Cours d'Algèbre et géométrie I

Bernard Keller

11/09/2018

Table des matières

Chapitre 1

Groupes

1.1 Motivation

1.1.1 Éléments de symétrie

— 3 symétries orthogonales : σ_A, σ_B, σ_C
— rotation ρ d'angle $\frac{2\pi}{3}$
— rotation ρ^2 d'angle $\frac{4\pi}{3}$
— l'identité
$D_3 = \{Id, \sigma_A, \sigma_B, \sigma_C, \rho, \rho^2\}$ est un groupe diédal.
On peut composer les éléments de l'ensemble D_3 et on restera dans D_3.
La composition est associative.
Elle admet un élément neutre, l'identité.
Chaque élément admet un inverse.

1.2 Définition et premiers exemples

Définition

Un groupe est un couple $(G, *)$, où G est un ensemble et :

$$* : G \times G \to G, (g, h) \mapsto g * h$$

est son appellation telle que :

1. $*$ est associative, c'est à dire :

$$(x * y) * z = x * (y * z)$$

2. $*$ admet un élément neutre e, c'est à dire :

$$e * x = x = x * e$$

3. tout élément $x \in G$ admet un inverse x', c'est à dire :

$$x * x' = e = x' * x$$

Remarques

1. Souvent, on écrit xy au lieu de $x * y$

2. L'élément neutre e est unique : en effet, si e' est un deuxième élément neutre, on a :

$$e = e'e = e'$$

3. L'inverse est unique : en effet, soit x" un deuxième inverse. On a :

$$x'' = ex'' = (x'x)x'' = x'(xx'') = x'e = x'$$

On note désormais x^{-1} l'inverse de x.

4. Pour tous $x, y \in G$, on a $(xy)^{-1} = y^{-1}x^{-1}$.
En effet, on a :

$$(xy)(y^{-1}x^{-1}) = (x(yy^{-1}))x^{-1} = (xe)x^{-1} = e$$
$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}(xy)) = y^{-1}(ey)$$

Définition

Un groupe G est abélien ou commutatif si xy=yx, pour tous $x, y \in G$.

Remarque

Souvent, on notre + la loi de groupe d'un groupe abélien. On note alors 0, l'élément neutre et -x l'élément inverse de $x \in G$.

Exemples

1. $D_3 = \{Id, \sigma_A, \sigma_B, \sigma_C, \rho, \rho^2\}$ n'est pas commutatif car $\sigma_C \circ \sigma_A = \rho$ et $\sigma_A \circ \sigma_C = \rho^{-1} = \rho^2 \neq \rho$.
2. $(\mathbb{Z}, +)$ est un groupe abélien.
3. $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes abéliens.
4. $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ est un groupe abélien pour la multiplication. De même pour $\mathbb{R}^*$ et $\mathbb{C}^*$.
5. Si E est un espace vectoriel sur $\mathbb{R}$ ou $\mathbb{C}$, alors $(E, +)$ est un groupe abélien.
6. Soit $n \geq 1$ un entier, alors l'ensemble $GL_n(\mathbb{R})$ des matrices inversibles $n \times n$ est un groupe pour la multiplication des matrices. Il est abélien ssi n=1.
De même pour $GL_n(\mathbb{Q})$ et $GL_n(\mathbb{C})$.

7. Soit X un ensemble (fini ou infini). Le groupe symétrique σ_X est formé des bijections $f : X \to X$. Sa multiplication est la composition des applications. Son élément neutre est Id_X. L'inverse d'une bijection $f : X \to X$ est la bijection réciproque $f^{-1} : X \to X$. En particulier, pour $n \geq 1$, on a le groupe symétrique :

$$\sigma_n = \sigma_{\{1,2,...,n\}} = \text{groupe de permutations de } \{1, ..., n\}$$

Notons que $|\sigma_n| = n!$.

Notation

Soit G un groupe. Soient $g \in G$ et $n \in \mathbb{N}$.
On note g^n, l'élément de G défini par récurrence :

$$\begin{aligned} g^0 &= e \\ g^{n+1} &= g^n g \ , \ \forall n \geq 0 \end{aligned}$$

Si $n > 0$, on pose $g^{-n} = (g^n)^{-1}$.

Lemme

Soient G un groupe et $m, n \in \mathbb{Z}$. On a $g^{m+n} = g^m g^n$ et $(g^n)^{-1} = g^{-n}$.

Démonstration

Il faut distinguer des cas. Les détails sont laissés en exercice.

Lemme

Soient G et H deux groupes.
Posons :

$$K = G \times H = \{(g, h) | g \in G, h \in H\}$$

Alors K est un groupe pour la loi :

$$K \times K \to K,\ ((g, h), (g', h')) \mapsto (gg', hh')$$

Démonstration

Clairement la loi est associative. Elle admet $e_K = (e_G, e_H)$ pour élément neutre et l'inverse de (g, h) est (g^{-1}, h^{-1}), $\forall g \in G, h \in H$.

Définition

$G \times H$ muni de cette loi est le groupe produit de G par H.

Exercice

$G \times H$ est abélien ssi G et H sont abéliens.

