

# PROGRAMME ALGÈBRE L3

S<sub>5</sub> } 1<sup>ère</sup> partie : Théorie des groupes  
} 2<sup>ème</sup> partie : Théorie des anneaux et corps

S<sub>6</sub> } 3<sup>ère</sup> partie : Théorie des modules.  
} 4<sup>ème</sup> partie : Théorie de GALOIS.

1<sup>ère</sup> partie: chap I: ISOMORPHISME, GRUPE QUOTIENT et théorème de Lagrange

## I-1) Isomorphisme de groupe

Définition I-1-1:

On appelle homomorphisme de groupes toute application

$$\phi: G_1 \longrightarrow G_2$$

$$(xy) \mapsto \phi(xy) = \phi(x)\phi(y).$$

On appelle isomorphisme de groupes, tout homomorphisme  $\phi$  bijectif (à la fois injectif et surjectif)

Si  $\phi: G_1 \rightarrow G_2$  est un isomorphisme, alors on note

$$G_1 \approx G_2 \text{ (on lit } G_1 \text{ isomorphe à } G_2\text{)}$$

### Théorème I-1-1 :

Soient  $G$  et  $\bar{G}$  deux groupes : Si  $\varphi: G \rightarrow \bar{G}$  est un isomorphisme, alors :

$$(1^\circ) |g| = |\varphi(g)| \quad \forall g \in G$$

(2°)  $G$  est abélien  $\Leftrightarrow \bar{G}$  est abélien

(3°)  $G$  est cyclique  $\Leftrightarrow \bar{G}$  cyclique.

(4°) L'équation  $x^k = b$ ,  $b \in G$  et  $k \in \mathbb{Z}$  a le même nombre de solutions que  $x^k = \varphi(b)$  dans  $\bar{G}$

Lemme : Si  $\varphi: G \rightarrow \bar{G}$  est un isomorphisme alors

$$\varphi(a^n) = (\varphi(a))^n \quad \forall n \in \mathbb{Z}$$

Preuve :

Si on montre  $\varphi(a^n) = (\varphi(a))^n$  pour  $n \in \mathbb{N}$ .

Ensuite

$$\begin{aligned} \varphi(a^{-n}) &= \varphi((a^{-1})^n) \\ &= \left( \varphi(a^{-1}) \right)^n \\ &= \left( (\varphi(a))^{-1} \right)^n \\ &= (\varphi(a))^{-n} \end{aligned} \quad (*)$$

Provenons  $\varphi(a^{-1}) = \varphi(a)^{-1}$  ?

$$a \cdot a^{-1} = e$$

$$\varphi(aa^{-1}) = \varphi(e) = e_{\bar{G}}$$

$$\varphi(a) \varphi(a^{-1}) = e_G$$

$$\varphi(a^{-1}) = (\varphi(a))^{-1}$$

D'int pour recurrence.

$$n=1, \varphi(a^1) = (\varphi(a))^1$$

$$\text{supposons que } \varphi(a^n) = (\varphi(a))^n.$$

$$\varphi(a^{n+1}) = \varphi(a^n \cdot a)$$

$$= \varphi(a^n) \cdot \varphi(a)$$

$$= (\varphi(a))^n \varphi(a) = (\varphi(a))^{n+1}$$

$$\text{On a aussi } \varphi(a^{-n}) = \varphi((a^{-1})^n) = (\varphi(a^{-1}))^n.$$

Preuve du théorème:

(1°) supposons  $|g|=n$  alors  $g^n=e$  ('par def').

$$\varphi(g^n) = e.$$

$$(\varphi(g))^n = e.$$

$$|\varphi(g)| \leq n.$$

$$\text{Et } (\varphi(g))^j = e \Rightarrow \varphi(g^j) = e \Rightarrow g^j = e$$

$$\text{Et } j < n$$

$$\Rightarrow |g| < n$$

(contradiction).



