Homomorphisme de groupes-Groupe cyclique

Les morphismes de groupes jouent un rôle important dans le chiffrement et déchiffrement d'un texte, d'une image,…(code César, RSA, signature électronique, …).
Morphisme vient du mot grec morphé signifiant forme.

I. Homomorphisme ou morphisme de groupes

Définition Soient $(E,*)$ et $(F,\perp)$ deux groupes et $f:E\to F$ une application
f est un homomorphisme (ou morphisme) de groupes si et seulement si :
$\forall (a,b)\in E^2$ on a : $f(a*b)=f(a)\perp f(b)$

Exemples (à prouver)
Les applications suivantes sont des morphismes de groupes :

$$f:(\mathbf{R},+)\to(\mathbf{R}^*,\times),\ x\mapsto e^x \quad ; \quad g:(]0,+\infty[,\times)\to(\mathbf{R},+),\ x\mapsto Ln(x)$$

Propriétés Soit $n\in\mathbf{Z}^*$
1) Si $(G,*)$ est un groupe **abélien** alors les applications suivantes sont des morphismes de groupes :

$$f:(G,*)\to(G,*),\ x\mapsto x^{-1} \quad ; \quad g:(G,*)\to(G,*),\ x\mapsto x^n \quad ; \quad h:(G,*)\to(G,*),\ x\mapsto x^2$$

2) Si $(G,+)$ est **abélien** alors les applications suivantes sont des morphismes de groupes:

$$f:(G,+)\to(G,+),\ x\mapsto -x \quad ; \quad g:(G,+)\to(G,+),\ x\mapsto nx \quad ; \quad h:(G,+)\to(G,+),\ x\mapsto 2x$$

Preuve à faire en exercice (pourquoi a-t-on besoin de la commutativité ?)

Exemples $(\mathbf{Z},+)$, $(Z/nZ,+)$ et $(\mathbf{R}^*,\times)$ sont des groupes abéliens d'où :
1) Pour chaque $a\in\mathbf{Z}$, les applications suivantes sont des morphismes de groupes :

$$f:(\mathbf{Z},+)\to(\mathbf{Z},+),\ x\mapsto ax \quad ; \quad g:(Z/nZ,+)\to(Z/nZ,+),\ \overline{x}\mapsto \overline{a}\,\overline{x}$$

2) Pour chaque $n\in\mathbf{Z}$, les applications suivantes sont des morphismes de groupes :

$$h:(\mathbf{R}^*,\times)\to(\mathbf{R}^*,\times),\ x\mapsto x^n \quad ; \quad \varphi:(\mathbf{R}^*,\times)\to(\mathbf{R}^*,\times),\ x\mapsto x^2 \quad ; \quad \psi:(\mathbf{R}^*,\times)\to(\mathbf{R}^*,\times),\ x\mapsto \frac{1}{x}$$

Propriétés Soit $f:(E,*)\to(F,\perp)$ un morphisme de groupes, on a :
1) $f(e_E)=e_F$ où e_E et e_F désignent respectivement l'élément neutre de $(E,*)$ et $(F,\perp)$
2) $\forall x\in E,\ f(x^{-1})=\left(f(x)\right)^{-1}$: l'image de l'inverse est égale à l'inverse de l'image

Preuve : utilisez les propriétés du calcul dans un groupe (écrire $e_E*e_E=e_E$ et $x*x^{-1}=e_E$)

II. Noyau et image d'un morphisme de groupes

Définitions Soit $f:(E,*)\to(F,\perp)$ un morphisme de groupes.

1) On note $Ker(f)=\{x\in E\ /\ f(x)=e_F\}$ et s'appelle le noyau du morphisme f

C'est-à-dire $\boxed{x\in Ker(f)\Leftrightarrow x\in E\ et\ f(x)=e_F}$

2) On note $\mathrm{Im}(f)=\{f(x)\in F\ /\ x\in E\}$ et s'appelle l'image du morphisme f

C'est-à-dire $\boxed{y\in \mathrm{Im}(f)\Leftrightarrow \exists x\in E\ tel\ que\ y=f(x)}$

Exemples (à prouver), pour les morphismes de groupes suivants on a :

1) $\begin{array}{ccccc} f:(\mathbf{Z},+) & \to & (\mathbf{Z},+), & on\ a: & Ker(f)=\{0\}\ et\ \mathrm{Im}(f)=2\mathbf{Z} \\ x & \mapsto & 2x & & \end{array}$