1.3 Sous-groupe

Définition

Soit G un groupe. Un sous-groupe de G est une partie de $H \subseteq G$ telle que :

1. $e_G \in H$
2. $\forall h, h' \in H$, on a $hh' \in H$
3. $\forall h \in H$, on a $h^{-1} \in H$

Notation

On note $H \leq G$ lorsque H est un sous-groupe de G.

Lemme

Une partie $H \subseteq G$ est un sous-groupe ssi $H \neq \emptyset$ et pour tous $h_1, h_2 \in H$, on a $h_1 h_2^{-1} \in H$.

Démonstration

"$\Rightarrow$" $H \neq \emptyset$ car $e_G \in H$. Si $h_1, h_2 \in H$ alors $h_2^{-1} \in H$ (c) et donc $h_1 h_2^{-1} \in H$ (b).
"$\Leftarrow$" Comme H est non vide, on peut choisir un $h \in H$. Alors $hh^{-1} = e_G \in H$. Soient $h_1, h_2 \in H$. On a $h_2^{-1} = eh_2^{-1} \in H$. Donc $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$

Remarque

1. Soit H un sous-groupe de G. Alors la loi de G induit une application $H \times H \mapsto H$, $(h_1, h_2) \mapsto h_1 h_2$ (bien définie par b)). Muni de cette loi, H devient un groupe d'élément neutre $e_H = e_G$. Désormais tout sous-groupe d'un groupe est considéré comme un groupe de cette façon.
2. Si $H \leq G$ et $K \leq H$, alors $K \leq G$

Exemple

Soit G un groupe.

1. e$\leq G$
2. $G \leq G$
3. Posons $Z(G) = \{g \in G | hg = gh, \forall h \in G\}$ Clairement, on a $e \in Z(G)$. On montre ensuite que la multiplication de deux éléments de $Z(G)$ est toujours dans $Z(G)$.
   Enfin, on montre que soient $g \in Z(G)$ et $h \in G$, on a $hg^{-1} = g^{-1}h$, donc $g^{-1} \in Z(G)$.
   Par conséquent, $Z(G)$ est un sous-groupe de G.

Définition

Z(G) est appelé le centre de G.

Exemple

$Z(GL_n(\mathbb{R})) = \mathbb{R}^*.I_n$

Exemples de sous-groupes (suite)

Soit $n \geq 1$. Les parties suivantes sont des sous-groupes de $GL_n(\mathbb{R})$:
— $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | detA = 1\}$
— $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | A^t A = I_n\}$
— $SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O_n(\mathbb{R})$

Notation

$\mathbb{U} = \{z \in \mathbb{C} | |z| = 1\}$
$\mathbb{U}_n = \{z \in \mathbb{C} | z^n = 1\}$ où $n \geq 1$
$\mathbb{U}_n$ = racines n-ièmes de 1
Ce sont des sous-groupes de $\mathbb{C}^*$

Remarque

On a $\mathbb{U}_n \leq \mathbb{U} \leq \mathbb{C}^*$ et $\mathbb{U}_n \leq \mathbb{U}_{mn}$ $\forall n, m \geq 1$.

Notation

Pour $n \in \mathbb{Z}$, on pose :

$$n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$$

Théorème

1. $n\mathbb{Z} \leq \mathbb{Z}$
2. Soit H un sous-groupe de $\mathbb{Z}$. Il existe un et un seul $n \in \mathbb{N}$ tq $H = n\mathbb{Z}$.
   Si $H \neq \{0\}$, alors n est le plus petit entier strictement positif contenu dans H.

Démonstration

1. est clair
2. Soit $H \leq \mathbb{Z}$. Si $H = \{0\}$, alors $H = 0.\mathbb{Z}$. Supposons donc que $H \neq \{0\}$.
   Soit $0 \neq x \in H$. Alors $-x \in H$. Donc H contient au moins un entier strictement positif.
   Soit $E = \{x \in H | x > 0\}$. Alors E est une partie non vide de $\mathbb{N}$.
   Donc il existe dans E un plus petit élément n. Comme $n \in H$, on a $n\mathbb{Z} \subseteq H$.
   Montrons que $n\mathbb{Z} \supseteq H$. Soit $x \in H$. Supposons $x > 0$, alors $x \in E$ et $x \geq n$.

La division euclidienne de x par n s'écrit $x = n.q + r$, où $q, r \in \mathbb{Z}$ et $0 \leq r \leq n$.
Comme x et nq sont dans H, r est dans H.
Or on a $0 \leq r < n$ et n était le plus petit entier positif contenu dans H. Donc r=0 et $x = nq \in n\mathbb{Z}$.
Donc $H = n\mathbb{Z}$. Finalement, si m,n sont des entiers positifs et $m\mathbb{Z} = n\mathbb{Z}$, alors $m = n$.

1.4 Sous-groupe engendré par une partie

Soit G un groupe.

Lemme

Si $(G_i)_{i \in I}$ est une famille de sous-groupes, alors $\cap_{i \in I} G_i$ est encore un sous-groupe.

Démonstration

Exercice facile.

Définition

Soit S une partie de G. Si $S = \emptyset$, on pose $< S >= \{e\}$.
Si $S \neq \emptyset$, on pose :

$$< S >= \cap_{H \ sous-groupe \ tq \ H \supseteq S} H$$

On appelle $< S >$ le sous-groupe engendré par S.