(2) Soient  $x, y \in \tilde{G}$   
 $\Rightarrow xy = \varphi^{-1}(\varphi^{-1}(x)) \varphi(\varphi^{-1}(y))$  car  $\varphi$  isomorphisme.  
 $= \varphi(\varphi^{-1}(x) \varphi^{-1}(y)).$   
 $= \varphi(\varphi^{-1}(y) \varphi^{-1}(x))$ . car  $G$  abélien.  
 $= \varphi(\varphi^{-1}(y)) \varphi(\varphi^{-1}(x))$

(m' raisonnement pour  $\leftarrow$ )

Exemple 1:  $x^4 = 1$ .

$S = \{1, -1\}$  dans  $\mathbb{R}$ .

$S' = \{1; -1; i, -i\}$  dans  $\mathbb{C}$ .

Donc  $\mathbb{R} \not\cong \mathbb{C}$  ( $\mathbb{R}$  et  $\mathbb{C}$  ne sont pas isomorphes).

Exemple 2: le groupe des quaternions:  $\mathbb{Q}_8$

$\mathbb{Q}_8 = \{\pm 1; \pm i; \pm j; \pm k\}$ .

$i^2 = j^2 = k^2 = -1$  ;  $ij = k$  ;  $jk = i$  ;  $ki = j$   
 $ji = -k$  ;  $kj = -i$  ;  $ik = -j$ .

$\mathbb{Q}_8$  n'est non abélien car  $ij \neq ji$

$\mathbb{Z}/8\mathbb{Z} = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$   
 $(\mathbb{Z}_8, +)$  est abélien. donc  $\mathbb{Q}_8 \neq \mathbb{Z}_8$ .

Définition I-1-2:

Un automorphisme  $\varphi: G_1 \rightarrow G_1$  est un isomorphisme de  $G_1$  dans lui-même.

Théorème: I-1-2:

Soit  $G$  un groupe.

$\text{Aut}(G) \subseteq \text{Perm}(G)$

↑ ensemble  
des automorphismes  
de  $G$

↑ ensemble des bijets dans  $G$ .

Définition I-1-3: Soient  $G$  un groupe et  $g \in G$

$$\begin{aligned} \varphi_g: G &\rightarrow G \\ x &\mapsto \varphi_g(x) = gxg^{-1} \end{aligned}$$

$\varphi_g$  est appelé automorphisme interne de  $G$ .

On note  $\text{Inn}(G)$ : l'ensemble des automorphismes internes de  $G$ .

Théorème I-1-3:

$$\text{Inn}(G) \subseteq \text{Aut}(G)$$

Définition I-1-4:

Soit  $G$  un groupe. Le centre du groupe  $G$  noté  $Z(G)$  est défini par:

$$Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}$$

Si  $G$  est abélien  $Z(G) = G$ .

Théorème I-1-4.

Soit  $G$  un groupe :

On a :  $Z(G) \leq G$ .

Preuve :

On a :  $ex = xe = x \quad \forall x \in G$ .

$\Rightarrow e \in Z(G)$  donc  $Z(G) \neq \emptyset$ .

Supposons,  $a, b \in Z(G)$ .

donc  $bx = xb \quad \forall x \in G$ .

$$b^{-1}bx = b^{-1}xb.$$

$$x = b^{-1}xb.$$

$$xb^{-1} = b^{-1}xb\ b^{-1}$$

$$xb^{-1} = b^{-1}x \quad \forall x \in G.$$

donc  $b^{-1} \in Z(G)$ .

$$(ab^{-1})x = a(b^{-1}x) = ax \cancel{=} b^{-1}x = x(ab^{-1})$$

donc  $ab^{-1} \in Z(G)$ ,  $Z(G) \leq G$ .

