

TD N° 1:

Exercice 2.

a) Montrer que $(\forall x \in E, ux = x)$

Soit $x \in E$ alors $\exists y \in E$ tq $\delta_a(y) = x$
(car δ_a surj) donc $ay = x$

et on a : $ua = a$

$$\Rightarrow ux = u(ay)$$

$$\Rightarrow ux = (ua)y = ay = x$$

(car \cdot est associative)

b/

$a \in E$ (arrivé), δ_a est surjective

donc $\exists u \in E$ tel que $\delta_a(u) = a$

$$\text{i.e., } ua = a$$

ce qui donne l'hypothèse de la question 1)

Par la question 1) : $\forall x \in E$ on a $ux = x$

D'autre part, δ_a surjective, et $a \in E$ (arrivée),
donc il existe $u' \in E$ tq $\delta_a(u') = a$

$$\text{i.e., } au' = a$$

ce qui donne une hypothèse semblable à celle
de 1) par δ_a .

Avec un raisonnement sur δ_a , on obtient :

$$\forall x \in E, xu' = x$$

Ainsi en appliquant à u et u' on trouve

$$uu' = u$$

$$= u'$$

c'est à dire que (E, \cdot) admet un élément neutre

c/

on a u est l'élément neutre de (E, \circ)

$a \in E$ (arrivé) alors il admet un antécédent par γ_a donc :

$$\exists a' \in E \text{ tel que } \gamma_a(a') = u \quad (\gamma_a \text{ surj})$$

$$i.e. \quad aa' = u$$

Ainsi a est inversible à dr

de \tilde{m} car étant symétrique

donc il existe $a'' \in E$ / $\gamma_a(a'') = u$

$$i.e. \quad a''a = u$$

$$\text{on a } aa' = u$$

$$\text{donc } a''(aa') = a''u = a''$$

$$\text{et } a''(aa') = (a''a)a' = ua' = a'$$

$$\text{d'où } a'' = a'$$

Par conséquent, a est inversible

Exercice 2:

$f: G \longrightarrow G'$ un homomorphisme de groupes.

1/ Soit $x \in G$ d'ordre fini

$$i.e. \quad \exists n > 0 \quad / \quad x^n = e_G$$

$$\text{alors } f(x^n) = (f(x))^n$$

$$\text{or } x^n = e_G \text{ alors } f(x^n) = f(e_G) = e_{G'}$$

$$\text{d'où } (f(x))^n = e_{G'} \quad \text{il résulte que}$$

$$|f(x)| \text{ divise } n$$

2/ Les homomorphismes de groupes

$$(\mathbb{Z}/7\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/13\mathbb{Z}, +)$$

Soit f un tel homomorphisme

\bar{n} = classe de $n[7]$,

\hat{n} = classe de $n[13]$

$$f(\bar{n}) = f(n \cdot \bar{1}) = f(\bar{1} + \dots + \bar{1}) = n f(\bar{1})$$

Ainsi f est complètement déterminé par $f(\bar{1})$
d'autre part,

$$\begin{aligned} f(\bar{0}) &= f(\bar{1} + \bar{6}) \\ &= f(\bar{1}) + 6f(\bar{1}) \\ &= 7f(\bar{1}) \end{aligned}$$

f homomorphisme de groupe alors $f(\bar{0}) = \bar{0}$
nécessairement $f(\bar{1}) = \bar{0}$
vérifier P

	$f(\bar{1})$	P
$\bar{7}$	$\hat{0}$	P
	$\hat{1}$	P
	$\hat{2}$	P
	\vdots	
	\hat{n}	P

$$P \neq 0[3]$$

Donc: le seul homom de $\mathbb{Z}/7\mathbb{Z} \longrightarrow \mathbb{Z}/13\mathbb{Z}$ est $f=0$

Les homomorphismes de groupes de $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$

Soit g un tel homomorphisme et soit $n \in \mathbb{Z}/3\mathbb{Z}$

$$g(\bar{n}) = g(n \cdot \bar{1})$$

$$= n \cdot g(\bar{1})$$

Ainsi, g est donnée par la connaissance de $g(\bar{1})$

On a aussi :

$$g(\bar{0}) = g(\bar{3})$$

$$\text{car } (\bar{0} = \bar{3})$$

$$\bar{3} = \bar{1} + \bar{2}$$

$$= g(\bar{1}) + 2g(\bar{1})$$

$$= 3g(\bar{1})$$

Or g homomorphisme de groupe $(+)$ alors

$$g(\bar{0}) = \hat{0}$$

$$g(\bar{1}) \quad 3g(\bar{1})$$

$\bar{0}$	$\hat{0}$	oui
$\bar{1}$	$\hat{3}$	non
$\bar{2}$	$\hat{6}$	"
$\bar{3}$	$\hat{9}$	"
$\bar{4}$	$\hat{0}$	oui
$\bar{5}$	$\hat{3}$	non
$\bar{6}$	$\hat{6}$	" "
$\bar{7}$	$\hat{9}$	" "
$\bar{8}$	$\hat{0}$	oui
$\bar{9}$	$\hat{3}$	non
$\bar{10}$	$\hat{6}$	" "
$\bar{11}$	$\hat{9}$	" "

