Monoïdes - Groupes

III/ *Groupe*

1. Définition

Un ensemble E muni d'une opération * est un **groupe** si
- La loi $*$ est associative
- E admet un élément neutre pour la loi *
- Chaque élément de E admet un symétrique pour la loi *

Si, de plus, la loi * est commutative, on dit que $(E,*)$ est un **groupe commutatif** ou **groupe abélien**

Exemples de groupes abéliens :

- $(\mathbb{Z},+),(\mathbb{R},+),(\mathbb{C},+)$: 0 est élément neutre. Le symétrique de x est son opposé $-x$
- $(\mathbb{R}^*,\times),(\mathbb{C}^*,\times)$: 1 est élément neutre.

  Le symétrique de x est son inverse $x^{-1}=\frac{1}{x}$. On note alors $\frac{y}{x}=y\,x^{-1}=x^{-1}y$
- Groupe(s) d'ordre 2

+	0	1
0	0	1
1	1	0

*	-1	1
-1	-1	1
1	1	-1

XOR	false	true
false	false	true
true	true	false

o	id	Sym.%O
id	id	Sym.%O
Sym.%O	Sym.%O	id

o	id	Sym.%Ox
id	id	Sym.%Ox
Sym.%Ox	Sym.%Ox	id

- Quelques groupes finis

$(\mathbb{Z}/6\mathbb{Z},+)$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}/5\mathbb{Z}-\{0\},\times)$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Le groupe à 3 éléments

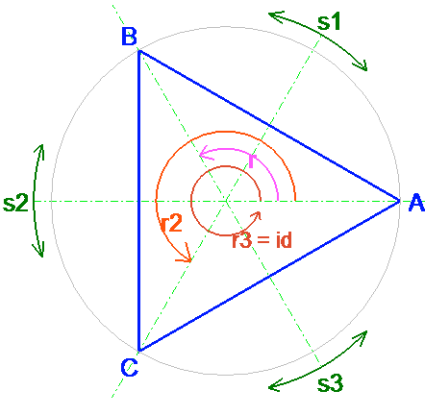
	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Un groupe à 4 éléments

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Exemples de groupes non commutatifs :

- L'ensemble des isométries du plan euclidien $\mathbb{R}^2$ pour la composée.
- L'ensemble des permutations (bijections) d'un ensemble quelconque A.
- L'ensemble $GL(n)$ des matrices $n\times n$ inversibles, pour le produit.
- L'ensemble des fonctions affines non constantes de $\mathbb{R}$ dans $\mathbb{R}$.
- Le groupe des isométries d'un triangle équilatéral pour la composée $\rightarrow$



Contre-exemples :

- $(\mathbb{N},+)$, $(\mathbb{R},\times)$.
- $(\mathbb{Z}/6\mathbb{Z}-\{0\},\times)$
- L'ensemble des fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$.

Rappels : comme dans tout monoïde,

- L'élément neutre est unique. On le note *e* (ou 1 en notation $\times$, ou 0 en notation +)
- Le symétrique d'un élément donné *a* est unique. On le note a^{-1} (ou $-a$ en notation +)
- Tout élément d'un groupe est régulier : $\forall a,x,y \in E$ / $\begin{array}{l} a*x=a*y \Rightarrow x=y \\ \text{et } x*a=y*a \Rightarrow x=y \end{array}$

2. Propriété fondamentale

Soit $(E,*)$ un groupe.