Définition I-1-5 :

Soient  $G$  un groupe et  $a \in G$ . On appelle

centralisateur de  $a$  dans  $G$ , note  $C(a)$ ,

l'ensemble défini par  $C(a) = \{x \in G / ax = x^a\}$

Théorème I-1-5 :

$\forall a \in G$ , on a :  $C(a) \leq G$ .

Preuve:

Soient  $G$  un groupe et  $a \in G$ .

$ea = ae \Rightarrow e \in C(a)$ , donc  $C(a) \neq \emptyset$ .

Soient  $x, y \in C(a)$  donc  $ax = xa$  et  $ay = ya$ .

$$x^{-1}ax = x^{-1}xa = x^{-1}ya = yx^{-1}y.$$

$$x^{-1}a = ax^{-1}. \Rightarrow x^{-1} \in C(a).$$

$$a(xy) = xay \quad \text{car } x \in C(a)$$

$$= (xy)a \quad \text{car } y \in C(a).$$

$\Rightarrow xy \in C(a)$  d'où  $C(a) \leq G$

Théorème I-1-6:

Si  $\varphi: G \rightarrow H$  est un isomorphisme alors :

(1°)  $\varphi(Z(G)) = Z(H)$ .

(2°)  $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$

(3°)  $|a| = |\langle a \rangle| = |\varphi(\langle a \rangle)| = |\langle \varphi(a) \rangle| = |\varphi(a)|$

Preuve (exercice)

I-2) Groupe quotient et Théorème de Lagrange

Définition I-2-1:

Soit  $G$  un groupe et soit  $H$  un sous-ensemble de  $G$  et  $a \in G$ :

On appelle une  $H$ -classe à gauche représentée par l'ensemble  $aH = \{ah \mid h \in H\}$ .

De m<sup>e</sup>, on appelle  $H$ -classe à droite représentée par l'ensemble  $Ha = \{ha \mid h \in H\}$ .

L'ordre (nombre d'élém) de  $aH$  est noté  $|aH|$

$$\text{u} \quad \text{u} \quad \text{u} \quad |Ha| \quad \text{u} \quad |Ha|$$

Théorème I-2-1.

Si  $H \leq G$ , alors on a  $a \in aH$  et  $a \in Ha$ .

Preuve:

On observe  $a = ae \Rightarrow a \in aH$ .

De m<sup>e</sup>  $a = ae \underset{\substack{\downarrow \\ \in H}}{\Rightarrow} a \in Ha$ .

Théorème I-2-2 :

Si  $H \leq G$  et si  $a, b \in G$ , alors :

(1)  $aH = H \Leftrightarrow a \in H$ .

(2) Existe un  $a$ :  $aH = bH$  ou  $aH \cap bH = \emptyset$ .

(3)  $aH = bH \Leftrightarrow H = aH a^{-1}$

(4)  $|aH| = |bH|$

(5)  $aH = Ha \Leftrightarrow H = aH a^{-1}$

(6)  $aH \leq G \Leftrightarrow a \in H$

Preuve:

1)

$\Rightarrow)$   $a \cdot H = H$ .

On a  $a = ae$  avec  $e \in H$ .

$\Rightarrow a \in aH = H$ .

$\Leftarrow)$  Supposons  $a \in H$ .

Soit  $x \in aH \Rightarrow x = ah$ ,  $h \in H$ .

$x$  est formé par un produit de 2 éléments  $a \in H$  et  $h \in H$  puisque  $H \leq G$ , donc  $x = ah \in H$

donc  $aH \subset H$ .

Maintenant, soit  $x \in H \Rightarrow x = ex = a \cdot \underbrace{a^{-1}x}_{\in H}$   
donc  $x \in aH$  donc  $H \subset aH$ .

(2)

On suppose  $aH \cap bH \neq \emptyset$  et  $aH \neq bH$  alors

Fixe  $x \in aH$  et  $x \in bH$ .

Fixe  $h_1, h_2 \in H$  tq  $x = ah_1$  et  $x = bh_2$ .