Conclusion :

Les valeurs possible pour $f(\bar{1})$ sont 0, 4, 8

Donc il y a trois homomorphismes de

$$\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$$

$$\bar{1} \longmapsto \hat{0}$$

$$\bar{1} \longmapsto \hat{4} \quad g=0$$

$$\bar{1} \longmapsto \hat{8}$$

Exe 4: G, K deux groupes.

H_1 et H_2 deux ss-groupes distingués de G et K respectivement.

1/ - H_1 un ss-groupe distingué d'un groupe G
Alors $\forall g \in G \forall h_1 \in H_1 \quad gh_1g^{-1} \in H_1$

- H_2 un ss-groupe distingué d'un groupe K
Alors $\forall k \in K \forall h_2 \in H_2 \quad kh_2k^{-1} \in H_2$,
pour montrer que $H_1 \times H_2 \triangleleft G \times K$

il suffit de montrer que
 $\forall a \in G \times K \quad \forall b \in H_1 \times H_2 \quad aba^{-1} \in H_1 \times H_2$

- $a \in G \times K \Rightarrow a = (g, k) \quad / \quad g \in G \quad k \in K$

- $b \in H_1 \times H_2 \Rightarrow b = (h_1, h_2) \quad / \quad h_1 \in H_1, h_2 \in H_2$

$$aba^{-1} = (g, k)(h_1, h_2)(g, k)^{-1} \\ = (g, k)(h_1, h_2)(g^{-1}, k^{-1})$$

$$= (gh_1g^{-1}, kh_2k^{-1}) \in H_1 \times H_2$$

car $gh_1g^{-1} \in H_1$ et $kh_2k^{-1} \in H_2$
Alors $H_1 \times H_2 \triangleleft G \times K$

$$2/ \quad \psi : G \times K \longrightarrow G/H_1 \times K/H_2 \\ (g, k) \longmapsto (gH_1, kH_2)$$

ψ est un homomorphisme de gpe bien défini et surjectif par construction.

$$(g, k) \in \ker \psi \Rightarrow$$

$$(gH_1, kH_2) = (e_{G/H_1}, e_{K/H_2})$$

$\Rightarrow g \in H_1$ et $k \in H_2$
 Ainsi $\text{Ker } \varphi \subseteq H_1 \times H_2$

D'inclusion inverse est clair

D'où $\text{Ker } \varphi = H_1 \times H_2$

1^{er} theoreme d'isomorphisme

donne:

$$G \times_{\text{Ker } \varphi} \cong \text{Im } \varphi$$

$$\text{Ainsi : } G \times_{H_1 \times H_2} \cong G/H_1 \times_{H_2}$$

Si on prend : $H = \{e\}$

Alors $H \triangleleft G$ et

$$G \cong H \times G/H, \quad G/H = G$$

Cependant cette isomorphisme n'a pas toujours lieu :

Contre-exemple : $G = S_3$ et $H = A_3$

On a $A_3 \triangleleft S_3$

$$|S_3| = 6$$

$$|A_3| = 3$$

$$|S_3/A_3| = [A : S_3] = 2$$

Par suite A_3 et S_3/A_3 sont cyclique

car d'ordre premiers

D'autre part, le produit de groupes cyclique d'ordre premier est cyclique

Par suite :

$A_3 \times S_3/A_3$ est un groupe cyclique
 (car $2 \wedge 3 = 1$)

Or S_3 n'est pas cyclique Alors S_3 ne peut pas etre isomorphe à $A_3 \times S_3/A_3$

Ex 6: G un groupe abélien

Alors tout sous-groupe de G est distingué
Soit H un sous-groupe de G , alors $H \triangleleft G$
or G est simple, alors
deux cas sont possibles

Cas 1: $H = \{e\}$

Cas 2: $H = G$

Nécessairement $|G|$ est premier

Supposons que G n'est pas cyclique, donc il n'existe pas de $x \in G$ tel que $\text{ord}(x) = |G|$

Mais on sait que $\text{ord}(x)$ divise $|G|$

Ainsi: $\langle x \rangle = \{e, x, x^2, \dots, x^{\text{ord}(x)}\}$ est un sous-groupe de G avec $\langle x \rangle \subsetneq G$ et $\langle x \rangle \triangleleft G$
contradiction, nécessairement, G est cyclique.

