Chapitre 1: Relations Binaires

I. Révisions et compléments

- Produit cartésien.
- Relation de A vers B.
- Graphe.
- Relation réciproque d'une relation.
- Relation d' équivalence.
- Classe d'équivalence.
- Relation d'ordre.
- Ensemble quotient.

Congruences modulo n dans $\mathbb{Z}$

Soit n un entier naturel **non nul.** Considérons la relation $\mathcal{R}$ dans $\mathbb{Z}$ définie quels que soient x et y de $\mathbb{Z}$ par

$$\text{« } n \quad \text{divise} \quad x-y \text{ »}$$

ou encore

$$(\exists\, k \in \mathbb{Z}) \qquad x-y=kn.$$

Cette relation $\mathcal{R}$ est **réflexive**, car pour tout x de $\mathbb{Z}$ on a :

$$\exists\, 0 \in \mathbb{Z} \qquad x-x=0=0\times n$$

elle est **symétrique** car, *quels que soient* x et y de $\mathbb{Z}$ on a

$$[(\exists\, k \in \mathbb{Z})\, x-y=kn] \implies (\exists\, -k \in \mathbb{Z})\, y-x=(-k)n$$

enfin elle est **transitive,** car quels que soient x, y, z de $\mathbb{Z}$ on a :

si $\quad [(\exists\, k \in \mathbb{Z})\, x-y=kn] \quad$ et $\quad [\exists\, k' \in \mathbb{Z}\ y-z=k'n]$

alors

$$(\exists\, (k+k') \in \mathbb{Z}) \qquad x-z=x-y+y-z=(k+k')n.$$

La relation $\mathcal{R}$ dans $\mathbb{Z}$ étant **reflexive, symétrique** et **transitive** est une relation d'équivalence dans $\mathbb{Z}$; elle est appelée **congruence modulo** n; elle se note, quels que soient x et y de $\mathbb{Z}$:

$$x \equiv y \qquad (\text{mod}\, n).$$

EXEMPLE

1. Prenons $n = 3$. On a :

$$0 \equiv 3 \equiv 6 \equiv -18 \equiv 300 \equiv 81 \ \ldots\ldots\ldots \pmod 3$$
$$1 \equiv 4 \equiv 7 \equiv -2 \equiv -5 \ \ldots\ldots\ldots \pmod 3$$
$$2 \equiv 5 \equiv 8 \equiv -1 \equiv -4 \ \ldots\ldots\ldots \pmod 3$$

Soit a un entier relatif. Cherchons l'ensemble de tous les entiers relatifs congrus à a, modulo 3, c'est-à-dire la **classe d'équivalence de a** pour la relation dans $\mathbb{Z}$ « congruence modulo 3 ». On peut noter $\dot{a}$ cette classe; on a donc *pour tout* x de $\mathbb{Z}$

$$(x \in \dot{a}) \iff (\exists\, k \in \mathbb{Z}) \quad x - a = 3k$$

ou encore

$$\dot{a} = \{x \in \mathbb{Z} \mid (\exists\, k \in \mathbb{Z})\ x = a + 3k\}.$$

On a donc (q entier naturel quelconque)

$$\dot{0} = \{\ldots -3q, \ldots -6, -3, 0, 3, 6, \ldots, 3q \ldots\}$$
$$\dot{1} = \{\ldots -3q+1, \ldots -5, -2, 1, 4, 7, \ldots, 3q+1 \ldots\}$$
$$\dot{2} = \{\ldots -3q+2, \ldots -4, -1, 2, 5, 8, \ldots, 3q+2 \ldots\}$$

Ces trois classes sont distinctes et on pourrait voir que toute classe d'équivalence pour la relation « congruence modulo 3 » est égale à l'une d'entre elle. Nous allons démontrer ce résultat dans le cas de n quelconque.

