Chapitre 11

Structures algébriques usuelles

11.1 Introduction historique

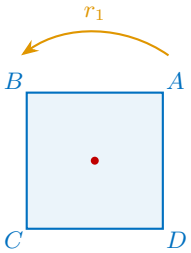
> *La Mathématique est l'art de donner le même nom à des choses différentes. [...] Il convient que ces choses, différentes par la matière, soient semblables par la forme, qu'elles puissent pour ainsi dire se couler dans le même moule.*
>
> Henri Poincaré - *Science et méthode*, Flammarion, 1908

11.1.1 Des équations aux structures

En 1770, dans ses *Réflexions sur la résolution algébrique des équations*, **Lagrange** montre que la difficulté de résoudre une équation tient à la manière dont certaines expressions de ses racines se transforment lorsqu'on permute ces racines. **Évariste Galois** pousse l'idée à son terme : dans la lettre à Auguste Chevalier qu'il écrit en mai 1832, la veille du duel où il trouve la mort, le mot « groupe » désigne un ensemble de permutations stable par composition. En 1854, **Arthur Cayley** détache la notion des permutations : un groupe est pour lui un ensemble de symboles dont le produit de deux quelconques appartient encore à l'ensemble, le produit étant associatif sans être forcément commutatif, et il range les produits dans un tableau à double entrée. Les autres structures suivent le même chemin, des exemples vers l'abstraction : **Richard Dedekind** appelle *corps* en 1871 les ensembles de nombres stables par les quatre opérations, **David Hilbert** parle d'*anneau* de nombres en 1897, et **Emmy Noether** fonde en 1921 la théorie abstraite des anneaux.

11.1.2 Un même tableau

Le principe de Poincaré se voit sur un exemple. Les quatre rotations r_0, r_1, r_2, r_3 d'angles 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ qui laissent un carré globalement invariant se composent entre elles, et les quatre nombres 1, i, -1, $-\mathrm{i}$ se multiplient entre eux. Les deux tables ont exactement la même forme : chaque couleur désigne un élément, et il suffit de lire r_k comme i^k pour passer de l'une à l'autre. Ce chapitre donne un nom à ce que ces deux situations ont en commun, la structure de *groupe*, et à la correspondance qui les identifie, un *isomorphisme* (section 11.3) ; il fait de même pour les ensembles munis de deux opérations, les *anneaux* et les *corps* (section 11.4).



r_1 envoie A sur B

$\circ$	r_0	r_1	r_2	r_3
r_0	r_0	r_1	r_2	r_3
r_1	r_1	r_2	r_3	r_0
r_2	r_2	r_3	r_0	r_1
r_3	r_3	r_0	r_1	r_2

$r_k \longleftrightarrow \mathrm{i}^k$

$\times$	1	i	-1	$-\mathrm{i}$
1	1	i	-1	$-\mathrm{i}$
i	i	-1	$-\mathrm{i}$	1
-1	-1	$-\mathrm{i}$	1	i
$-\mathrm{i}$	$-\mathrm{i}$	1	i	-1

11.2 Lois de composition interne

Les chapitres précédents ont manipulé de nombreuses opérations : l'addition et la multiplication des nombres (chapitres 3, 4 et 7), la composition des applications (chapitre 2), la réunion, l'intersection et la différence symétrique des parties d'un ensemble (chapitre 1). Cette section dégage le vocabulaire qui leur est commun ; on évite volontairement les lois artificielles, fabriquées pour l'exercice, qui n'éclairent rien.

11.2.1 Définitions

Définition : Soit E un ensemble. Une **loi de composition interne** sur E est une application

$$\star : \left| \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x \star y \end{array} \right.$$

On dit alors que $(E, \star)$ est un ensemble muni d'une loi de composition interne.

Le mot « interne » rappelle que le résultat $x \star y$ appartient encore à E. On note souvent la loi multiplicativement, $x \star y = xy$, ou additivement, $x \star y = x + y$; la notation additive est réservée aux lois commutatives.

Exemples :

- L'addition et la multiplication sont des lois de composition interne sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. La soustraction en est une sur $\mathbb{Z}$, mais pas sur $\mathbb{N}$, puisque $1 - 2 \notin \mathbb{N}$; la division n'en est une ni sur $\mathbb{R}$, à cause de 0, ni sur $\mathbb{Z}$.
- Pour un ensemble E, la composition $(f, g) \mapsto f \circ g$ est une loi de composition interne sur l'ensemble $\mathcal{F}(E, E)$ des applications de E dans E.
- La réunion, l'intersection et la différence symétrique sont des lois de composition interne sur l'ensemble $\mathcal{P}(E)$ des parties de E.

Définition : Soit $\star$ une loi de composition interne sur E.

- La loi $\star$ est **associative** si, pour tous x, y, z de E, $(x \star y) \star z = x \star (y \star z)$.
- La loi $\star$ est **commutative** si, pour tous x, y de E, $x \star y = y \star x$. Deux éléments x et y tels que $x \star y = y \star x$ sont dits **permutables**, ou encore on dit qu'ils **commutent**.

Remarques :

- La soustraction sur $\mathbb{Z}$ n'est pas associative : $(1 - 1) - 1 = -1$, alors que $1 - (1 - 1) = 1$. C'est pourquoi l'écriture $1 - 1 - 1$ n'a de sens que par une convention de lecture, de gauche à droite.
- La composition des applications est associative (chapitre 2, proposition 3), mais elle n'est pas commutative dès que E a au moins deux éléments : si $a \neq b$ et si f et g sont les applications constantes égales à a et à b, alors $f \circ g = f$ et $g \circ f = g$.
- Lorsque la loi est associative, le résultat d'un produit $x_1 \star x_2 \star \cdots \star x_n$ ne dépend pas de la place des parenthèses, et on les omet. Ce résultat d'*associativité généralisée* est admis : sa démonstration, par récurrence forte sur le nombre de facteurs, est sans difficulté de principe mais lourde à rédiger. En revanche, l'ordre des facteurs compte, sauf si la loi est commutative.

11.2.2 Élément neutre, éléments inversibles

Définition : Soit $\star$ une loi de composition interne sur E. Un élément e de E est **neutre** pour $\star$ si

$$\forall x \in E, \qquad x \star e = e \star x = x.$$

Proposition 1 : Une loi de composition interne admet au plus un élément neutre.

∘ Démonstration : Si e et e' sont neutres, alors $e \star e' = e'$ puisque e est neutre, et $e \star e' = e$ puisque e' est neutre. Donc $e = e'$. □

Exemples :

- Les nombres 0 et 1 sont neutres pour l'addition et pour la multiplication des nombres ; l'identité id_E est neutre pour la composition dans $\mathcal{F}(E,E)$.
- Dans $\mathcal{P}(E)$, la partie vide est neutre pour la réunion et pour la différence symétrique, et E est neutre pour l'intersection.
- L'addition sur $\mathbb{N}^*$ n'a pas d'élément neutre. Pour la soustraction sur $\mathbb{Z}$, on a $x-0=x$ pour tout x, mais $0-x\neq x$ dès que $x\neq 0$: l'entier 0 n'est neutre que d'un côté, ce qui ne suffit pas.

Définition : Soit $\star$ une loi de composition interne associative sur E, admettant un élément neutre e. Un élément x de E est **inversible** s'il existe $x'\in E$ tel que

$$x\star x' = x'\star x = e.$$

L'élément x' est alors appelé un **inverse** de x, ou un **symétrique** de x ; en notation additive, on parle d'**opposé**.

Proposition 2 : Soit $\star$ une loi associative sur E, d'élément neutre e, et x, y deux éléments de E.