- Pour tous *a* et *b* dans *E*, l'équation $a*x=b$ a une solution unique : c'est $a^{-1}*b$
- Pour tous *a* et *b* dans *E*, l'équation $x*a=b$ a une solution unique : c'est $b*a^{-1}$

Autre formulation :

Pour tout élément *a* de *E*,

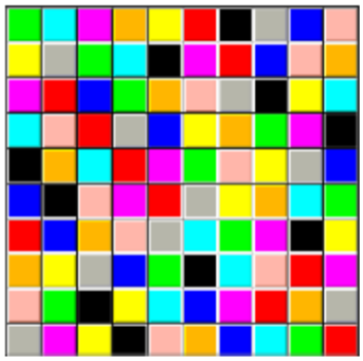
- l'application $\varphi_a : \begin{array}{ccc} E & \to & E \\ x & \to & a*x \end{array}$ est bijective (c'est une permutaion de *E*)

  On l'appelle translation à gauche associée à l'élément *a*
  En notation additive, $\varphi_a(x)=a+x$
- l'application $\psi_a : \begin{array}{ccc} E & \to & E \\ x & \to & x*a \end{array}$ est bijective (c'est une permutaion de *E*)

  On l'appelle translation à droite associée à l'élément *a*
  En notation additive, $\psi_a(x)=x+a$

Corollaire :

Si $(E,*)$ est un groupe fini, sa table de Pythagore est un **carré latin** :
chaque élément figure une fois et une seule dans chaque ligne
et une fois et une seule dans chaque colonne
(mais réciproque fausse)



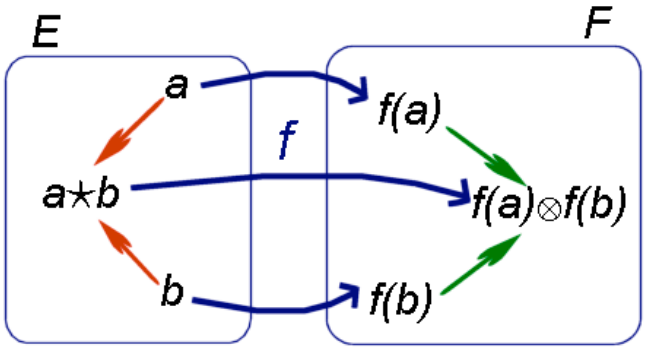
3. Morphisme de groupes

Définition

Soient $(E,\star)$ et $(F,\otimes)$ deux groupes et f une application de E dans F.

f est un **morphisme de groupes** si :

$$\forall a,b\in E\,/\,f(a\star b)=f(a)\otimes f(b)$$



Exemples :

- Si $(E,+)$ est un groupe commutatif, pour tout $n\in\mathbb{Z}$, $\begin{matrix}E & \to & E\\ a & \to & na\end{matrix}$ est un morphisme de groupe

  Mais si le groupe $(E,\times)$ n'est pas commutatif, $\begin{matrix}E & \to & E\\ a & \to & a^n\end{matrix}$ n'est pas un morphisme de groupe

- Si $(E,\star)$ est un groupe , pour tout $a\in E$, $\begin{matrix}\mathbb{Z} & \to & E\\ a & \to & a^n\end{matrix}$ est un morphisme de groupes

- $\begin{matrix}\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z}\\ x & \to & \text{classe de } x \text{ mod n}\end{matrix}$ est un morphisme de groupes additifs.

- Soit $(GL(n),\times)$ le groupe des matrices $n\times n$ inversibles.

  $\begin{matrix}GL(n) & \to & \mathbb{R}^*\\ A & \to & \det(A)\end{matrix}$ est un morphisme du groupe $GL(n)$ (non commutatif) vers $(\mathbb{R}^*,\times)$ (commutatif)

- $x\to\ln(x)$ est un morphisme du groupe multiplicatif $\mathbb{R}_+^*$ vers le groupe additif $\mathbb{R}$.

- $\theta\to e^{i\theta}$ est un morphisme du groupe additif $\mathbb{R}$ vers le groupe multiplicatif $\mathbb{C}^*$.