II. Entiers modulo n. Ensembles Z/nZ

Soit $\mathcal{R}$ la relation « **congruence modulo** n » dans $\mathbb{Z}$ et soit a un entier relatif quelconque; la **classe d'équivalence** de a, notée $\dot{a}$, pour la relation $\mathcal{R}$ est l'ensemble de tous les éléments x de $\mathbb{Z}$ congrus à a modulo n; on a donc :

$$\dot{a} = \{x \in \mathbb{Z} \mid (\exists\, k \in \mathbb{Z})\ x = a + kn\}$$

Tout élément de $\dot{a}$ est un **représentant** de cette classe, par exemple a, $a+n$, $a+5n$, $a-7n$ etc.

La division euclidienne va nous permettre de trouver pour chaque classe un représentant particulier ce qui nous permettra de trouver toutes les classes d'équivalence pour la relation « congruence modulo n ».

Soit x un entier relatif quelconque, effectuons la division euclidienne de x par n; il existe un entier q unique et un **entier unique** tel que :

$$x = qn + r \quad \text{et} \quad 0 \leqslant r < n$$

on a donc :

$$\dot{x} = \dot{r} \quad \text{et} \quad 0 \leqslant r < n.$$

On obtient donc toutes les classes d'équivalence pour la congruence modulo n en donnant à r toutes les valeurs possibles : il y en a n

$$0,\quad 1,\quad 2,\quad \ldots,\quad n-1.$$

Les classes correspondantes :

$$\dot{0},\ \dot{1},\ \dot{2},\ \ldots,\ \overbrace{\dot{n-1}}$$

sont toutes distinctes

L'**ensemble quotient** de $\mathbb{Z}$ par la relation $\mathcal{R}$ « congruence modulo n », c'est-à-dire l'ensemble des classes d'équivalence pour la relation $\mathcal{R}$ a donc n éléments; on le note $\mathbb{Z}/n\mathbb{Z}$, d'où :

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \ldots, \overset{\bullet}{n-1}\}$$

Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont appelés **entiers modulo n.**

EXEMPLES

2. Prenons $n = 2$. On a $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$; $\dot{0}$ est l'ensemble des entiers relatifs de la forme $2k$ $(k \in \mathbb{Z})$ c'est l'ensemble des entiers pairs; $\dot{1}$ est l'ensemble des entiers relatifs de la forme $2k+1$ $(k \in \mathbb{Z})$, c'est l'ensemble des entiers impairs.

3. Prenons $n = 5$. On a $\mathbb{Z}/5\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}\}$.
   $\dot{0}$ est l'ensemble des entiers relatifs de la forme $5k$ $(k \in \mathbb{Z})$
   $\dot{1}$ est l'ensemble des entiers relatifs de la forme $5k+1$ $(k \in \mathbb{Z})$
   $\dot{2}$ est l'ensemble des entiers relatifs de la forme $5k+2$ $(k \in \mathbb{Z})$
   $\dot{3}$ est l'ensemble des entiers relatifs de la forme $5k+3$ $(k \in \mathbb{Z})$
   $\dot{4}$ est l'ensemble des entiers relatifs de la forme $5k+4$ $(k \in \mathbb{Z})$

Chapitre 2:
Loi de composition interne. Généralités.

Définitions:

1°)

Etant donné un ensemble G toute application:

$$* : G \times G \rightarrow G$$
$$(x, y) \rightarrow x * y$$

est appelée loi de composition interne sur G. L'élément $x * y \in G$ est appelé le composé des éléments x, y de G pour la loi interne $*$.

2°)

Un ensemble muni d'une loi de composition est appelé un magma.

3°)

La loi $*$ *est* ***associative*** *si tous les éléments* $x, y, z \in G$ *satisfont la condition suivante*:

$$(x * y) * z = x * (y * z)$$

4°)

On dit que G possède un **élément neutre** $e \in G$ si pour tous les éléments $x \in G$ on a:

$$x * e = e * x = x$$

5°)

Pour tous les éléments $x * y \in G$, il existe un élément unique a tel que $x * a = y$ et un élément unique b tel que $b * x = y$.

6°)

La loi est commutative si tous les éléments $x * y \in G$ satisfont la condition suivante :

$$x * y = y * x:$$

6°) Monoïdes

Définitions

a) On dit qu'un magma (G,*) est unifère s'il admet un élément neutre.

b) Un magma unifère et associatif est appelé un monoïde.