Remarque

$< S >$ est le plus petit des sous-groupe contenant S.

Définition

$S \subseteq G$ est une partie génératrice si $< S >= G$.
G est monogène s'il admet un singleton comme partie génératrice.
G est cyclique s'il est monogène et fini.

Exemples

$(\mathbb{Z}, +)$ est monogène (engendré par S=1) et infini.
$\mathbb{U}_n$, $n \geq 1$, est monogène et fini, donc cyclique.

Lemme

Soit S une partie non vide de G. On a :

$$< S >= \{g_1 g_2 ... g_n | n \in \mathbb{N}, g_i \in S \ ou \ g_i^{-1} \in S \ pour \ tout \ i\}$$

Démonstration

Notons H le membre de droite. Clairement, H est un sous-groupe et contient S. Donc $H \supseteq < S >$.
Soit K un autre sous-groupe contenant S. Alors pour tout $s \in S$, on a $s \in K$ et $s^{-1} \in K$.
Comme K est stable par produit, K contient H donc H est le plus petit sous-groupe de G contenant S, cad $H =< S >$.

1.5 Morphismes de groupes

Définition

Soient G et H deux groupes. Un morphisme de groupes (appelé aussi homomorphisme) est une application $f : G \to H$ tq $f(xy) = f(x)f(y)$ $\forall x, y \in G$

Remarque

Dans ce cas, on a automatiquement $f(e_H) = e_H$ et $f(x^{-1}) = f(x)^{-1}$, $\forall x \in G$
En effet, on a :
$f(e) = f(ee) = f(e)f(e)$. En multipliant à gauche par $f(e)^{-1}$, on trouve $e = f(e)$
$f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e$. En multipliant à droite par $f(x)^{-1}$, on trouve $f(x^{-1}) = f(x)^{-1}$

Exemples

1. $x \mapsto exp(x)$ est un morphisme de groupe de $(\mathbb{R}, +)$ vers $(\mathbb{R}^*, \cdot)$
2. $x \mapsto ln(x)$ est un morphisme de groupe de $(\mathbb{R}^*, \cdot)$ vers $(\mathbb{R}, +)$
3. det : $GL_n(\mathbb{R}) \to \mathbb{R}^*$ est un morphisme de groupes. De même pour $GL_n(\mathbb{C})$ et $GL_n(\mathbb{Q})$
4. Soient E et F deux espaces vectoriels sur $\mathbb{R}$, soit $f : E \to F$ une application linéaire. Alors en particulier, f est un morphisme de groupes de $(E, +)$ vers $(F, +)$.
5. Soient G un groupe et $H \leq G$ un sous-groupe. Alors l'inclusion $H \mapsto G$ est un morphisme de groupe

Théorème

Soit G un groupe. Pour tout $g \in G$, il existe un unique morphisme de groupes $f : (\mathbb{Z}, +) \to G$ tel que $f(1) = g$.

Démonstration

Pour l'existence, posons $f(n) = g^n, n \in \mathbb{Z}$, alors $f(1) = g^1 = g$ et $f(m + n) = g^{n+m} = g^n g^m = f(n)f(m)$ pour tous $n, m \in \mathbb{Z}$
Pour l'unicité, notons que si $n > 1$, on a $f(n) = f(1 + ... + 1) = f(1)...f(1) = g...g = g^n$
On doit aussi avoir $f(0) = e$ et $f(-n) = f(n)^{-1} = g^{-n}$ pur tout $n > 0$.

Théorème

Soient G un groupe et $n \geq 1$. Pour tout $g \in G$ tq $g^n = e$, il existe un unique morphisme de groupes $f : \mathbb{U}_n \to G$ tq $f(c) = g$, où $c = e^{\frac{2\pi i}{n}}$

Démonstration

On a $\mathbb{U}_n = \{1, c, ..., c^{n-1}\}$.
Montrons l'unicité. On doit avoir :

$$f(c^k) = f(c)^k = g^k \qquad \forall 0 \leq k \leq n - 1$$

Pour montrer l'existence, définissons f par cette formule. Vérifions que f est un morphisme.
Soient $0 \leq k \leq n - 1$. Soit $k + l = qn + r$, la division euclidienne de $k + l$ par n. On a :

$$f(c^k c^l) = f(c^{k+l}) = f(c^r) = g^r$$

$$f(c^k)f(c^l) = g^k g^l = g^{k+l} = g^r$$

Lemme

1. La composée de deux morphismes de groupes est un morphisme de groupes .
2. Si $f : G \to H$ est un morphisme de groupes et f est bijectif, alors l'application réciproque $f^{-1} : H \to G$ est encore un morphisme de groupes .

