Chapitre 4

Morphismes

Le chapitre précédent a défini les groupes ; celui-ci définit les applications qui les respectent. Un morphisme est une application qui *transporte la loi* : peu importe que l'on calcule avant ou après l'avoir appliquée, le résultat est le même. Cette exigence, en apparence modeste, est d'une puissance remarquable — elle suffit à faire de deux groupes très différents deux copies l'un de l'autre.

4.1 Définitions

4.1.1 Morphisme de groupes

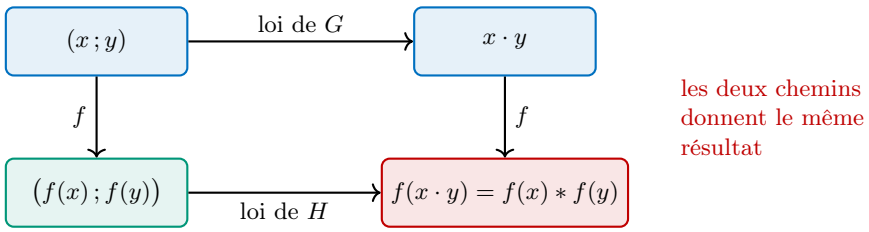
Définition : Soient $(G\,;\cdot)$ et $(H\,;*)$ deux groupes. On appelle **morphisme de groupes**, ou **homomorphisme**, toute application $f : G \longrightarrow H$ telle que :

$$\forall (x\,;y) \in G^2,\ f(x \cdot y) = f(x) * f(y)$$

Autrement dit, f « respecte » les lois de composition interne. On appelle de plus :

- **endomorphisme** tout morphisme d'un groupe dans lui-même ;
- **isomorphisme** tout morphisme bijectif ;
- **automorphisme** tout endomorphisme bijectif.

Remarque : L'égalité de la définition se lit comme un **diagramme commutatif** : partant de deux éléments de G, on peut soit les composer dans G puis appliquer f, soit appliquer f à chacun puis composer dans H. Les deux chemins aboutissent au même résultat.



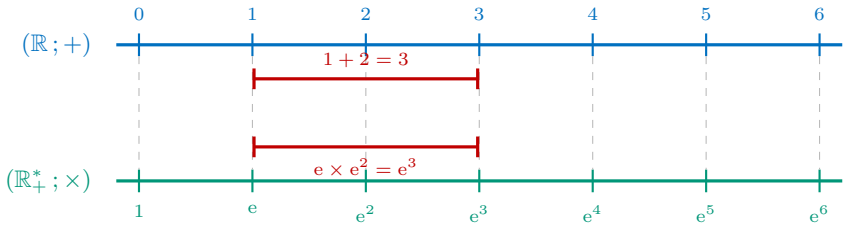
Exemple : L'application exponentielle est un morphisme de groupes :

$$\begin{array}{rcl} \varphi : (\mathbb{R}\,;+) & \longrightarrow & (\mathbb{R}_+^*\,;\times) \\ x & \longmapsto & \mathrm{e}^x \end{array}$$

En effet, les deux ensembles sont bien des groupes, et pour tout $(x\,;y) \in \mathbb{R}^2$:

$$\varphi(x+y) = \mathrm{e}^{x+y} = \mathrm{e}^x \times \mathrm{e}^y = \varphi(x) \times \varphi(y)$$

Elle est de plus bijective, de réciproque le logarithme népérien : c'est donc un **isomorphisme**. Les groupes $(\mathbb{R}\,;+)$ et $(\mathbb{R}_+^*\,;\times)$ sont ainsi deux présentations d'un même objet, l'addition d'un côté correspondant exactement à la multiplication de l'autre.



Les deux graduations se correspondent point par point : un déplacement additif en haut devient une multiplication en bas. C'est exactement le principe de la règle à calcul, et c'est ce que signifie l'existence d'un isomorphisme.