(i) Si x est inversible, son inverse est unique ; on le note x^{-1}, ou $-x$ en notation additive.

(ii) Si x est inversible, x^{-1} l'est aussi, et $(x^{-1})^{-1}=x$.

(iii) Si x et y sont inversibles, $x\star y$ l'est aussi, et

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

∘ Démonstration :

▷ *(i)* Si x' et x'' sont deux inverses de x, l'associativité donne

$$x' = x'\star e = x'\star(x\star x'') = (x'\star x)\star x'' = e\star x'' = x''.$$

▷ *(ii)* Les égalités $x^{-1}\star x = x\star x^{-1} = e$ disent aussi que x est un inverse de x^{-1}.

▷ *(iii)* Par associativité, $(x\star y)\star(y^{-1}\star x^{-1}) = x\star(y\star y^{-1})\star x^{-1} = x\star x^{-1} = e$, et de même $(y^{-1}\star x^{-1})\star(x\star y)=e$. □

Remarque : L'erreur la plus répandue est d'écrire $(xy)^{-1}=x^{-1}y^{-1}$. L'ordre s'inverse, comme lorsqu'on se déchausse : on retire d'abord la chaussure, mise en dernier, puis la chaussette. Le chapitre 2 l'a déjà rencontré sous la forme $(g\circ f)^{-1}=f^{-1}\circ g^{-1}$ (proposition 7). Les deux écritures coïncident lorsque x et y commutent.

Exemples :

- Dans $(\mathbb{Z},\times)$, les seuls éléments inversibles sont 1 et -1 ; dans $(\mathbb{Q},\times)$, ce sont tous les rationnels non nuls.
- Dans $(\mathcal{F}(E,E),\circ)$, les éléments inversibles sont exactement les bijections de E dans E, et l'inverse est la bijection réciproque : c'est le théorème 1 du chapitre 2.
- Dans $(\mathcal{P}(E),\cup)$, seule la partie vide est inversible, puisque $A\cup B=\varnothing$ impose $A=\varnothing$. Dans $(\mathcal{P}(E),\Delta)$, au contraire, toute partie est inversible et elle est son propre inverse, puisque $A\,\Delta\,A=\varnothing$ (chapitre 1).

11.2.3 Distributivité et parties stables

Définition : Soit $\star$ et $\top$ deux lois de composition interne sur E. La loi $\top$ est **distributive** par rapport à la loi $\star$ si, pour tous x, y, z de E,

$$x\top(y\star z) = (x\top y)\star(x\top z) \qquad \text{et} \qquad (y\star z)\top x = (y\top x)\star(z\top x).$$

Exemple : La multiplication des nombres est distributive par rapport à l'addition, mais l'addition ne l'est pas par rapport à la multiplication : $1+(2\times 3)=7$, alors que $(1+2)\times(1+3)=12$. Dans $\mathcal{P}(E)$, l'intersection est distributive par rapport à la réunion, et la réunion par rapport à l'intersection (chapitre 1) : les deux lois jouent des rôles symétriques, ce qui n'arrive pas pour les nombres.

Définition : Soit $\star$ une loi de composition interne sur E et A une partie de E. On dit que A est **stable** par $\star$ si

$$\forall (x,y)\in A^2, \qquad x\star y\in A.$$

La restriction de $\star$ à $A\times A$ est alors une loi de composition interne sur A, appelée **loi induite** sur A, et encore notée $\star$.

Exemples :

- L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est stable par multiplication (chapitre 4, proposition 11). En revanche, l'ensemble $\mathbb{R}_-^*$ des réels strictement négatifs ne l'est pas, puisque le produit de -1 par lui-même vaut 1.
- L'ensemble des entiers impairs est stable par multiplication, mais pas par addition, puisque $1+1=2$.
- L'ensemble des bijections de E dans E est stable par composition (chapitre 2, proposition 7).

Le tableau suivant rassemble les propriétés des lois rencontrées ; dans les deux dernières colonnes, il indique l'élément neutre et dit si tous les éléments sont inversibles. On y suppose que E a au moins deux éléments.

Loi	associative	commutative	élément neutre	tout élément inversible
$(\mathbb{N},+)$	✓	✓	0	×
$(\mathbb{Z},-)$	×	×	aucun	sans objet
$(\mathbb{Z},\times)$	✓	✓	1	×
$(\mathbb{R}^*,\times)$	✓	✓	1	✓
$(\mathcal{F}(E,E),\circ)$	✓	×	id_E	×
$(\mathcal{P}(E),\cup)$	✓	✓	$\varnothing$	×
$(\mathcal{P}(E),\Delta)$	✓	✓	$\varnothing$	✓

Les lignes où toutes les cases sont cochées décrivent des groupes, au sens de la section suivante.

11.3 Groupes

11.3.1 Définition et premiers exemples

Définition : Un **groupe** est un ensemble G muni d'une loi de composition interne $\star$ telle que :

- la loi $\star$ est associative ;
- la loi $\star$ admet un élément neutre e ;
- tout élément de G est inversible pour $\star$.

Si de plus la loi est commutative, le groupe est dit **commutatif**, ou **abélien**.

Un groupe est donc un ensemble dans lequel on peut toujours « défaire » une opération. Le mot *abélien* honore **Niels Henrik Abel**, qui étudia vers 1829 les équations dont les permutations des racines commutent. Sauf mention contraire, on note la loi d'un groupe multiplicativement, xy, son neutre e ou 1, et l'inverse de x par x^{-1} ; la notation additive, avec 0 et $-x$, est réservée aux groupes abéliens.

Exemples :

- Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition, sont des groupes abéliens de neutre 0.
- Les ensembles $\mathbb{Q}^*$, $\mathbb{Q}_+^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ et $\mathbb{C}^*$, munis de la multiplication, sont des groupes abéliens de neutre 1 ; la proposition 7 y ajoutera $\mathbb{U}$ et les $\mathbb{U}_n$ du chapitre 4.
- En revanche, $(\mathbb{N},+)$ n'est pas un groupe, puisque 1 n'a pas d'opposé dans $\mathbb{N}$; ni $(\mathbb{Z},\times)$, puisque 2 n'a pas d'inverse dans $\mathbb{Z}$; ni $(\mathbb{R},\times)$, puisque 0 n'est pas inversible.

Exemple : Pour tout ensemble E, $(\mathcal{P}(E),\Delta)$ est un groupe abélien, comme l'annonçait le chapitre 1. La commutativité est claire, le neutre est $\varnothing$ et chaque partie est son propre inverse ; reste l'associativité. Un élément x de E appartient à $A\,\Delta\,B$ si et seulement s'il appartient à exactement une des deux parties, c'est-à-dire si et seulement si la somme $\mathbf{1}_A(x)+\mathbf{1}_B(x)$ est impaire. En appliquant deux fois cette remarque, x appartient à $(A\,\Delta\,B)\,\Delta\,C$ si et seulement si $\mathbf{1}_A(x)+\mathbf{1}_B(x)+\mathbf{1}_C(x)$ est impaire, puisque $\mathbf{1}_{A\Delta B}(x)$ a la même parité que $\mathbf{1}_A(x)+\mathbf{1}_B(x)$. Cette condition est symétrique en A, B, C, et le même calcul pour $A\,\Delta\,(B\,\Delta\,C)$ donne la même condition. Ainsi

$$(A\,\Delta\,B)\,\Delta\,C = A\,\Delta\,(B\,\Delta\,C)$$

est l'ensemble des éléments qui appartiennent à un nombre impair des trois parties.

11.3.2 Règles de calcul

Proposition 3 : Soit G un groupe et a, b, x, y des éléments de G.