Démonstration

1. Soient $G \xrightarrow{\psi} H \xrightarrow{\varphi} K$ des morphismes de groupes . Pour $x, y \in G$, on a :

$$\varphi\psi(x, y) = \varphi(\psi(xy)) = \varphi(\psi(x)\psi(y)) = \varphi(\psi(x))\varphi(\psi(y)) = \varphi \circ \psi(x) \cdot \varphi \circ \psi(y)$$

2. Soient $x, y \in H$. Il s'agit de monter que :

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$$

Comme f est injective, il suffit de monter que les images par f des deux cotés sont égales. En effet, on a :

$$f(f^{-1}(xy)) = xy \; et \; f(f^{-1}(x)f^{-1}(y)) = xy$$

Définition

Un isomorphisme est un morphisme de groupes bijectif. Deux groupes G et H sont isomorphes s'il existe un isomorphisme $f : G \to H$.
On écrit alors $G \cong H$, et on écrit une flèche $\xrightarrow{\sim}$ pour désigner un isomorphisme.

Exemples

1. On a des isomorphismes inverses l'un de l'autre (exp et ln)
2. Soit $\sigma \in O_2$ tq $\sigma(1) = 2$ et $\sigma(2) = 1$. On a un isomorphisme :

$$\begin{array}{lll} (\{\pm 1\}, \cdot) & \xrightarrow{\sim} & O_2 \\ 1 & \mapsto & Id \\ -1 & \mapsto & \sigma \end{array}$$

3. Soit D_3 le groupe des symétries d'un triangle équilatéral ($D_3 = \{Id, \sigma_A, \sigma_B, \sigma_C, \rho, \rho^2\}$), on a :

$$f : D_3 \xrightarrow{\sim} O_3$$

en envoyant chaque élément de symétrie g sur la permutation des sommets $f(g)$ qu'il induit.

Définition

Soit G un groupe. Un automorphisme de G est un isomorphisme $f : G \to G$.
On note $Aut(G)$ l'ensemble des automorphismes de G. C'est un sous-groupe du groupe symétrique O_G de l'ensemble G.

Exemple

Pour tout $g \in G$, on a l'application de conjugaison par g :

$$cg : G \to G, \; x \mapsto gxg^{-1}$$

C'est un morphisme de groupes car $cg(xy) = cg(x)cg(y)$
C'est bijectif : sa réciproque est cg^{-1} car $cg^{-1}(cg(x)) = x \; \forall x \in G$ et $cg(cg^{-1}(x)) = x \; \forall x \in G$
Donc cg est un automorphisme de G appelé l'automorphisme intérieur associé à g

Propriété

1. L'application $G \to Aut(G)$, $g \mapsto cg$ est un morphisme de groupes
2. L'ensemble des automorphismes intérieurs est un sous-groupe de $Aut(G)$

Démonstration

En exercice

Soient G et H deux groupes et $f : G \to H$ un morphisme.

Définition

Le noyau de f est :

$$Ker(f) = \{g \in G | f(g) = e\} \subseteq G$$

L'image de f est :

$$Im(f) = \{f(g) | g \in G\} \subseteq H$$

Théorème

1. $Ker(f) \leq G$
2. $Ker(f) = \{e\}$ ssi f est injective
3. $Im(f) \leq H$
4. $Im(f) = H$ ssi f est surjective

Démonstration

1. On a $e \in Ker(f)$ car $f(e) = e$. Soient $x, y \in Ker(f)$, alors :

   $$f(xy^{-1}) = f(x)f(y)^{-1} = e.e^{-1}$$

   Donc $xy^{-1} \in Ker(f)$
2. Supposons f injective. Alors $f(g) = e = f(e)$ implique $g = e$. Donc $Ker(f) = \{e\}$.
   Réciproquement, supposons que $Ker(f) = \{e\}$. Soient $x, y \in G$ tq $f(x) = f(y)$.
   Alors $f(xy^{-1}) = f(x)f(y)^{-1} = e$. Donc $xy^{-1} \in Ker(f) = \{e\}$.
   Donc $xy^{-1} = e$ et $x = y$.
3. On a $e = f(e) \in Im(f)$. Soient $f(x), f(y) \in Im(f)$. Alors :

   $$f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in Im(f)$$

4. est clair.

Théorème

1. Soit G' un sous-groupe de G. Alors $f(G')$ est un sous-groupe de $Im(f)$
2. Soit H' un sous-groupe de H. Alors $f^{-1}(H')$ est un sous-groupe de G contenant $Ker(f)$
3. Les applications $G' \mapsto f(G')$ et $H' \mapsto f^{-1}(H')$ sont des bijections inverses l'une de l'autre entre l'ensemble des sous-groupes de G contenant $Ker(f)$ et l'ensemble des sous-groupes de $Im(f)$

Démonstration

1. On a $e = f(e) \in f(G')$. Si $x, y \in G'$ et donc $f(x), f(y) \in f(G')$, alors :
$$f(x)f(y)^{-1} = f(xy^{-1}) \in f(G')$$
2. On a $f(e) = e \in H'$ donc $e \in f^{-1}(H')$.
Soient $x, y \in f^{-1}(H')$, alors :
$$f(xy^{-1}) = f(x)f(y)^{-1} \in H'$$
Donc $xy^{-1} \in H'$.
3. Soit $G' \leq G$ un sous-groupe contenant $Ker(f)$, alors clairement $G' \subseteq f^{-1}(f(G'))$
Réciproquement, soit $x \in f^{-1}(f(G'))$. Alors $f(x) \in f(G')$. Soit $y \in G'$ tq $f(x) = f(y)$.
Alors $y^{-1}x \in Ker(f) \subseteq G'$. Donc :
$$x = y.y^{-1}x \in G'$$
Soit H' un sous-groupe de $Im(f)$. Alors clairement $H' \supseteq f(f^{-1}(H'))$.
Réciproquement, soit $f(g) \in H'$. Alors $g \in f^{-1}(H')$ et $f(g) \in f(f^{-1}(H'))$.