meth 2: Supposons que $|G| = n \cdot p$ ($n \wedge p = 1$)

et $G = \langle g \rangle$ cyclique alors

$$g^{np} = e = (g^n)^p$$

donc si on pose $x = g^n$

$$\langle x \rangle \triangleleft G \text{ d'ordre } p \text{ car } x^p = (g^n)^p = e$$

Absurde car G est simple

D'où $|G|$ est premier

Ex 5:

G un groupe

$$1) \text{Aut}(G) = \{ \text{Automorphisme de } G \}$$

$$= \{ \varphi: G \longrightarrow G \mid \varphi \text{ homom. bijectif} \}$$

$$(\text{Aut}(G), \circ),$$

La composée d'automorphismes reste un automorphisme

$$\begin{aligned}
 & \varphi_1 \circ \varphi_2 (g_1 * g_2) \\
 & \varphi_1 (\varphi_2 (g_1 * g_2)) \\
 & \varphi_1 (\varphi_2 (g_1) * \varphi_2 (g_2)) \\
 & \varphi_1 (\varphi_2 (g_1)) * \varphi_1 (\varphi_2 (g_2))
 \end{aligned}$$

$$(\varphi_1 \circ \varphi_2)(g_1) * \varphi_1 \circ \varphi_2 (g_2)$$

On a :

$$\text{car : } (\varphi_1 \circ \varphi_2)^{-1} = \varphi_2^{-1} \circ \varphi_1^{-1}$$

$$\varphi_1 \circ \varphi_2 \circ (\varphi_2^{-1} \circ \varphi_1^{-1})$$

$$\varphi_1 (\varphi_2 \circ \varphi_2^{-1}) \circ \varphi_1^{-1}$$

$$\varphi_1 \circ \text{id}_G \circ \varphi_1^{-1} = \varphi_1 \circ \varphi_1^{-1} = \text{id}_G$$

$$\text{Aut}(G) \neq \emptyset \quad \text{car} \quad \text{id}_G \in \text{Aut}(G)$$

$$\text{id}_G = e_{\text{Aut}(G)}$$

On vient de voir que :

$$\text{Aut}(G) \neq \emptyset$$

stable par \circ

$$e_{\text{Aut}(G)} = \text{id}_G$$

Chaque $e \in \text{Aut}(G)$ est inversible

Par suite

$(\text{Aut}(G), \circ)$ est un groupe

$$2) \quad a \in G, \quad \varphi : G \longrightarrow G$$

$$x \longmapsto axa^{-1}$$

Maq φ_a est un automorphisme de G ,

Soient $x, x' \in G$

$$\begin{aligned}
 \text{On a : } \varphi_a (xx') &= a (xx') a^{-1} \\
 &= axa^{-1} \cdot ax'a^{-1} \\
 &= \varphi_a (x) \cdot \varphi_a (x')
 \end{aligned}$$

Donc φ_a endomorphisme

$$\begin{aligned}
 \varphi_a \circ \varphi_{a^{-1}}(n) &= \varphi_a(\varphi_{a^{-1}}(n)) \\
 &= \varphi_a(a^{-1}na) \\
 &= aa^{-1}naa^{-1} \\
 &= n
 \end{aligned}$$

$$(\varphi_{a^{-1}} \circ \varphi_a)(n) = n$$

$\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = \text{Id}_G$
 c/c φ_a est automorphisme
 φ_a s'appelle automorphisme intérieur
 $\text{Int}(G) = \{ \varphi_a, a \in G \}$

3/ Soit $\varphi: G \longrightarrow \text{Aut}(G)$
 $a \longmapsto \varphi(a) = \varphi_a$

Montrons que φ est un homomorphisme

Soient $a, b \in G$

$$\varphi(a \cdot b) = \varphi_{ab} = ?? \varphi_a \circ \varphi_b$$

Soit $n \in G$

$$\begin{aligned}
 \varphi_{ab}(n) &= (ab)n(ab)^{-1} \\
 &= abnb^{-1}a^{-1} \\
 &= a(\varphi_b(n))a^{-1} \\
 &= \varphi_a(\varphi_b(n)) = (\varphi_a \circ \varphi_b)(n)
 \end{aligned}$$

D'où le résultat

$$\text{Ker } \varphi = \{ a \in G \mid \varphi(a) = \text{id}_G \}$$

$$a \in \text{Ker } \varphi \Leftrightarrow \varphi(a) = \text{id}_G$$

$$\Leftrightarrow \varphi_a = \text{id}_G$$

$$\Leftrightarrow \forall n \in G \mid \varphi_a(n) = n$$

$$\Leftrightarrow \forall n \in G \mid an\bar{a} = n$$

$$\Leftrightarrow \forall n \in G, an = na$$

Alors $\text{Ker } \varphi = Z(G)$
 $\text{Im } (\varphi) = \varphi(G)$
 $= \text{Int}(G)$