(i) *Simplification.* Si $ax=ay$, alors $x=y$; si $xa=ya$, alors $x=y$.

(ii) *Équations.* L'équation $ax=b$, d'inconnue $x\in G$, a pour unique solution $x=a^{-1}b$, et l'équation $xa=b$ a pour unique solution $x=ba^{-1}$.

∘ Démonstration :

▷ *(i)* On multiplie l'égalité $ax=ay$ à gauche par a^{-1} : par associativité, $(a^{-1}a)x=(a^{-1}a)y$, soit $x=y$. Le second cas est symétrique.

▷ *(ii)* L'élément $a^{-1}b$ est solution, puisque $a(a^{-1}b)=(aa^{-1})b=b$. Si x est une solution, alors $ax=a(a^{-1}b)$, et la simplification donne $x=a^{-1}b$. Le second cas est symétrique. □

Remarques :

- Dans la table d'un groupe fini, comme celles de l'introduction, chaque élément apparaît donc exactement une fois dans chaque ligne et dans chaque colonne : la ligne de a contient les produits ax, qui sont deux à deux distincts par simplification. Cayley l'avait observé dès 1854.
- Dans un groupe non abélien, les solutions $a^{-1}b$ et ba^{-1} des deux équations sont en général différentes. L'erreur la plus répandue est de « diviser par a » sans préciser de quel côté : l'écriture $\frac{b}{a}$ n'a pas de sens dans un tel groupe.

Définition : Soit G un groupe et $x\in G$. On définit les **puissances** de x par récurrence :

$$x^0=e,\qquad x^{n+1}=x^nx \text{ pour } n\in\mathbb{N},\qquad x^{-n}=(x^{-1})^n \text{ pour } n\in\mathbb{N}^*.$$

En notation additive, on écrit nx au lieu de x^n : ainsi $0x=0$, $(n+1)x=nx+x$ et $(-n)x=n(-x)$.

Proposition 4 : Soit G un groupe, x et y deux éléments de G, m et n deux entiers relatifs. Alors

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

Si de plus x et y commutent, alors $(xy)^n=x^ny^n$.

∘ Démonstration : On démontre la première égalité pour m et n dans $\mathbb{N}$, par récurrence sur n. Elle est vraie pour $n=0$, puisque $x^mx^0=x^me=x^m$. Si elle est vraie au rang n, alors

$$x^mx^{n+1}=x^m(x^nx)=(x^mx^n)x=x^{m+n}x=x^{m+n+1}.$$

Les autres égalités se démontrent de la même façon pour des exposants positifs, à l'aide de la proposition 2 pour les inverses et de la commutation de x et y pour la dernière. L'extension aux exposants négatifs est admise : elle ne présente aucune difficulté, mais demande de distinguer les cas selon les signes de m, de n et de $m+n$. □

Remarque : Sans l'hypothèse de commutation, $(xy)^2 = xyxy$ et $x^2y^2 = xxyy$. Par simplification à gauche par x et à droite par y, ces deux éléments sont égaux si et seulement si $yx = xy$: l'identité $(xy)^2 = x^2y^2$ caractérise la commutation de x et y.

11.3.3 Le groupe des permutations d'un ensemble

Théorème 1 : Groupe des permutations :
Soit E un ensemble non vide. L'ensemble $\mathfrak{S}_E$ des bijections de E dans E, muni de la composition, est un groupe, de neutre id_E, dans lequel l'inverse de f est sa bijection réciproque f^{-1}. Ses éléments sont appelés les **permutations** de E.

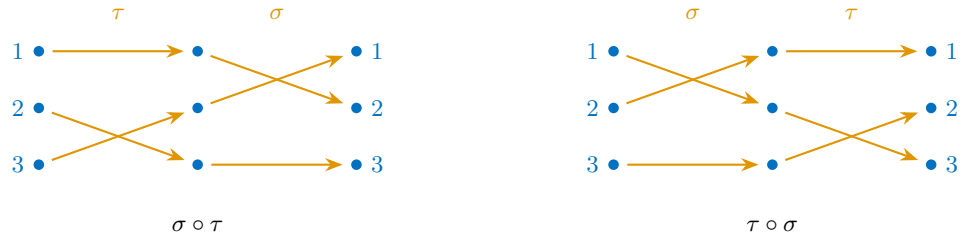
∘ Démonstration : La composée de deux bijections est une bijection (chapitre 2, proposition 7) : la composition est une loi de composition interne sur $\mathfrak{S}_E$. Elle est associative (chapitre 2, proposition 3). L'identité est une bijection, neutre pour la composition. Enfin, si f est une bijection, f^{-1} est une bijection qui vérifie $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_E$ (chapitre 2, théorème 1). □

Lorsque $E = [\![1, n]\!]$, on note $\mathfrak{S}_n$ ce groupe, appelé **groupe symétrique** d'indice n ; le chapitre 17 l'étudiera en détail en vue des déterminants. C'est le groupe de Lagrange et de Galois : une permutation des racines d'une équation est un élément de $\mathfrak{S}_n$.

Proposition 5 : Si E possède au moins trois éléments, le groupe $\mathfrak{S}_E$ n'est pas abélien.

∘ Démonstration : Soit a, b, c trois éléments distincts de E. On note σ la permutation qui échange a et b et fixe les autres éléments, et τ celle qui échange b et c et fixe les autres. Alors $(\sigma \circ \tau)(a) = \sigma(a) = b$, tandis que $(\tau \circ \sigma)(a) = \tau(b) = c$. Ainsi $\sigma \circ \tau \neq \tau \circ \sigma$. □

La figure détaille le calcul dans $\mathfrak{S}_3$, avec $a = 1$, $b = 2$ et $c = 3$: on suit chaque élément de gauche à droite, en appliquant d'abord la permutation écrite à droite dans la composée.



On lit à gauche $\sigma \circ \tau : 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1$, et à droite $\tau \circ \sigma : 1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2$: les deux composées font tourner les trois éléments, mais en sens contraires.

Remarque : Si E a un seul élément, $\mathfrak{S}_E = \{\mathrm{id}_E\}$; s'il en a deux, $\mathfrak{S}_E$ a deux éléments, l'identité et l'échange, et il est abélien. La proposition 5 est donc optimale.

11.3.4 Groupe produit

Proposition 6 : Soit $(G, \star)$ et $(H, *)$ deux groupes, de neutres e et e'. On munit $G \times H$ de la loi définie par

$$(g, h) \cdot (g', h') = (g \star g',\ h * h').$$

Alors $(G \times H, \cdot)$ est un groupe, appelé **groupe produit**, de neutre (e, e'), dans lequel l'inverse de (g, h) est (g^{-1}, h^{-1}).

∘ Démonstration : Chaque propriété se vérifie composante par composante. Par exemple, l'associativité de $\star$ et celle de $*$ donnent

$$\big((g, h) \cdot (g', h')\big) \cdot (g'', h'') = \big((g \star g') \star g'',\ (h * h') * h''\big) = (g, h) \cdot \big((g', h') \cdot (g'', h'')\big),$$

et de même $(g,h)\cdot(e,e') = (e,e')\cdot(g,h) = (g,h)$ et $(g,h)\cdot(g^{-1},h^{-1}) = (g^{-1},h^{-1})\cdot(g,h) = (e,e')$. □

Exemple : Le groupe $(\mathbb{R}^2,+)$, où $(x,y)+(x',y') = (x+x',y+y')$, est le groupe produit de $(\mathbb{R},+)$ par lui-même : c'est l'addition des vecteurs du plan. On définit de même $(\mathbb{R}^n,+)$, que le chapitre 14 munira d'une structure plus riche, celle d'espace vectoriel.

