Groupes

I/ *Notion de 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 $\frac{y}{x}=yx^{-1}=x^{-1}y$
- 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

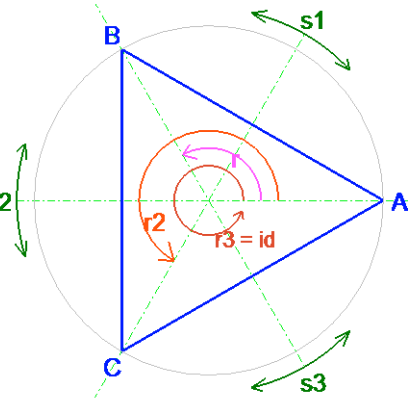
	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

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 $\longrightarrow$



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*,

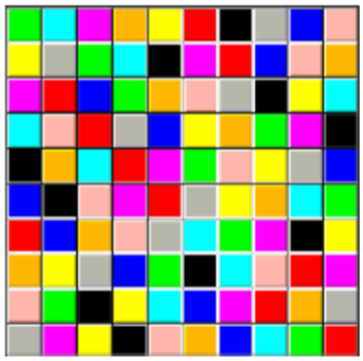
- l'application $\varphi_a : \begin{array}{ccc} E & \to & E \\ x & \to & a*x \end{array}$ est bijective (c'est une permutation de *E*)

  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 permutation 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)



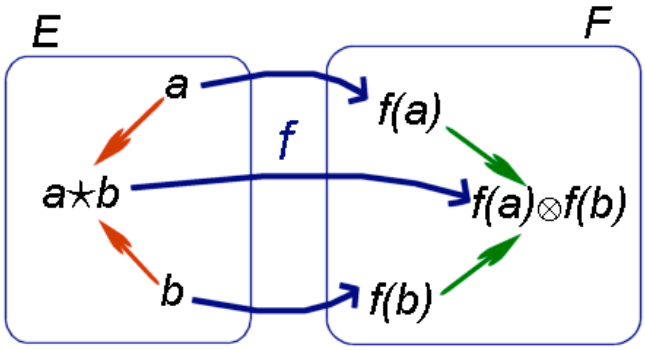
II/ *Morphisme de groupes*

1. 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 $a\in E$, $\begin{matrix}\mathbb{Z}&\to&E\\n&\to&a^n\end{matrix}$ 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 $\mathbb{C}^*$.

2. 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 dont 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 $Ker\,f=\{e\}$

3. 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)
- Le morphisme $\theta \to e^{i\theta}$ du groupe additif $\mathbb{R}$ vers le groupe multiplicatif $\mathbb{C}^*$ n'est pas un isomorphisme.

  Son noyau est l'ensemble des multiples de 2π .

  Son image est le cercle trigonométrique $U = \{z \in \mathbb{C} / |z| = 1\}$

  Mais il induit un isomorphisme entre le groupe (additif) des classes modulo 2π et le groupe (multiplicatif) des complexes de module 1.

III/ *Sous-groupes*

1. Définition

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

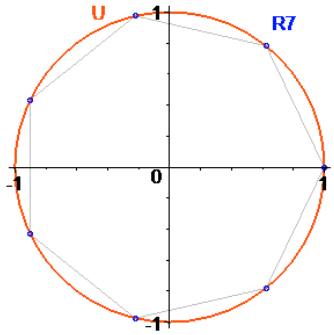
F est un **sous-groupe de *E*** si $(F,\star)$ est un groupe

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.

2. 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 et $\langle r \rangle$ est un groupe multiplicatif isomorphe au groupe $(\mathbb{Z},+)$
- Dans $(\mathbb{Z},+)$, $\langle n \rangle = n\mathbb{Z}$. Ce sont les seuls sous-groupes.

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 $\mathbb{Z}/n\mathbb{Z}$.

3. 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 nombre premier est cyclique.

4. 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 $(\mathbb{Z}/n\mathbb{Z},\times)$.