Exemple : Trois autres morphismes, à garder en mémoire :

- le module $z \mapsto |z|$ de $(\mathbb{C}^*\,;\times)$ dans $(\mathbb{R}_+^*\,;\times)$, puisque $|zz'| = |z|\,|z'|$;
- la conjugaison $z \mapsto \overline{z}$ de $(\mathbb{C}\,;+)$ dans lui-même, qui est un *automorphisme* ;
- pour n fixé, l'application $k \mapsto nk$ de $(\mathbb{Z}\,;+)$ dans lui-même, qui est un endomorphisme injectif mais non surjectif dès que $n \geqslant 2$.

En revanche, $x \mapsto x+1$ n'est *pas* un morphisme de $(\mathbb{R}\,;+)$ dans lui-même : on aurait $f(x+y) = x+y+1$ alors que $f(x)+f(y) = x+y+2$.

4.1.2 Propriétés élémentaires

Propriété 1 : Soit $f : (G\,;\cdot) \longrightarrow (H\,;*)$ un morphisme de groupes, et notons e_G et e_H les neutres respectifs. Alors :

$$f(e_G) = e_H \qquad \text{et} \qquad \forall x \in G,\ f\left(x^{-1}\right) = f(x)^{-1}$$

∘ *Démonstration :* Image du neutre : comme $e_G \cdot e_G = e_G$, on obtient en appliquant f :

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$$

En composant les deux membres par $f(e_G)^{-1}$, qui existe puisque H est un groupe, il vient $e_H = f(e_G)$.

Image du symétrique : soit $x \in G$. En appliquant f à l'égalité $x \cdot x^{-1} = e_G$:

$$f(x) * f\left(x^{-1}\right) = f\left(x \cdot x^{-1}\right) = f(e_G) = e_H$$

et de même dans l'autre ordre. L'élément $f\left(x^{-1}\right)$ est donc le symétrique de $f(x)$, qui est unique d'après le chapitre 3. □

Remarque : Un morphisme transporte donc *toute* la structure, et non la seule loi : il envoie le neutre sur le neutre et les symétriques sur les symétriques. C'est pourquoi il est inutile de vérifier ces deux points quand on définit un morphisme — ils sont automatiques.

Propriété 2 : Soient $f : (G\,;\cdot) \to (H\,;*)$ et $g : (H\,;*) \to (K\,;\perp)$ deux morphismes de groupes. Alors :

- la composée $g \circ f$ est un morphisme de G dans K ;
- si f est un *isomorphisme*, alors f^{-1} en est un également.

∘ *Démonstration :* Composée : pour $(x\,;y) \in G^2$, on applique successivement les deux hypothèses :

$$\big(g \circ f\big)(x \cdot y) = g\big(f(x) * f(y)\big) = g\big(f(x)\big) \perp g\big(f(y)\big) = \big(g \circ f\big)(x) \perp \big(g \circ f\big)(y)$$

Réciproque : soit $(x\,;y) \in H^2$. Comme f est bijective, on peut écrire $x = f\left(f^{-1}(x)\right)$ et de même pour y, d'où :

$$\begin{aligned} f^{-1}(x * y) &= f^{-1}\Big(f\big(f^{-1}(x)\big) * f\big(f^{-1}(y)\big)\Big) \\ &= f^{-1}\Big(f\big(f^{-1}(x) \cdot f^{-1}(y)\big)\Big) \\ &= f^{-1}(x) \cdot f^{-1}(y) \end{aligned}$$

la deuxième ligne utilisant que f est un morphisme, et la troisième que $f^{-1} \circ f = \mathrm{Id}$. □

Remarque : On dit que deux groupes sont **isomorphes** lorsqu'il existe un isomorphisme de l'un vers l'autre. La proposition précédente montre que cette relation est *symétrique*, ce qui autorise à dire que deux groupes isomorphes sont « les mêmes » : ils ne diffèrent que par le nom de leurs éléments.