11.3.5 Sous-groupes

Définition : Soit G un groupe, de neutre e. Une partie H de G est un **sous-groupe** de G si :

- $e \in H$;
- H est stable par la loi de G : pour tous x, y de H, $xy \in H$;
- H est stable par passage à l'inverse : pour tout x de H, $x^{-1} \in H$.

Un sous-groupe H de G, muni de la loi induite, est lui-même un groupe : l'associativité est héritée de G, le neutre de G est dans H et y reste neutre, et l'inverse dans G d'un élément de H est dans H. Tout groupe G possède au moins deux sous-groupes, $\{e\}$ et G lui-même.

Proposition 7 : *(Caractérisation des sous-groupes.)* Une partie H d'un groupe G est un sous-groupe de G si et seulement si

$$H \neq \varnothing \qquad \text{et} \qquad \forall (x,y) \in H^2, \quad xy^{-1} \in H.$$

En notation additive, la condition s'écrit $x - y \in H$.

∘ Démonstration : Un sous-groupe contient e, donc il est non vide, et si x et y sont dans H, alors y^{-1} est dans H, puis xy^{-1}. Réciproquement, supposons la condition vérifiée, et soit $a \in H$.

▷ *Neutre.* Avec $x = y = a$, on obtient $e = aa^{-1} \in H$.

▷ *Inverses.* Pour $y \in H$, avec $x = e$, on obtient $y^{-1} = ey^{-1} \in H$.

▷ *Stabilité.* Pour x et y dans H, on sait que $y^{-1} \in H$, donc $xy = x(y^{-1})^{-1} \in H$. □

♡ **Méthode : Pour montrer qu'un ensemble muni d'une loi est un groupe**, on cherche d'abord à le reconnaître comme une partie d'un groupe connu, et l'on applique la proposition 7. On évite ainsi de vérifier l'associativité, qui est héritée, et l'on n'a que deux points à contrôler.

Exemples :

- L'ensemble $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*,\times)$: il contient 1, et si $|z| = |w| = 1$, alors $\left|\frac{z}{w}\right| = \frac{|z|}{|w|} = 1$. C'est ce qu'annonçait le chapitre 4. De même, pour $n \in \mathbb{N}^*$, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$, puisque $1 \in \mathbb{U}_n$ et que $z^n = w^n = 1$ entraîne $\left(\frac{z}{w}\right)^n = \frac{z^n}{w^n} = 1$.
- Pour $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ des multiples de n est un sous-groupe de $(\mathbb{Z},+)$, puisque $0 = n \times 0$ et que $nk - nk' = n(k-k')$. Le chapitre 12 montrera que ce sont les seuls sous-groupes de $\mathbb{Z}$, et en tirera toute l'arithmétique des entiers.
- Les similitudes directes $z \mapsto az + b$, avec $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$, forment un sous-groupe du groupe $\mathfrak{S}_{\mathbb{C}}$ des permutations de $\mathbb{C}$, comme l'annonçait le chapitre 4 : l'identité en est une, et les remarques qui suivent le théorème 5 de ce chapitre montrent que la composée de deux similitudes directes et la réciproque d'une similitude directe sont encore des similitudes directes.
- L'ensemble $\mathbb{R}^*_-$ n'est pas un sous-groupe de $(\mathbb{R}^*,\times)$, puisqu'il ne contient pas 1 ; l'ensemble $\mathbb{N}$ n'est pas un sous-groupe de $(\mathbb{Z},+)$, puisque $0 - 1 \notin \mathbb{N}$.

Proposition 8 : L'intersection d'une famille non vide de sous-groupes d'un groupe G est un sous-groupe de G.

∘ Démonstration : Soit $(H_i)_{i\in I}$ une famille de sous-groupes, avec $I \neq \varnothing$, et H leur intersection. Le neutre appartient à chaque H_i, donc à H. Si x et y sont dans H, ils sont dans chaque H_i, donc xy^{-1} aussi, et $xy^{-1} \in H$. La proposition 7 conclut. □

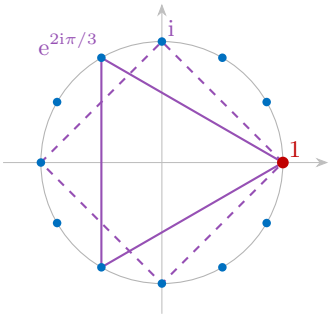
Remarque : Une réunion de sous-groupes n'est pas un sous-groupe en général : $2\mathbb{Z}\cup 3\mathbb{Z}$ contient 2 et 3, mais pas leur somme 5. L'erreur la plus répandue est de croire que la réunion est « le plus petit sous-groupe contenant les deux » ; ce plus petit sous-groupe existe, c'est l'intersection de tous les sous-groupes qui contiennent les deux, et pour $2\mathbb{Z}$ et $3\mathbb{Z}$ c'est $\mathbb{Z}$ tout entier, puisqu'il contient $3-2=1$.

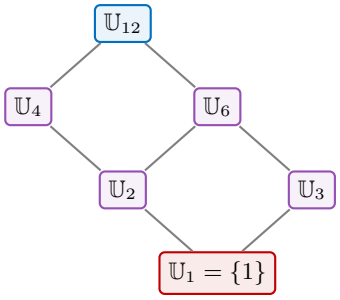
Les groupes $\mathbb{U}_n$ fournissent un exemple où l'on peut décrire toutes les inclusions entre sous-groupes.

Proposition 9 : Soit d et n deux entiers naturels non nuls. Alors $\mathbb{U}_d \subset \mathbb{U}_n$ si et seulement si d divise n.

∘ *Démonstration :* Si $n = dk$ avec $k \in \mathbb{N}^*$ et si $z^d = 1$, alors $z^n = (z^d)^k = 1$: ainsi $\mathbb{U}_d \subset \mathbb{U}_n$. Réciproquement, si $\mathbb{U}_d \subset \mathbb{U}_n$, le nombre $\omega = \mathrm{e}^{2\mathrm{i}\pi/d}$ appartient à $\mathbb{U}_n$, donc $\mathrm{e}^{2\mathrm{i}\pi n/d} = 1$. D'après le chapitre 4, ceci impose $\frac{2\pi n}{d} \in 2\pi\mathbb{Z}$, c'est-à-dire $\frac{n}{d} \in \mathbb{Z}$: l'entier d divise n. □

La figure représente $\mathbb{U}_{12}$ sur le cercle, avec ses sous-groupes $\mathbb{U}_3$ et $\mathbb{U}_4$, puis le schéma des inclusions entre les $\mathbb{U}_d$ pour les diviseurs d de 12 : un trait relie $\mathbb{U}_d$, en bas, à $\mathbb{U}_{d'}$, en haut, lorsque $\mathbb{U}_d \subset \mathbb{U}_{d'}$ sans intermédiaire.





$\mathbb{U}_3$: triangle, $\mathbb{U}_4$: carré en pointillés

Le triangle et le carré inscrits dans le cercle sont les sous-groupes $\mathbb{U}_3$ et $\mathbb{U}_4$; ils n'ont en commun que le neutre 1, ce que le schéma des inclusions traduit par le fait que le seul $\mathbb{U}_d$ situé sous $\mathbb{U}_3$ et sous $\mathbb{U}_4$ est $\mathbb{U}_1$. Ce schéma est celui de la divisibilité entre les diviseurs de 12.