7°) Groupes

Définition

Un magma $(G,*)$ est un groupe s'il vérifie les trois conditions suivantes :

i) La loi * est associative c'est-à-dire $\forall x, y, z \in G, x*(y*z) = (x*y)*z$.

ii) La loi * admet un élément neutre c'est-à-dire $\exists e \in G / \forall x \in G, x*e = e*x = x$.

iii) Tout élément est symétrisable c'est-à-dire, $\forall x \in G, \exists x' \in G / x*x' = x'*x = e$.

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

Exemple : $(Z; +)$ est un groupe mais pas $(N; +)$.

Propriétés:

Soit (G;*) un groupe alors on a les propriétés suivantes :

1. G ≠ ∅;
2. L'élément neutre est unique.
3. Tout élément de G a un symétrique unique.

Démonstration.

1°) Comme il existe au moins un élément neutre on a le premier point.

2°) Supposons qu'il existe e et e' deux éléments neutres de G, alors

e * e' = e car e' est un élément neutre

e * e' = e' car e est un élément neutre

donc e = e'.

3°) Supposons qu'il existe un élément x ayant deux symétriques x' et x'' donc $x * x'$ = e et $x'' * x$ = e alors

x'' *($x * x'$)= x'' * e = x''

mais par associativité de * on a

x'' * ($x * x'$) =($x'' * x$) * x' = e * x' = x' et donc

x' = x''

8°) Sous-Groupes

Définition

Soit (G;*) un groupe et soit F ⊂ G une partie de G. On dit que F est un sous-groupe de G si et seulement si (F;∗) est un groupe.

Proposition

Soit (G;∗) un groupe et soit F ⊂ G une partie de G. F est un sous-groupe de G si et seulement si les conditions suivantes sont satisfaites :

a) $e \in F$ (F contient l'élément neutre)

b) $\forall x, y \in F; x * y \in F$ (F est stable par la loi *)

c) $\forall x \in F$ le symétrique de x par * est dans F.

Exemple :

L'ensemble des nombres pairs est un sous groupe de (ℤ; +) ; mais pas l'ensemble des nombres impairs.

PROPOSITION. *L'intersection de deux sous-groupes d'un groupe G est un sous-groupe de G. Plus généralement, l'intersection d'une famille quelconque de sous-groupes d'un groupe G est un sous-groupe de G.*

Preuve. Il suffit pour le montrer de prouver le second point. Soit donc $(H_i)_{i\in I}$ une famille de sous-groupes d'un groupe G. Posons $K = \bigcap_{i\in I} H_i$ l'intersection de tous les H_i. L'ensemble K est non-vide, car il contient le neutre e puisque celui-ci appartient à chacun des sous-groupes H_i. Soient x et y deux éléments de K. Pour tout $i \in I$, on a $x.y^{-1} \in H_i$ puisque H_i est un sous-groupe. Donc $x.y^{-1} \in K$. Ce qui prouve que K est un sous-groupe de G. □

9°) Elément régulier

Définition

On dit que *z est un élément régulier de* (G;*) si et seulement si:

1) $\forall x, y \in G \quad [(x * z = y * z) \Rightarrow (x = y)]$
2) $\forall x, y \in G \quad [(z * x = z * y) \Rightarrow (x = y)]$

Remarque:

Dans un groupe tout élément est régulier.

Remarque:

Si x et y ont pour symétrique x' et y', $x * y$ est symétrisable et on a:

$$(x * y)' = y' * x'$$

Relation d'équivalence compatible avec une loi interne:

Considérons l'ensemble $\mathbb{Z}$ des entiers relatifs; cet ensemble peut être muni:

1) De la relation « **congruence modulo n** » **.**
2) D'une **loi interne**, l'addition des entiers relatifs.

La relation $x \equiv y \quad (mod.n)$

Qui s'écrit aussi $x - y \in n\mathbb{Z}$

$signifie \quad (\exists k \in \mathbb{Z}) \quad x - y = kn$

est une relation d'équivalence définie sur $\mathbb{Z}$.