4.2 Noyau et image

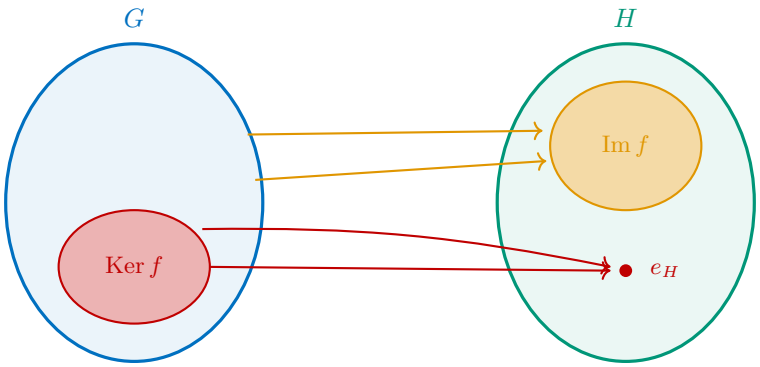
Définition : Soit $f : (G\,;\cdot) \longrightarrow (H\,;*)$ un morphisme de groupes. On appelle :

- **noyau** de f l'ensemble des éléments envoyés sur le neutre :

$$\mathrm{Ker}\, f = \left\{x \in G \;\middle|\; f(x) = e_H\right\}$$

- **image** de f l'ensemble des valeurs atteintes :

$$\mathrm{Im}\, f = \left\{y \in H \;\middle|\; \exists x \in G,\ f(x) = y\right\}$$



tout le noyau s'écrase sur le neutre e_H,
tandis que l'image est la zone effectivement atteinte

Propriété 3 : Soit $f : (G\,;\cdot) \longrightarrow (H\,;*)$ un morphisme de groupes. Alors $\mathrm{Ker}\, f$ est un **sous-groupe de G**, et $\mathrm{Im}\, f$ est un **sous-groupe de H**.

∘ *Démonstration :* Nous utilisons la caractérisation du chapitre 3.

Le noyau : d'après la proposition 1, $f(e_G) = e_H$, donc $e_G \in \mathrm{Ker}\, f$, qui n'est pas vide. Soient ensuite x et y dans $\mathrm{Ker}\, f$, de sorte que $f(x) = f(y) = e_H$. Alors :

$$f\left(x \cdot y^{-1}\right) = f(x) * f\left(y^{-1}\right) = f(x) * f(y)^{-1} = e_H * e_H^{-1} = e_H$$

donc $x \cdot y^{-1} \in \mathrm{Ker}\, f$.

L'image : de même, $e_H = f(e_G)$ appartient à $\mathrm{Im}\, f$, qui n'est pas vide. Soient x et y dans $\mathrm{Im}\, f$: il existe a et b dans G tels que $f(a) = x$ et $f(b) = y$. Alors :

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

qui est bien de la forme $f(\cdot)$, donc appartient à $\mathrm{Im}\, f$. □

Théorème 1 : Caractérisation des morphismes injectifs et surjectifs :
Soit $f : (G\,;\cdot) \longrightarrow (H\,;*)$ un morphisme de groupes. Alors :

$$f \text{ est injectif} \iff \mathrm{Ker}\, f = \{e_G\}$$

$$f \text{ est surjectif} \iff \mathrm{Im}\, f = H$$

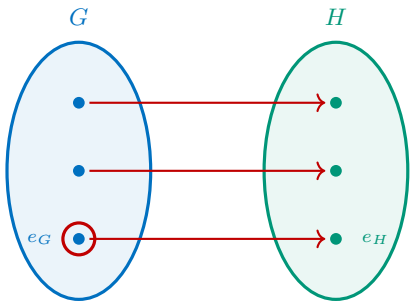
∘ *Démonstration :* Injectivité, sens direct : supposons f injective. L'inclusion $\{e_G\} \subset \operatorname{Ker} f$ est acquise par la proposition 1. Réciproquement, soit $x \in \operatorname{Ker} f$: alors $f(x) = e_H = f(e_G)$, et l'injectivité donne $x = e_G$. D'où l'égalité.

