Groupes, anneaux, corps

I – Notion de loi de composition interne

Dans toute cette partie, E désigne un ensemble non vide quelconque.

1) Définitions

Définition 1 On appelle *loi de composition interne* (en abrégé LCI) sur E toute application :

$$\star : E \times E \longrightarrow E$$

On dit alors que le couple $(E, \star)$ est un *magma*.

Notation : si $(x, y) \in E^2$, l'image $\star\big((x, y)\big)$ sera notée $x \star y$.

Exemple 1 Les applications suivantes sont des lois de composition interne.

- $\star$ dans $\mathbb{N}$:
$$+ : \left\{ \begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ (m, n) & \longmapsto & m + n \end{array} \right. \qquad \text{(addition des entiers naturels)}$$
- $\star$ la soustraction dans $\mathbb{Z}$
- $\star$ dans $\mathbb{R}^{\mathbb{R}}$:
$$\circ : \left\{ \begin{array}{ccc} \mathbb{R}^{\mathbb{R}} \times \mathbb{R}^{\mathbb{R}} & \longrightarrow & \mathbb{R}^{\mathbb{R}} \\ (f, g) & \longmapsto & f \circ f \end{array} \right. \qquad \text{(composition des applications)}$$
- $\star$ dans $\mathscr{P}(E)$, la réunion ou l'intersection

Il est facile de construire des applications qui ne sont pas des lois de compositions internes, comme par exemple : $\left\{ \begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{C} \\ (a, b) & \longmapsto & a + ib \end{array} \right.$ (où i est le nombre complexe tel que $i^2 = -1$)

Définition 2 (partie stable par une loi de composition interne) Soit $\star$ une loi de composition interne sur E. Une partie A de E est dite *stable* par la loi $\star$ si :

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

Exemple 2

1. L'addition et la multiplication sont des lois de compositions internes dans $\mathbb{Z}$ et l'ensemble des entiers naturels $\mathbb{N}$ est une partie stable pour ces deux opérations.
2. Par contre, si $\mathbb{Z}$ est muni de la différence des entiers, alors $\mathbb{N}$ n'est pas stable (puisque, par exemple, $(1, 2) \in \mathbb{N}^2$ mais $-1 = 1 - 2 \notin \mathbb{N}$).

2) Propriétés remarquables d'une loi de composition interne

Nous listons ici les propriétés intéressantes que « doit » vérifier une loi de composition interne pour que l'ensemble E, muni de cette loi, soit suffisamment « intéressant ».

On suppose ici que $(E, \star)$ est un magma.

(a) Associativité

Définition 3 On dit que $\star$ est *associative* si :

$$\forall (x, y, z) \in E^3, \qquad (x \star y) \star z = x \star (y \star z)$$

Exemple 3

- ⋆ Dans $\mathbb{Z}$, les addition $+$ et multiplication $\times$ sont des LCI associatives. On peut en effet écrire que :

$$\forall m, n, p \in \mathbb{Z}, \qquad (m+n)+p = m+(n+p) \qquad \text{et} \qquad (mn)p = m(np)$$

  On écrit même ces quantités « $m+n+p$ » et « mnp » sans se soucier guère du parenthésage.
- ⋆ Dans $\mathbb{R}^{\mathbb{R}}$, la LCI $\circ$ est associative :

$$\forall f, g, h \in \mathbb{R}^{\mathbb{R}}, \qquad (f \circ g) \circ h = f \circ (g \circ h)$$

- ⋆ Dans $\mathscr{P}(E)$, on sait que l'intersection et la réunion sont associatives.
- ⋆ Dans $\mathbb{Z}$, la différence des entiers « $-$ » est une loi de composition interne qui n'est pas associative. Par exemple, 1, 2 et 3 sont des entiers relatifs et :

$$(1-2)-3 = -4 \qquad \text{tandis que} \qquad 1-(2-3) = 2$$

- ⋆ De même, la division (qui est une LCI dans $\mathbb{R}^*$) n'est pas associative.

Remarque : si $\star$ est associative dans E, on peut écrire $x \star y \star z$ sans ambiguïté.

(b) Élément neutre

Définition 4 (élément neutre) Soit $e \in E$. On dit que e est un élément neutre pour $\star$ si :

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

Exemple 4

- ⋆ Dans les sous-ensembles de $\mathbb{C}$ usuels ($\mathbb{N}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}$,...), 1 est un élément neutre pour la multiplication et 0 est le neutre pour l'addition.
- ⋆ Dans $\mathbb{R}^{\mathbb{R}}$, l'application $\mathrm{Id}_{\mathbb{R}}$ est un élément neutre pour la composition.
- ⋆ Dans $\mathscr{P}(E)$, l'ensemble vide $\varnothing$ est un élément neutre pour l'intersection, tandis que E est un élément neutre pour la réunion.
- ⋆ Dans $\mathbb{Z}$, la soustraction n'admet pas d'élément neutre (s'il en existe un, celui-ci vaut 0, ce qui n'est pas possible).

Proposition 1 (unicité du neutre) Si un magma $(E, \star)$ admet un élément neutre, alors il est unique.

