Loi de composition-groupes

Les opérations naturelles sur les nombres, addition, multiplication, dont découlent soustraction et multiplication, ont fait apparaître des propriétés qui vont conduire aux concepts de loi de composition interne et de structures tels que groupes, anneaux, idéaux et corps.

I Loi de composition interne

Etant donné un ensemble $\mathbb{E}$, une loi de composition interne sur $\mathbb{E}$ est une application f de $\mathbb{E} \times \mathbb{E}$ dans $\mathbb{E}$.

Exemples :

1) L'addition sur les entiers naturels est une loi de composition interne sur $\mathbb{N}$:

$$f : \begin{matrix} \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ (n, m) \to n + m \end{matrix}$$

2) La multiplication les entiers relatifs est une loi de composition interne sur $\mathbb{Z}$:

$$f : \begin{matrix} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ (n, m) \to n \times m \end{matrix}$$

3) L'application suivante est une loi de composition interne sur $\mathbb{R}^2$

$$f : \begin{matrix} \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2 \\ \big((x, y)\,;(x', y')\big) \to (x\,x' - \,y\,y', x\,y' + \,y\,x') \end{matrix}$$

C'est d'ailleurs le produit sur les nombres complexes comme nous l'abordons sur le fichier consacré à la construction des nombres complexes.

Attention : La division sur les nombres réels ne définit pas une loi de composition interne sur $\mathbb{R}$ car le couple (1,0) n'a pas d'image, mais la soustraction oui.

II Groupe

Afin d'étendre les propriétés des lois internes d'addition et de multiplication sur les nombres à des objets plus vastes, on qualifie de **groupe**, tout ensemble $\mathbb{E}$ muni d'une loi interne f, dont

nous noterons l'image d'un couple d'éléments de $\mathbb{E}$ sous la forme $f(x,y) = x \perp y$ (prononcer x truc y) possédant les trois propriétés suivantes. :

1) <u>La loi ⊥ est associative</u> :

$$\forall\, (\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}) \in \mathbb{E}^{\boldsymbol{3}} :\quad (\boldsymbol{x} \perp \boldsymbol{y}) \perp \boldsymbol{z} = \boldsymbol{x} \perp (\boldsymbol{y} \perp \boldsymbol{z})$$

2) <u>Il existe un élément neutre pour la loi ⊥</u>

$$\exists\, \boldsymbol{e} \in \mathbb{E} : \forall\, \boldsymbol{x} \in \mathbb{E} :\quad \boldsymbol{x} \perp \boldsymbol{e} = \boldsymbol{e} \perp \boldsymbol{x} = \boldsymbol{x}$$

3) <u>Tout élément possède un symétrique pour la loi ⊥</u>

$$\forall\, \boldsymbol{x} \in \mathbb{E} :\ \exists\, \boldsymbol{y} \in \mathbb{E}\ \ \boldsymbol{x} \perp \boldsymbol{y} = \boldsymbol{y} \perp \boldsymbol{x} = \boldsymbol{e}$$

Le groupe est dit commutatif ou abélien si, en plus, la loi est commutative :

$$(\boldsymbol{x},\boldsymbol{y}) \in \mathbb{E}^{\boldsymbol{2}} :\quad \boldsymbol{x} \perp \boldsymbol{y} = \boldsymbol{y} \perp \boldsymbol{x}$$

<u>Propriétés et notations</u>

<u>Propriété 1</u>

Un élément x d'un groupe admet un unique symétrique que nous noterons x^{-1} (notation d'inverse) sauf lorsque la loi est notée $+$ auquel cas nous le noterons sous forme d'opposé $(-x)$

Notons que l'on a alors :

$$\forall\, \boldsymbol{x} \in \mathbb{E}\ :\left(\boldsymbol{x}^{-\boldsymbol{1}}\right)^{-\boldsymbol{1}} = \boldsymbol{x}$$

<u>Preuve de l'unicité du symétrique</u> :