11.3.6 Morphismes de groupes

Définition : Soit $(G,\star)$ et $(G',*)$ deux groupes. Une application $f : G \to G'$ est un **morphisme de groupes** si

$$\forall (x,y) \in G^2, \qquad f(x\star y) = f(x) * f(y).$$

Un morphisme bijectif est un **isomorphisme** ; on dit alors que G et G' sont **isomorphes**. Un morphisme de G dans lui-même est un **endomorphisme**, et un isomorphisme de G sur lui-même un **automorphisme**.

Un morphisme « transporte » la loi : on obtient le même résultat en composant dans G puis en appliquant f, ou en appliquant f puis en composant dans G'.

Exemples :

- L'exponentielle est un isomorphisme de $(\mathbb{R},+)$ sur $(\mathbb{R}_+^*,\times)$, puisque $\mathrm{e}^{x+y} = \mathrm{e}^x\mathrm{e}^y$ et qu'elle est bijective (chapitre 5) ; le logarithme est l'isomorphisme réciproque.
- L'application $t \mapsto \mathrm{e}^{\mathrm{i}t}$ est un morphisme de $(\mathbb{R},+)$ dans $(\mathbb{U},\times)$, et l'exponentielle complexe $z \mapsto \mathrm{e}^z$ un morphisme de $(\mathbb{C},+)$ dans $(\mathbb{C}^*,\times)$ (chapitre 4).
- Le module $z \mapsto |z|$ est un morphisme de $(\mathbb{C}^*,\times)$ dans $(\mathbb{R}_+^*,\times)$, et, pour $n \in \mathbb{Z}$, l'application $z \mapsto z^n$ est un endomorphisme de $(\mathbb{C}^*,\times)$, puisque $(zw)^n = z^n w^n$.
- Dans un groupe G, pour $x \in G$ fixé, l'application $n \mapsto x^n$ est un morphisme de $(\mathbb{Z},+)$ dans G : c'est la première égalité de la proposition 4.

Proposition 10 : Soit $f : G \to G'$ un morphisme de groupes, et e, e' les neutres de G et de G'. Alors

$$f(e) = e', \qquad f(x^{-1}) = f(x)^{-1} \quad \text{et} \quad f(x^n) = f(x)^n \quad \text{pour tous } x \in G \text{ et } n \in \mathbb{Z}.$$

∘ Démonstration : On a $f(e) = f(ee) = f(e)f(e)$, et la simplification par $f(e)$ dans G' donne $e' = f(e)$. Ensuite $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$, et de même dans l'autre ordre, donc $f(x^{-1})$ est l'inverse de $f(x)$. La dernière égalité s'obtient par récurrence pour $n \in \mathbb{N}$, puis par passage à l'inverse pour $n < 0$. □

Proposition 11 : La composée de deux morphismes de groupes est un morphisme de groupes. La réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

∘ Démonstration : Si $f : G \to G'$ et $g : G' \to G''$ sont des morphismes, alors, pour tous x, y de G,

$$(g \circ f)(xy) = g\big(f(x)f(y)\big) = g\big(f(x)\big)\, g\big(f(y)\big) = (g \circ f)(x)\,(g \circ f)(y).$$

Si f est un isomorphisme et si x', y' sont dans G', on pose $x = f^{-1}(x')$ et $y = f^{-1}(y')$; alors $f(xy) = f(x)f(y) = x'y'$, donc $f^{-1}(x'y') = xy = f^{-1}(x')f^{-1}(y')$. □

Proposition 12 : Soit $f : G \to G'$ un morphisme de groupes.
(i) L'image $f(H)$ d'un sous-groupe H de G est un sous-groupe de G'.
(ii) L'image réciproque $f^{-1}(H')$ d'un sous-groupe H' de G' est un sous-groupe de G.

∘ Démonstration :

▷ *(i)* L'ensemble $f(H)$ contient $f(e) = e'$. Si x' et y' sont dans $f(H)$, on les écrit $x' = f(x)$ et $y' = f(y)$ avec x, y dans H ; alors $x'y'^{-1} = f(x)f(y)^{-1} = f(xy^{-1})$, et $xy^{-1} \in H$.

▷ *(ii)* L'ensemble $f^{-1}(H')$ contient e, puisque $f(e) = e' \in H'$. Si x et y sont dans $f^{-1}(H')$, alors $f(xy^{-1}) = f(x)f(y)^{-1}$ appartient à H', donc $xy^{-1} \in f^{-1}(H')$. □

Définition : Soit $f : G \to G'$ un morphisme de groupes, et e' le neutre de G'. On appelle :
- **noyau** de f le sous-groupe $\operatorname{Ker} f = f^{-1}(\{e'\}) = \{x \in G \mid f(x) = e'\}$ de G ;
- **image** de f le sous-groupe $\operatorname{Im} f = f(G)$ de G'.

Ce sont bien des sous-groupes d'après la proposition 12, appliquée au sous-groupe $\{e'\}$ de G' et au sous-groupe G de G. Les notations viennent de l'allemand *Kern* et de l'anglais *image*.

Théorème 2 : Noyau et injectivité :
Soit $f : G \to G'$ un morphisme de groupes, de noyau $K = \operatorname{Ker} f$, et x, y deux éléments de G.
(i) On a $f(x) = f(y)$ si et seulement si $x^{-1}y \in K$: les antécédents de $f(x)$ sont les éléments xk, pour $k \in K$.
(ii) Le morphisme f est injectif si et seulement si $\operatorname{Ker} f = \{e\}$.

∘ Démonstration :

▷ *(i)* D'après la proposition 10, $f(x^{-1}y) = f(x)^{-1}f(y)$, qui vaut e' si et seulement si $f(x) = f(y)$. Ainsi $f(y) = f(x)$ si et seulement si $k = x^{-1}y$ appartient à K, c'est-à-dire si et seulement si $y = xk$ avec $k \in K$.

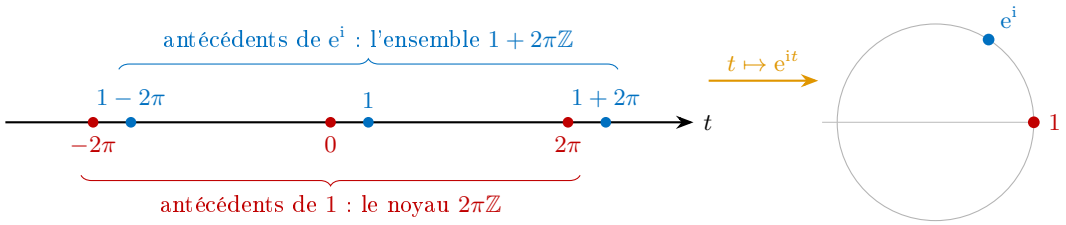
▷ *(ii)* Si f est injectif, e est le seul antécédent de e', donc $K = \{e\}$. Réciproquement, si $K = \{e\}$ et si $f(x) = f(y)$, le point (i) donne $x^{-1}y = e$, soit $y = x$. □

♡ **Méthode : Pour montrer qu'un morphisme de groupes est injectif**, on ne compare pas deux images quelconques : on cherche les éléments dont l'image est le neutre, et l'on vérifie qu'il n'y a que le neutre. Une seule équation, $f(x) = e'$, remplace l'équation à deux inconnues $f(x) = f(y)$.