Elle permet de définir l'ensemble quotient

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, \dots, \overdot{n-1}\}$$

ensemble des classes d'équivalence relative à la congruence modulo n. chacune de ces classes étant appelée *entier modulo n.*

$Soient\ \dot{a}\ et\ \dot{b} \in \mathbb{Z}/n\mathbb{Z}$

$Soit\ a' = a + nk\ un\ représentant\ quelconque\ de\ \dot{a}$ $\quad a \equiv a' \quad (mod.n)$

$Soit\ b' = b + nk'un\ représentant\ quelconque\ de\ \dot{b}$ $\quad b \equiv b' \quad (mod.n)$

$Donc\ a' + b' = a + b + n(k + k')\ est\ un\ représentant\ quelconque\ de\ \widehat{a + b}$ $\quad a + b \equiv a' + b' \quad (mod.n)$

$Conclusion\ (\forall a' \in \dot{a})\ (\forall b' \in \dot{b}) \quad \widehat{a' + b'} = \widehat{a + b}$

Exercice:

Démontrer que quelque soient a, a', b et b' de $\mathbb{Z}$, on a:

$(\forall a' \in \dot{a})\ (\forall b' \in \dot{b}) \quad \widehat{a'b'} = \widehat{ab}$

Définition:

$Soit\ E\ un\ ensemble\ muni\ d'une\ relation\ d'équivalence\ \mathcal{R}\ et\ d'une\ loi\ interne\ notée\ \mathrm{T};on\ dit\ que\ la\ relation\ \mathcal{R}\ est\ compatible\ avec\ la\ loi\ interne\ \mathrm{T}\ si\ et\ seulement\ si\ quelque\ soient\ a,a',b,b'$:

$$\begin{cases} a \sim a' & (mod.\mathcal{R}) \\ b \sim b' & (mod.\mathcal{R}) \end{cases} \Longrightarrow \quad [a\mathrm{T}b \sim a'\mathrm{T}b' \quad (mod.\mathcal{R})]$$

Exercice:

Soient a,a',b,b'$\in \mathbb{Z}\ et\ n \in \mathbb{N}.\ montrez\ que$:

$$\begin{cases} a \equiv a' & (mod.n) \\ b \equiv b' & (mod.n) \end{cases} \Longrightarrow \begin{cases} a+b \equiv a' + b' & (mod.n) \\ ab \equiv a'b' & (mod.n) \end{cases}$$

Les groupes finis

DÉFINITION ET NOTATION. On appelle *groupe fini* un groupe G qui, en tant qu'ensemble, n'a qu'un nombre fini d'éléments. Ce nombre d'éléments (qui n'est autre que le cardinal de l'ensemble G) est appelé l'*ordre* du groupe G, noté $o(G)$ ou $|G|$.

EXEMPLE .

Soit n un entier strictement positif. Soit X un ensemble fini à n éléments. Le groupe $\mathcal{S}(X)$ des bijections de X sur X est alors un groupe fini d'ordre $n!$, que l'on appelle (indépendamment de l'ensemble X) le *groupe symétrique* sur n éléments, et que l'on note S_n.

THÉORÈME (dit théorème de Lagrange) *Soit H un sous-groupe d'un groupe fini G. Alors H est fini, et l'ordre de H divise l'ordre de G.*

REMARQUES. On peut représenter un groupe fini G d'ordre n par un tableau à n lignes et n colonnes portant dans la case d'intersection de la ligne indexé par un élément x de G et de la colonne indexé par un élément y de G la valeur du produit $x.y$. Il est facile de vérifier que tout élément de G apparaît une fois et une seule dans chaque ligne et chaque colonne de la table. Il est clair enfin qu'un groupe fini est abélien si et seulement si sa table est symétrique par rapport à la diagonale principale.