$y \in b'H$  alors  $y = bh_3 = a \underbrace{h_2^{-1}h_3}_{\in aH}$ .

$\in aH$

$\Rightarrow y \in bH \Rightarrow y \in aH$ . ( $bH \subseteq aH$ ).

De la même manière on montre ( $aH \subseteq bH$ ).

d'où  $aH = bH$  (contradiction).

3) à faire

4)

$$\varphi: aH \rightarrow bH$$

$\varphi(ax) = bx$  est injective.

Théorème I-2-3 : (Théorème de Lagrange).

Si  $G$  est un groupe fini et  $H$  un sous-groupe de  $G$ , alors :

$|H|$  divise  $|G|$ .

De plus, le nombre de  $H$ -classes à gauche distinctes est simplement  $\frac{|G|}{|H|}$ .

Preuve :

$$G = H \cup a_1 H \cup a_2 H \cup a_3 H \cup \dots \cup a_n H$$

où  $a_1 = e$ ,  $a_2 \neq a_3$ ,  $\dots$ ,  $a_n \in G$ .

$a_i H \cap a_j H = \emptyset$  si  $i \neq j$  et  $|a_i H| = |a_j H| = H$   $\circledast$

$\circledast$  voir point 2) du théorème I-2-2.

et ainsi :  $|G| = |H| + |a_2 H| + \dots + |a_n H| = n|H|$ .

$$|G| = n|H| \Rightarrow |H| / |G| \quad (|H| \text{ divise } |G|)$$

Définition I-2-2 :

Si  $G$  est un groupe fini et  $H \leq G$ . Alors le rapport  $k = \frac{|G|}{|H|}$  est appelé indice de  $G$  par  $H$ .

On note  $k = [G : H]$ .

Corollaire 1 :

Tout groupe d'ordre premier est cyclique.

Preuve :

On suppose  $|G| = p$  (premier) et not  $a \in G$ ,  $a \neq e$ .

Posons :

$$\cdot H = \langle a \rangle.$$

$|H| / |G|$  puisque  $p$ , premier, et  $a \neq e$   
 $(|H| \neq 1)$   $\Rightarrow |H| = p$  ou  $|H| = |a| = p$   
 $= |G|$ .

d'où  $G$  est cyclique.

Corollaire 2 :

Si  $|G| < \infty$  alors  $|a| / |G| \nmid a \in G$ .

Preuve :

$\langle a \rangle \subset G$  donc  $|\langle a \rangle| = |a|$ . (voir cours L<sub>2</sub>).

d'où  $|a| / |G|$ .

Corollaire 3 :

$\forall a \in G$ ,  $a^{|G|} = e$

Preuve :

$$|G| = k \quad |a| \Rightarrow a^{|G|} = a^{k \cdot |a|} = (a^{|a|})^k \\ = (e)^k = e.$$

## Theorème I-2-4 :

Soient  $G$  un groupe et  $H \leq G$ .

- (1)  $aH = Ha$  et  $Hhb = Hb$ .  $\forall h \in H$
- (2)  $aH = Ha \Leftrightarrow aHa^{-1} \subseteq H$ .

Exemple I-2-3 :

$$S_3 = \{(1); (1,2); (1,3); (2,3); (123); (132)\}$$

$$\text{et } H = \langle (13) \rangle \leq S_3. \quad H = \{(1); (13)\}$$

$H$ -classes à gauche	$H$ -classes à droite
$(13)H = (1)H = H$	$H(1) = H(13) = H$
$(12)H = \{(12)(1); (12)(13)\}$ $= \{(12); (132)\} = (132)H$	$H(12) = \{(12); (13)(12)\}$ $= \{(12); (123)\} = H(123)$
$(23)H = \{(23); (23)(13)\}$ $= \{(23); (123)\} = (123)H$	$H(23) = \{(23); (13)(23)\}$ $= \{(23); (132)\} = H(132)$
$aH \neq Ha \quad \forall a \in S_3$	