1.6 Ordre d'un élément

Soit G un groupe.

Définition

L'ordre de G est le cardinal $|G|$ de l'ensemble G.

Exemples

1. L'ordre de $(\mathbb{Z}, +)$ est infini
2. L'ordre de $\mathbb{U}_n$ est n

Notation

Pour $g \in G$, on pose $< g >:=< \{g\} >$.

Propriété

Soit $g \in G$. On suppose qu'il existe $n \geq 1$ tq $g^n = e$.

1. On a $< g >= \{g^i | 0 \leq i \leq n-1\}$. En particulier, l'ordre de $< g >$ est $\leq n$
2. Si on note d l'ordre de $< g >$, alors :
$$d = min\{t \geq 1 | g^t = e\}$$

Démonstration

1. " $\supseteq$ " est clair. Réciproquement, on sait que tout élément de $< g >$ est de la forme g^i pour un $i \in \mathbb{Z}$.
Soit $i = qn + r$ la division euclidienne de i par n. Alors on a :
$$g^i = g^{qn+r} = g^r \in \{g^k | 0 \leq k \leq n-1\}$$
2. Posons $s = min\{t \geq 1 | g^t = e\}$. Alors par 1), on a :
$$< g >= \{g^i | 0 \leq i \leq s-1\}$$
Pour $0 \leq i < j \leq s-1$, les puissances g^i et g^j sont distinctes. Sinon, on aurait $g^{j-i} = e$ mais $j - i < s$. Donc $s = | < g > | = d$.

Définition

Soit $g \in G$. Si $< g >$ est infini, l'ordre de g est infini.
Si $< g >$ est fini, l'ordre de g est le plus petit entier $d \geq 1$ tq $g^d = e$

Remarque

1. Donc on a que l'ordre de g est égale à l'ordre de $< g >$
2. Si $d < \infty$ est l'ordre de G, alors :

$$d\mathbb{Z} = \{n \in \mathbb{Z} | g^n = e\}$$

3. Etant donné $t \geq 1$, l'élément g est d'ordre t ssi $g^t = e$ et $g^{t'} \neq e$ pour tout diviseur strict t' de t.

Exemple

Soient $n \geq 1$ et $k \in \mathbb{Z}$. Soit $c = e^{\frac{2\pi i}{n}} \in \mathbb{U}$.
Alors $c^k \in \mathbb{U}_n$ est d'ordre $\dfrac{ppcm(n,k)}{k}$

Théorème de Lagrange

Soit G un groupe fini. Alors, l'ordre de tout sous-groupe $G' \leq G$ divise l'ordre de G.

Corollaire

Soit G un groupe fini, alors tout élément $g \in G$ est d'ordre fini et son ordre divise l'ordre de G.

Conséquence

Soit G un groupe fini dont l'ordre est un nombre premier.
Alors tout sous-groupe de G est égal à G ou à $\{e\}$.
En particulier, si $e \neq g \in G$, alors $G =< g >$. Donc G est cyclique.

Démonstration

Soit H un sous-groupe de G.
Pour $g \in G$, on pose :

$$gH = \{gh | h \in H\}$$

alors $|gH| = |H|$, $\forall g \in G$, car on a les bijections réciproques l'une de l'autre.
Montrons que pour tous $g, g' \in G$, on a :

$$gH \cap g'H \neq 0 \Rightarrow gH = g'H$$

En effet, si on a $gh = g'h'$, pour $h, h' \in H$, alors pour $h'' \in H$, on a :

$$gh'' = g'g'^{-1}gh'' = g'h'h^{-1}h'' \in g'H$$

Donc $gH \subseteq g'H$ et de même $g'H \subseteq gH$. Donc $gH = g'H$.
Notons que la réunion des gH, $g \in G$, est G car $g = g.e \in gH$, pour $g \in G$. Il s'ensuit que $\{gH | g \in G\}$ est une partition de G.
Chaque gH a le même nombre d'éléments : $|H|$
Donc

$$|G| = |H|.|\{gH | g \in G\}|$$

1.7 Les treillis des sous-groupes

Définition

Soit X un ensemble. Une relation R sur X est un sous-ensemble $R \subseteq X \times X$.
On note xRy ("x est en relation avec y") lorsque $(x, y) \in R$.

Définition

Une relation R est une relation d'ordre ssi :
— (réflexivité) $\forall x \in X$, xRx
— (antisymétrique) $\forall x, y \in X$ $(xRy \ et \ yRx) \Rightarrow x = y$
— (transitive) $\forall x, y, z \in X$ $(xRy \ et \ yRz) \Rightarrow xRz$

Définition

Un ensemble (X, R) muni d'une relation d'ordre s'appelle un ensemble ordonné.