GROUPES MONOGENES ET GROUPES CYCLIQUES

PROPOSITION ET DÉFINITION. *Soient G un groupe et X un sous-ensemble non-vide de G. L'intersection de tous les sous-groupes de G qui contiennent X est un sous-groupe de G, appelé le sous-groupe de G engendré par X, noté $\langle X \rangle$, et qui est le plus petit (pour l'inclusion) sous-groupe de G contenant X.*

Sous-groupe engendré par un élément

DÉFINITION ET PROPOSITION. *Soit G un groupe. Soit x un élément de G. On appelle sous-groupe monogène engendré par x dans G le sous-groupe engendré par le singleton $\{x\}$. On le note $\langle x \rangle$. C'est le plus petit sous-groupe de G contenant x, et l'on a:*

$$\langle x \rangle = \{x^m \, ; \, m \in \mathbb{Z}\}.$$

Preuve. Le sous-groupe $\langle x \rangle$ contient x, donc (par stabilité pour la loi de G) il contient aussi $x.x = x^2$, $x^2.x = x^3$, et par récurrence x^m pour tout entier $m \geq 1$. Il contient aussi nécessairement le symétrique x^{-1} de x, donc aussi $x^{-1}.x^{-1} = x^{-2}$, et par récurrence x^{-m} pour tout entier $m \geq 1$. Enfin il contient le neutre $e = x.x^{-1}$ que l'on note par convention x^0. Ceci montre que $\langle x \rangle \supset \{x^m \, ; \, m \in \mathbb{Z}\}$. Il est clair réciproquement que $\{x^m \, ; \, m \in \mathbb{Z}\}$ est un sous-groupe de G contenant x. □

REMARQUE. Attention: l'énoncé précédent est formulé pour la notation multiplicative du groupe G. Dans le cas d'une loi notée comme une addition, il faut remplacer x^n par $nx = x + x + \cdots + x$ et x^{-1} par $-x$. Par exemple, dans le groupe $\mathbb{Z}$ muni de l'addition, $\langle x \rangle = \{mx\,;\, m \in \mathbb{Z}\}$.

DÉFINITION. Soit G un groupe. Soit x un élément de G. On dit que x est d'ordre fini dans G lorsqu'il existe des entiers $m \geq 1$ tel que $x^m = e$. Dans ce cas, on appelle ordre de x le plus petit d'entre eux. En d'autres termes:

$$(x \text{ est d'ordre } n \text{ dans } G) \Leftrightarrow (x^n = e \text{ et } x^m \neq e \text{ si } 1 \leq m < n).$$

Remarquons qu'alors le symétrique de x est $x^{-1} = x^{n-1}$.

PROPOSITION. *Soit G un groupe. Soit x un élément de G. Si x est d'ordre fini $n \geq 1$ dans G, alors le sous-groupe $\langle x \rangle$ est fini d'ordre n, et l'on a:*

$$\langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{n-1}\}.$$

Preuve. Soit x^m avec $m \in \mathbb{Z}$ un élément quelconque de $\langle x \rangle$. Par division euclidienne de m par n, il existe des entiers uniques q et r tels que $m = nq + r$ avec $0 \leq r \leq n-1$. On a $x^m = x^{nq+r} = (x^n)^q.x^r = e^q.x^r = x^r$, ce qui prouve que $\langle x \rangle$ est inclus dans l'ensemble $E := \{x^r\,;\, 0 \leq r \leq n-1\}$. La réciproque étant claire, on a $\langle x \rangle = E$. Il reste à vérifier que E est formé des n éléments distincts $e, x, x^2, x^3, \ldots, x^{n-1}$. Pour cela, supposons que $x^i = x^j$ avec $0 \leq i, j \leq n-1$; alors $x^{i-j} = e$ avec $-n < i - j < n$, ce qui, par minimalité de l'ordre n de x, implique $i - j = 0$ et donc $i = j$. On a donc bien $E = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$, ce qui achève la preuve. □

REMARQUE .

Il résulte de la proposition précédente et du théorème de Lagrange que, si le groupe G est fini, tout élément est d'ordre fini divisant $|G|$.

Groupes monogènes, groupes cycliques.

DÉFINITIONS. Un groupe G est dit *monogène* lorsqu'il est engendré par un de ses éléments, c'est-à-dire lorsqu'il existe un élément $x \in G$ tel que $G = \langle x \rangle$.