Soit (y,z) un couple de symétriques d'un élément x quelconque, alors :

$$x \perp y = e$$

En composant à gauche avec z :

$$z \perp (x \perp y) = z \perp e$$

En appliquant l'associativité :

$$(z \perp x) \perp y = z$$

D'où :

$$e \perp y = z$$

Finalement :

$$y = z$$

Propriété 2

Soit $(\mathbb{E}, \perp)$ un groupe d'élément neutre e, alors on note :

$$\boldsymbol{x^0 = e}$$

Et pour tout entier naturel n :

$$\boldsymbol{x^n = x \perp x \perp \cdots \perp x}$$

$$\boldsymbol{\left(x^{-1}\right)^n = x^{-1} \perp x^{-1} \perp \cdots \perp x^{-1}}$$

Où x apparaît n fois

On a alors :

$$\forall \mathbf{x} \in \mathbb{F} : \boldsymbol{\left(x^{-1}\right)^n = (x^n)^{-1}} \quad \textbf{qui sera noté} \quad \boldsymbol{x^{-n}}$$

$$\boldsymbol{\left(x^{-1}\right)^{-n} = x^n}$$

Preuve

Par récurrence sur $n \in \mathbb{N}$ en notant $P(n)$ la première des propriétés précédentes.

Initialisation : pour $n = 0$

$$(x^{-1})^0 = e$$

$$(x^0)^{-1} = e^{-1} = e$$

Donc $P(0)$ est vraie

Hérédité :

Soit $n \in \mathbb{N}$ tel que $P(n)$ soit vraie. Alors :

$$(x^{-1})^{n+1} \perp x^{n+1} = ((x^{-1})^n \perp x^{-1}) \perp (x \perp x^n)$$

$$= (x^{-1})^n \perp (x^{-1} \perp x) \perp x^n$$

$$= (x^n)^{-1} \perp e \perp x^n$$

$$= (x^n)^{-1} \perp x^n = e$$

En remplaçant dans cette relation x par x^{-1} :

$$x^{n+1} \perp (x^{-1})^{n+1} = e$$

On en déduit :

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

Donc $P(n+1)$ est vraie

Conclusion :

$P(n)$ est vraie pour tout $n \in \mathbb{N}$

Exemples de groupes commuatifs :

$(\mathbb{Z},+)$ est un groupe commutatif mais pas $(\mathbb{N},+)$ car 1 n'a pas de symétrique dans $\mathbb{N}$ mais dans $\mathbb{Z}$, le symétrique étant par ailleurs l'opposé.

L'ensemble des rotations du plan de centre l'origine d'un repère de ce plan forme un groupe commutatif pour la composition des rotations.

$(\mathbb{Q}^*,\times)$ est un groupe commutatif où le symétrique d'un nombre est son inverse.

Exemple de groupe non commuatif

Définissons sur un ensemble $\mathbb{E}$ formé de tableaux de nombres réels à deux lignes et deux colonnes appelés matrices 2 x 2 , la loi interne suivante, qualifiée de produit matriciel :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} a\,a' + c\,b' & a\,c' + c\,d' \\ b\,a' + d\,b' & b\,c' + d\,d' \end{pmatrix}$$

On note alors d'une part :

$$\left[\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}\right] * \begin{pmatrix} a" & c" \\ b" & d" \end{pmatrix} = \begin{pmatrix} a\,a' + c\,b' & a\,c' + c\,d' \\ b\,a' + d\,b' & b\,c' + d\,d' \end{pmatrix} * \begin{pmatrix} a" & c" \\ b" & d" \end{pmatrix}$$

$$= \begin{pmatrix} a\,a'a" + c\,b'a" + a\,c'b" + c\,d'b" & a\,a'c" + c\,b'c" + a\,c'd" + c\,d'd" \\ b\,a'a" + d\,b'a" + b\,c'b" + d\,d'b" & b\,a'c" + d\,b'c" + b\,c'd" + d\,d'd" \end{pmatrix}$$

