(-x) + \ldots + (-x)}_{-n \text{ fois}} & \text{si } n \text{ négatif} \\ e = 0 & \text{si } n = 0 \end{cases}$$

• *Notation hors programme.* L'ordre d'un groupe G est souvent noté $\mathrm{ord}(G)$ ou $|G|$ (plutôt que $\mathrm{card}(G)$).

Exemples.

○ Les couples $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{R}^n,+)$ sont des exemples de groupes.

○ L'ensemble des bijections d'un ensemble dans lui-même forme un groupe pour la loi de composition (loi notée $\circ$).

○ L'ensemble des matrices carrées d'un même ordre (notion vue au chapitre 2) forme un groupe pour l'addition (mais pas pour la multiplication, car les matrices ne sont pas toutes inversibles).

○ *Contre-exemples.* $(\mathbb{N},+)$ et $(\mathbb{R},\times)$ ne sont pas des groupes.

Définition et caractérisation des sous-groupes ●●●

Soit $(G,*)$ un groupe. Si H est un sous-ensemble de G, alors la loi induite par $*$ sur H en fait un groupe si, et seulement si :

○ H contient l'élément neutre de $(G,*)$.

○ Pour tout $(a,b) \in H^2$: $a * b^{-1} \in H$.

On dit alors que H est un *sous-groupe* de $(G,*)$.

Démonstration. *Simple vérification.* Vérifions que $(H,*)$ est un groupe s'il vérifie les deux propriétés ci-dessus. On note e l'élément neutre de $(G,*)$:

○ H n'est pas vide, car il contient e.

○ La loi $*$ étant associative sur G, elle l'est sur H.

○ Montrons que tout élément de H admet un inverse dans H. Soit $x \in H$. Comme $(e,x) \in H^2$, on a $e * x^{-1} \in H$ (avec x^{-1} l'inverse de x dans G), ce qui implique que x admet un inverse dans H (qui est x^{-1}).

○ Montrons que la loi $*$ est interne sur H (c'est-à-dire que H est stable pour la loi $*$). Pour $(a,b) \in H^2$, $b^{-1} \in H$ d'après ci-dessus. Donc par hypothèse : $a * b = a * \left(b^{-1}\right)^{-1} \in H$.

Remarques.

• *Utilisation fréquente.* Cette propriété est très utilisée en pratique pour vérifier qu'une structure est un groupe, en utilisant un groupe connu plus grand, car elle permet un raisonnement plus rapide que la définition fondamentale des groupes.

• *Conservation du neutre et des inverses.* La démonstration indique que si H est un sous-groupe de G, alors son élément neutre est celui de G. De plus, l'inverse d'un élément de H dans H est le même que celui dans G.

Exemples.

○ L'ensemble des complexes de module 1 est un sous-groupe de $(\mathbb{C}^*,\times)$, qui est noté $\mathbb{U}$. Pour $n \in \mathbb{N}^*$, l'ensemble des racines $n^{\text{ièmes}}$ de l'unité, noté $\mathbb{U}_n$, est lui-même un sous-groupe de $(\mathbb{U},\times)$.

○ L'ensemble des isométries du plan affine euclidien usuel est un sous-groupe des bijections du plan muni de la loi de composition.

○ L'ensemble des matrices inversibles réelles d'ordre n, noté $\mathrm{GL}_n(\mathbb{R})$, n'est pas un sous-groupe du groupe $(\mathcal{M}_n(\mathbb{R}),+)$. En revanche, $\mathrm{GL}_n(\mathbb{R})$ est un groupe pour la loi de multiplication matricielle (alors que $\mathcal{M}_n(\mathbb{R})$ ne l'est pas).

Propriété : les sous-groupes de $\mathbb{Z}$ ●●●

Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$ lorsque $n\in\mathbb{N}$.