$Z(G) =$ le centre de G
 $Z(G) = \{a \in G \mid ax = xa, \forall x \in G\}$
 $Z(G) \neq \emptyset$ car $e_G \in Z(G)$
 $Z(G) \leq G$

4/ * Si G est abélien
 alors $Z(G) = G$ car chaque élé de G commute avec les autres

dans ce cas : $\text{Ker } \varphi = G$

$\text{Im } \varphi = \{\text{id}\} = \text{Int}(G)$

* Si $Z(G) = \{e\}$

$\text{Ker } \varphi = \{e\}$

$\text{Im } \varphi \simeq G$

i.e. : $\text{Int}(G) \simeq G$

car $G/\text{Ker } \varphi \simeq \text{Int}(G) = \varphi(G)$

i.e. $G/\{e\} \simeq G \simeq \text{Int}(G)$

Exercice 7:

G un groupe, $A \in \mathcal{P}(G)$

$N(A) = \{x \in G \mid xA = Ax\}$

= normalisateur de A dans G

$C(A) = \{x \in G \mid ax = xa, \forall a \in A\}$

= centralisateur de A dans G .

1/ Mq $N(A)$ est un ss-gr. de G

- On a $N(A) \neq \emptyset$ car $e_G \in N(A)$

$e_G A = A \cdot e_G = A$

Soient $x, y \in N(A)$

Mq $xy^{-1} \in N(A)$

e, i : $xy^{-1}A = Axy^{-1}$

On a :
$$\begin{aligned} xy^{-1}A &= xy^{-1}A(xy^{-1}) \\ &= xy^{-1}(Ay)y^{-1} \quad (\text{car } y \in N(A), yA = Ay) \\ &= xy^{-1}(yA)y^{-1} \\ &= xAy^{-1} \\ &= Axy^{-1} \quad (x \in N(A)) \end{aligned}$$

Alors $xy^{-1} \in N(A)$

donc $N(A)$ est un s-gpe de G .

2/ Mq si H ss-gp de G alors H est distingué dans $N(H)$

Montrons d'abord que H est un ss-gpe de G .

On a H est un s-gpe de G .

Donc il suffit de montrer que $H \subseteq N(H)$

Soit $x \in A$, Mq $xH = Hx$

Soit $y \in xH$, alors $\exists h \in H$,

$$\begin{aligned} y &= xh \\ &= xh\tilde{x}^{-1}x \quad (\tilde{x}^{-1} \in H) \\ &= h'x \quad (xh\tilde{x}^{-1}) \in H \end{aligned}$$

donc $xH \subseteq Hx$
de m, soit $y \in Hx$ alors $\exists h \in H$,

$$\begin{aligned} y &= hx \\ &= x\tilde{x}^{-1}hx = xh' = xh \quad (\tilde{x}^{-1}hx \in H) \end{aligned}$$

alors $Hx \subseteq xH$, donc $xH = Hx$

alors $x \in N(H)$

c/c

$H \subseteq N(H)$

alors H est un ss-gpe de $N(H)$

$$* \text{ Ma } H \triangleleft N(H)$$

$$\text{Soit } x \in N(H), \quad xHx^{-1} = Hx\bar{x}^{-1} \quad \left(\begin{array}{l} x \in N(H) \\ xH = Hx \end{array} \right)$$

$$= H$$

$$\text{alors } H \triangleleft N(H)$$

$N(H)$ = le plus grand (\subseteq) ss-grpe de G , qui est normal

3) Ma que $C(A)$ est un ss-grpe

$$C(A) \neq \emptyset \quad \text{car } e_G \in C(A)$$

$$\text{Soient } x, y \in C(A)$$

$$\text{Soit } x \in C(A) \text{ donc } xa = ax, \forall a \in A$$

$$\text{donc } xA = Ax$$

$$\text{donc } C(A) \subseteq N(A)$$

$$\text{Soient } x, y \in C(A)$$

$$\left\{ \begin{array}{l} xa = ax, \quad \forall a \in A \\ yb = by, \quad \forall b \in A \end{array} \right.$$

$$\left\{ \begin{array}{l} xa = ax, \quad \forall a \in A \\ yb = by, \quad \forall b \in A \end{array} \right.$$