D'autre part :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \left[\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} * \begin{pmatrix} a" & c" \\ b" & d" \end{pmatrix}\right] = \begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} a'\,a" + c'\,b" & a'\,c" + c'\,d" \\ b'\,a" + d'\,b" & b'\,c" + d'\,d" \end{pmatrix}$$

$$= \begin{pmatrix} a\,a'a" + a\,c'b" + c\,b'a" + c\,d'b" & a\,a'c" + a\,c'd" + c\,b'c" + c\,d'd" \\ b\,a'a + b\,c'\,b" + d\,b'a" + d\,d'b" & b\,a'c" + b\,c'd" + d\,b'c" + d\,d'd" \end{pmatrix}$$

On constate donc :

$$\left[\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}\right] * \begin{pmatrix} a" & c" \\ b" & d" \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} * \left[\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} * \begin{pmatrix} a" & c" \\ b" & d" \end{pmatrix}\right]$$

La loi est donc associative.

En revanche, elle n'est pas commutative comme le montre l'exemple simple :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

Notons alors qu'il y a un élément neutre :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Et que :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} * \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a\,d - b\,c & 0 \\ 0 & a\,d - b\,c \end{pmatrix}$$

Autrement dit, si on se restreint aux seules matrices 2 x2 telles que $a\,d - b\,c \neq 0$ (cette quantité est appelée déterminant de la matrice) alors, toute matrice possède un symétrique pour la loi * car :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} * \begin{pmatrix} \frac{d}{a\,d - b\,c} & -\frac{c}{a\,d - b\,c} \\ -\frac{b}{a\,d - b\,c} & \frac{a}{a\,d - b\,c} \end{pmatrix} = \begin{pmatrix} \frac{d}{a\,d - b\,c} & -\frac{c}{a\,d - b\,c} \\ -\frac{b}{a\,d - b\,c} & \frac{a}{a\,d - b\,c} \end{pmatrix} * \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

L'ensemble des matrices 2 x2, muni de la loi interne précédente, a donc une structure de groupe non commutatif

III Sous-groupe d'un groupe

Etant donné un groupe $(\mathbb{E}, \perp)$ et $\mathbb{F}$ un sous-ensemble non vide de $\mathbb{E}$, alors l'application f que représente la loi $\perp$ sur $\mathbb{E} \times \mathbb{E}$ définit par sa restriction à $\mathbb{F} \times \mathbb{F}$ une application qui n'est pas nécessairement interne sur $\mathbb{F}$. Il faut pour cela que l'addition reste stable. On a alors :

$$(\mathbb{F}, \perp)\ \textbf{groupe} \Leftrightarrow\ \forall\,(\mathbf{x}, \mathbf{y}) \in \mathbb{F}^{\mathbf{2}} : \boldsymbol{x} \perp \boldsymbol{y}\ \in \mathbb{F}\ \ \textbf{et}\ \ \forall\,\mathbf{x} \in \mathbb{F} : \boldsymbol{x}^{-\mathbf{1}}\ \in \mathbb{F}$$

$$\Leftrightarrow\ \forall\,(\mathbf{x}, \mathbf{y}) \in \mathbb{F}^{\mathbf{2}} : \boldsymbol{x} \perp \boldsymbol{y}^{-\mathbf{1}}\ \in \mathbb{F}$$

$(\mathbb{F}, \perp)$ vérifiant une des propriétés équivalentes ci-dessus est qualifié de sous-groupe de $(\mathbb{E}, \perp)$

Preuve

Il suffit de montrer la première équivalence, la seconde étant une forme contractée de la première.

$\left(\Rightarrow\right)$ Si $(\mathbb{F}, \perp)$ est un groupe alors nécessairement la loi interne $\perp$ est stable sur $\mathbb{F}$

Le symétrique de tout élément x de $\mathbb{F}$ pour la loi $\perp$ sur $\mathbb{E}$ est également le symétrque pour la loi $\perp$ restreinte à $\mathbb{F}$

$\left(\Leftarrow\right)$ L'associativité de $\perp$ sur $\mathbb{E}$ induit celle de $\perp$ sur $\mathbb{F}$