Exemples :

- Le noyau du morphisme $t \mapsto \mathrm{e}^{\mathrm{i}t}$ de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$ est $2\pi\mathbb{Z}$. Le théorème 2 redonne alors le résultat du chapitre 4 : $\mathrm{e}^{\mathrm{i}t} = \mathrm{e}^{\mathrm{i}s}$ si et seulement si $s - t \in 2\pi\mathbb{Z}$, la notation additive remplaçant $x^{-1}y$ par $s - t$.
- Pour $n \in \mathbb{N}^*$, le noyau de $z \mapsto z^n$ sur $(\mathbb{C}^*, \times)$ est $\mathbb{U}_n$; celui du module est $\mathbb{U}$, et celui de l'exponentielle complexe est $2\mathrm{i}\pi\mathbb{Z}$. Aucun de ces morphismes n'est injectif, à l'exception de $z \mapsto z^n$ pour $n = 1$, qui est l'identité.

La figure illustre le premier exemple. Les antécédents de 1 forment le noyau $2\pi\mathbb{Z}$, et ceux de e^{i} forment l'ensemble $1 + 2\pi\mathbb{Z}$, obtenu en translatant le noyau : chaque point du cercle a ainsi des antécédents régulièrement espacés de 2π.



Les points rouges, envoyés sur 1, et les points bleus, envoyés sur e^{i}, se déduisent les uns des autres par la translation de 1 : c'est le point (i) du théorème 2.

11.3.7 Isomorphismes

Deux groupes isomorphes ne se distinguent que par le nom de leurs éléments : un isomorphisme f transporte toute la table de G sur celle de G', puisque le produit xy est envoyé sur le produit $f(x)f(y)$. C'est le sens précis de la phrase de Poincaré.

Exemples :

- Dans l'introduction, l'application $r_k \mapsto \mathrm{i}^k$ est un isomorphisme du groupe des quatre rotations du carré sur $(\mathbb{U}_4, \times)$: la rotation $r_j \circ r_k$, d'angle $\frac{(j+k)\pi}{2}$, est envoyée sur $\mathrm{i}^{j+k} = \mathrm{i}^j\mathrm{i}^k$.
- L'exponentielle montre que les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes. Une propriété de l'un se traduit dans l'autre : par exemple, dire que tout réel s'écrit $2 \times \frac{x}{2}$ revient à dire que tout réel strictement positif a une racine carrée.
- Les groupes $(\mathbb{Z}, +)$ et $(\mathbb{U}_4, \times)$ ne sont pas isomorphes, puisqu'il n'existe pas de bijection entre un ensemble infini et un ensemble à quatre éléments. Les groupes $(\mathbb{U}_4, \times)$ et $(\mathcal{P}(\{1, 2\}), \Delta)$, qui ont tous deux quatre éléments, ne le sont pas non plus : dans le second, tout élément vérifie $x \,\Delta\, x = \varnothing$, alors que dans le premier $\mathrm{i}^2 = -1 \neq 1$, et cette propriété serait transportée par un isomorphisme.

11.4 Anneaux et corps

Les ensembles de nombres portent deux lois, l'addition et la multiplication, liées par la distributivité. Cette section étudie ce que l'on peut dire en ne retenant que ces règles ; elle prépare l'arithmétique de $\mathbb{Z}$ (chapitre 12) et celle des polynômes (chapitre 13), et elle fournira au chapitre 16 l'exemple des matrices carrées.

11.4.1 Anneaux

Définition : Un **anneau** est un ensemble A muni de deux lois de composition interne, notées $+$ et $\times$, telles que :

- $(A, +)$ est un groupe abélien, dont le neutre est noté 0 ou 0_A ;
- la loi $\times$ est associative et admet un élément neutre, noté 1 ou 1_A ;
- la loi $\times$ est distributive par rapport à la loi $+$, au sens de la section 11.2 : pour tous a, b, c de A,

$$a(b + c) = ab + ac \qquad \text{et} \qquad (b + c)a = ba + ca.$$

L'anneau est dit **commutatif** si la loi $\times$ est commutative.

On écrit souvent ab au lieu de $a \times b$. Le neutre 1 fait partie de la définition : tous les anneaux considérés sont *unitaires*. L'ensemble $2\mathbb{Z}$ des entiers pairs, stable par addition et par multiplication, n'est donc pas un anneau, faute de neutre pour la multiplication.

Exemples :

- Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition et de la multiplication, sont des anneaux commutatifs.
- Soit X un ensemble non vide. L'ensemble $\mathcal{F}(X, \mathbb{R})$ des fonctions de X dans $\mathbb{R}$, muni des opérations définies point par point, $(f+g)(x) = f(x) + g(x)$ et $(fg)(x) = f(x)g(x)$, est un anneau commutatif ; son zéro est la fonction nulle, et son unité la fonction constante égale à 1. Chaque règle se vérifie en un point x, où elle devient une règle de calcul dans $\mathbb{R}$.
- Pour tout ensemble E, $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif, de zéro $\varnothing$ et d'unité E. On sait déjà que $(\mathcal{P}(E), \Delta)$ est un groupe abélien et que l'intersection est associative et commutative, de neutre E. Pour la distributivité, un élément x appartient à $A \cap (B \,\Delta\, C)$ si et seulement s'il appartient à A et à exactement une des parties B et C, c'est-à-dire à exactement une des parties $A \cap B$ et $A \cap C$: ainsi $A \cap (B \,\Delta\, C) = (A \cap B) \,\Delta\, (A \cap C)$.
- Le chapitre 13 construira l'anneau commutatif $\mathbb{K}[X]$ des polynômes, et le chapitre 16 l'anneau des matrices carrées, qui n'est pas commutatif.

Proposition 13 : *(Règles de calcul.)* Soit A un anneau, a et b deux éléments de A, et $n \in \mathbb{Z}$. Alors

$$0a = a0 = 0, \qquad (-a)b = a(-b) = -(ab), \qquad (-a)(-b) = ab, \qquad (na)b = a(nb) = n(ab),$$

où na désigne le multiple de a dans le groupe $(A, +)$, au sens de la proposition 4. Si de plus $1 = 0$ dans A, alors $A = \{0\}$.

∘ Démonstration :

▷ *Produit par zéro.* Par distributivité, $0a = (0+0)a = 0a + 0a$, et la simplification dans le groupe $(A, +)$ donne $0a = 0$. De même, $a0 = 0$.

▷ *Signes.* On a $ab + (-a)b = \big(a + (-a)\big)b = 0b = 0$, donc $(-a)b$ est l'opposé de ab ; de même pour $a(-b)$. En appliquant deux fois ce résultat, $(-a)(-b) = -\big(a(-b)\big) = -\big(-(ab)\big) = ab$.

▷ *Multiples.* L'application $x \mapsto xb$ est un endomorphisme du groupe $(A, +)$, par distributivité ; la proposition 10 donne donc $(na)b = n(ab)$ pour tout $n \in \mathbb{Z}$. De même pour $x \mapsto ax$.

▷ *Anneau nul.* Si $1 = 0$, alors pour tout $a \in A$, $a = 1a = 0a = 0$. □

L'anneau $\{0\}$, appelé **anneau nul**, est sans intérêt ; on l'exclura dans la définition des anneaux intègres et des corps.

Théorème 3 : Factorisation et binôme dans un anneau :
Soit A un anneau, et a, b deux éléments de A qui commutent. Pour tout entier $n \geqslant 1$,

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k},$$

et pour tout entier $n \geqslant 0$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

∘ Démonstration : Les démonstrations de la proposition 5 et du théorème 2 du chapitre 3 se transposent mot pour mot. Elles n'utilisent en effet que l'associativité, la distributivité, la commutation de a et b, qui permet de regrouper un produit de a et de b en $a^k b^\ell$, et le calcul sur les multiples $\binom{n}{k} x$, qui sont des multiples entiers au sens de la proposition 4 et qui se comportent comme des coefficients d'après la proposition 13. □

Remarque : L'hypothèse $ab = ba$ est indispensable. En développant, $(a+b)^2 = a^2+ab+ba+b^2$, qui n'est égal à $a^2 + 2ab + b^2$ que si $ba = ab$. L'erreur la plus répandue, au chapitre 16, sera d'appliquer la formule du binôme à deux matrices qui ne commutent pas.