$$(xy)a = x(ya)$$

$$= x(ay)$$

$$= (xa)y$$

$$= (ax)y$$

$$= a(xy)$$

$$\text{donc } xy \in C(A)$$

$$xa = ax \Rightarrow xa\bar{x}^{-1} = ax\bar{x}^{-1}$$

$$\Rightarrow xa\bar{x}^{-1} = a$$

$$\Rightarrow \bar{x}^{-1}xa\bar{x}^{-1} = \bar{x}^{-1}a$$

$$\text{d'où } a\bar{x}^{-1} = \bar{x}^{-1}a$$

$$\text{Donc } \bar{x}^{-1} \in C(A)$$

$$\text{donc } C(A) \text{ est un ss-grpe de } A.$$

$$* \text{ Mg } C(A) \trianglelefteq N(A)$$

On a déjà $C(A) \subseteq N(A)$

$$\text{Mg } \forall x \in N(A) \quad \text{Mg } C(A) = x C(A) x^{-1}$$

Soit $y \in C(A)$, donc $ay = ya \quad \forall a \in A$

$$\text{donc } x x^{-1} (ay) = x x^{-1} (ya)$$

$$y \in C(A), \quad \text{Mg } x y x^{-1} \in C(A)$$

Soit $a \in A$

$$x y x^{-1} a = a x y x^{-1} \quad ???$$

$$x^{-1} \in N(A) \Rightarrow x^{-1} A = A x^{-1} \quad (1)$$

$$\Rightarrow \exists b \text{ tq } x^{-1} a = b x^{-1}$$

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

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

car $y \in C(A)$

$b \in A$ et $x \in N(A)$, donc $\exists c \in A$ tq $x b = c x$

$$\text{D'où } x y x^{-1} a = x b y x^{-1} = c x y x^{-1} \in A x y x^{-1}$$

Ainsi on a établi que $x y x^{-1} A \subseteq A x y x^{-1}$

Avec un calcul similaire on montre que

$$A x y x^{-1} \subseteq x y x^{-1} A$$

$$\text{D'où } A x y x^{-1} = x y x^{-1} A$$

$$4/ \quad \text{Mg } C(G) \trianglelefteq G$$

On remarque que $N(G) = G$

et d'après 3) $C(G) \trianglelefteq N(G)$

$$\text{il, } C(G) \trianglelefteq G$$

$$N(G) = \{x \in G \mid x G = G x\}$$

Exercice 8:

$$f: H \times K \xrightarrow{f} G$$

$$(h, k) \longmapsto h k$$

$$f(x) = f(y) \Rightarrow x = y$$

$$f(x) * (f(y))^{-1} = e \Rightarrow f(x * y^{-1}) = f(e) = e_G$$

1/ Considérons la relation binaire défini par:

$$(h, k) R (h', k') \Leftrightarrow f(h, k) = f(h', k')$$

M que R est une relation d'équi
soit $(h, k) \in H \times K$

On a:

$$f(h, k) = f(h, k) \Leftrightarrow (h, k) R (h, k)$$

alors R est réflexive

Soient $(h, k), (h', k') \in H \times K$

$$(h, k) R (h', k')$$

$$\Leftrightarrow f(h, k) = f(h', k')$$

$$\Leftrightarrow f(h', k') = f(h, k)$$

$$\Leftrightarrow (h', k') R (h, k)$$

Alors R est symétrique

Soient $(h, k), (h', k'), (h_1, k_1) \in H \times K$

On a

$$(h, k) R (h', k') \text{ et } (h_1, k_1) R (h', k')$$

$$\Leftrightarrow \begin{cases} f(h, k) = f(h', k') \\ f(h_1, k_1) = f(h', k') \end{cases}$$

$$\Leftrightarrow f(h, k) = f(h_1, k_1) \Leftrightarrow (h, k) R (h_1, k_1)$$

alors R est transitive

donc R est une relation d'équivalence

Soient $(h, k), (h', k') \in H \times K$

$$\begin{aligned}
 (*) \quad (h, k) &= (h', k') &\Leftrightarrow (h, k) \mathcal{R} (h', k') \\
 &&\Leftrightarrow f(h, k) = f(h', k') \\
 &&\Leftrightarrow hk = h'k' \\
 &&\Leftrightarrow h^{-1}h = h'^{-1}h' \\
 &&\Leftrightarrow h^{-1}h = k'^{-1}k' \\
 &&\Leftrightarrow hh^{-1} \text{ et } k'^{-1}k' \in H \cap K
 \end{aligned}$$

$$\begin{array}{ccc}
 \frac{H \times K}{\mathcal{R}} & \xrightarrow{\psi} & HK \\
 \overline{(h, k)} & \longmapsto & h, k
 \end{array}$$

$$\begin{aligned}
 \psi(\overline{(h, k)}) &= \psi(\overline{(h', k')}) \\
 hk = h'k' &\Rightarrow k'^{-1}h' = k^{-1}h \\
 &\Leftrightarrow \overline{(h, k)} = \overline{(h', k')} \\
 &\Leftrightarrow \overline{(h, k)} = \overline{(h', k')}
 \end{aligned}$$

ψ est surjective par construction

* $\overline{(h, k)}, \overline{(h', k')} \in \frac{H \times K}{\mathcal{R}}$

$$\begin{aligned}
 \psi(\overline{(h, k)}) &= \psi(\overline{(h', k')}) \\
 \Rightarrow hk &= h'k' \\
 \Rightarrow h^{-1}h &= h'^{-1}h' \\
 \Rightarrow \overline{(h, k)} &= \overline{(h', k')}
 \end{aligned}$$