Démonstration Soient $e, e' \in E$ des éléments neutres de $(E, \star)$. Montrons que $e = e'$.

- ⋆ Comme e est élément neutre pour $\star$, on a $e \star e' = e'$.
- ⋆ Comme e' est élément neutre pour $\star$, on a $e \star e' = e$.

Donc $e = e'$. ■

(c) Élément inversible

Définition 5 (élément inversible) On suppose que $(E, \star)$ admet $e \in E$ pour élément neutre. Un élément x de E est dit *inversible* si :

$$\exists\, y \in E, \qquad x \star y = y \star x = e$$

Exemple 5

- ⋆ Dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ munis de l'addition, tout élément x est inversible, son inverse étant $-x$.
- ⋆ Tout élément x de $(\mathbb{R}^*, \times)$ est inversible d'inverse $\dfrac{1}{x}$.
- ⋆ Dans $\mathbb{N}$ muni de l'addition, le seul élément inversible est 0 (d'inverse 0).
- ⋆ Dans $\mathbb{R}^{\mathbb{R}}$ muni de la composition, les éléments inversibles sont les applications bijectives.
- ⋆ Dans $\mathscr{P}(E)$ muni de la réunion, le seul élément inversible est $\varnothing$.
- ⋆ Dans $\mathscr{P}(E)$ muni de l'intersection, le seul élément inversible est E.

Proposition 2 (propriétés de l'inverse) Soit $(E, \star)$ un magma associatif d'élément neutre e.

- ⋆ Il y a unicité de l'inverse lorsqu'il existe.
  Si $x \in E$ est inversible, on notera x^{-1} son inverse.
- ⋆ Si $x \in E$ est inversible pour $\star$, alors x^{-1} est inversible d'inverse :

$$(x^{-1})^{-1} = x$$

- ⋆ Soit $x \in E$ un élément inversible. Pour tout $(y, z) \in E^2$, on a :

$$x \star y = x \star z \Longrightarrow y = z$$

  et :

$$y \star x = z \star x \Longrightarrow y = z$$

- ⋆ Si x et y sont deux éléments inversibles dans E, alors $x \star y$ est un élément inversible d'inverse :

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

Démonstration

⋆ Soit $x \in E$ un élément inversible. Supposons que $y, z \in E$ soient tels que :

$$x \star y = y \star x = e \qquad \text{et} \qquad x \star z = z \star x = e$$

Montrons que $y = z$. Par associativité de $\star$, on a :

$$(z \star x) \star y = z \star (x \star y) \qquad e \star y = z \star e$$

ce qui donne (puisque e est élément neutre pour $\star$) l'égalité $y = z$.

⋆ Si x est inversible d'inverse x^{-1}, alors :

$$x \star x^{-1} = x^{-1} \star x = e$$

Par définition de l'inversibilité, x^{-1} est inversible et on a $(x^{-1})^{-1} = x$ (par unicité de l'inverse).

⋆ Soient $y, z \in E$ tel que $x \star y = x \star z$. Comme x est inversible, on a :

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

et donc, par associativité de $\star$:

$$(x^{-1} \star x) \star y = (x^{-1} \star x) \star z \qquad \text{c'est-à-dire} \qquad e \star y = e \star z$$

Comme e est élément neutre pour $\star$, on obtient $y = z$. La deuxième propriété se démontre de la même manière.

⋆ Soient x et y deux éléments inversibles de E. On a :

$$\begin{aligned}(y^{-1} \star x^{-1}) \star (x \star y) &= y^{-1} \star (x^{-1} \star x) \star y \qquad \text{(par associativité de } \star) \\ &= y^{-1} \star e \star y \\ &= y^{-1} \star y \\ &= e\end{aligned}$$

ce qui démontre que $x \star y$ est inversible d'inverse $y^{-1} \star x^{-1}$. ■

Remarque : si la loi du groupe est additive, on notera bien entendu l'inverse « $-x$ ». Par exemple, dans $(\mathbb{Z}, +)$, l'entier 2 est inversible et son inverse est -2.

(d) Commutativité

Définition 6 La LCI $\star$ est dite commutative dans E si :

$$\forall x, y \in E, \qquad x \star y = y \star x$$

Exemple 6

1. La multiplication et l'addition dans $\mathbb{C}$ ($\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$) sont commutatives.
2. L'intersection et la réunion sont commutatives dans $\mathscr{P}(E)$.
3. Dans $\mathbb{R}^{\mathbb{R}}$, on sait que la composition n'est pas commutative.

Remarque : lorsque $\star$ est commutative, certaines des propriétés précédentes de $\star$ peuvent être simplifiées :

⋆ $e \in E$ est élément neutre si : $\forall x \in E,\ x \star e = x$;

⋆ un élément x de E est inversible s'il existe $y \in E$ tel que $x \star y = e$.