Propriétés

- Si $f\ (E,\star)\to(F,\otimes)$ est un morphisme de groupes, e l'élément neutre de E, ε celui de F, alors
  - $f(e)=\varepsilon$ (en notation additive, $f(0)=0$)
  - $\forall a\in E\,/\,f(a^{-1})=f(a)^{-1}$ et $\forall n\in\mathbb{Z}\,/\,f(a^n)=f(a)^n$ (en notation additive, $f(na)=nf(a)$)
- La composée de deux morphismes de groupes est un morphisme de groupes.
- La réciproque d'un morphisme de groupes inversible est un morphisme de groupes.

Noyau

Soit $f\ (E,\star)\to(F,\otimes)$ un morphisme de groupes, e l'élément neutre de E, ε celui de F.

Le **noyau** de f est l'ensemble des éléments de E ont l'image par f est ε

Notation $Ker\,f=\{x\in E\,/\,f(x)=\varepsilon\}$

- C'est un sous-groupe de E (voir § 4)
- f est injective si et seulement si $Ker\,f=\{e\}$

Isomorhisme de groupes

Soit f $(E,\star) \to (F,\otimes)$ un morphisme de groupes.

f est un **isomorhisme de groupes** si f est inversible (bijective)

On dit alors que $(E,\star)$ et $(F,\otimes)$ sont **isomorphes**.

Exemples :

- $(\mathbb{Z}/4\mathbb{Z},+)$ et $(\mathbb{Z}/5\mathbb{Z}-\{0\},\times)$ sont isomorphes, mais pas $(\mathbb{Z}/4\mathbb{Z},+)$ et $(G,\star)$

$(\mathbb{Z}/4\mathbb{Z},+)$				
	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}/5\mathbb{Z}-\{0\},\times)$				
	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}/5\mathbb{Z}-\{0\},\times)$				
	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$(G,\star)$				
	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$0 \to 1$, $1 \to 2$, $2 \to 4$, $3 \to 3$

- Le groupe des permutations de $\{A,B,C\}$ est isomorphe au groupe des isométries d'un triangle équilatéral ABC
- Le groupe des permutations de $\{A,B,C,D\}$ n'est pas isomorphe au groupe des isométries d'un carré $ABCD$
- $x \to \ln(x)$ est un isomorphisme de $\mathbb{R}_+^*$ vers $\mathbb{R}$.
- Tous les groupes d'ordre 3 sont isomorphes.
- Si $(E,\star)$ est un groupe , pour tout $a \in E$, $\begin{matrix} E & \to & E \\ x & \to & a^{-1} \star x \star a \end{matrix}$ est un isomorphisme de groupes (automorphisme intérieur)

4. Sous-groupe

Définition

Soient $(E,\star)$ un groupe d'élément neutre e et F une partie de E .

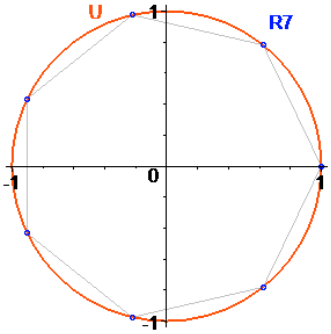
F est un **sous-groupe de *E*** si $(F,\star)$ est un groupe

Condition nécessaire et suffisante

$$F \text{ est un } \textbf{sous-groupe de } \boldsymbol{E} \Leftrightarrow \begin{cases} F \neq \varnothing \\ \forall a,b \in F / a \star b \in F \\ \forall a \in F / a^{-1} \in F \end{cases} \Leftrightarrow \begin{cases} e \in F \\ \forall a,b \in F / a^{-1} \star b \in F \end{cases}$$

$$\text{En notation additive } (F,+) \text{ est un sous-groupe de } (E,+) \Leftrightarrow \begin{cases} F \neq \varnothing \\ \forall a,b \in F / a+b \in F \\ \forall a \in F / -a \in F \end{cases} \Leftrightarrow \begin{cases} e \in F \\ \forall a,b \in F / b-a \in F \end{cases}$$