2) $\begin{array}{ccccc} g:(Z/4Z,+) & \to & (Z/4Z,+), & on\ a: & Ker(g)=\{\bar{0},\bar{2}\}\ et\ \mathrm{Im}(g)=\{\bar{0},\bar{2}\} \\ \bar{x} & \mapsto & \bar{2}\bar{x} & & \end{array}$

3) $\begin{array}{ccccc} h:(\mathbf{Z},+) & \to & (\Omega_3,\times), & où\ \Omega_3=\{1,j,j^2\}\ et\ j=e^{\frac{2i\pi}{3}}\ on\ a: & Ker(h)=3\mathbf{Z}\ et\ \mathrm{Im}(h)=\Omega_3 \\ n & \mapsto & j^n & & \end{array}$

Théorème Si $f:(E,*)\to(F,\perp)$ est un morphisme de groupes alors on a :

1) $Ker(f)$ est un sous-groupe de $(E,*)$

2) $\mathrm{Im}(f)$ est un sous-groupe de $(F,\perp)$

Preuve

1) $f:(E,*)\to(F,\perp)$ est un morphisme de groupes donc $f(e_E)=e_F$ d'où $e_E\in Ker(f)$ et

$\forall x,y\in Ker(f),\ x*y^{-1}\in E$ car $(E,*)$ es un groupe et

$f(x*y^{-1})=f(x)\perp f(y^{-1})=e_F\perp(f(y))^{-1}=e_F\perp(e_F)^{-1}=e_F\perp e_F=e_F$ d'où $(x*y^{-1})\in Ker(f)$

2) idem $f(e_E)=e_F$ donc $e_F\in\mathrm{Im}(f)$, **montrez que** $\forall u,v\in\mathrm{Im}(f)$ on a $u*v^{-1}\in\mathrm{Im}(f)$

III. Image d'un groupe cyclique par un morphisme de groupes

Théorème (image d'un groupe cyclique)

Soit $f:(E,*)\to(F,\perp)$ un morphisme de groupes on a :

1) Si $a\in E$ alors $f(\langle a\rangle)=\langle f(a)\rangle$ c'est-à-dire :

$\boxed{\text{si } a \text{ est un générateur d'un groupe } (G,*) \text{ alors } f(a) \text{ est un générateur du groupe } (f(G),\perp)}$

2) $\boxed{\text{Si } (E,*) \text{ est un groupe cyclique, alors } (\mathrm{Im}(f),\perp) \text{ est un groupe cyclique}}$

Preuve $y\in f(G)\Leftrightarrow\exists x\in G,\ y=f(x)\Leftrightarrow\exists n\in\mathbf{Z},\ y=f(a^n)$ car $x\in G\Leftrightarrow\exists n\in\mathbf{Z},\ x=a^n$

d'où $y\in f(G)\Leftrightarrow\exists n\in\mathbf{Z},\ y=(f(a))^n$ car f est un morphisme de groupes

Exemples pour les morphismes de groupes suivants on a :

1) $\begin{array}{ccccc} f:(\mathbf{Z},+) & \to & (\mathbf{Z},+), & on\ a: & \mathrm{Im}(f)=\langle f(1)\rangle=\langle 2\rangle=2\mathbf{Z}\ car\ \mathbf{Z}=\langle 1\rangle \\ x & \mapsto & 2x & & \end{array}$

2) $g:(Z/4Z,+) \to (Z/4Z,+)$, $\bar{x} \mapsto \bar{3}\bar{x}$ *on a* : $\mathrm{Im}(g) = \langle g(\bar{1}) \rangle = \langle \bar{3} \rangle = Z/4Z$

3) $h:(\mathbf{C}^*,\times) \to (\mathbf{C}^*,\times)$, $x \mapsto x^2$ *on a* $\Omega_4 = \{-1,1,i,-i\} = \langle i \rangle$ *d'où* $h(\Omega_4) = \langle h(i) \rangle = \langle -1 \rangle = \{-1,1\}$

IV. Injectivité d'un morphisme de groupes et complément sur les applications définis sur des ensembles finis

Rappels et compléments

Soit $f : E \to F$ une application

- f est injective de E dans $F \Leftrightarrow \forall x, y \in E$ si $f(x) = f(y)$ alors $x = y$
- f est surjective de E sur $F \Leftrightarrow \forall y \in F, \exists x \in E$ tel que $y = f(x)$
- f est surjective de E sur $F \Leftrightarrow f(E) = F$
- f est bijective de E sur $F \Leftrightarrow f$ est injective et surjective de E sur F