11.4.2 Groupe des inversibles, anneaux intègres

Définition : Soit A un anneau. Un élément a de A est **inversible** s'il l'est pour la loi $\times$, c'est-à-dire s'il existe $b \in A$ tel que $ab = ba = 1$. On note $A^\times$ l'ensemble des éléments inversibles de A.

Proposition 14 : Pour tout anneau A, $(A^\times, \times)$ est un groupe, appelé **groupe des inversibles** de A.

∘ *Démonstration :* D'après la proposition 2, le produit de deux inversibles est inversible, et l'inverse d'un inversible est inversible : $A^\times$ est stable par $\times$ et par passage à l'inverse. Il contient 1, et la loi $\times$ y est associative. □

Exemples :

- On a $\mathbb{Z}^\times = \{-1, 1\}$, et $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{C}^\times = \mathbb{C}^*$.
- Une fonction f de $\mathcal{F}(X, \mathbb{R})$ est inversible si et seulement si elle ne s'annule pas : son inverse est alors $\frac{1}{f}$, et si $f(x_0) = 0$, l'égalité $f(x_0)g(x_0) = 1$ est impossible.
- Dans $(\mathcal{P}(E), \Delta, \cap)$, la seule partie inversible est E, puisque $A \cap B = E$ impose $A = B = E$.

Définition : Un anneau A est **intègre** s'il est commutatif, non nul, et si

$$\forall (a, b) \in A^2, \qquad ab = 0 \implies (a = 0 \text{ ou } b = 0).$$

Dans un anneau quelconque, deux éléments non nuls a et b tels que $ab = 0$ sont appelés des **diviseurs de zéro**.

Exemples :

- Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres : c'est la règle du produit nul.
- Si X a au moins deux éléments, l'anneau $\mathcal{F}(X, \mathbb{R})$ n'est pas intègre. Pour $x_0 \in X$, les fonctions indicatrices $f = \mathbf{1}_{\{x_0\}}$ et $g = \mathbf{1}_{X \setminus \{x_0\}}$ sont non nulles, mais $fg = 0$, puisqu'en chaque point l'une des deux s'annule.
- De même, si E a au moins deux éléments distincts a et b, l'anneau $(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre, puisque $\{a\} \cap \{b\} = \varnothing$.

Remarques :

- Dans un anneau intègre, on peut simplifier par un élément non nul : si $ab = ac$ et $a \neq 0$, alors $a(b - c) = 0$, donc $b = c$. Dans un anneau qui ne l'est pas, cette simplification est fausse, et c'est l'erreur la plus répandue : avec les fonctions f et g de l'exemple, $fg = f \times 0$, mais $g \neq 0$.
- Les congruences du chapitre 2 montrent un phénomène voisin : $2 \times 3 \equiv 0$ [6], alors que ni 2 ni 3 ne sont congrus à 0 modulo 6. Le chapitre 12 expliquera pourquoi cela n'arrive pas modulo un nombre premier.

11.4.3 Corps

Définition : Un **corps** est un anneau commutatif $\mathbb{K}$, non nul, dans lequel tout élément non nul est inversible :

$$1 \neq 0 \qquad \text{et} \qquad \mathbb{K}^\times = \mathbb{K} \setminus \{0\}.$$

Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, comme l'annonçait le chapitre 4 ; l'anneau $\mathbb{Z}$ n'en est pas un. Dans cette définition, un corps est toujours commutatif.

Proposition 15 : Tout corps est un anneau intègre.

∘ Démonstration : Soit $\mathbb{K}$ un corps, et a, b deux éléments de $\mathbb{K}$ tels que $ab = 0$. Si $a \neq 0$, a est inversible, et $b = a^{-1}(ab) = a^{-1}0 = 0$. □

La réciproque est fausse : $\mathbb{Z}$ est intègre sans être un corps.

Remarque : Comme l'annonçait le chapitre 7, $\mathbb{R}$ est un *corps totalement ordonné* : c'est un corps muni d'une relation d'ordre total compatible avec l'addition, et telle que le produit de deux éléments positifs est positif. Le corps $\mathbb{C}$ ne peut pas être ordonné de cette façon. Dans un tel corps, en effet, tout carré est positif, puisque $x^2 = (-x)^2$ et que x ou $-x$ est positif ; on aurait donc $-1 = \mathrm{i}^2 \geqslant 0$, puis $0 \geqslant 1$ en ajoutant 1 ; comme $1 = 1^2 \geqslant 0$, on obtiendrait $1 = 0$, ce qui est absurde dans un corps. C'est pourquoi on ne compare jamais deux nombres complexes.

11.4.4 Sous-anneaux

Définition : Soit A un anneau. Une partie B de A est un **sous-anneau** de A si

$$1_A \in B \qquad \text{et} \qquad \forall (x,y) \in B^2, \quad x - y \in B \ \text{ et } \ xy \in B.$$

D'après la proposition 7, B est alors un sous-groupe de $(A, +)$, stable par $\times$ et contenant 1_A : muni des lois induites, c'est un anneau, de même zéro et de même unité que A. Ainsi $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, lui-même sous-anneau de $\mathbb{R}$, lui-même sous-anneau de $\mathbb{C}$.

♡ **Méthode : Pour montrer qu'un ensemble muni de deux lois est un anneau**, on cherche, comme pour les groupes, à le reconnaître comme une partie d'un anneau connu, et l'on vérifie les trois conditions de la définition de sous-anneau. L'associativité, la distributivité et la commutativité éventuelle sont alors héritées.

Exemples :

- L'ensemble $\mathbb{D}$ des nombres décimaux (chapitre 7) est un sous-anneau de $\mathbb{Q}$: il contient 1, et si $x = \frac{k}{10^n}$ et $y = \frac{\ell}{10^m}$, alors $x - y = \frac{10^m k - 10^n \ell}{10^{n+m}}$ et $xy = \frac{k\ell}{10^{n+m}}$ sont décimaux. Il n'est pas un corps, puisque l'inverse $\frac{1}{3}$ de 3 n'est pas décimal.
- L'ensemble $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid (a,b) \in \mathbb{Z}^2\}$ des *entiers de Gauss* est un sous-anneau de $\mathbb{C}$: il contient 1, et pour $x = a + \mathrm{i}b$ et $y = c + \mathrm{i}d$,

$$x - y = (a - c) + \mathrm{i}(b - d), \qquad xy = (ac - bd) + \mathrm{i}(ad + bc),$$

dont les parties réelle et imaginaire sont entières.

Exemple : Cherchons les inversibles de $\mathbb{Z}[\mathrm{i}]$. Si $x = a + \mathrm{i}b$ est inversible, d'inverse y, alors $|x|^2|y|^2 = |xy|^2 = 1$. Or $|x|^2 = a^2 + b^2$ et $|y|^2$ sont des entiers naturels, donc $a^2 + b^2 = 1$, ce qui impose $(a,b) \in \{(\pm 1, 0), (0, \pm 1)\}$. Réciproquement, 1, -1, i et $-\mathrm{i}$ sont inversibles dans $\mathbb{Z}[\mathrm{i}]$, d'inverses 1, -1, $-\mathrm{i}$ et i. Ainsi

$$\mathbb{Z}[\mathrm{i}]^\times = \{1, \mathrm{i}, -1, -\mathrm{i}\} = \mathbb{U}_4,$$

et l'on retrouve le groupe de l'introduction comme groupe des inversibles d'un anneau.