Exemple

1. $(\mathbb{R}, \leq)$ est un ensemble ordonné.
2. Soit $n \geq 1$, X l'ensemble des diviseurs positifs de n, avec R la relation $xRy \Leftrightarrow x \ divise \ y$, est un ensemble ordonné.
3. X un ensemble, $P(x)$ l'ensemble des parties de X avec $ARB \Rightarrow A \subseteq B$

Définition

Soit (X, R) un ensemble ordonné et soit $A \subseteq X$ un ensemble. Un minorant (resp majorant) de A est un $x \in X$ tq xRa $\forall a \in A$ (resp aRx, $\forall a \in A$), le plus petit (resp le plus grand) élément de A est un minorant (resp un majorant) qui est dans A.

Dorénavant notons $\leq$ toute relation d'ordre sur un ensemble X.

Définition

Un treillis est un ensemble ordonné $(X, \leq)$ tq $\forall (x, y) \in X \times X$ il existe dans X un plus petit majorant $Sup(x, y)$ de $\{x, y\}$ et un plus grand minorant $Inf(x, y)$ de $\{x, y\}$.

Exemples

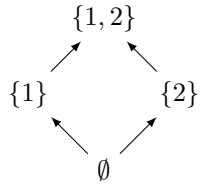
1. $(\mathbb{R}, \leq)$ est un treillis (évident)
2. Soit $n \geq 1$ un entier, $X = \{d \in \mathbb{N} | d \ divise \ n\}$ muni de $x \leq y \Leftrightarrow x|y$ est un treillis pour $sup(k, l) = ppcm(k, l)$ (qui est encore un diviseur de n) et $inf(k, l) = pgcd(k, l)$
3. X un ensemble, $P(x)$ l'ensemble des parties de X. $(P(x), \subseteq)$ est un treillis avec $A, B \in P(x)$ $sup(A, B) = A \cup B$ et $inf(A, B) = A \cap B$
4. V un K-espace vectoriel , K un corps $(\mathbb{R}, \mathbb{C}, ...)$, $Gr(V)$ l'ensemble des sous K-espace vectoriel de V est un treillis pour $\subseteq$ car :
   $\forall U, W \in Gr(V)$ $sup(U, W) = \{u + w \in V | u \in U, w \in W\}$ est le plus petit sous espace vectoriel de V qui contient U et W, et $inf(U, W) = U \cap W$ est le plus grand sous espace vectoriel de V inclus dans U et dans V.
5. G un groupe, $L(G)$ l'ensemble des sous-groupes de G est un treillis pour $\subseteq$ car :
   $H, H' \in L(G)$ $sup(H, H') =< H, H' >$ (groupe engendré par H et H'), et $inf(H, H') = H \cap H'$

Définition

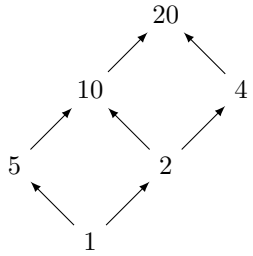
Soit $(X, \leq)$ un treillis. Son diagramme de Hasse est le graphe orienté où :
— les sommets sont les éléments $x \in X$
— on met une flèche $x \to y$ si y est minimal parmi les éléments $\geq x$ distincts.

Exemple

1. $(P(\{1,2\}, \subseteq))$:



2. $(X = \{\text{ensemble des diviseurs de } 20\}, |)$, on a $X = \{1, 2, 4, 5, 10, 20\}$:



Lemme

Soit $n \geq 1$ un entier, $\zeta = e^{\frac{2i\pi}{n}} \in \mathbb{U}_n$.
Les sous-groupes de $\mathbb{U}_n$ sont exactement les $\zeta^{d\mathbb{Z}}$ avec $d|n$. De plus $\zeta^{d\mathbb{Z}} \subseteq \zeta^{d'\mathbb{Z}} \Leftrightarrow d'|d$

Démonstration

Soit $e : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{U}_n \\ k & \mapsto & \zeta^k \end{array}$.
C'est un morphisme de groupes. Donc $\forall H$ sous-groupe de $\mathbb{U}_n$, $e^{-1}(H) = \{k \in \mathbb{Z} | e(k) \in H\}$ est un sous-groupe de $\mathbb{Z}$.
De plus $e^{-1}(H) \supseteq e^{-1}(1)$ (car $1 \in H$).
On connaît les sous-groupes de $\mathbb{Z}$: les $d\mathbb{Z}$.
$\exists d \in \mathbb{N}$ tq $e^{-1}(H) = d\mathbb{Z}$ donc $e^{-1}(1) = \{k \in \mathbb{Z} | \zeta^k = e^{\frac{2i\pi k}{n}} = 1\} = n\mathbb{Z}$
Donc $n \in n\mathbb{Z} \subseteq d\mathbb{Z} \Rightarrow d|n$. Donc $H = \zeta^{d\mathbb{Z}}$ avec $d|n$.

$$\zeta^{d\mathbb{Z}} \subseteq \zeta^{d'\mathbb{Z}} \Leftrightarrow d\mathbb{Z} \subseteq d'\mathbb{Z} \Leftrightarrow d'|d$$