Donc ψ est injective.

par suite ψ est bijective et donc $\frac{H \times K}{\mathcal{R}}$ est équivalent à HK .

et on a :

$$|\frac{H \times K}{\mathcal{R}}| = \frac{|H \times K|}{|H \cap K|} = \frac{|H| |K|}{|H \cap K|}$$

$$|H \times K| = |H| |K|$$

par suite

$$|HK| = \frac{|H| |K|}{|H \cap K|}$$

$$B = \{ef \times H \cap K \mid H \cap K \times \{ef\}\} \subset H \times K$$

$$x R y \Leftrightarrow xy^{-1} \in B \quad (H \times K / B)$$

$$21 \quad M q \quad HK \text{ ss-gr de } G \Leftrightarrow HK = KH$$

(\Rightarrow) - Supp que HK ss-gr de G

$$h k \in HK \Rightarrow (h k^{-1}) \in HK$$

$$\Rightarrow h^{-1} h^{-1} \in HK$$

$$\text{donc } \exists h_0 \in H \text{ et } k_0 \in K \mid h^{-1} h^{-1} = h_0 k_0$$

$$\Rightarrow h k = k_0^{-1} h_0$$

$$\text{puisque : } \begin{cases} k_0^{-1} \in K \text{ car } k_0 \in K \\ h_0^{-1} \in H \text{ car } h_0 \in H \\ h k = k_0^{-1} h_0^{-1} \in KH \end{cases}$$

$$c/c \quad HK \subset KH$$

* par l'absurde supposons que $HK \neq KH$
 $\exists (h, k) \in H \times K$ tel que $kh \notin HK$ (groupe)

$$(kh)^{-1} = h^{-1} k^{-1} \in HK$$

$$\text{donc } (h^{-1} k^{-1})^{-1} = kh \in HK$$

$$kh \in HK \text{ absurde}$$

$$\text{alors } HK = KH$$

(\Leftarrow) Supp que $HK = KH$:

$$\text{On a : } HK \neq \{\emptyset\} \text{ car } e = e \cdot e \in HK$$

$$xy^{-1} = (h_0 k_0) \cdot (h' k')^{-1} = h_0 (h_0^{-1} h') k'$$

$$\text{On a } h_0^{-1} h' \in KH = HK$$

$$\text{donc } \exists h'' \in H \text{ et } k'' \in K \mid$$

$$h_0^{-1} h' = h'' k''$$

$$\Rightarrow xy^{-1} = h_0 (h'' k'') k' = (h_0 h'') (k'' k') \in HK$$

$$c/c \quad HK \text{ ss-gr de } G$$

3/ On suppose que $H \triangleleft G$

alors on a $HK = KH$

$\forall h \in H$ on a $h \in G$ et $H \triangleleft G$

$$\Rightarrow KH = HK$$

* $\langle HUK \rangle =$ le plus petit ss-gr contenant HUK .

$$HUK \subseteq HK$$

$$H = He \subseteq HK$$

$$K = eK \subseteq HK$$

Soit B tel que /

$$HUK \subseteq B \subseteq HK$$

On a $H \subseteq B$ et $K \subseteq B$

B un ss-gr $\Rightarrow HK \subseteq B$

$$\text{donc } B = HK$$

4/ Il faut que :

$$H \triangleleft G \text{ et } K \triangleleft G \Rightarrow HK \triangleleft G$$

On a : $H \triangleleft G$ et $K \triangleleft G$

Alors $HK = KH$ et par suite HK est un ss-groupe de G .

Soit $g \in G$ alors :

$$gHKg^{-1} = HgKg^{-1}$$

$$= HKe = HK$$

$$\Rightarrow HK \triangleleft G$$

c/c HK ss-gr de G

5/

(a)

$$G = HK$$

$$H \triangleleft G \Rightarrow HK = KH$$

$hk \in HK = KH$ alors il existe $(h', k') \in H \times K$
t.q. $hk = k'h'$.

D'autre part :

$$h k = k' h' \Rightarrow \underbrace{h k h^{-1}}_{\in K} = \underbrace{k' h' h^{-1}}_{\substack{\in K \\ \in H}} \in HK$$

$K \text{ cor } K \triangleleft G$

$$\begin{aligned} \Rightarrow k' h' h^{-1} \in K &\Rightarrow h' h^{-1} \in k^{-1} k \in K \\ &\Rightarrow h' h^{-1} \in H \cap K = \{e\} \\ &\Rightarrow h' h^{-1} = e \\ &\Rightarrow h' = h \end{aligned}$$

de m $k' = k$

(b) Soit $x \in G = HK$
 alors il existe $h, k \in H \times K$ tel que $x = hk$.
 Supposons qu'il existe $(h', k') \in H \times K$
 tel que $x = h'k'$

alors $hk = h'k' \quad (*)$

$$\Rightarrow \underbrace{h^{-1}h}_{\in H} = \underbrace{k'k^{-1}}_{\in K} \in H \cap K$$