(e) Distributivité d'une loi par rapport à une autre

Définition 7 (distributivité) Soit Δ une (autre) loi de composition interne sur E. On dit que $\star$ est *distributive par rapport à* Δ si on a :

$$\forall x, y, z \in E, \qquad x \star (y \Delta z) = (x \star y) \Delta (x \star z) \qquad \text{et} \qquad (y \Delta z) \star x = (y \star x) \Delta (z \star x)$$

Exemple 7

1. La multiplication est distributive par rapport à l'addition dans $\mathbb{C}$:

$$\forall x, y, z \in \mathbb{C}, \qquad x(y + z) = xy + xz$$

2. L'intersection (respectivement l'intersection) est distributive par rapport à la réunion (respectivement la réunion) dans $\mathscr{P}(E)$.

II – Structure de groupe

Soit G un ensemble non vide.

1) Définition et exemples

Définition 8 (groupe) Soit $(G, \star)$ un magma. On dit que $(G, \star)$ est un *groupe* si :

(G_1) la loi $\star$ est associative ;

(G_2) la loi $\star$ admet un élément neutre (noté e_G) ;

(G_3) tous les éléments de G sont inversibles pour $\star$.

Si de plus la loi $\star$ est commutative, on parle de groupe *commutatif* (ou de groupe *abélien*).

Quelques exemples usuels

- ⋆ Si $(E, \star)$ est un magma admettant un élément neutre e, alors $(\{e\}, \star)$ est un groupe, appelé *groupe trivial*.
- ⋆ Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des groupes abéliens dits *additifs* (c'est-à-dire sont des groupes lorsqu'ils sont munis de l'addition).
- ⋆ Le couple $(\mathbb{N}, +)$ n'est pas un groupe ((G_3) n'étant pas vérifiée).
- ⋆ $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$ sont des groupes abéliens dits *multiplicatifs*.
- ⋆ **Rappels :**
  - — l'ensemble des nombres complexes de module 1 est :

$$\mathbb{U} = \left\{ z \in \mathbb{C} \,\middle|\, |z| = 1 \right\} = \left\{ \mathrm{e}^{i\theta} \,\middle|\, \theta \in \mathbb{R} \right\}$$

  - — pour tout $n \in \mathbb{N}^*$, l'ensemble des racines $n^{\text{ème}}$ de l'unité est :

$$\mathbb{U}_n = \left\{ z \in \mathbb{C} \,\middle|\, z^n = 1 \right\} = \left\{ \mathrm{e}^{i\frac{2k\pi}{n}} \,\middle|\, k \in [\![0, n-1]\!] \right\} \subset \mathbb{U}$$

    Alors $\mathbb{U}$ est un groupe abélien, de même que $\mathbb{U}_n$ pour tout $n \in \mathbb{N}^*$ (ces derniers étant de cardinaux finis).
- ⋆ Si E est un ensemble non vide, l'ensemble des bijections de E dans E, noté S_E, est un groupe muni de la composition (que l'on appelle *groupe symétrique de* E). L'élément neutre est Id_E.

2) Puissances dans un groupe

Lorsque la loi $\star$ est clairement identifiée (notamment quand on travaille dans un groupe multiplicatif ou additif), on peut s'affranchir de la notation « $x \star y$ » en écrivant simplement « xy ». C'est ce qu'on fait usuellement dans le groupe $(\mathbb{R}^*, \times)$ par exemple.

Définition 9 (itérés ou puissances d'un élément d'un groupe) Soit G un groupe d'élément neutre e et soit $x \in G$. Pour tout entier relatif n, on définit la puissance $n^{\text{ème}}$ de x par récurrence de la manière suivante :

- ⋆ $x^0 = e$;
- ⋆ si $n \in \mathbb{N}$, $x^{n+1} = x^n x$;
- ⋆ si $n < 0$, $x^n = (x^{-1})^{-n}$.

Exemple 8

1. Dans le groupe $(\mathbb{C}^*, \times)$, les puissances d'un élément correspond à la propriété d'exponentiation usuelle.
2. Dans le groupe additif $(\mathbb{C}, +)$, les puissances de $x \in \mathbb{C}$ correspondent en fait à :
   - — $\forall n \in \mathbb{N}^*,\ nx = x + \cdots + x$ (n fois) ;
   - — $\forall n \in \mathbb{Z} \setminus \mathbb{N},\ nx = -(-n)x$

Autrement dit, les puissances *additives* correspondent aux multiples.

3. Dans S_E, la puissance n^{e} (avec $n \in \mathbb{N}^*$) de $\sigma \in S_E$ est définie par :

$$\sigma^n = \sigma \circ \cdots \circ \sigma \qquad (n \text{ fois})$$

Par exemple, $f : x \longmapsto 2x$ est un élément de $S_{\mathbb{R}}$ et :

$$\forall n \in \mathbb{Z}, \qquad f^n : x \longmapsto 2^n x$$

Proposition 3 Soit G un groupe.