Démonstration : $\forall k \in \{1 \ldots n-1\}$ / k est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n

En effet k est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists x \in \mathbb{Z} \ / \ k\,x \equiv 1 \bmod n \Leftrightarrow \exists x, y \in \mathbb{Z} \ / \ k\,x + n\,y = 1$

ce qui équivaut, d'après le théorème de Bezout, à $\mathrm{PGCD}(k,n) = 1$

Donc $\varphi(n)$ est 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 $n = p\,q$ 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 $M = 23456$,

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

IV/ *Action d'un groupe sur un ensemble*

1. Définition

Soit $(G,\star)$ un groupe d'élément neutre *e* et *E* un ensemble.

On dit que *G* opère sur *E* quand on a défini une application $\begin{array}{ccc} G\times E & \to & E \\ (g,x) & \to & \varphi_g(x) \end{array}$ telle que

- $\forall x\in E/\varphi_e(x)=x$, c'est-à-dire $\varphi_e=id_E$
- $\forall x\in E\ /\forall g,h\in G\ /\varphi_g(\varphi_h(x))=\varphi_{g\star h}(x)$, c'est-à-dire $\forall g,h\in G\ /\varphi_g\circ\varphi_h=\varphi_{g\star h}$

Remarque :

Pour tout $g\in G$, l'application φ_g est alors une bijection dans *E* (une permutation de *E*)

et l'application $g\longrightarrow\varphi_g$ est un morphisme de groupes entre *G* et le groupe des permutations de *E*

Notation : $\varphi_g(x)$ est parfois noté $g\bullet x$ ou même gx. Les conditions s'écrivent alors :

- $\forall x\in E/e\bullet x=x$
- $\forall x\in E\ /\forall g,h\in G\ /g\bullet(h\bullet x)=(g\star h)\bullet x$

Exemples :

- Soit $(G,\star)$ un groupe. Pour tout $g\in G$ on pose $\varphi_g:\begin{array}{ccc} G & \to & G \\ x & \to & g\star x\star g^{-1}\end{array}$

  G agit ainsi sur lui-même par "conjugaison"
- Soient $(G,\star)$ un groupe et *H* un sous-groupe. Soit *E* l'ensemble des classes à gauche suivant *H*.

  Pour tout $g\in G$ on pose $\varphi_g:\begin{array}{ccc} E & \to & E \\ xH & \to & (g\star x)H\end{array}$. *G* opère ainsi sur les classes à gauche.
- Soit $GL(n)$ le groupe des matrices $n\times n$ inversibles et $M_n(\mathbb{R})$ l'ensemble des matrices $n\times n$.

  $GL(n)$ agit sur $M_n(\mathbb{R})$ en posant pour tout $P\in GL(n)$ $\varphi_P:\begin{array}{ccc} M_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ A & \to & PAP^{-1}\end{array}$
- Soit $GL(\mathbb{R}^2)$ le groupe des isométries vectorielles du plan. $GL(\mathbb{R}^2)$ agit sur le plan $\mathbb{R}^2$ en posant, pour toute isométrie *f* et tout point *M*, $\varphi_f(M)=f.M=$ le point *M* ' tel que $\overrightarrow{OM'}=f\left(\overrightarrow{OM}\right)$

2. Orbite d'un élément

Soit $(G,\star)$ un groupe opérant sur un ensemble *E* et *x* un élément de *E*.

L'orbite de *x* sous l'action de *E* est l'ensemble $Gx=\{\varphi_g(x)\ /\ g\in G\}$. On le note aussi $O(x)$.

Exemples :

- Soient $(G,\star)$ un groupe et *H* un sous-groupe. Soit *E* l'ensemble des classes à gauche suivant *H*.

  G opère sur les classes à gauche par $\varphi_g:\begin{array}{ccc} E & \to & E \\ xH & \to & (g\star x)H\end{array}$

  L'orbite de n'importe quelle classe sous l'action de *G* est l'ensemble *E* de toutes les classes.

  en effet pour tous *x* et *y*, $\varphi_{y\star x^{-1}}(xH)=(y\star x^{-1}\star x)H=yH$

- $GL(n)$ agit sur $M_n(\mathbb{R})$ par $\varphi_P : \begin{matrix} M_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ A & \to & P\,A\,P^{-1} \end{matrix}$

  L'orbite de A sous l'action de $GL(n)$ est l'ensemble des matrices semblables à A

  Cas particulier : Orbite de I_n : ……, Orbite de $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} (a \neq b)$: ……

- $GL(\mathbb{R}^2)$ agit sur le plan $\mathbb{R}^2$, donc il en est de même pour les sous-groupes de $GL(\mathbb{R}^2)$.