Or $H \cap K = \{e\}$ alors :

$$\begin{aligned} (*) &\Rightarrow h^{-1}h = e = k'k^{-1} \\ &\Rightarrow h = h' \text{ et } k = k' \end{aligned}$$

D'où l'unicité.

$$\begin{aligned} (c) \quad \psi : H \times K &\longrightarrow G = HK \\ (h, k) &\longmapsto hk \end{aligned}$$

Nous avons déjà établi que ψ est une application bien définie de plus elle est surjective par construction

$$K = \{e\} \Rightarrow h' h^{-1} = e$$

$$\Rightarrow h' = h \quad \text{uni (b)}$$

* homomorphisme:

$$\begin{aligned}
 (h, k), (h', k') &\in H \times K \\
 \psi((h, k)(h', k')) &= \psi(hh', kk') \\
 &= (hh') \cdot (kk') \\
 &= h(h'k)k' \\
 &= h(kh')k' \quad (\text{car } \forall x, y \in H \times K, xy = yx) \\
 &= hkh'k' \\
 &= \psi(h, k) \psi(h', k')
 \end{aligned}$$

Ainsi ψ est un homomorphisme surjectif

$$\begin{aligned}
 (h, k) \in \text{Ker } \psi &\Rightarrow \psi(h, k) = e \\
 &\Rightarrow hk = e \\
 &\Rightarrow h = k^{-1} \in K
 \end{aligned}$$

$$\Rightarrow \begin{cases} h \in H \cap K \Rightarrow h = e \\ k^{-1} \in H \cap K \Rightarrow k = e \end{cases}$$

$$\Rightarrow (h, k) = (e, e) = e_{H \times K}$$

$$\Rightarrow \text{Ker } \psi = \{ e_{H \times K} \}$$

ψ surjectif

D'où ψ est bijective, c'est donc une isomorphisme

$$G \simeq H \times K$$

Exercice 9:

$G = \langle x \rangle$ cyclique d'ordre n

H un sous-gr de G alors H est cyclique

$$H \subseteq G = \{ e, x, x^2, \dots, x^{n-1} \}$$

Soit k le plus petit entier ($< n$) tel que $x^k \in H$

$$\text{Vérifier } H = \langle x^k \rangle$$

$x^B \in H \Rightarrow \langle x^B \rangle \subseteq H$
 car $x^B \in H \Rightarrow$ toutes les puissances de x^B sont dans H .

* Montrons que $H \subseteq \langle x^B \rangle$

$y \in H \subseteq G \Rightarrow \exists \lambda \in \{0, \dots, n-1\}$ tel que:
 $y = x^\lambda$.

nécessairement $\lambda \geq B$

par divisions euclidienne, $\exists t, r \in \mathbb{N}$ tel que:

$$\lambda = Bt + r \text{ et } r < B$$

$$x^\lambda = x^{Bt} \cdot x^r$$

$$= (x^B)^t \cdot x^r$$

On a: $x^\lambda \in H$

$$(x^B)^t \in H, \text{ car } x^B \in H$$

$$\Rightarrow x^\lambda \cdot (x^B)^{-t} = x^r \in H$$

* à cause de la minimalité de B , on trouve
 $r=0$.

$$\text{C'est à dire } x^\lambda = (x^B)^t \in \langle x^B \rangle$$

$$\text{D'où } H = \langle x^B \rangle$$

$$d = \frac{n}{B} \quad (x^B)^d = (x^B)^{\frac{n}{B}} = x^{B \cdot \frac{n}{B}} = x^n = e$$

Ainsi: Or (x^B) divise $\frac{n}{B}$

Soit: $t \in \mathbb{N}$: $(x^B)^t = e$

$$\Rightarrow x^{Bt} = e \Rightarrow \frac{n}{B} \mid Bt$$

$$\Rightarrow \frac{n}{B} \mid e$$

Ainsi, $\text{ord}(x^B) = \frac{n}{B}$

$$\text{Donc aussi } |H| = \frac{n}{B}$$

Ex 3:

$$n, p \in \mathbb{N}^*$$

$$n \wedge p = 1$$

$(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +)$ est un groupe abélien

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

$$x \longmapsto (x + n\mathbb{Z}, x + p\mathbb{Z})$$

f est une application.

posons : $x + n\mathbb{Z} = \bar{x}$

$$x + p\mathbb{Z} = \hat{x}$$

$$f(x+y) = (\overline{x+y}, \widehat{x+y})$$

$$= (\bar{x} + \bar{y}, \hat{x} + \hat{y})$$

$$= (\bar{x}, \bar{x}) + (\bar{y}, \bar{y})$$

$$= f(x) + f(y)$$

Ainsi f est un homomorphisme de groupe additif.