⋆ Soit $x \in G$. Alors :

$$\forall (m,n) \in \mathbb{Z}^2, \qquad x^{m+n} = x^n x^m = x^m x^n$$

⋆ Soient x et y deux éléments de G qui commutent (c'est-à-dire tels que $xy = yx$). Alors :

$$\forall (m,n) \in \mathbb{Z}^2, \qquad x^n y^m = y^m x^n$$

et :

$$\forall n \in \mathbb{Z}, \qquad (xy)^n = x^n y^n = y^n x^n$$

Démonstration Il suffit de procéder par récurrence en distinguant les cas d'exposants positifs et négatifs. ■

Remarque : en notation additive, on obtient par exemple pour la première propriété :

$$\forall x \in G,\ \forall (m,n) \in \mathbb{Z}^2, \qquad (m+n)x = mx + nx$$

3) Groupe produit

Soient $n \in \mathbb{N}^*$ et $(G_1, \star_1), \ldots, (G_n, \star_n)$ des groupes. On définit une loi de composition interne $\star$ sur le produit $G = G_1 \times \cdots \times G_n$ en posant, pour tous $(g_1, \ldots, g_n), (h_1, \ldots, h_n) \in G$:

$$(g_1, \ldots, g_n) \star (h_1, \ldots, h_n) = (g_1 \star_1 h_1, \ldots, g_n \star_n h_n)$$

Proposition 4 Le magma $(G, \star)$ est un groupe d'élément neutre $(e_{G_1}, \ldots, e_{G_n})$. Il est abélien si tous les groupes sous-jacents le sont. On l'appelle le groupe produit de $G_1, \ldots, G_n$.

Démonstration On se place dans le cas $n = 2$, le cas général étant similaire.

⋆ Tout d'abord, il est clair que $\star$ est une loi de composition interne dans G.

⋆ L'associativité de $\star_1$ et $\star_2$ implique l'associativité de $\star$ dans G.

⋆ En notant e_1 et e_2 les éléments neutres de G_1 et G_2 respectivement, il est facile de vérifier que $e = (e_1, e_2) \in G$ est élément neutre dans G.

⋆ Enfin, pour tout $g = (g_1, g_2) \in G$, il est facile de voir que g est inversible dans G d'inverse $g^{-1} = (g_1^{-1}, g_2^{-1}) \in G$.

■

Exemple 9 ⋆ On sait que $(\mathbb{R}, +)$ est un groupe abélien donc, pour tout $n \in \mathbb{N}^*$, le couple $(\mathbb{R}^n, +)$ est un groupe où l'addition $+$ est ici défini par :

$$\forall (x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{R}^n, \qquad x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

L'élément neutre est $(0, \ldots, 0)$.

⋆ On sait que $(\mathbb{R}, +)$ et $(\mathbb{U}, \times)$ sont des groupes. Donc $\mathbb{R} \times \mathbb{U}$ est un groupe dont la loi $\star$ est définie par :

$$\forall (x,u), (y,v) \in \mathbb{R} \times \mathbb{U}, \qquad (x,u) \star (y,v) = (x+y, uv)$$

L'élément neutre est $(0, 1)$.

4) Notion de sous-groupe

Définition 10 Soient $(G, \star)$ un groupe et H un sous-ensemble non vide de G. On dit que H est un sous-groupe de G (pour la loi $\star$) si :

$(SG)_1$ $\forall h, k \in H,\ h \star k \in H$ (on dit que H est stable pour la loi $\star$) ;

$(SG)_2$ $\forall h \in H,\ h^{-1} \in H$.

Exemple 10 ⋆ $(\mathbb{R}, +)$ est un sous-groupe de $(\mathbb{C}, +)$;

⋆ $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

Remarque : si H est une partie non vide de G, alors :

$$H \text{ est un sous-groupe de } G \iff \forall h, k \in H,\ h \star k^{-1} \in H$$

L'intérêt de cette définition réside dans la proposition suivante.

Proposition 5 Soient $(G, \star)$ un groupe et H un sous-groupe de G. Alors $(H, \star)$ est un groupe.

Démonstration ⋆ D'après $(SG)_1$, $(H, \star)$ est un magma.

⋆ Comme $H \neq \varnothing$, on peut considérer un élément h de H. Alors $h^{-1} \in H$ d'après $(SG)_2$ et donc $e_G = h \star h^{-1} \in H$ d'après $(SG)_1$.

⋆ La loi $\star$ étant associative dans G, elle l'est aussi dans tout sous-ensemble de G, donc en particulier dans H.

⋆ Tous les éléments de H sont inversibles pour $\star$ (puisque $(G, \star)$ est un groupe et les inverses appartiennent à H d'après $(SG)_2$.

Donc $(H, \star)$ est un groupe. ■

Ainsi, pour montrer qu'un ensemble muni d'une loi est un groupe, il suffit de montrer qu'il s'agit d'un sous-groupe d'un groupe connu.

Exemple 11 Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z} = \left\{nk \,\middle|\, k \in \mathbb{Z}\right\}$ est un groupe en tant que sous-groupe de $(\mathbb{Z}, +)$.

Proposition 6 Soit $(G, \star)$ un groupe et H, K deux sous-groupes de G. Alors $H \cap K$ est un sous-groupe de G.

Démonstration On utilise la proposition précédente. Notons e l'élément neutre de G.

⋆ Comme H et K sont des sous-groupes de G, on a $e \in H \cap K$. En particulier, $H \cap K \neq \varnothing$.