Notons *e* l'élément neutre de $\mathbb{E}$ pour la loi $\perp$

Soit $x \in \mathbb{F}$ alors $x^{-1} \in \mathbb{F}$ donc $x \perp x^{-1} = e \ \in \mathbb{F}$

e est donc élément neutre de $\mathbb{F}$pour la loi restreinte

$(\mathbb{F}, \perp)$ est un donc un groupe

IV Propriétés des sous-groupes d'un groupe

1) Intersection de sous-groupes

Etant donné deux sous-groupes $(\mathbb{F}, \perp)$ **et** $(\mathbb{F}', \perp)$ **d'un même groupe** $(\mathbb{E}, \perp)$ **alors** $(\mathbb{F} \cap \mathbb{F}', \perp)$ **est un sous-groupe de** $(\mathbb{E}, \perp)$

Plus généralement, l'intersection d'une famille quelconque (finie ou non) de sous-groupes est un sous-groupe

2) Sous-groupe engendré par un élément

Etant donné un groupe $(\mathbb{E}, \perp)$ **et** $\boldsymbol{a}$ **un élément de** $\mathbb{E}$**, le plus petit sous groupe contenant** $\boldsymbol{a}$ **est l'intersection de tous les sous-groupes contenant** $\boldsymbol{a}$**. On l'appelle sous-groupe engendré par** $\boldsymbol{a}$ **et on le note** $\langle \boldsymbol{a} \rangle$**. Il est défini par :**

$$\langle \boldsymbol{a} \rangle = \{\boldsymbol{a^n} \ : \ \boldsymbol{n} \ \in \mathbb{Z}\}$$

Preuve **:**

Premier point **:**

Notons $\mathbb{F}$ l'intersection des sous-groupes contenant a. Il est clair que $\langle a \rangle$ étant un sous groupe contenant a , on a :

$$\mathbb{F} \subset \langle a \rangle$$

Comme $\langle a \rangle$ est le plus petit des sous groupes contenant a et que $\mathbb{F}$ est un sous groupe contenant , on a aussi :

$$\langle a \rangle \subset \mathbb{F}$$

D'où l'égalité.

Second point :

Notons $\mathbb{F} = \{a^n \ : \ n \in \mathbb{Z}\}$

Soit $(x, y) \in \mathbb{F}^2$ alors :

$$\exists\, (n\,, m) \in \mathbb{Z}^2 : x = a^n\,, \ \ y = a^m$$

Donc :

$$x \perp y^{-1} = a^n \perp (a^m)^{-1} = a^n \perp a^{-m} = a^{n-m} \in \mathbb{F}$$

Donc $(\mathbb{F}, \perp)$ est un sous-groupe de $(\mathbb{E}, \perp)$ qui contient a car $a = a^1$

Or tout sous groupe contenant a doit contenir de façon évidente tous les éléments de $\mathbb{F}$. Donc $\mathbb{F}$ est le plus petit d'entre eux.

Un cas particulier important est celui pour lequel $\mathbb{E}$ a un nombre fini d'éléments. Dans ce cas, en désignant par e l'élément neutre de $\mathbb{E}$

$$\exists\, \boldsymbol{p} \in \mathbb{N} : \boldsymbol{a^p = e} \quad \textbf{et si} \ \ \boldsymbol{p > 0} : \ \forall\, \boldsymbol{q} \in [\![\mathbf{0}; \boldsymbol{p-1}]\!] : \boldsymbol{a^q \neq e}$$

$$\forall\, \boldsymbol{n} \in \mathbb{N} : \boldsymbol{a^n = e} \Rightarrow \boldsymbol{p} \in \mathfrak{D}_{\mathbb{N}}(\boldsymbol{n})$$

$$\langle \boldsymbol{a} \rangle = \{\boldsymbol{a^n} \ : \ \boldsymbol{n} \in [\![\mathbf{0}; \boldsymbol{p-1}]\!]\}$$

p qui est le nombre d'élément de $\langle a \rangle$ est appelé ordre de a

Preuves :