Exemple

1. Treillis de $\mathbb{U}_{20}$:
   D'après le lemme précédent, les sous-groupes de $\mathbb{U}_{20}$ sont $< \zeta^{20} >, < \zeta^{10} >, < \zeta^5 >, < \zeta^4 >, < \zeta^2 >, < \zeta^1 >$:
   prendre une photo du diagramme de Hasse
2. Treillis des sous-groupes de $D_3 = \{Id, \sigma_A, \sigma_B, \sigma_C, \rho, \rho^2\}$.
   Soit H un sous-groupe de D_3, $|H| \in \{1, 2, 3, 6\}$, donc on a :
   — $|H| = 1 \Rightarrow H = \{Id\}$
   — $|H| = 2 \Rightarrow H =< \sigma_A >, < \sigma_B >, < \sigma_C >$
   — $|H| = 3 \Rightarrow H =< \rho >, < \rho^2 >$

image du diagramme de Hasse

3. Treillis des sous-groupes de D_4, on pose :
   — τ_i la réflexion par rapport à Δ_i
   — ρ la rotation d'angle $\frac{2\pi}{4}$
   On a $D_4 = \{Id, \rho, \rho^2, \rho^3, \tau_1, \tau_2, \tau_3, \tau_4\}$.
   Soit H un sous-groupe de D_4, $|H| \in \{1, 2, 4, 8\}$, donc on a :
   — $|H| = 1 \Rightarrow H = \{Id\}$
   — $|H| = 2 \Rightarrow H =< \rho^2 >, < \tau_1 >, < \tau_2 >, < \tau_3 >, < \tau_4 >$
   — $|H| = 4 \Rightarrow H =< \rho >, < \tau_1, \tau_3 >, < \tau_2, \tau_4 >$
   image du diagramme de Hasse

Chapitre 2

Actions de groupes

2.1 Relations d'équivalence

Définition

X un ensemble. Une relation R sur X est une relation d'équivalence ssi :

1. (réflexivité) $\forall x \in X \ xRx$
2. (symétrie) $\forall x, y \in X \ xRy \Leftrightarrow yRx$
3. (transitivité) $\forall x, y, z \in X \ (xRy \ et \ yRz) \Rightarrow xRz$

Exemples

Soit G un groupe.

1. $H \subseteq G$ un sous-groupe. On définit $g, g' \in G \ g \sim_H g'$ si $\exists h \in H | g' = gh$. C'est une relation d'équivalence.
2. $\forall g, g' \in G$, on définit $g \sim g'$ si $\exists x \in G | g' = xgx^{-1}$. C'est une relation d'équivalence.
3. $X = L(G)$ l'ensemble des sous-groupes de G avec la relation $H \sim H'$ si $\exists g \in G | H' = gHg^{-1}$

Définition

Soit (X, R) un ensemble muni d'une relation d'équivalence.
La classe d'équivalence de $x \in X$ est $\bar{x} = \{y \in X | xRy\}$.
Le quotient de X par R est $X/R = \{\bar{x} | x \in X\}$.
L'application $\begin{array}{ccc} X & \to & X/R \\ x & \mapsto & \bar{x} \end{array}$ s'appelle la surjection canonique.

Exemple

Dans le cas 1) de l'exemple précédent, $g \in G$, $\bar{g} = \{gh | h \in H\} = gH$ et on note $G/\sim_H = G/H$.
G/H n'est pas un groupe en général.

Propriété

1. X/R est une partition de X
2. $\forall x, y \in X \ xRy \Leftrightarrow \bar{x} = \bar{y}$

Démonstration

1. Soit $\bar{x}, \bar{y} \in X/R$. Supposons $\bar{x} \cap \bar{y} \neq \emptyset$ et montrons que $\bar{x} = \bar{y}$.
   $\exists z \in \bar{x} \ et \ z \in \bar{y}$.
   Montrons que $\bar{x} \subseteq \bar{y}$:
   Soit $z' \in \bar{x}$, $z'Rz$ et $zRz' \Rightarrow z'Ry \Rightarrow z' \in \bar{y}$.

On montre que $\bar{y} \subseteq \bar{x}$ par un raisonnement identique.
Cela montre que les classes d'équivalences sont disjointes ou confondues.
Et $\forall x \in X \ x \in \bar{x}$. Donc les classes d'équivalences forment une partition de X.

2. "$\Rightarrow$" Supposons xRy, soit $z \in \bar{x}$, on a $zRy \ z \in \bar{y}$.
   Donc de même, on a $\bar{y} \subseteq \bar{x}$. Donc $\bar{x} = \bar{y}$
   "$\Leftarrow$" Supposons $\bar{x} = \bar{y}$, $y \in \bar{y} = \bar{x}$, $y \in \bar{x}$, donc yRx.

Théorème

Soit (X, R) un ensemble avec une relation d'équivalence.
Soit π la surjection canonique.
Soit f une application de X dans Y. Les assertions suivantes sont équivalentes :

1. $(\forall x, y \in R \ xRy \Rightarrow f(x) = f(y))$
2. $(\exists! \bar{f} : X/R \to Y$ telle que $f = \bar{f} \circ \pi)$

Démonstration

Supposons 1).