⋆ Soit $(x, y) \in (H \cap K)^2$. En particulier, $(x, y) \in H^2$ et H est un sous-groupe de G donc $xy^{-1} \in H$. De la même manière, $xy^{-1} \in K$. On a donc $xy^{-1} \in H \cap K$.

Finalement, $H \cap K$ est un sous-groupe de G. ■

Remarque : la propriété est fausse pour la réunion. Par exemple, $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ mais $2\mathbb{Z} \cup 3\mathbb{Z}$ n'en est pas un. En effet, 2 et 3 appartiennent à cet ensemble mais $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ (puisque 5 n'est ni un multiple de 2, ni un multiple de 3).

III – Morphismes de groupes

Dans cette partie, $(G, \star)$ et (H, Δ) désignent deux groupes (de neutres notés e_G et e_H) et $f : G \longrightarrow H$ est une application.

Commençons par un exemple. Considérons l'application $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^*$. On sait que :

- ⋆ $(\mathbb{R}, +)$ est un groupe ;
- ⋆ $(\mathbb{R}_+^*, \times)$ est un groupe ;
- ⋆ $\forall x, y \in \mathbb{R},\ \exp(x + y) = \exp x \times \exp y$

Ainsi, la fonction exp préserve la structure des deux groupes $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$. On parle de *morphisme de groupes*.

1) Définition et premières propriétés

Définition 11 (morphisme de groupes) On dit que f est un *morphisme* de groupes de G vers H si :

$$\forall x, y \in G, \qquad f(x \star y) = f(x) \Delta f(y)$$

On dit que f est un *isomorphisme de groupes si f est bijectif.*

Exemple 12 Les applications suivantes sont des morphismes de groupes :

- ⋆ $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$ (isomorphisme) ;
- ⋆ $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$;
- ⋆ $\varphi : \left\{ \begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \theta & \longmapsto & \mathrm{e}^{i\theta} \end{array} \right.$
- ⋆ $f_n : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}, +) \\ k & \longmapsto & nk \end{array} \right.$ (où $n \in \mathbb{Z}^*$)
- ⋆ $\theta : \left\{ \begin{array}{ccc} G & \longrightarrow & H \\ g & \longmapsto & e_H \end{array} \right.$ est un morphisme de groupes (dit trivial)

Dans la suite de cette section, $f : G \longrightarrow H$ est un morphisme de groupes.

Proposition 7 On a :

(*i*) $f(e_G) = e_H$;

(*ii*) pour tout $x \in G$, on a $f(x^{-1}) = f(x)^{-1}$;

(*iii*) pour tout $(n, x) \in \mathbb{Z} \times G$, on a $f(x^n) = f(x)^n$.

Démonstration (*i*) On sait que $e_G \star e_G = e_G$ donc (comme f est un morphisme de groupes) :

$$f(e_G) = f(e_G \star e_G) = f(e_G) \Delta f(e_G)$$

En simplifiant par $f(e_G)$ dans le groupe H, on a bien $f(e_G) = e_H$.

(*ii*) Soit $x \in G$. Comme f est un morphisme de groupes, on a :

$$f(x^{-1}) \Delta f(x) = f(x^{-1} \star x) = f(e_G) = e_H$$

De la même manière, $f(x) \Delta f(x^{-1}) = e_H$. Donc, par unicité de l'inverse, $f(x^{-1}) = f(x)^{-1}$.

(*iii*) Soit $x \in \mathbb{N}$. On démontre par récurrence que, pour tout entier naturel n, on a $f(x^n) = f(x)^n$. Ensuite, si $n \in \mathbb{Z} \setminus \mathbb{N}$, on a :

$$\begin{aligned} f(x^n) = f\left((x^{-n})^{-1}\right) &= f(x^{-n})^{-1} && \text{(d'après } (ii)\text{)} \\ &= \left(f(x)^{-n}\right)^{-1} && \text{(d'après la récurrence précédente car } -n \geqslant 0\text{)} \\ &= f(x)^n \end{aligned}$$

■

Proposition 8 (image, image réciproque) (*i*) Si G' est un sous-groupe de G, alors $f(G')$ est un sous-groupe de H.

(*ii*) Si H' est un sous-groupe de H, alors $f^{-1}(H')$ est un sous-groupe de G.

Démonstration (*i*) Posons $\tilde{H} = f(G')$. On sait que $e_H = f(e_G)$ (puisque f est un morphisme de groupes). Comme $e_G \in G'$, on a bien $e_H \in \tilde{H}$. Soit maintenant $(h,k) \in \tilde{H}^2$. Par définition de $\tilde{H}$, il existe $(a,b) \in G'^2$ tel que $h = f(a)$ et $k = f(b)$. On a alors (par propriétés de morphismes) :

$$h\Delta k^{-1} = f(a)\Delta f(b)^{-1} = f(a)\Delta f(b^{-1}) = f(a \star b^{-1})$$

Comme G' est un groupe, on sait que $a \star b^{-1} \in G'$ et donc $h\Delta k^{-1} \in \tilde{H}$. Finalement, $\tilde{H} = f(G')$ est un sous-groupe de H.