Si de plus x est d'ordre fini $n \geq 1$, alors on dit que le groupe G est *cyclique* d'ordre n, et l'on a d'après ce qui précède:

$$G = \{e, x, x^2, x^3, \ldots, x^{n-1}\}.$$

Sinon, $x^i \neq x^j$ pour tous $i \neq j$ dans $\mathbb{Z}$, et $G = \{x^m \,;\, m \in \mathbb{Z}\}$ est monogène infini.

Il est clair qu'un groupe monogène (en particulier un groupe cyclique) est toujours abélien.

PROPOSITION (Sous-groupe d'un groupe monogène infini). *Tout sous-groupe non-trivial d'un groupe monogène infini est monogène infini.*

Preuve. On a $G = \{x^m ; m \in \mathbb{Z}\}$ avec $x \neq e$ qui n'est pas d'ordre fini. Soit H un sous-groupe de G distinct de $\{e\}$. Il existe donc dans H des éléments de la forme x^ℓ avec $\ell \in \mathbb{Z}^*$. Comme l'inverse d'un élément de H appartient à H, on peut préciser qu'il existe dans H des éléments de la forme x^ℓ avec $\ell \in \mathbb{N}^*$. Soit alors d le plus petit entier strictement positif tel que $x^d \in H$. Posons $K = \{x^{dm} ; m \in \mathbb{Z}\}$. Il est clair que $K \subseteq H$ (car $x^d \in H$ et H est stable par produit et passage à l'inverse). Réciproquement, soit x^m un élément quelconque de H (avec $m \in \mathbb{Z}$). Par division euclidienne de m par d, il existe $a, r \in \mathbb{Z}$ uniques tels que $m = ad + r$ avec $0 \leq r < d$. On a $x^r = x^{m-ad} = x^m.(x^d)^{-a}$ avec $x^m \in H$ et $(x^d)^{-a} \in K \subset H$, et donc $x^r \in H$. Par minimalité de d, on a donc forcément $r = 0$; d'où $x^m = x^{ad}$ et donc $x^m \in K$. Ceci prouve que $H \subset K$. On conclut que $H = K = \langle x^d \rangle$. □

PROPOSITION (Sous-groupe d'un groupe cyclique). *Tout sous-groupe d'un groupe cyclique est cyclique. Plus précisément, si $G = \langle x \rangle$ est un groupe cyclique d'ordre $n \geq 1$, alors il existe pour tout diviseur q de n un et un seul sous-groupe d'ordre q, et c'est le sous-groupe cyclique engendré par x^d où $n = dq$.*

Preuve. On a $G = \{e, x, x^2, x^3, \ldots, x^{n-1}\}$. Il est clair que, si q est un diviseur de n, et si l'on pose $n = pq$ avec $p \in \mathbb{N}^*$, alors $\langle x^p \rangle = \{e, x^p, x^{2p}, x^{3p}, x^{(q-1)p}\}$ est un sous-groupe de G cyclique d'ordre q. Réciproquement, soit H un sous-groupe de G. D'après le théorème de Lagrange, l'ordre q de H doit diviser l'ordre de G. On peut supposer $H \neq \{e\}$, c'est-à-dire $q \neq 1$. Comme dans la preuve de la proposition précédente, on peut considérer d le plus petit entier $1 \leq d \leq n-1$ tel que $x^d \in H$, et montrer que $H = \langle x^d \rangle$. Comme H est d'ordre q, on déduit que $dq = n$ et $H = \{e, x^d, x^{2d}, x^{3d}, \ldots, x^{(q-1)d}\}$. □

Groupes finis d'ordre premier

PROPOSITION. *Soit G un groupe fini d'ordre premier p. Alors:*

1. *G est cyclique,*
2. *les seuls sous-groupes de G sont $\{e\}$ et G,*
3. *tous les éléments de G distincts de e sont des générateurs de G.*

Preuve. Comme $p > 1$, $G \neq \{e\}$. Soit $x \in G$ quelconque distinct de e. Posons $H = \langle x \rangle$ le sous-groupe de G engendré par x. D'après le théorème de Lagrange, l'ordre q de H doit diviser p. Comme p est premier, et comme $q \neq 1$ puisque $x \neq e$, on a forcément $q = p$. Donc $H = G$, c'est-à-dire $G = \langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{p-1}\}$. Ceci prouve les points 1 et 2, et le point 3 résulte alors immédiatement du théorème 2.3.2. □

Homomorphisme de groupe

On considère dans ce paragraphe deux groupes (G, $\perp$) et (H, $\top$). On note e_G et e_H les neutres respectifs de G et H. ($\top$ se prononce truc).