Démonstration. *Démonstration classique à bien savoir faire.* Il est facile de vérifier que ces ensembles sont des sous-groupes de $(\mathbb{Z},+)$. Montrons de plus qu'il n'existe pas d'autre sous-groupe en considérant G un sous-groupe quelconque de $(\mathbb{Z},+)$ et en montrant qu'il est de cette forme. Si G ne contient aucun entier positif, alors il est réduit à $\{0\}$ et vaut donc $0\mathbb{Z}$. Dans le cas contraire, considérons $a=\min\left(G\cap\mathbb{N}^*\right)$ (plus petit élément positif de G) et montrons que $G=a\mathbb{Z}$ par double inclusion. Tout d'abord, comme $a\in G$, on a $a\mathbb{Z}\subset G$ par stabilité. Pour l'inclusion réciproque, considérons un élément $b\in G$ et montrons que c'est un multiple de a. On effectue la division euclidienne de b par a, ce qui donne $b=aq+r$ avec $q\in\mathbb{Z}$ et $0\leqslant r<a$. Comme b et a sont dans G, $r=b-aq$ aussi, ce qui implique que $r=0$ par définition de a. Cela implique que a divise b, c'est-à-dire que $b\in a\mathbb{Z}$.

Propriétés : règles de calcul pour les groupes ●●●

Soit $(G,*)$ un groupe, dont l'élément neutre est noté e.

- $\forall(a,b)\in G^2\quad (a*b)^{-1}=b^{-1}*a^{-1}$.
- Tout élément est *régulier* ou « simplifiable » : $\forall(a,b,c)\in G^3\quad \begin{cases} a*b=a*c & \Rightarrow b=c \\ b*a=c*a & \Rightarrow b=c \end{cases}$.

Démonstration. *Simples vérifications.*

- Pour $(a,b)\in G^2$:

$(a*b)*(b^{-1}*a^{-1})=a*b*b^{-1}*a^{-1}=a*a^{-1}=e$

On procède de même en inversant le sens, afin de conclure que $a*b$ est inversible et que son inverse est $b^{-1}*a^{-1}$.

- On peut composer par a^{-1} à gauche dans l'égalité. De même à droite. D'où l'assertion.

Remarque. Le mot « simplifier » est un abus de langage pour dire « composer par l'inverse ». Ceci n'est bien sûr possible que lorsque l'inverse existe, ce qui est toujours assuré dans un groupe, car tout élément est inversible. Ne pas oublier, qu'en général, il n'est pas toujours possible de « simplifier » de la sorte (penser à une matrice non inversible par exemple).

Définitions et propriétés : constructions de groupes ●●○

1. *Intersection.*
   Toute intersection de sous-groupes d'un même groupe est un sous-groupe.

2. *Produit.*
   Si $(G_1,*_1)$ et $(G_2,*_2)$ sont deux groupes alors on appelle *groupe produit* l'ensemble $G_1\times G_2$ muni de la loi :
   $$((x_1,x_2),(y_1,y_2))\mapsto(x_1*_1y_1,x_2*_2y_2)$$

3. *Engendrement.*
   Si A est une partie d'un groupe $(G,*)$, alors le sous-groupe de G *engendré* par A est l'intersection de tous les sous-groupes de G contenant A et il est noté $\langle A\rangle$. C'est le plus petit sous-groupe de G contenant A et il est constitué du neutre de G et des éléments de G qui s'écrivent $a_1^{\varepsilon_1}*a_2^{\varepsilon_2}*\ldots*a_k^{\varepsilon_k}$, où $k\in\mathbb{N}^*$, $a_i\in A$ et $\varepsilon_i\in\{-1,+1\}$.

Démonstrations. *Simples vérifications.*

1. Soient H_i, $i \in I$, des sous-groupes d'un groupe noté $(G,*)$ (avec I un ensemble quelconque, non nécessairement fini). Alors $\bigcap_{i\in I} H_i$ contient e. De plus, si $(a,b) \in \left(\bigcap_{i\in I} H_i\right)^2$, alors $ab^{-1} \in H_i$ pour tout $i \in I$ car H_i est un groupe : ab^{-1} est donc dans $\bigcap_{i\in I} H_i$.

2. Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes dont les éléments neutres sont notés e_1 et e_2. Vérifions que la loi proposée confère à $G_1 \times G_2$ une structure de groupe. On a bien (e_1,e_2) qui est un élément neutre sur $G_1 \times G_2$, et l'associativité est immédiate. Soit $(x,y) \in G_1 \times G_2$. Alors (x,y) composé par (x^{-1},y^{-1}) donne bien (e_1,e_2), ce qui achève la vérification.