(*ii*) Posons :

$$\tilde{G} = f^{-1}(H') = \left\{g \in G \,\middle|\, f(g) \in H'\right\}$$

Tout d'abord, e_G appartient à $\tilde{G}$. En effet, on a $f(e_G) = e_H$ (puisque f est un morphisme de groupes) et on sait que $e_H \in H'$ car H' est un sous-groupe de H. Soit maintenant $(g,h) \in \tilde{G}^2$ et montrons que $g \star h^{-1} \in \tilde{G}$. Pour cela, montrons que $f(g \star h^{-1}) \in H'$. On a (en utilisant les propriétés de morphismes de f) :

$$f(g \star h^{-1}) = f(g)\Delta f(h^{-1}) = f(g)\Delta f(h)^{-1} \in H'$$

car H' est un morphisme de groupes et car $(g,h) \in \tilde{G}^2$. Finalement, $\tilde{G} = f^{-1}(H')$ est un sous-groupe de G. ■

Exemple 13 Considérons le morphisme de groupes :

$$f : \left\{ \begin{array}{ccc} (\mathbb{Z},+) & \longmapsto & (\mathbb{Z},+) \\ n & \longmapsto & 2n \end{array} \right.$$

D'après la proposition précédente, $2\mathbb{Z} = f(\mathbb{Z})$ est un sous-groupe (pour $+$) de $\mathbb{Z}$ (ce que l'on savait déjà).

2) Noyau d'un morphisme de groupes

Le noyau est lié à l'injectivité.

Définition 12 (noyau) On appelle *noyau de* f, noté $\mathrm{Ker}(f)$, le sous-ensemble de G suivant :

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

Le noyau de f est donc l'ensemble des antécédents par f de e_H, c'est-à-dire $\mathrm{Ker}(f) = f^{-1}(\{e_H\})$. Par conséquent :

Proposition 9 Le noyau $\mathrm{Ker}(f)$ de f est un sous-groupe de G.

Démonstration C'est une application directe de la proposition 8 avec le groupe trivial $(\{e_H\}, \Delta)$. ■

L'importance majeure de l'étude du noyau réside dans le résultat suivant :

Théorème 1 Le morphisme de groupes $f : G \longrightarrow H$ est injectif si et seulement si $\mathrm{Ker}(f) = \{e_G\}$.

Démonstration On raisonne par double implication.

- ⋆ On suppose que $\mathrm{Ker}(f) = \{e_G\}$. Montrons que f est injectif. Soit $(x, y) \in G^2$ tel que $f(x) = f(y)$. Alors $f(xy^{-1}) = e_H$ et donc $xy^{-1} \in \mathrm{Ker}(f)$, d'où l'on déduit que $x = y$. Donc f est injectif.
- ⋆ Supposons que f est injectif. Soit $x \in G$. Alors :

$$\begin{aligned} x \in \mathrm{Ker}(f) &\iff f(x) = e_H \iff f(x) = f(e_G) \qquad \text{(car } f \text{ est un morphisme de groupes)} \\ &\iff x = e_G \end{aligned}$$

car f est injectif. Ainsi, $\mathrm{Ker}(f) = \{e_G\}$.

On obtient bien l'équivalence annoncée. ■

Exemple 14 ⋆ Pour tout $n \in \mathbb{Z}^*$, on a $\mathrm{Ker}(f_n) = \{0\}$ donc f_n est injectif.

⋆ On a $\mathrm{Ker}(\varphi) = 2\pi\mathbb{Z} \neq \{0\}$ donc φ n'est pas injectif.

3) Image d'un morphisme de groupes

L'image est liée à la surjectivité.

Définition 13 (image) Soit $f : G \longrightarrow H$ un morphisme de groupes. On appelle *image de* f, notée $\mathrm{Im}(f)$, le sous-ensemble de H suivant :

$$\begin{aligned} \mathrm{Im}(f) &= \left\{ h \in H \,\middle|\, \exists\, g \in G,\ h = f(g) \right\} \\ &= \left\{ f(g) \,\middle|\, g \in G \right\} \end{aligned}$$

Comme $\mathrm{Im}(f) = f(G)$, la proposition 8 nous permet d'obtenir le premier point du résultat suivant.

Proposition 10 ⋆ L'image $\mathrm{Im}(f)$ de f est un sous-groupe de H.

⋆ Le morphisme f est surjectif si et seulement si $\mathrm{Im}(f) = H$.

Démonstration Le deuxième point est évident. ■

Exemple 15 On reprend l'exemple précédent.

1. On a $\mathrm{Im}(f_n) = n\mathbb{Z} = \mathbb{Z}$ si et seulement si $n \in \{-1, 1\}$. Donc f_n est surjectif si et seulement si $n \in \{-1, 1\}$.
2. On a $\mathrm{Im}(\varphi) = \mathbb{U}$ donc φ est surjectif.