## I-3) clématité :

Définition I-3-1 :

Soit  $G$  un groupe. Un sous-groupe  $H$  de  $G$  est dit normal si et seulement si  $aH = Ha \quad \forall a \in G$

On note  $H \triangleleft G$  (on dit  $H$  est un sous-groupe normal de  $G$  ou bien  $H$  est normal dans  $G$ )

Exemple :  $A_3 = \{(1); (132); (123)\} \leq S_3$ .

$$(12)A_3 = \{(12)(1); (12)(132); (12)(123)\} \\ = \{(12); (13); (23)\}.$$

$$A_3(12) = \{(12); (132)(12); (123)(12)\} \\ = \{(12); (23); (13)\}.$$

$A_3 \triangleleft S_3$

est-ce que toujours :  $(aH)(bH) = abH$  ?

$$(12)H(23)H = (12)(23)H = (123)H.$$

$$(132)H(23)H = (132)(23)H = (13)H.$$

Cette multiplication est bien définie si la condition de normalité est bien définie.

Supposons :  $aH = a'H$  et  $bH = b'H$  et  $H \triangleleft G$ .

est-ce que  $a'b'H = abH$  ?

$$\begin{aligned} a'b'H &= a'bH \\ &= a'Hb \quad \text{car } bH = Hb \\ &= aHb \quad \text{car } a'H = aH \\ &= abH \quad \text{car } Hb = bH. \end{aligned}$$

Théorème I - 3-1 :

Si  $G$  est un groupe et  $H \triangleleft G$ . Alors l'en-

semble  $G/H = \{aH \mid a \in G\}$  forme un groupe par l'opératice définie par  $(aH)(bH) = abH$ .

### Preuve (TD)

(1°)  $eH = H$  où  $e$  = élém neutre du groupe.

$$H(aH) = eaH = aH = (aH)H$$

Donc  $H$  est l'élément neutre de  $G/H$ .

(2°)  $(aH)(a^{-1}H) = (\underbrace{aa^{-1}}_e)H = H$

donc  $a^{-1}H$  est l'inverse de  $aH \quad \forall a \in G$

(3°) Soient  $a, b, c \in G$

$$\begin{aligned} \text{On a : } & (aHbH)cH = (abH)(cH) \\ & = abcH = aH(bcH) \\ & = aH(bHcH). \end{aligned}$$

$G/H : (aH)(bH) = abH \quad (H \triangleleft G)$

Exemple 2-3-2 :

1°)  $G$  est abélien et  $H \leq G$ .

$$a+H = \{a+h \mid h \in H\}$$

$$= \{h+a \mid h \in H\} = H+a. \quad \forall a \in G.$$

$H \triangleleft G$ .

Exemple 2.0) Soit  $G$  un groupe,  $Z(G) \triangleleft G$ .

$$Z(G) = \{g \in G \mid gx = xg \text{ } \forall x \in G\}$$

3°) Groupe Diédral.

$$D_n = \{1, x, x^2, \dots, x^{n-1}, y, xy, x^2y, \dots, x^{n-1}y\}$$

$x$ : est une rotation

$y$ : est une réflexion

$$\circ(x) = n \text{ et } \circ(y) = 2$$

On a  $\langle x \rangle \triangleleft D_n$ .

4°)  $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$ .

$$\{ A \in M_n(\mathbb{R}) \mid \det(A) = 1 \}$$

Propriétés de la normalité.

(I) Si  $H \triangleleft G$  alors l'ordre de l'élément  $aH$  dans le groupe  $G/H$  est  $|aH| = k$  où  $k$  est le plus petit entier naturel tq  $a^k \in H$ ,

$$(aH)^k = \underbrace{(aH)(aH) \cdots (aH)}_k$$

$$= a^k H$$

$$\Rightarrow a^k \in H$$

(2°) Pour tout groupe  $G$ , nous avons 3 sous-groupes normaux distincts possibles qui sont :

$\{e\}$ ,  $Z(G)$  et  $G$ .