Théorème Soit $f : E \to F$ une application

Si E et F sont deux ensembles finis non vides tel que $\boxed{card(E) = card(F)}$ alors on a :

f est injective de E dans $F \Leftrightarrow f$ est surjective de E sur $F \Leftrightarrow f$ est bijective de E sur F

En particulier :

Si E est **un ensemble fini non vide** et $f : E \to E$ une application alors on a :

f est injective de E dans $E \Leftrightarrow f$ est surjective de E sur $E \Leftrightarrow f$ est bijective de E sur E

Théorème (injectivité d'un morphisme de groupes)

Soit $f : (E,*) \to (F,\perp)$ est un morphisme de groupes on a :

1) f est injective de E dans $F \Leftrightarrow Ker(f) = \{e_E\}$ où e_E désigne l'élément neutre de $(E,*)$

2) f est surjective de E sur $F \Leftrightarrow \mathrm{Im}(f) = F$

Preuve à faire en exercice

Exemples pour les morphismes de groupes suivants on a :

1) $f:(\mathbf{Z},+) \to (\mathbf{Z},+)$, $x \mapsto 2x$

on a : *f est injective de* $\mathbf{Z}$ *dans* $\mathbf{Z}$ *car* $Ker(f) = \{0\}$

mais f n'est pas sujective de $\mathbf{Z}$ *sur* $\mathbf{Z}$ *car* $\mathrm{Im}(f) = 2\mathbf{Z}$ *et* $\mathrm{Im}(f) \neq \mathbf{Z}$

2) $g:(Z/4Z,+) \to (Z/4Z,+)$, $\bar{x} \mapsto \bar{3}\bar{x}$ *on a* : $\mathrm{Im}(g) = \langle g(\bar{1}) \rangle = \langle \bar{3} \rangle = Z/4Z$

on a : *g est injective de* $Z/4Z$ *dans* $Z/4Z$ *car* $Ker(g) = \{\bar{0}\}$ *et* $Z/4Z$ *est un ensemble fini*

d'où g est une bijection de $Z/4Z$ *sur* $Z/4Z$ *et par suite* $\mathrm{Im}(g) = Z/4Z$

3) $h:(\Omega_4,\times) \to (\Omega_4,\times)$, $x \mapsto x^2$ *où* $\Omega_4 = \{-1,1,i,-i\} = \langle i \rangle$ *d'où* $f(\Omega_4) = \langle f(i) \rangle = \langle -1 \rangle = \{-1,1\}$

on a : h n'est injective Ω_4 dans Ω_4 car $Ker(h)=\{-1,1\}$ et Ω_4 est un ensemble fini d'où
h n'est pas une bijection de Ω_4 sur Ω_4 et h n'est pas une surjection de Ω_4 sur Ω_4 de plus $\mathrm{Im}(h)=\{-1,1\}$

V. Chiffrement et déchiffrement par un morphisme de groupes (d'un texte, d'une image…)

Le chiffrement classique d'un texte consiste à utiliser une bijection entre l'ensemble des 26 lettres de l'alphabet : il s'agit de remplacer des lettres par d'autres lettres. Par exemple le chiffrement de César consiste simplement à décaler les lettres de l'alphabet de quelques crans vers la droite ou la gauche.
Exemple :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

On peut ainsi chiffrer un message à la main ou écrire un programme de chiffrement sur ordinateur.

De nos jours il y a plusieurs méthodes plus au moins complexes pour chiffrer/déchiffrer un message en utilisant des ordinateurs et par conséquent, il est plus commode d'utiliser des chiffres que des lettres.

On peut utiliser par exemple la bijection suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Par ailleurs il est plus pratique d'utiliser le groupe $(Z/26Z,+)$ que l'ensemble $\{0,1,2,\ldots,25\}$ et utilisez les morphismes de groupes **bijectifs** de la forme : Pour $a\in\mathbf{N}^*$ tel que $p\gcd(a,26)=1$

$$\begin{array}{rccc}\varphi:(Z/26Z,+) & \to & (Z/26Z,+)\\ \overline{x} & \mapsto & \overline{a}\,\overline{x}\end{array}$$