IV – Anneaux et corps

1) Structure d'anneau

Définition 14 (anneau) Soit A un ensemble non vide muni de deux LCI notées $+$ et $\times$. On dit que $(A, +, \times)$ est un *anneau* si :

(A_1) $(A, +)$ est un groupe abélien ;

(A_2) $\times$ est associative ;

(A_3) $\times$ est distributive par rapport à $+$;

(A_4) la loi $\times$ admet un élément neutre.

Si la loi $\times$ est de plus commutative, on dit que l'anneau est commutatif.

Notation : en général, le neutre pour $+$ est noté 0 (ou 0_A) et le neutre pour $\times$ est noté 1 (ou 1_A).

Remarque : si $(A, +, \times)$ est un anneau, alors :

$$\forall x \in A, \qquad 0 \times x = (0 + 0) \times x = 0 \times x + 0 \times x$$

car 0 est élément neutre pour $+$ puis par distributivité de $\times$ par rapport à $+$. Comme $0 \times x$ est inversible pour $+$, on a $0 \times x = 0$.

Exemple 16

- ⋆ Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux pour l'addition et la multiplication usuelles.
- ⋆ Si E est un ensemble et si A est un anneau, alors A^E est un anneau.
- ⋆ Le seul anneau dans lequel $0 = 1$ est l'anneau nul $\{0\}$ (il s'agit bien d'un anneau). En effet, si $0 = 1$, alors :

$$\forall x \in A, \qquad 0 \times x = 0 = 1 \times x = x$$

Définition 15 (éléments inversibles d'un anneaux) Soit $(A, +, \times)$ un anneau.

- ⋆ Un élément a de A est dit inversible si il l'est pour la loi $\times$ *i.e.* si :

$$\exists\, b \in A, \qquad a \times b = b \times a = 1$$

- ⋆ On note $A^\times$ l'ensemble des éléments inversibles de A.

✎✎✎ **Exercice 1** Soit $(A, +, \times)$ un anneau. Montrer que $A^\times$, muni de la multiplication, est un groupe.

Exemple 17

1. $\mathbb{Z}^\times = \{-1, 1\}$;
2. $\mathbb{C}^\times = \mathbb{C}^*$, $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$
3. $\mathscr{M}_n(\mathbb{K})^\times = \mathrm{GL}_n(\mathbb{K})$
4. anneau nul : $\{0\}^\times = \{0\}$ (dans un tel anneau, $1 = 0$).

Définition 16 (anneau intègre) Soit $(A, +, \times)$ un anneau. On dit que A est *intègre* si A est non nul (c'est-à-dire $A \neq \{0_A\}$) et si :

$$\forall a, b \in A, \qquad ab = 0_A \Longrightarrow a = 0_A \text{ ou } b = 0_A$$

Remarques :

- ⋆ En pratique, travailler dans un anneau intègre permet de résoudre des équations produit-nul.

⋆ Si A est un anneau intègre, alors :

$$\forall a, x, y \in A, \qquad ax = ay \Longrightarrow a = 0 \text{ ou } x = y$$

Exemple 18 ⋆ Les anneaux, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{K}[X]$ sont intègres.

⋆ L'anneau $\mathscr{M}_n(\mathbb{K})$ ne l'est pas si $n \geqslant 2$. En effet, on sait que le produit de deux matrices non nulles peut être nul. Par exemple :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

⋆ $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un anneau non intègre.

2) Structure de corps

Définition 17 (corps) Un anneau $(A, +, \times)$ est appelé *corps* si :

(C_1) A est commutatif (pour la loi $\times$) ;

(C_2) $A \neq \{0\}$;

(C_3) tous ses éléments non nuls sont inversibles pour la loi $\times$.

Exemple 19 Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, $\mathbb{Z}$ et $\mathbb{R}^{\mathbb{R}}$ n'en sont pas.

Remarques :

⋆ Si A est un corps, alors $A^{\times} = A \setminus \{0_A\}$.

⋆ Dans un corps, on peut additionner, soustraire, multiplier et diviser (sauf par 0). En particulier, tout corps est un anneau intègre. En effet, si $a, b \in A$ est tel que $ab = 0_A$ et si $a \neq 0$, alors a est inversible dans A (puisque A est un corps) et on a $b = 0$ après division par a.

3) Sous-anneau

Définition 18 (sous-anneau) Soient $(A, +, \times)$ un anneau et B une partie non vide de A. On dit que B est un sous-anneau de A (pour les lois $+$ et $\times$) si :

$$B \text{ est un sous-anneau de } A \iff \begin{cases} 1 \in B \\ \forall (x, y) \in B^2,\ x - y \in B \\ \forall (x, y) \in B^2,\ x \times y \in B^2 \end{cases}$$

L'intérêt de la notion est la même que pour les sous-groupes.

Proposition 11 Si B est un sous-anneau de $(A, +, \times)$, alors $(B, +, \times)$ est un anneau.

Démonstration analogue à celle pour les sous-groupes ■

Exemple 20 ⋆ $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, qui est lui-même un sous-anneau de $\mathbb{R}$, qui est lui-même un sous-anneau de $\mathbb{C}$;

⋆ $\mathbb{Z}[i] = \left\{a + ib \,\middle|\, (a,b) \in \mathbb{Z}^2\right\}$ (anneau des entiers de Gauss) est un sous-anneau de $\mathbb{C}$ (donc est un anneau).