Exemples



- $(E,\star)$ et $(\{e\},\star)$ sont des sous-groupes (triviaux) de $(E,\star)$.
- Tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, pour un certain entier n.
- L'ensemble U des complexes de module 1 est un sous-groupe de $(\mathbb{C}^*,\times)$
- L'ensemble R_n des racines $n^{\text{ièmes}}$ de l'unité est un sous-groupe de U.
- L'ensemble des translations est un sous-groupe commutatif du groupe (non commutatif) des isométries du plan.
- L'ensemble des matrices orthogonales de déterminant +1 est un sous-groupe de l'ensemble des matrices orthogonales 2×2
- Le noyau d'un morphisme de groupes $(E,\star) \to (F,\otimes)$ est un sous-groupe de E.

Sous-groupe engendré par un élément

Soient $(E,\star)$ un groupe d'élément neutre e et a un élément de E .

Le **sous-groupe engendré par *a*** est l'ensemble des puissances de a.

Notation : $\langle a \rangle = \{ a^n / n \in \mathbb{Z} \} = \{ \ldots, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots \}$

en notation additive : $\langle a \rangle = \{ n\ a / n \in \mathbb{Z} \} = \{ \ldots, -2a, -a, 0, a, 2a, 3a, \ldots \}$

Exemples :

- Pour une rotation r d'angle $2\pi/5$ dans l'ensemble des isométries, $\langle r \rangle = \{ id, r, r^2, r^3, r^4 \}$
- Pour une rotation r d'angle θ tel que $\dfrac{\theta}{\pi}$ n'est pas une fraction, les rotations $\ldots, r^{-2}, r^{-1}, id, r, r^2, r^3, \ldots$ sont toutes distinctes 2 à 2.
- Dans $(\mathbb{Z},+)$, $\langle n \rangle = n\mathbb{Z}$

L'**ordre** d'un élément dans un groupe est l'**ordre** (i.e. le cardinal) du sous-groupe qu'il engendre.

Exemples :

- Dans $(\mathbb{Z}/4\mathbb{Z},+)$, 0 est d'ordre 1 , 1 et 3 d'ordres 4 et 2 d'ordre 2
- Dans $(\mathbb{Z}/5\mathbb{Z}-\{0\},\times)$, 1 est d'ordre 1 , 2 et 3 sont d'ordre 4 et 4 est d'ordre 2

Si un groupe fini est engendré par un élément, on dit que c'est **un groupe cyclique.**
Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

5. Classes suivant un sous-groupe

Soient $(E,\star)$ un groupe et H un sous-groupe de E.

À tout élément $x \in E$ on associe sa **classe à gauche suivant *H*** : $xH = \{x \star a \,/\, a \in H\}$

en notation additive, la classe de x suivant H est $x + H = \{x + a \,/\, a \in H\}$

Exemples

- Soit $n \in \mathbb{Z}^*$. $n\mathbb{Z}$ est un sous-groupe. Il y a n classes :

  classe de $0 = n\mathbb{Z} = \{n\,k \,/\, k \in \mathbb{Z}\}$, classe de $1 = 1 + n\mathbb{Z} = \{n\,k + 1 \,/\, k \in \mathbb{Z}\}$,

  …, classe de $(n-1)$ = classe de $(-1) = n\mathbb{Z} + (n-1) = n\mathbb{Z} - 1$

- Dans le groupe $\{id, r, r^2, s_1, s_2, s_3\}$ des isométries d'un triangle équilatéral,
  - l'ensemble $\{id, r, r^2\}$ des rotations constitue un sous-groupe H. Les classes à gauche sont :

    $id\,H = r\,H = r^2\,H = H$ (les rotations) et $s_1H = s_2H = s_3H = \{s_1, s_2, s_3\}$ (les symétries)
  - l'ensemble $\{id, s_1\}$ constitue un sous-groupe K. Les classes à gauche sont :