* $\forall q$ f est surj:

$$\text{Soit } (\bar{x}, \hat{y}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

$$\forall q \quad \exists a \in \mathbb{Z} \quad / \quad f(a) = (\bar{x}, \hat{y})$$

Cà d :

$$\begin{cases} \bar{x} = a + n\mathbb{Z} \\ \hat{y} = a + p\mathbb{Z} \end{cases}$$

\Rightarrow

$$\begin{cases} \bar{x} = a + n\ell \quad / \quad \ell \in \mathbb{Z} \\ \hat{y} = a + p\ell' \quad / \quad \ell' \in \mathbb{Z} \end{cases}$$

$$\Rightarrow x-y = n\ell - p\ell$$

or $n \wedge p = 1$ d'après th de Bezout

$$\exists d, p \in \mathbb{Z} / 1 = dn + pp \quad (*)$$

donc $(*) (x-y) \Rightarrow x-y = dn(x-y) + pp(x-y)$

d'où il suffit de prendre :

$$\begin{cases} \varphi = d(x-y) \\ \varphi' = p(x-y) \end{cases}$$

$$\text{Ker } f, x \in \text{Ker } f \Rightarrow \begin{cases} x + n\mathbb{Z} = 0 \\ n + p\mathbb{Z} = 0 \end{cases}$$

$$\Rightarrow n/x \text{ et } p/x$$

$$\Rightarrow n/p/x \text{ car } p \wedge n = 1$$

$$\text{D'où } x \in np\mathbb{Z}$$

$$\text{et par suite } \text{Ker } f \subseteq np\mathbb{Z}$$

$$\text{D'autre part, si } x \in np\mathbb{Z}$$

alors :

$$\begin{matrix} n/x \\ p/n \end{matrix} \Rightarrow \begin{cases} x + n\mathbb{Z} = 0 \\ x + p\mathbb{Z} = 0 \end{cases} \Rightarrow p(x) = 0 \Rightarrow x \in \text{Ker } f$$

$$\text{Par conséquent, on a :}$$

$$\text{Ker } f = np\mathbb{Z}$$

$$n \wedge p = 1 \Rightarrow \exists u, v \in \mathbb{Z} / un + pv = 1$$

$$(a + n\mathbb{Z}, b + p\mathbb{Z}) \in \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$$

$$\begin{aligned} a - b &= (a - b)un + (a - b)vp \\ \Downarrow \\ a - (a - b)un &= b + (a - b)vp \end{aligned}$$

presons alors:

$$\begin{aligned} x &= a - (a-b) \vee n = b + (a-b) \vee p \\ x + n\mathbb{Z} &= a - (a-b) \vee n + n\mathbb{Z} \\ &= a + n\mathbb{Z} \end{aligned}$$

$$\begin{aligned} x + p\mathbb{Z} &= b + (a-b) \vee p + p\mathbb{Z} \\ &= b + p\mathbb{Z} \end{aligned}$$

D'où :

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{p} \end{aligned}$$

i.e

$$f(x) = (a + n\mathbb{Z}, b + p\mathbb{Z})$$

Remarque:

$$\begin{aligned} f(x) &= (\bar{x}^{[n]}, \bar{x}^{[p]}) \\ &= (\overline{a - (a-b) \vee n}^{[n]}, \overline{b + (a-b) \vee p}^{[p]}) \\ &= (\bar{a}^{[n]}, \bar{b}^{[p]}) \\ &= \end{aligned}$$

f surjective et $\text{Ker} f = p n \mathbb{Z}$

D'après le 1^{er} théorème d'isomorphisme

$$\frac{\mathbb{Z}}{\text{Ker} f} \cong \text{Im}(f)$$

i.e, $\frac{\mathbb{Z}}{np\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}} \quad (p \wedge n = 1)$

Si $n \wedge p \neq 1$, l'isomorphisme précédent $\Rightarrow f(x) = 0$

n'a pas lieu

$$\Rightarrow x \in \text{Ker} f$$

Contre exemple:

$$n = p = 2$$

$$G = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0})\}$$

$$\begin{aligned} 2(\bar{1}, \bar{1}) &= (\bar{0}, \bar{0}) \\ 2(\bar{0}, \bar{1}) &= (\bar{0}, \bar{0}) \quad , \quad 2(\bar{1}, \bar{0}) = (\bar{0}, \bar{0}) \end{aligned}$$

$\text{Card } G = 4$ mais tous les éléments de G
 sont d'ordre ≤ 2 Donc G n'est pas
 cyclique.
 par suite G ne peut pas être isomorphe
 à $\mathbb{Z}/4\mathbb{Z}$ cyclique d'ordre 4.

SIGMA
 Club

www.minfosma.gnomio.com