3. L'intersection de tous les sous-groupes de G contenant A et bien un sous-groupe de G par la première proposition ci-dessus ; la définition de $\langle A \rangle$ est donc correcte. On note H l'ensemble des éléments qui s'écrivent comme compositions finies d'éléments de A et de leurs symétriques par la loi $*$. Montrons que $\langle A \rangle = H$ par double inclusion :

◦ H est un sous-groupe car : $\forall a \in H\ a * a^{-1} = e_G \in H$; H est stable par produit ; tout élément est inversible dans H. De plus $A \subset H$, donc $\langle A \rangle \subset H$.

◦ Réciproquement, $\langle A \rangle$ est un sous-groupe donc, par stabilité, il doit contenir tous les éléments de A, tous leurs inverses, tous leurs composés possibles : on en déduit que $H \subset \langle A \rangle$.

Remarques.

• *Légères généralisations.* On peut de même parler de groupe produit d'un nombre fini de groupes. Par ailleurs, on parle de sous-groupe engendré par un élément a en faisant référence à $\langle \{a\} \rangle$, que l'on note plus simplement $\langle a \rangle$.

• *Attention aux réunions.* En général, la réunion de deux sous-groupes n'est pas un sous-groupe. Voici un contre-exemple simple : $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z},+)$, notamment car il ne contient pas $5 = 2+3$.

Exemples.

1. Dans $(\mathbb{Z},+)$, l'intersection des sous-groupes $4\mathbb{Z}$ et $6\mathbb{Z}$ est un sous-groupe, donc de la forme $n\mathbb{Z}$. En regardant de plus près, on constate même que $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$.

2. Il n'y a pas besoin de vérifier explicitement que $\mathbb{Z} \times \mathbb{Q}$ est un groupe lorsqu'il est muni de l'addition de couples qui découle des additions usuelles sur $\mathbb{Z}$ et $\mathbb{Q}$, puisque c'est un groupe produit.

3. Pour tout $n \in \mathbb{Z}$, $\langle n \rangle = \langle -n \rangle = n\mathbb{Z}$. Par ailleurs, $\langle n \rangle$ est l'intersection de tous les sous-groupes de $\mathbb{Z}$ contenant l'entier n, et également l'ensemble des sommes finies de n et de son symétrique $-n$.

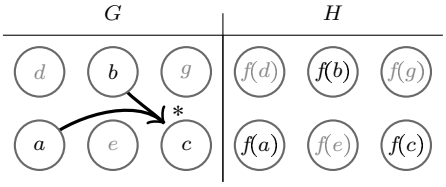
Définition : morphisme de groupes ●●●

Une fonction f d'un groupe $(G,*)$ dans un groupe $(H,\perp)$ est appelée *morphisme de groupes* si :

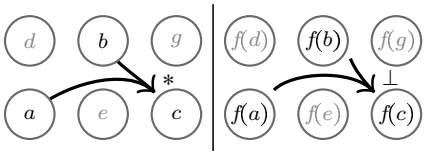
$$\forall (a,b) \in G^2 \quad f(a*b) = f(a) \perp f(b)$$

Un morphisme (de groupes) bijectif est appelé *isomorphisme* (de groupes) ; dans ce cas, le groupe de départ et celui d'arrivée sont dits *isomorphes.*

Remarque. *Explication sémantique et épistémologique.* Illustrons ceci, en considérant $(a,b) \in G^2$, $c = a*b$, et f une bijection de G dans H :



La composition $f(a) \perp f(b)$ peut valoir, a priori, n'importe quelle valeur ; en revanche, si f est un morphisme de groupe, il n'y a qu'une possibilité, celle-ci :



On constate que les deux fléchages ci-dessus sont superposables car de même forme, c'est-à-dire « isomorphes » au sens étymologique du terme (*ísos* : égal ; *morphê* : forme). De façon plus générale, les représentations graphiques de deux groupes isomorphes se superposent toujours parfaitement, aux noms près des éléments. En faisant abstraction des noms des éléments et en notant les neutres de façon générique, des groupes isomorphes deux à deux possèdent donc une « unique » représentation graphique. Cela explique le choix du mot *isomorphisme*. Par ailleurs, cette notion d'isomorphisme est fondamentale en algèbre et c'est même, en un certain sens, sa raison d'être : l'algèbre étudie des structures sur les ensembles et non les ensembles eux-mêmes. Ainsi, pour l'algébriste, toute étude se fait « à isomorphisme près ».