↓  
s.g propres

(3°) Si  $G$  un groupe,  $H$  un sous-groupe de  $G$ .  
et  $[G : H] = \infty$ ,  $eH = He = H$  alors

(4°) Définition : Un groupe  $G$  est dit simple s'il n'existe pas un sous-groupe normal  $H$  tel que  $H = \{e\}$  ou  $H = G$ .  
Autrement dit  $G$  est simple si les seuls sous-groupes normaux possibles sont  $H = \{e\}$  et  $H = G$ .

Exemple groupe simple :  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$

I-3-3 classification des groupes jusqu'à l'ordre 6.

ORDRES	Exemples de Représentants
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$ ou $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$ ou $S_3$

cas où  $o(a) = 4$ .

cas où  $o(a) \geq 2$   
 $G$  n'est pas cyclique

<del>①</del>	e	a	$a^2$	$a^3$
e	e	a	$a^2$	$a^3$
a	a	$a^2$	$a^3$	e
$a^2$	$a^2$	$a^3$	e	a
$a^3$	$a^3$	e	a	$a^2$

<del>②</del>	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	<del>e</del>

$U(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

table de Cayley

Tout groupe d'ordre 4 non cyclique tel qu'il existe des éléments d'ordre 2 est appelé Klein 4-groupe

Donc il existe un isomorphisme  $\varphi$  défini par  $\varphi(1) = e$ ;  $\varphi(3) = a$ ;  $\varphi(5) = b$ ;  $\varphi(7) = c$

I-3-4) Normalité et homomorphisme.

Définition: P-3-1:

Si  $H \trianglelefteq G$ , alors  $G/H = \{aH \mid a \in G\}$  est un groupe par rapport à  $(aH)(bH) = abH$ . On définit par l'homomorphisme naturel l'appelation  $\widetilde{\pi}: G \rightarrow G/H$

$$\widetilde{\pi}(x) = xH$$

HB:  $x, y \in G$ ,  $\widetilde{\pi}(xy) = xyH = (xH)(yH) = \widetilde{\pi}(x)\widetilde{\pi}(y)$

$\Rightarrow \tilde{\pi}$  est un homomorphisme de groupes.

Theorème I-3-4-1:

- Si  $\varphi: G_1 \rightarrow G_2$  est un homomorphisme, alors
- (1) Si  $\varphi$  est surjective et  $H_1 \trianglelefteq G_1$  alors  $\varphi(H_1) \trianglelefteq G_2$
  - (2) Si  $H_2 \trianglelefteq G_2$  alors  $\varphi^{-1}(H_2) \trianglelefteq G_1$

Preuve:

W On suppose  $\varphi: G_1 \rightarrow G_2$ , homomorphisme surjectif avec  $H_1 \trianglelefteq G_1$  i.e.  $\forall h \in H_1 \forall g \in G_1$   $y \varphi(hg) = y \varphi(h)y^{-1} \subseteq \varphi(H_1)$  ?

Soit  $y \in \varphi(H_1)$   $\Rightarrow \exists h \in H_1$  tq  $y = \varphi(h)y^{-1}$   
 $\Rightarrow \exists x \in G_1$  tq  $\varphi(x) = y$   
 $\Rightarrow y = \varphi(x)\varphi(h)\varphi^{-1}(x) = \varphi(x)\varphi(h)\varphi(x^{-1})$   
 $\Rightarrow y = \underbrace{\varphi(xhx^{-1})}_{\in H_1} \in \varphi(H_1)$

d'où  $\varphi(H_1) \subseteq \varphi(H_1)$

$\Rightarrow \varphi(H_1) \trianglelefteq G_2$ .