Exemple : Soit $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2\}$. C'est un sous-anneau de $\mathbb{R}$: il contient 1, il est stable par différence, et

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

C'est même un corps. Comme $\sqrt{2}$ est irrationnel (chapitre 7), l'écriture $a + b\sqrt{2}$ d'un élément est unique, et si $a + b\sqrt{2} \neq 0$, alors $a - b\sqrt{2} \neq 0$: sinon on aurait $b \neq 0$ et $\sqrt{2} = \frac{a}{b}$. Le produit $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ est donc un rationnel non nul, et

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Par exemple, $\frac{1}{1+2\sqrt{2}} = \frac{-1+2\sqrt{2}}{7}$, puisque $(1 + 2\sqrt{2})(-1 + 2\sqrt{2}) = 8 - 1 = 7$. On dit que $\mathbb{Q}[\sqrt{2}]$ est un *sous-corps* de $\mathbb{R}$: c'est un sous-anneau qui est un corps.

11.4.5 Morphismes d'anneaux

Définition : Soit A et B deux anneaux. Une application $f : A \to B$ est un **morphisme d'anneaux** si, pour tous x, y de A,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y) \qquad \text{et} \qquad f(1_A) = 1_B.$$

Un morphisme d'anneaux bijectif est un **isomorphisme d'anneaux**.

Un morphisme d'anneaux est en particulier un morphisme du groupe $(A, +)$ dans $(B, +)$: il vérifie $f(0) = 0$ et $f(-x) = -f(x)$, d'après la proposition 10. La condition $f(1_A) = 1_B$, en revanche, ne découle pas des deux autres, puisque l'application nulle les vérifie.

Exemples :

- La conjugaison $z \mapsto \overline{z}$ est un automorphisme de l'anneau $\mathbb{C}$: elle est compatible avec la somme et le produit (chapitre 4), envoie 1 sur 1, et elle est sa propre réciproque.
- Pour $x_0 \in X$, l'évaluation $f \mapsto f(x_0)$ est un morphisme d'anneaux de $\mathcal{F}(X, \mathbb{R})$ dans $\mathbb{R}$, puisque les opérations sont définies point par point.
- L'application $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$, bien définie grâce à l'unicité de l'écriture, est un automorphisme de $\mathbb{Q}[\sqrt{2}]$: elle respecte la somme, envoie 1 sur 1, et

  $$\sigma\big((a + b\sqrt{2})(c + d\sqrt{2})\big) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}).$$

  Elle joue pour $\mathbb{Q}[\sqrt{2}]$ le rôle de la conjugaison pour $\mathbb{C}$, et l'inverse calculé plus haut s'écrit $\frac{1}{x} = \frac{\sigma(x)}{x\,\sigma(x)}$, comme $\frac{1}{z} = \frac{\overline{z}}{z\overline{z}}$. C'est le point de vue moderne sur les travaux de Galois : le groupe qu'il associe à une équation s'interprète comme un groupe d'automorphismes de corps.
- L'application $z \mapsto 2z$ de $\mathbb{C}$ dans $\mathbb{C}$ est un morphisme du groupe $(\mathbb{C}, +)$, mais pas un morphisme d'anneaux, puisque $2 \times 1 \neq 1$.

Proposition 16 : Soit $f : A \to B$ un morphisme d'anneaux.

(i) Si a est inversible dans A, alors $f(a)$ est inversible dans B et $f(a^{-1}) = f(a)^{-1}$. La restriction de f à $A^\times$ est donc un morphisme du groupe $A^\times$ dans le groupe $B^\times$.

(ii) Si A est un corps et si B n'est pas l'anneau nul, alors f est injectif.

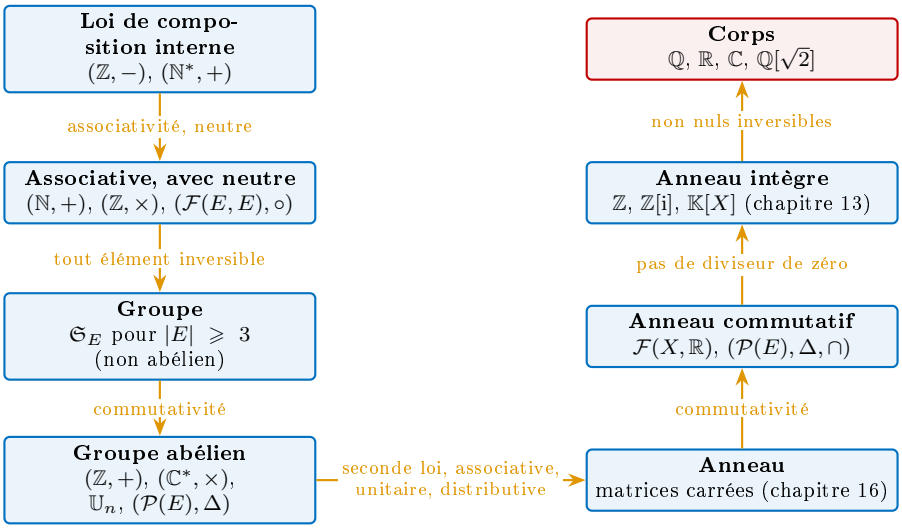
∘ Démonstration :

▷ *(i)* On a $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$, et de même dans l'autre ordre.

▷ *(ii)* D'après le théorème 2, appliqué au morphisme de groupes $f : (A, +) \to (B, +)$, il suffit de montrer que $f(a) = 0$ impose $a = 0$. Si $f(a) = 0$ et $a \neq 0$, alors a est inversible, et le point (i) dit que $0 = f(a)$ est inversible dans B ; alors $1_B = 0 \times f(a)^{-1} = 0$, et B serait l'anneau nul d'après la proposition 13. □

11.5 Bilan

Le schéma range les structures du chapitre de la plus pauvre à la plus riche ; chaque flèche ajoute une propriété, indiquée sur la flèche, et chaque boîte rappelle des exemples. Une structure plus riche hérite de tous les résultats établis pour les structures qu'elle prolonge : ce que l'on démontre une fois pour les groupes vaut pour $\mathbb{U}$, pour $\mathfrak{S}_E$, pour $(\mathcal{P}(E), \Delta)$ et pour le groupe additif de tout anneau.



Chaque exemple est placé dans la boîte la plus riche qui lui convienne : $\mathbb{Z}$ est un anneau intègre mais pas un corps, et $\mathcal{F}(X, \mathbb{R})$ un anneau commutatif qui n'est pas intègre dès que X a deux éléments.

Pour chaque structure, les outils se correspondent : une sous-structure se reconnaît par quelques conditions, et un morphisme transporte les lois. Le tableau les rassemble.

Structure	Sous-structure de G ou de A	Morphisme f
groupe	$H \neq \varnothing$ et $xy^{-1} \in H$ (prop. 7)	$f(xy) = f(x)f(y)$; injectif si et seulement si $\operatorname{Ker} f = \{e\}$ (th. 2)
anneau	$1 \in B$, $x - y \in B$ et $xy \in B$	$f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, $f(1) = 1$
corps	sous-anneau qui est un corps	tout morphisme vers un anneau non nul est injectif (prop. 16)

Le chapitre 12 appliquera ces notions au groupe $(\mathbb{Z}, +)$, dont il déterminera tous les sous-groupes, et le chapitre 14 ajoutera aux groupes abéliens une multiplication par des scalaires, pour obtenir les espaces vectoriels. Le chapitre 17 étudiera le groupe $\mathfrak{S}_n$ et deux morphismes fondamentaux, la signature et le déterminant.