Justification. On a tout d'abord $\mathbb{Z}[i] \subset \mathbb{C}$. Ensuite, $\mathbb{Z}[i]$ contient 1 car $1 = 1 + 0 \times i$ (et 1 et 0 sont des entiers). Enfin, pour tout $(x,y) \in \mathbb{Z}[i]^2$, il existe $(a,b,a',b') \in \mathbb{Z}^4$ tel que $x = a + ib$ et $y = a' + ib'$ et donc $x - x' \in \mathbb{Z}[i]$ et $xx' \in \mathbb{Z}[i]$ (calculs immédiats).

⋆ L'ensemble $\mathscr{C}(\mathbb{R},\mathbb{R})$ des fonctions continues sur $\mathbb{R}$ à valeurs réelles est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$ (donc est un anneau).

4) Identités remarquables

Soit $(A,+,\times)$ un anneau. On définit les puissances positives entières d'un élément $a \in A$ de la même manière que dans un groupe. On ne peut définir a^n pour $n \in \mathbb{Z} \setminus \mathbb{N}$ que si a est inversible (sous-entendu pour $\times$). De plus, si $(a,b) \in A^2$ est tel que $ab = ba$, alors :

$$\forall (m,n) \in \mathbb{N}^2, \qquad a^m b^n = b^n a^m \qquad \text{et} \qquad (ab)^n = a^n b^n = b^n a^n$$

On a les deux identités suivantes :

Proposition 12 (binôme de Newton et identité de Bernoulli) Soit $(A,+,\times)$ un anneau.

⋆ **Formule du binôme de Newton :** pour tout $(a,b) \in A^2$ tel que $ab = ba$ et pour tout entier naturel n, on a

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

⋆ **Identité de Bernoulli :** pour tout $(a,b) \in A^2$ tel que $ab = ba$ et pour tout entier naturel n non nul, on a

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

Démonstration ⋆ déjà fait

⋆ On a :

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} &= a\sum_{k=0}^{n-1} a^k b^{n-1-k} - b\sum_{k=0}^{n-1} a^k b^{n-1-k} \\ &= \sum_{k=0}^{n-1} a^{k+1} b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \qquad (\text{car } ab = ba) \\ &= \sum_{k=1}^{n} a^k b^{n-k} - \sum_{k=0}^{n} a^k b^{n-k} \\ &= b^n - a^n\end{aligned}$$

d'après la relation de Chasles. ■

Remarque : en choisissant $a = 1$ (et $b = a$), on obtient (puisque 1 et a commutent) :

$$\forall n \in \mathbb{N}^*, \qquad 1 - a^n = (1-a)\sum_{k=0}^{n-1} a^k$$

5) Morphisme d'anneaux

On introduit, comme pour les groupes, la notion de morphisme d'anneaux.

Définition 19 (morphisme d'anneaux) Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux (unitaires). Une application $\varphi : A \longrightarrow B$ est un morphisme d'anneaux si :

(M_1) pour tout $(a, b) \in A^2$, on a $\varphi(a +_A b) = \varphi(a) +_B \varphi(b)$;

(M_2) pour tout $(a, b) \in A^2$, on a $\varphi(a \times_A b) = \varphi(a) \times_B \varphi(b)$;

(M_3) $\varphi(1_A) = 1_B$.

On dit que φ est un isomorphisme d'anneaux si φ est de plus bijectif.

Remarques :

- ⋆ Si φ est un morphisme d'anneaux, alors φ est en particulier un morphisme de groupes de $(A, +_A)$ vers $(B, +_B)$.
- ⋆ En particulier, on a $\varphi(0_A) = \varphi(0_B)$ et, pour tout $a \in A$, on a $\varphi(-a) = -\varphi(a)$ (voir les propriétés des morphismes de groupes).

Exemple 21 Pour tout $n \in \mathbb{Z}$, l'application $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ k & \longmapsto & nk \end{array} \right.$ est un morphisme d'anneaux.

On introduit les notions de noyau et d'image de morphismes d'anneaux qui permettent d'étudier respectivement les caractères injectif et surjectif du morphisme.

Définition 20 (image, noyau) Soit $f : A \longrightarrow B$ un morphisme d'anneaux.

- ⋆ On appelle noyau de f, noté $\mathrm{Ker}(f)$, le sous-ensemble de A suivant :

$$\mathrm{Ker}(f) = \big\{ a \in A \,\big|\, f(a) = 0_A \big\}$$

- ⋆ On appelle image de f, notée $\mathrm{Im}(f)$, le sous-ensemble de B suivant :

$$\mathrm{Im}(f) = \big\{ b \in B \,\big|\, \exists\, a \in A,\ b = f(a) \big\}$$

À nouveau :

$$f \text{ est injectif } \iff \mathrm{Ker}(f) = \{0_A\}$$

et :

$$f \text{ est surjectif } \iff \mathrm{Im}(f) = B$$