(2) On suppose  $\varphi: G_1 \rightarrow G_2$  homomorphisme et  $H_2 \trianglelefteq G_2$ .

$$y \varphi^{-1}(H_2) y^{-1} \subseteq \varphi^{-1}(H_2) \quad \forall y \in G_2.$$

Soit  $x \in y \varphi^{-1}(H_2) y^{-1} \Rightarrow x = ypy^{-1}$  avec  $p \in \varphi^{-1}(H_2)$

$$p \in \varphi^{-1}(H_2) = \varphi(p) \in H_2.$$

$$\varphi(g) = \varphi(gpg^{-1}) = \varphi(g)\varphi(p)\varphi(g^{-1}) \underset{e_{G_2}}{\in} \varphi(g)H_2\varphi^{-1}(g) \underset{e_{G_2}}{\in} G_2$$

$$\varphi(g)H_2\varphi^{-1}(g) \subseteq H_2 \quad (\text{avec } H_2 \trianglelefteq G_2).$$

$$\Rightarrow \varphi(x) \in H_2 \Rightarrow x \in \varphi^{-1}(H_2) \Rightarrow$$

$$g\varphi^{-1}(H_2)g^{-1} \subseteq \varphi^{-1}(H_2) \Rightarrow \varphi^{-1}(H_2) \trianglelefteq G_2.$$

*Corollaire :*

Puisque  $\ker \varphi \trianglelefteq G_2$  alors l'homomorphisme

$\varphi: G_2 \rightarrow G_2/\ker \varphi$  admet  $\text{Ker } \varphi \trianglelefteq G_2$ :

*Théorème I-3-4-2 :*

Si  $\varphi: G_2 \rightarrow G_2$  est un homomorphisme. Alors

$$\bar{\varphi}: G_2/\ker \varphi \longrightarrow \varphi(G_2).$$

$x \ker \varphi \mapsto \bar{\varphi}(x \ker \varphi) = \varphi(x)$ , est

un isomorphisme.

*Preuve :*

Soient  ~~$x \ker \varphi$~~  et  $y \ker \varphi \in G_2/\ker \varphi$

$$\bar{\varphi}((x \ker \varphi)(y \ker \varphi)) = \bar{\varphi}(xy \ker \varphi)$$

$$= \varphi(xy)$$

$$= \varphi(x)\varphi(y)$$

$$= \bar{\varphi}(x \ker \varphi)\bar{\varphi}(y \ker \varphi)$$

$\Rightarrow \bar{\varphi}$  est un homomorphisme.

(10)

• my  $\bar{\varphi}$  est bijective (a' faire).

Exemple 1 :  $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ .

$$H = \{(0,0); (0,2); (2,0); (2,2)\}.$$

$$G/H = \{H; (1,0)+H; (0,1)+H; (1,1)+H\}$$

$$(1,0)+H + (1,0)+H = (2,0)+H = H.$$

$$\Rightarrow \boxed{|(1,0)+H| = \infty.}$$

$$|(0,2)+H| = \infty.$$

$$|(0,1)+H| = \infty.$$

$$|(1,1)+H| = \infty.$$

VS

$$K = \{(0,0); (1,0); (2,0); (3,0)\}.$$

$$G/K = \{K; (0,2)+K; (0,2)+K; (0,3)+K\}.$$

$$\boxed{|(1,0)+K| = 4.}$$

$$\cancel{X} (1,0)+K + (1,0)+K = (2,0)+K.$$

$$(2,0)+K + (1,0)+K + (1,0)+K = (3,0)+K.$$

$$(1,0)+K + (1,0)+K + (1,0)+K + (1,0)+K = (0,0)+K$$

$$(0,1)+K + (0,1)+K = (0,2)+K.$$

$$(0,1)+K + (0,1)+K + (0,1)+K = (0,3)+K.$$

$$(0,2)+K + (0,2)+K + (0,2)+K + (0,2)+K = (0,0)+K \\ = K.$$

$$|(0,1)+K| = 4 \neq |(0,1)+H| = \infty.$$