Exemples.

○ La conjugaison complexe est un isomorphisme de $(\mathbb{C},+)$ dans lui-même.

○ La fonction exponentielle est un isomorphisme de groupes :

$$\begin{array}{ccc}(\mathbb{R},+) & \to & (\mathbb{R}^{*+},\times)\\ x & \mapsto & \mathrm{e}^x\end{array}$$

○ Le déterminant des matrices d'ordre n (cf. page 138 du chapitre 2) est un morphisme de groupes de $(\mathrm{Gl}_n(\mathbb{C}),\times)$ dans $(\mathbb{C}^*,\times)$.

Propriétés des morphismes de groupes

Soit f un morphisme de groupes de $(G,*)$ dans $(H,\perp)$. On note e_G et e_H les éléments neutres.

1. L'image de l'élément neutre (de départ) est l'élément neutre (d'arrivée) : $f(e_G)=e_H$.
2. L'image d'un inverse est l'inverse de l'image : $\forall x\in G\ \ f(x)^{-1}=f(x^{-1})$.
3. Les images directes et réciproques par f de sous-groupes sont des sous-groupes.
4. L'ensemble des antécédents de e_H par f est un sous-groupe appelé *noyau* de f. Il est noté $\mathrm{Ker}\, f$ et :
$$f \text{ injective} \iff \mathrm{Ker}\, f=\{e_G\}$$
5. Une composition de morphismes de groupes est encore un morphisme de groupes.
6. La réciproque d'un isomorphisme est elle-même un isomorphisme.

Démonstration. *Ces courtes démonstrations forment un bon exercice d'entraînement sur les groupes.*

1. $f(e_G)\perp f(e_G)=f(e_G*e_G)=f(e_G)$. Donc, en composant ceci par $f(e_G)^{-1}$, on obtient $f(e_G)=e_H$.

2. Pour tout $x\in G$:
$$f(x)\perp f(x^{-1})=f(x*x^{-1})=f(e_G)=e_H$$
D'où le résultat.

3. ○ Soient K un sous-groupe de G et $(a,b)\in K^2$. Premièrement, $e_H=f(e_G)\in f(K)$. Deuxièmement :
$$\begin{array}{rcll} f(a)\perp f(b)^{-1} & = & f(a)\perp f(b^{-1}) & \text{d'après 2}\\ & = & \underbrace{f(a*b^{-1})}_{\in f(K)} & \end{array}$$
○ Soient K un sous-groupe de H et a, b deux antécédents par f de deux éléments de K. $e_G\in f^{-1}(\{e_H\})\subset f^{-1}(K)$; de plus, $f(a*b^{-1})=f(a)\perp f(b)^{-1}\in K$ car K est un groupe. Donc $a*b^{-1}\in f^{-1}(K)$.

4. ○ $\mathrm{Ker}\, f$ est un sous-groupe de G d'après le point précédent et parce que $\{e_H\}$ est un sous-groupe de H.

○ Supposons f injective. Alors e_H n'a pas d'autre antécédent que e_G, et donc $\mathrm{Ker}\, f=\{e_G\}$.

○ Supposons que $\mathrm{Ker}\, f=\{e_G\}$ et considérons $(a,b)\in G^2$ tel que $f(a)=f(b)$. Alors $f(a*b^{-1})=e_H$ et par suite $a*b^{-1}=e_G$ car c'est le seul élément du noyau. Donc $a=b$ et f est injective.