Définition On dit qu'une application $f : G \longrightarrow H$ est un **homomorphisme** de groupe si:

- $f(e_G) = e_H$.
- Si x et y sont éléments de G, $f(x \perp y) = f(x) \top f(y)$.

De plus:

- Si G=H, nous dirons que f est un **endomorphisme**.
- Si f est bijective, nous dirons que f est un **isomorphisme**. Si il existe un isomorphisme entre G et H, nous dirons que G et H sont **isomorphes** et nous noterons G $\simeq$H.
- Si f est à la fois un isomorphisme et un endomorphisme, nous dirons que f est un **automorphisme**.

Remarque La notion d'isomorphisme joue en algèbre un rôle dual à celui des homéomorphismes en topologie ou des difféomorphismes en géométrie différentielle. Des groupes qui seront isomorphes auront les mêmes propriétés algébriques. Ainsi, l'étude algébrique d'un groupe pourra se faire sur n'importe quel groupe qui lui est isomorphe.

Proposition Soit x un élément de G, $f(x^{-1}) = (f(x))^{-1}$.

Démonstration Choisissons x dans G. On a $e_H = f(e_G) = f(x \perp x^{-1}) = f(x) \top f(x^{-1})$ et donc par définition de l'inverse d'un élément d'un groupe,

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

Définition Soit f un homomorphisme de G dans H. Nous noterons $Ker f$ ou $Ker(f)$ l'ensemble $\{x \in G; f(x) = e_H\}$. Cet ensemble s'appelle le **noyau** de l'homomorphisme f.
Remarque En allemand, noyau se dit **Ker**nel.
Remarque Le noyau d'un homomorphisme n'est jamais vide. En effet, le neutre du groupe de départ est toujours élément du noyau.
Théorème Soit f un homomorphisme entre G et H. On a équivalence entre:

- f est injective.
- $Ker f$ est réduit à l'élément neutre de G.

Démonstration Si f est injective, l'image du neutre de G par f étant le neutre de H, aucun autre élément de G ne peut avoir e_H comme image. (Ou sinon cela contredit l'injectivité de f). Donc le noyau de f se réduit à $\{e_G\}$.

Si cette dernière propriété est vérifiée, prenons x et y dans G telles que $f(x) = f(y)$. Alors f étant un homomorphisme, $f(x \perp y^{-1}) = e_H$. Donc $x \perp y^{-1}$ est élément de $Ker f$. Mais le noyau de f étant réduit à $\{e_G\}$, cela implique que $x \perp y^{-1} = e_G$ et donc que $x = y$.

Proposition Soit $f : G \longrightarrow H$ un homomorphisme . Alors:

- Ker f est un sous groupe de G.
- Im f (= l'image de f= $\{f(x); x \in G\}$) est un sous groupe de H.

Démonstration Montrons que le noyau de f est un sous groupe de G. e_G est naturellement élément de Ker f. Soient x et y des éléments de Ker f. Alors $f(x \perp y^{-1}) = f(x) \top f(y)^{-1} = e_H$. Ceci prouve que $x \perp y^{-1}$ est élément de Ker f.

Montrons maintenant que Im f est un sous groupe de H. Remarquons que $e_H = f(e_G)$ et donc que e_H est élément de Im f. Soient encore $f(x)$ et $f(y)$ des éléments de Im f. Alors $f(x).f(y)^{-1} = f(x.y^{-1})$ est bien élément de Im f. C.q.f.d.

Proposition L'application composée de deux homomorphismes est encore un homomorphisme.