1er cas : $a = e$

La propriété est triviale

2ème cas : $a \neq e$

$\{a^n \ : \ n \in \mathbb{N}\}$ est un ensemble fini donc :

$$\exists\, (n\,, m) \in \mathbb{N}^2 : n \neq m \ \text{ et } \ a^n = a^m$$

Supposons par exemple $n > m$, on a alors :

$$a^n \perp a^{-m} = a^m \perp a^{-m}$$

Soit :

$$a^{n-m} = e$$

En posant $q = n - m$ on a :

$$a^q = e$$

Posons :

$$p = Min\,\{q \in \mathbb{N} : a^q = e\}$$

Alors si $p > 0$, on a bien évidemment :

$$\forall\, q \in [\![0; p-1]\!] : a^q \neq e$$

Soit alors $n \in \mathbb{N}$ tel que :

$$a^n = e$$

La division euclidienne de n par p s'écrit :

$$\exists\,(q,r) \in \mathbb{N}^2 : n = p\,q + r\,,\ 0 \leq r < p$$

Donc :

$$a^{p\,q+r} = e$$

Soit :

$$(a^p)^q \perp a^r = e$$

$$(e)^q \perp a^r = e$$

Finalement :

$$a^r = e$$

Donc , puisque : $0 \leq r < p$:

$$r = 0$$

Donc p divise n

De plus , la division euclidienne montre que

$$\langle a \rangle = \{a^r : r \in [\![0; p-1]\!]\}$$

3) <u>Groupe monogène ou cyclique</u>

Etant donné un groupe $(\mathbb{E}, \perp)$, on dit qu'il est monogène ou cyclique, s'il possède un élément $\boldsymbol{a}$ tel que :

$$\mathbb{E} = \langle \boldsymbol{a} \rangle = \{\boldsymbol{a^n} : \boldsymbol{n} \in \mathbb{Z}\}$$

4) Théorème de Lagrange

Etant donné un sous-groupe $(\mathbb{F}, \perp)$ d'un groupe $(\mathbb{E}, \perp)$ ayant un nombre fini d'éléments alors le nombre d'éléments de $\mathbb{F}$ divise celui de $\mathbb{E}$.

Preuve :

Notons n le nombre d'éléments de $\mathbb{E}$ et m celui de $\mathbb{F}$.

Considérons pour un élément a quelconque de $\mathbb{E}$, le sous-ensemble suivant :

$$a \perp \mathbb{F} = \{a \perp x \ : \ x \in \mathbb{F}\}$$

Montrons alors que $a \perp \mathbb{F}$ a le même nombre d'éléments que $\mathbb{F}$ en considérant l'application suivante :

$$f: \begin{cases} \mathbb{F} \to a \perp \mathbb{F} \\ x \to a \perp x \end{cases}$$

f est surjective par construction, montrons qu'elle est injective.

Soit $(x, y) \in \mathbb{F}^2$ alors

$$a \perp x = a \perp y \Rightarrow a^{-1} \perp (a \perp x) = a^{-1} \perp (a \perp y)$$

$$\Rightarrow (a^{-1} \perp a) \perp x = (a^{-1} \perp a) \perp y$$

$$\Rightarrow e \perp x = e \perp y$$

$$\Rightarrow x = y$$

Donc f est injective et donc bijective. On en déduit que $a \perp \mathbb{F}$ a le même nombre d'éléments que $\mathbb{F}$.

Montrons alors pour $(a, b) \in \mathbb{E}^2$ que les sous-ensembles $a \perp \mathbb{F}$ et $b \perp \mathbb{F}$ sont soit égaux, soit disjoints.