  Orbite d'un point sous l'action de $GL(\mathbb{R}^2)$: ……

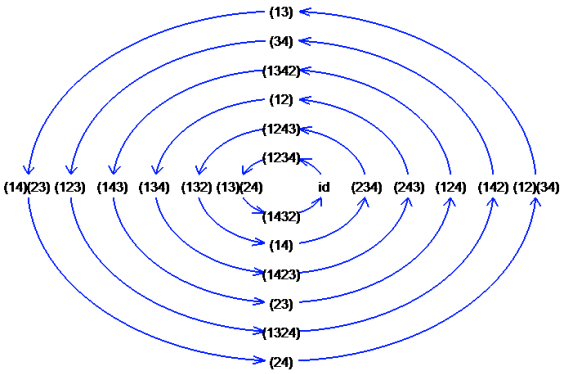
  Orbite d'un point sous l'action du sous-groupe engendré par la rotation d'angle $\frac{2\pi}{n}$: ……

  Orbite d'un point sous l'action du sous-groupe engendré par symétrie d'axe Ox : ……

- Le groupe des applications affines bijectives agit de même sur le plan.
  Orbite d'un point sous l'action du sous-groupe des rotations de centre O : ……
  Orbite d'un point sous l'action du sous-groupe des homothéties de centre O et de rapport > 0 : …
  Orbite d'un point sous l'action du sous-groupe engendré par la translation de vecteur $(1,1)$: ……
  Orbite de l'origine sous l'action du sous-groupe engendré par les translations
  de vecteurs $(1,0)$ et $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$: ……

- S_4 agit sur lui-même par $\varphi_\sigma(s) = \sigma \circ s$

  Les orbites sous l'action du sous-groupe engendré par le cycle $(1,2,3,4)$



Propriétés : Les orbites sous l'action de E forment une partition de E.
En effet la relation $x \mathcal{R} y \Leftrightarrow y \in O(x) \Leftrightarrow \exists g \in G / y = g \star x$ est une équivalence sur E.

3. Stabilisateur d'un élément

Soit $(G, \star)$ un groupe opérant sur un ensemble E et x un élément de E.
Le stabilisateur (ou groupe d'isotropie) de x sous l'action de E est le sous-groupe de G :
$I_x = \{ g \in G / \varphi_g(x) = x \}$. On le note aussi $\text{stab}(x)$.

Exemples

- Soient $(G, \star)$ un groupe et H un sous-groupe. Soit E l'ensemble des classes à gauche suivant H.

  G opère sur les classes à gauche par $\varphi_g : \begin{matrix} E & \to & E \\ xH & \to & (g \star x)H \end{matrix}$

  Le stabilisateur de n'importe quelle classe sous l'action de G est le sous-groupe H.
  En effet $\varphi_y(xH) = xH \Leftrightarrow (y \star x)H = xH \Leftrightarrow (y \star x) \in xH \Leftrightarrow \exists g \in H / y \star x = g \star x \Leftrightarrow y \in H$

- $GL(n)$ agit sur $M_n(\mathbb{R})$ par $\varphi_P : \begin{matrix} M_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ A & \to & PAP^{-1} \end{matrix}$

  Le stabilisateur de A est l'ensemble des matrices qui commutent avec A
- $GL(\mathbb{R}^2)$ agit sur le plan $\mathbb{R}^2$, donc il en est de même pour les sous-groupes de $GL(\mathbb{R}^2)$.

  Le stabilisateur de O est le groupe $GL(\mathbb{R}^2)$ entier.

  Le stabilisateur d'un autre point M est le sous-groupe $\{id, s\}$ où s est la symétrie d'axe OM.
- $GL(\mathbb{R}^2)$ agit de même sur l'ensemble des triangles (non ordonnés) du plan.