    $id\,K = s_1\,K = K$, $s_2K = r^2K = \{s_2, r^2\}$ et $s_3K = rK = \{s_3, r\}$

↗	id	r	r2	s1	s2	s3
id	id	r	r2	s1	s2	s3
r	r	r2	id	s3	s1	s2
r2	r2	id	r	s2	s3	s1
s1	s1	s2	s3	id	r	r2
s2	s2	s3	s1	r2	id	r
s3	s3	s1	s2	r	r2	id

Classes à gauche=classes à droite

↗	id	r	r2	s1	s2	s3
id	id	r	r2	s1	s2	s3
r	r	r2	id	s3	s1	s2
r2	r2	id	r	s2	s3	s1
s1	s1	s2	s3	id	r	r2
s2	s2	s3	s1	r2	id	r
s3	s3	s1	s2	r	r2	id

Classes à gauche

↗	id	r	r2	s1	s2	s3
id	id	r	r2	s1	s2	s3
r	r	r2	id	s3	s1	s2
r2	r2	id	r	s2	s3	s1
s1	s1	s2	s3	id	r	r2
s2	s2	s3	s1	r2	id	r
s3	s3	s1	s2	r	r2	id

Classes à droite

Propriété

Soient $(E,\star)$ un groupe et H un sous-groupe de E.

Les classes à gauche suivant H forment une partition de E en parties équipotentes.

Théorème de Lagrange

Soient $(E,\star)$ un groupe fini et H un sous-groupe de E.

L'ordre de H divise l'ordre de G.

Corollaire

- Dans un groupe fini, l'ordre tout élément est un diviseur de l'ordre du groupe.
- Tout groupe d'ordre égal à un entier premier est cyclique.

6. Indicatrice d'Euler

Définition

Soit n un naturel $\geqslant 2$.

L'indicatrice d'Euler, notée $\varphi(n)$ est le nombre d'entiers compris entre 1 et $n-1$ qui sont premiers avec n

. **Propriété**

$\varphi(n)$ est le nombre d'éléments inversibles du monoïde $(\mathbb{Z}/n\mathbb{Z},\times)$.

C'est donc aussi l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^{\times}$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème d'Euler

Soient n un naturel $\geqslant 2$ et x un naturel premier avec n.

Alors $x^{\varphi(n)} \equiv 1 \bmod n$

Application : RSA (Rivest, Shamir, Adelman 1978)

Clé privée :

2 nombres premiers "grands" p et q , leur produit n, un exposant "de décodage" d premier avec $\varphi(n)$

$x = (p,q,d)$

Clé publique :

Le produit $n = pq$ et l'entier r compris entre 1 et $\varphi(n)-1$ el que $e.d \equiv 1 \bmod \varphi(n)$

$y = (n,e)$

Protocole :

Chaque message M est un entier inférieur à n

Codage : $C_y(M) = M^e \bmod n$

Décodage : $D_x(M) = M^d \bmod n$

$(M^e)^d \equiv M \bmod n$ car $n = p.q$ et que $e.d = k.\phi(n)+1$

			Alice	Bob
Public	Clef de Codage	Exposant :e	4519	3893
		Modulo : n	68557	81493
Privé	Clef de décodage	Exposant : d	3867	2681
		Modulo : n	68557	81493
Pour		p	383	359
mémoire		q	179	227
		$\varphi(n) = (p-1).(q-1)$	67996	80908
			4519 x 3867 = 17474973 = 257 x 67996 + 1	3893 x 2681 =10437133 =129 x 80908 + 1

Exemple : Si Alice envoie à Bob le message $M = 65432$,

$C(M) = 65432^{3893} \bmod 81493 = 40694$, $D(C(M)) = 40694^{2681} \bmod 81493 = 65432$

Si Bob envoie à Alice le message $M = 23456$,

$C(M) = 23456^{4519} \bmod 68557 = 35780$, $D(C(M)) = 35780^{3867} \bmod 68557 = 23456$