Injectivité, réciproque : supposons $\operatorname{Ker} f = \{e_G\}$, et soient x et y tels que $f(x) = f(y)$. En composant par $f(y)^{-1}$:

$$f(x) * f(y)^{-1} = e_H \qquad \text{soit} \qquad f\left(x \cdot y^{-1}\right) = e_H$$

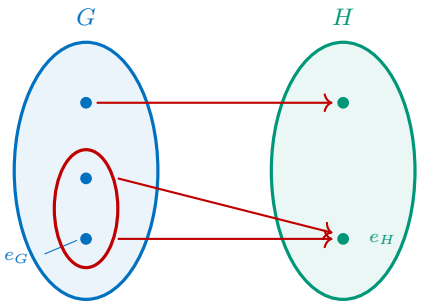
Donc $x \cdot y^{-1} \in \operatorname{Ker} f = \{e_G\}$, d'où $x \cdot y^{-1} = e_G$, c'est-à-dire $x = y$.

Surjectivité : l'inclusion $\operatorname{Im} f \subset H$ est toujours vraie. Dire que f est surjective, c'est dire que tout $y \in H$ possède un antécédent, c'est-à-dire que $H \subset \operatorname{Im} f$. Les deux propositions sont donc bien équivalentes. □



Ker $f = \{e_G\}$

f injectif



Ker f contient deux éléments

f non injectif

Le noyau mesure donc le *défaut d'injectivité* : plus il est gros, plus les éléments s'écrasent les uns sur les autres. Un noyau réduit au seul neutre signifie qu'aucun écrasement n'a lieu.

Méthode : C'est ce théorème que l'on utilise en pratique, car il remplace l'étude d'une équation quelconque par celle d'une seule :

1. Pour montrer que f est injectif :

> « Soit $x \in \operatorname{Ker} f$.
> ...
> Donc $x = e_G$, d'où $\operatorname{Ker} f = \{e_G\}$. »

2. Pour montrer que f est surjectif :

> « Soit $y \in H$.
> ...
> Donc il existe $x \in G$ tel que $f(x) = y$,
> d'où $H \subset \operatorname{Im} f$, puis $\operatorname{Im} f = H$. »

Remarque : Cette méthode sera d'un usage constant en algèbre linéaire, où la plupart des ensembles rencontrés sont des groupes et la plupart des applications des morphismes.

Attention toutefois : le théorème n'est valable que si les deux ensembles sont des **groupes** et l'application un **morphisme**. Pour une application quelconque, montrer que seul e_G s'envoie sur e_H ne prouve rien.

Exemple : Déterminons le noyau des morphismes rencontrés plus haut.

- Pour $\varphi : x \mapsto \mathrm{e}^x$ de $(\mathbb{R}\,;+)$ dans $(\mathbb{R}_+^*\,;\times)$, le neutre d'arrivée est 1, et $\mathrm{e}^x = 1$ équivaut à $x = 0$. Donc $\operatorname{Ker}\varphi = \{0\}$: le morphisme est injectif, ce que confirme la stricte croissance de l'exponentielle.
- Pour le module $z \mapsto |z|$ de $(\mathbb{C}^*\,;\times)$ dans $(\mathbb{R}_+^*\,;\times)$, le noyau est l'ensemble des complexes de module 1 :

$$\operatorname{Ker} f = \mathbb{U}$$

Le morphisme n'est donc pas injectif, et l'on retrouve au passage que $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$ — conséquence immédiate de la proposition 3, alors qu'il fallait le vérifier à la main au chapitre 3.

- Pour $k \mapsto nk$ de $(\mathbb{Z}\,;+)$ dans lui-même avec $n \geqslant 1$, le noyau est $\{0\}$ et l'image est $n\mathbb{Z}$. Le morphisme est injectif, et surjectif si et seulement si $n = 1$.

Remarque : Ce dernier exemple mérite qu'on s'y arrête : il fournit un isomorphisme entre $(\mathbb{Z}\,;+)$ et $(n\mathbb{Z}\,;+)$, alors même que $n\mathbb{Z}$ est une partie *stricte* de $\mathbb{Z}$. Un groupe infini peut donc être isomorphe à l'un de ses sous-groupes propres, situation impossible en dimension finie.