  Le stabilisateur d'un triangle équilatéral centré en O est le "groupe du triangle" isomorphe à S_3.
- Tout groupe $(G, \star)$ agit sur lui-même par $\varphi_g(h) = g \star h$

  le stabilisateur de tout élément est le sous-groupe $\{1_G\}$

Propriétés :

- Le stabilisateur d'un élément de E sous l'action de G est un sous-groupe de $(G, \star)$
- Si G est fini, pour tout $x \in E$ le nombre d'éléments de l'orbite de x suivant G est égal à l'ordre de G divisé par l'ordre de son stabilisateur : $Card(O(x)) = \dfrac{\mathrm{Card(G)}}{Card(\mathrm{stab}(x))}$

  Preuve :

  Soit $k = Card(\mathrm{Stab}(x))$

  Soit $y \in O(x)$. On va démontrer qu'il y a exactement k éléments de G tels que $y = \varphi_g(x)$.

  * Il existe un tel g par définition de "$y \in O(x)$"

  * Par ailleurs soient g et $h \in G$ $\varphi_g(x) = \varphi_h(x) \Leftrightarrow \varphi_{h^{-1}}(\varphi_g(x)) = \varphi_e(x) = x = \varphi_{h^{-1} \star g}(x) \Leftrightarrow h^{-1} \star g \in I_x$.

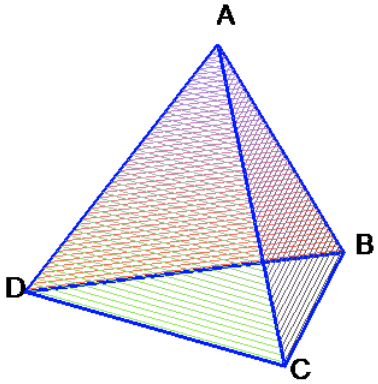
  Donc $\varphi_g(x) = \varphi_h(x) \Leftrightarrow h$ et g appartiennent à la même classe modulo le sous-groupe I_x.

  D'après la formule des classes (III.5.), toutes les classes ont le même cardinal que I_x donc il y a k éléments $h \in G$ tels que $\varphi_g(x) = \varphi_h(x)$.

  La propriété s'en déduit par le principe du berger.
- Corollaire : Si G et E sont finis, soient $O(x_1), O(x_2), ..., O(x_n)$ les orbites de E sous l'action de G.

  Comme les orbites constituent une partition de E, on a $Card(E) = \sum_i \dfrac{Card(G)}{Card(\mathrm{Stab}(x_i))}$

4. Exemple : Groupe des isométries du tétraèdre régulier



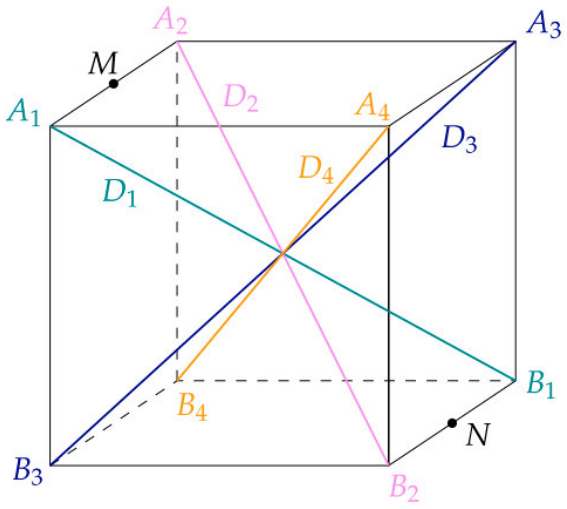
On fait agir le groupe $Isom(T)$ des isométries de l'espace euclidien laissant globalement invariant un tétraèdre régulier T sur l'ensemble des sommets $\{A,B,C,D\}$

On obtient ainsi un morphisme de groupes φ de $Isom(T)$ sur l'ensemble des permutations de $\{A,B,C,D\}$, isomorphe au groupe S_4 des permutations de $\{1,2,3,4\}$

on démontre que φ est un isomorphisme.

Donc $Isom(T)$ est isomorphe à S_4

5. Exemple : Groupe des isométries du cube



Soit $Isom(C)$ le groupe des isométries de l'espace euclidien laissant globalement invariant un cube C.

Soit $Isom^+(C)$ le sous-groupe composé des isométries directes (déterminant +1) : Ce sont les rotations.

Une action de groupe

On fait agir le groupe $Isom(C)$ sur l'ensemble $\{D_1,D_2,D_3,D_4\}$ des 4 "grandes" diagonales.