5. Immédiat à vérifier.

6. Supposons que f est bijectif. Alors sa réciproque f^{-1} est également bijective. Montrons que c'est un morphisme en considérant $(a,b)\in H^2$:

$$f\left(f^{-1}(a\perp b)\right) = a\perp b = f\left(f^{-1}(a) * f^{-1}(b)\right)$$

En composant cette égalité par f^{-1} on obtient :

$$f^{-1}(a\perp b) = f^{-1}(a) * f^{-1}(b)$$

Exemples.

◦ Le déterminant induit un morphisme du groupe des automorphismes d'un $\mathbb{C}$-espace vectoriel E de dimension finie dans le groupe $(\mathbb{C}^*,\times)$.

◦ Le déterminant induit également un morphisme du groupe des isométries $\mathcal{O}(E)$ d'un espace vectoriel euclidien E dans $\{-1,1\}$. Le noyau de ce morphisme est l'ensemble des isométries de déterminant 1, qui est appelé groupe spécial orthogonal et noté $\mathcal{O}^+(E)$ ou $\mathcal{SO}(E)$ (cf. chapitre 4 pour plus de détails).

◦ La « fonction trace », sur l'ensemble des matrices réelles carrées d'ordre n (cf. chapitre 2), est un morphisme de groupes additifs. Son image est $\mathbb{R}$ (il est donc surjectif) et son noyau est l'ensemble des matrices de trace nulle.

Théorème et définition : ordre d'un élément ●●○

On définit l'*ordre d'un élément* d'un groupe comme l'ordre du sous-groupe qu'il engendre.

1. En notant d l'ordre d'un élément x d'ordre fini dans un groupe $(G,\times)$ d'élément neutre e :

$$\forall k\in\mathbb{Z} \qquad x^k = e \iff d|k$$

2. L'ordre d'un élément d'un groupe fini divise l'ordre du groupe.

Démonstrations.

1. *Démonstration similaire à celle donnant les sous-groupes de $(\mathbb{Z},+)$ page 43, avec un début spécifique en plus.* Soit x un élément d'ordre fini d, dans un groupe noté $(G,.)$, dont l'élément neutre est noté e. Commençons par reformuler de façon plus explicite $\langle x\rangle$. Que l'ordre de x soit fini implique qu'il existe i et j deux entiers distincts tels que $x^i = x^j$, ce qui donne $x^{|j-i|} = e$. En posant $n = \min\{k\in\mathbb{N}^*,\ x^k = e\}$, on peut écrire $\langle x\rangle = \{x^k,\ k\in[\![0,n-1]\!]\}$. Or les éléments x^k, $k\in[\![0,n-1]\!]$, sont distincts, car sinon cela contredirait la définition de n (il existerait p et q distincts tels que $x^{|p-q|} = e$). On a ainsi $d = n$ et $x^d = e$, ce qui donne :

$$\langle x\rangle = \underbrace{\left\{e, x, x^2, \ldots, x^{d-1}\right\}}_{d \text{ éléments distincts}}$$

Pour tout $k\in\mathbb{Z}$, on effectue la division euclidienne de k par d : $k = qd+r$ avec $0\leqslant r<d$. Cela donne :

$$\begin{aligned} x^k = e &\iff x^r = e && \text{car } x^d = e \\ &\iff r = 0 && \text{car } 0\leqslant r<d \\ &\iff d|k \end{aligned}$$

2. *Démonstration non triviale.* On note G un groupe fini et x un élément dont l'ordre est noté d. *Voici deux démonstrations pour montrer que d divise* $\operatorname{card} G$ *:*

◦ *Démonstration partielle officielle. D'après le programme : « la démonstration n'est exigible que pour un groupe commutatif ». Plaçons-nous dans ce cas.* On note $x\in G$ et n l'ordre de G. On remarque que $t\mapsto tx$ est une bijection de G dans lui-même (attention, il ne s'agit pas d'un morphisme de groupes). On a donc :

$$\begin{aligned} \prod_{t\in G} t &= \prod_{t\in G}(tx) \\ \prod_{t\in G} t &= \prod_{t\in G} t \underbrace{\prod_{t\in G} x}_{=x^n} \\ e &= x^n \end{aligned}$$

La technique de démonstration ci-dessus sera réutilisée pour le théorème d'Euler, page 69.