Supposons pour cela qu'ils aient un élément commun z, alors :

$$\exists\, (x, y) \in \mathbb{F}^2 : z = a \perp x = b \perp y$$

Alors :

$$a = (b \perp y) \perp x^{-1} = b \perp (y \perp x^{-1})$$

Or $\mathbb{F}$ étant un sous-groupe : $y \perp x^{-1} \in \mathbb{F}$ et donc :

$$a \in b \perp \mathbb{F}$$

Et :

$$a \perp \mathbb{F} \subset b \perp \mathbb{F}$$

De façon analogue :

$$b = (a \perp x) \perp y^{-1} = a \perp (x \perp y^{-1})$$

Donc :

$$b \in a \perp \mathbb{F}$$

Et :

$$b \perp \mathbb{F} \subset a \perp \mathbb{F}$$

D'où l'égalité

Les sous-ensembles $a \perp \mathbb{F}$ ont donc tous le même nombre d'éléments que $\mathbb{F}$ (on dit qu'ils sont équipotents avec $\mathbb{F}$) et sont soient égaux soit disjoints pour les différentes valeurs de a.

Notons alors q le nombre de tels sous-ensembles distincts que l'on peut former, quand a décrit $\mathbb{E}$.

On a alors :

$$q \times m = n$$

Ce qui prouve le théorème.

V Morphisme de groupes

Un morphisme de groupe est une application d'un groupe $(\mathbb{E}, \perp)$ **dans un groupe** $(\mathbb{E}', \perp')$ **vérifiant :**

$$\forall (x, y) \in \mathbb{E}^2 : f(x \perp y) = f(x) \perp' f(y)$$

On définit son noyau par :

$$N(f) = \{x \in \mathbb{E} : f(x) = e'\} = f^{-1}(\{e'\})$$

Exemple : a étant un réel strictement positif , les fonctions exponentielles de base a permettent de définir des morphismes de groupe f définis comme suit :

$$f: \begin{cases} (\mathbb{R},+) \to (]0;+\infty[,\times) \\ x \to a^x \end{cases}$$

En effet :

$$\forall\,(x,y) \in \mathbb{R}^{\mathbf{2}} : \; f(x+y) = a^{x+y} = a^x \times a^y = f(x) \times f(y)$$

Propriété 1 :

Si on désigne par e l'élément neutre de $\mathbb{E}$ pour $\perp$ et e' celui de $\mathbb{E}'$ pour $\perp'$ alors :

$$\boldsymbol{f(e) = e'}$$

Preuve

$$f(e \perp e) = f(e) \perp' f(e)$$

Donc :

$$f(e) = f(e) \perp' f(e)$$

$$\big(f(e)\big)^{-1} \perp' f(e) = \big(f(e)\big)^{-1} \perp' f(e) \perp' f(e)$$

D'où :

$$e' = f(e)$$

Propriété 2 :

$$\forall\, \boldsymbol{x} \in \mathbb{E} \; : \; \boldsymbol{f\big(x^{-1}\big) = \big(f(x)\big)^{-1}}$$

Preuve :

Soit $x \in \mathbb{E}$ alors :

$$f(x \perp x^{-1}) = f(x) \perp' f(x^{-1})$$

Donc :

$$f(e) = f(x) \perp' f(x^{-1})$$

Soit :

$$e' = f(x) \perp' f(x^{-1})$$

D'où :

$$f(x^{-1}) = \big(f(x)\big)^{-1}$$

Propriété 3 :

$\boldsymbol{f}$ **injective** $\Leftrightarrow \boldsymbol{N(f) = \{e\}}$

Preuve :

$\left(\Rightarrow\right)$ Si f injective alors pour $x \in \mathbb{E}$

$$f(x) = e' \Rightarrow f(x) = f(e) \Rightarrow x = e$$

Donc $N(f) \subset \{e\}$

Réciproquement :

$f(e) = e'$ donc $\{e\} \subset N(f)$ d'où l'égalité

$\left(\Rightarrow\right)$ Si $N(f) = \{e\}$ alors pour $(x, y) \in \mathbb{E}^{\mathbf{2}}$:

$$f(x) = f(y) \Rightarrow f(x) \perp' \left(f(y)\right)^{-1} = e'$$

$$\Rightarrow f(x) \perp' f(y^{-1}) = e'$$

$$\Rightarrow f(x \perp y^{-1}) = e'$$

$$\Rightarrow x \perp y^{-1} \in N(f)$$

$$\Rightarrow x \perp y^{-1} = e$$

$$\Rightarrow x = y$$

Donc f injective