En effet si une isométrie f laisse le cube globalement invariant, l'image d'une diagonale (segment de longueur $c\sqrt{3}$ joignant 2 sommets) doit être un segment de longueur $c\sqrt{3}$ joignant 2 sommets donc une diagonale.

On obtient ainsi un morphisme de groupes φ de $Isom(C)$ sur le groupe S_4 des permutations de $\{1,2,3,4\}$.

On obtient également un morphisme de groupes ψ du sous-groupe $Isom^+(C)$ sur le groupe S_4

Le noyau de ψ est l'ensemble des rotations laissant chacune des diagonales globalement invariantes.

Si une telle rotation r n'est pas l'identité, supposons (quitte à changer la numérotation) que $r(A_1)=B_1$

Alors on aurait compte tenu de la conservation des distances $r(A_2)=B_2$ et $r(A_4)=B_4$

Comme le centre O est invariant, l'image du repère affine $\left(O,\overrightarrow{OA_1},\overrightarrow{OA_2},\overrightarrow{OA_4}\right)$ serait le repère $\left(O,\overrightarrow{OB_1},\overrightarrow{OB_2},\overrightarrow{OB_4}\right)$ et donc r serait l'homothétie de rapport -1 (symétrie S_O par rapport à l'origine), ce qui est impossible car $\det(S_O)=-1$.

Donc $Ker(\psi)=\{Id\}$ et par suite ψ est injective. Remarque : $Ker(\varphi)=\{Id,S_0\}$

Pour montrer que ψ est surjective, il suffit de montrer que chaque transposition de S_4 est l'image par ψ d'une rotation laissant le cube globalement invariant. En effet toute permutation est produit de transpositions.

Par exemple, pour la transposition $(1,2)$, on cherche une rotation qui amène la diagonale D_1 sur la diagonale D_2 en laissant chacune des diagonales D_3 et D_4 globalement invariantes.

La rotation d'angle π autour de l'axe passant par les milieux des arêtes $[A_1A_2]$ et $[B_1B_2]$ est une solution (d'ailleurs la seule car ψ est injective)

Ainsi ψ est un isomorphisme de $Isom^+(C)$ sur S_4. $Isom^+(C)$ a donc 24 éléments.

$Isom(C)$ est donc composé de 24 rotations et des 24 composées de ces rotations par S_O. Il est d'ordre 48.

$$Isom(C)\cong Isom^+(C)\times\{Id,S_O\}\cong S_4\times\mathbb{Z}/2\mathbb{Z}$$

Les 24 rotations sont :

l'application identité, qui est une rotation (d'angle nul et d'axe quelconque) ;
3 demi-tours d'axe passant par le centre de deux faces opposées (3 axes possibles) ;
6 quart de tours d'axe passant par le centre de deux faces opposées (3 axes possibles et 2 angles possibles) ;
6 demi-tours d'axe passant par les milieux de deux arêtes opposées (6 axes possibles) ;
8 tiers de tours d'axe passant par deux sommets opposés (4 axes possibles et 2 angles possibles).

Les 24 isométries négatives sont respectivement :

la symétrie centrale
3 symétries par rapport à un plan passant par le centre du cube et parallèle à une face (3 plans possibles) ;
6 composées des symétries précédentes avec un quart de tour d'axe perpendiculaire au plan de symétrie (3 plans possibles et 2 angles possibles) ;
6 symétries par rapport à un plan passant par deux arêtes opposées (6 plans possibles) ;
8 composées d'un sixième de tour d'axe passant par deux sommets opposés avec la symétrie par rapport au plan passant par le centre du cube et perpendiculaire à cet axe (4 axes possibles et 2 angles possibles).
Le plan de symétrie intersecte les arêtes du cube en formant un hexagone régulier.

https://www.wikiwand.com/fr/Cube

Un autre point de vue :

Le cube contient 2 tétraèdres réguliers, image l'un de l'autre par l'homothétie S_O de rapport -1 .

Il y a donc 2 sortes d'isométries du cube :

- Celles qui conservent chacun des tétraèdres : ce sont les isométries du tétraèdre.
- Les composées des précédentes par S_O : celles qui envoient chacun des tétraèdres sur l'autre.

Donc $Isom(C)\cong Isom(T)\times\{Id,S_O\}\cong S_4\times\mathbb{Z}/2\mathbb{Z}$