◦ *Démonstration générale.* On note $H = \langle x\rangle$.

∗ Montrons que $\{yH,\ y\in G\}$ est une partition

de G. Soient y_1 et y_2 dans G ; on suppose que $y_1H \cap y_2H \neq \varnothing$. Alors il existe $(k,l) \in \mathbb{Z}^2$ tel que $y_1x^k = y_2x^l$. Cela implique que $y_1 = y_2x^{l-k} \in y_2H$ et de même $y_2 \in y_1H$. Donc $y_1H = y_2H$. De plus, tout $y \in G$ est contenu dans un yH, car $e \in H$. On a donc bien une partition de G.

∗ Par ailleurs, la fonction $t \in H \mapsto yt \in yH$ est bijective. On en déduit que les yH ont tous le même cardinal, à savoir $\operatorname{card} H$.

∗ Conclusion : $\operatorname{card} H$ divise $\operatorname{card} G$ (le quotient étant le nombre d'éléments dans la partition ci-dessus).

Remarques.

• *Terminologie hors programme.* Ce résultat est parfois appelé « petit théorème de Lagrange ». De plus, pour a élément d'un groupe, le sous-groupe $\langle a \rangle$ est appelé *cycle* de a.

• *Remarque avancée.* Attention, si d est un diviseur de l'ordre du groupe, il n'existe pas toujours[1] d'élément d'ordre d.

Exemple. Plaçons-nous dans le groupe formé des bijections du plan muni de la loi de composition. Une homothétie est alors d'ordre infini, sauf si son rapport est 1 (dans ce cas son ordre vaut 1) ou -1 (dans ce cas son ordre vaut 2). Une rotation d'angle $\frac{2\pi}{5}$ est d'ordre 5.

2 Exemples fondamentaux

i Groupes monogènes ($(\mathbb{Z},+)$ et $(\mathbb{Z}/n\mathbb{Z},+)$)

Définitions : groupe monogène et groupe cyclique ●●○

○ Un groupe est dit *monogène* s'il est engendré par l'un (au moins) de ses éléments. Le cas échéant, un tel élément est qualifié de *générateur* du groupe.

○ Si, de plus, ce groupe est d'ordre fini, alors il est dit *cyclique*.

Remarques.

• *Propriétés immédiates : commutativité et non-unicité des générateurs.* Un groupe monogène est toujours abélien. Un groupe monogène peut avoir plusieurs générateurs : $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$ par exemple.

• *Remarque importante.* Attention, un groupe monogène n'est pas engendré par n'importe lequel de ses éléments (à l'exception triviale des groupes d'ordre 1). Seuls certains de ses éléments, ses générateurs, l'engendrent.

Exemples.

○ $(2\mathbb{Z},+)$ est un groupe monogène engendré par 2 ; le seul autre élément générant $2\mathbb{Z}$ est -2.

○ $\mathbb{U}_n$ est un groupe cyclique pour la multiplication. Ce groupe est d'ordre n et peut s'écrire de l'une des façons suivantes :

$$\begin{aligned}
\mathbb{U}_n &= \{z \in \mathbb{C},\ z^n = 1\} \\
&= \left\{ \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}},\ k \in \mathbb{Z} \right\} \\
&= \left\{ \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}},\ k \in [\![0, n-1]\!] \right\} \\
&= \left\langle \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}} \right\rangle \quad \text{(en référence à } (\mathbb{C}^*, \times)\text{)}
\end{aligned}$$

Remarquons que $\mathbb{U}_n$ peut contenir des éléments qui ne sont pas générateurs (par exemple i appartient à $\mathbb{U}_8$ mais il ne l'engendre pas, puisque $\langle \mathrm{i} \rangle = \mathbb{U}_4$).

[1] Les contre-exemples ne sont pas triviaux. Le plus petit contre-exemple est un groupe d'ordre 12, dit *groupe alterné de degré* 4, qui n'a pas d'élément d'ordre 6 : c'est le sous-groupe du groupe symétrique S_4 contenant les permutations de signature positive.