— unicité de $\bar{f}$:
Si $\bar{f}_1$ et $\bar{f}_2$ vérifient $\bar{f}_1 \circ \pi = f = \bar{f}_2 \circ \pi$.
Soit $\bar{x} \in X/R \ \bar{x} = \pi(x)$, et on a :

$$\bar{f}_1(\bar{x}) = (\bar{f}_1 \circ \pi)(x) = f = (\bar{f}_2 \circ \pi)(x) = \bar{f}_2(\bar{x})$$

— Existence de $\bar{f}$:
Soit $\chi \in X/R, \ \exists x \in X | \pi(x) = \bar{x} = \chi$.
On pose $\bar{f}(\chi) = f(x)$. Cette définition est indépendante du choix de x, car :
si $y \in X$ vérifie $\pi(y) = \chi \Rightarrow \pi(x) = \pi(y)$
D'après le lemme , on a $xRy \Rightarrow f(x) = f(y)$. Donc cette définition définit une application $\bar{f} : X/R \to Y$ et elle vérifie $f = \bar{f} \circ \pi$ par construction.

Supposons 2). Soit $x, y \in X, xRy \Rightarrow \pi(x) = \pi(y) \Rightarrow (\bar{f} \circ \pi)(x) = (\bar{f} \circ \pi)(y) \Rightarrow f(x) = f(y)$

Remarques

Lorsque f vérifie 1) du théorème, on dit que f passe au quotient par R et que $\bar{f}$ est induite par f.

Lemme

Soit (X, R), f vérifiant les assertions du théorème précédent :

1. $\bar{f}$ est surjective $\Leftrightarrow$ f l'est aussi
2. $\bar{f}$ est injective $\Leftrightarrow (\forall x, y \in X, \ f(x) = f(y) \Rightarrow xRy)$

Démonstration

1. Supposons $\bar{f}$ surjective, $f = \bar{f} \circ \pi$, or $\bar{f}$ et π sont surjectives.
   Supposons f surjective, soit $y \in Y$, $\exists x \in X | f(x) = \bar{f}(\pi(x)) = y$, $\bar{f}$ est surjective.
2. à faire en exercice

Propriété

Soit $n \geq 1$ entier, soit $e : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{U}_n \\ k & \mapsto & e^{\frac{2\pi i k}{n}} \end{array}$.
Soit R la relation d'équivalence $xRy \Leftrightarrow n | x - y$.
Notons $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/R$, alors e induit une bijection $\bar{e} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$ avec $e = \bar{e} \circ \pi$

Démonstration

L'existence de $\bar{e}$ découle du théorème et de $xRy \Leftrightarrow n|x-y \Leftrightarrow \exists k \in \mathbb{Z}|x = y + nk$.
Ceci implique que $e(x) = e(y)$.
La surjection de $\bar{e}$ découle du lemme et de la surjectivité de e.
L'injection de $\bar{e}$ découle de $\forall x, y \in \mathbb{Z}\ e(x) = e(y) \Leftrightarrow xRy$, et du lemme.

2.2 Définition d'une action de groupe

Définition

Soient X un ensemble, G un groupe. Une action de G sur X est une application $\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \to & g.x \end{array}$ telle que :

1. $\forall x \in X\ e.x = x$
2. $\forall g, h \in G\ \forall x \in X\ (gh).x = g.(h.x)$

Définition

Un G-ensemble est un ensemble muni d'une action du groupe G.

Exemple

1. Le groupe diédral $D_3 = \{Id, \sigma_A, \sigma_B, \sigma_C, \rho, \rho^2\}$ agit sur l'ensemble $\{1,2,3\}$ des sommets du triangle équilatéral.
2. Le groupe symétrique σ_n agit sur l'ensemble $X = \{1, \cdots, n\}$ par $\sigma.x := \sigma(x),\ \forall \sigma \in \sigma_n,\ \forall x \in X$.

   Soit G un groupe.
3. Soit $H \subseteq G$ un sous-groupe. Alors H agit sur G par :

   $$H \times G \to G,\ (h,g) \mapsto hg$$

   On appelle cette action, l'action de H sur G, par transition à gauche.
4. L'application $G \times G \to G,\ (g,x) \mapsto gxg^{-1}$ est une action de G sur lui-même (en effet, on a $e.x = e.x.e^{-1} = x$, $\forall x \in G$ et $(gh).x = ghx(gh)^{-1}g(hxh^{-1})g^{-1} = g(hx),\ \forall g, h \in G, \forall x \in G$).
   On l'appelle l'action de conjugaison de G sur lui-même.
5. Soit X l'ensemble des sous-groupes de G. L'application :

   $$G \times X \to X,\ (g,K) \mapsto gKg^{-1}$$

   est une action de groupe. On l'appelle l'action de conjugaison de G sur l'ensemble de ses sous-groupes.
6. Soit $n \geq 1$. L'application :

   $$GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n,\ (g,v) \mapsto g(v)$$

   est une action de groupe.
7. Soit $n \geq 1$. L'application :

   $$\begin{array}{ccc} GL_n(\mathbb{R}) \times M_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ (P,M) & \mapsto & PMP^{-1} \end{array}$$

   est une action de groupe de $GL_n(\mathbb{R})$ sur $M_n(\mathbb{R})$.

Propriété

Soient G un groupe et X un ensemble.

1. Une action de G sur X : pour tout $g \in G$, soit $\varphi_g : X \to X$ l'application $x \mapsto gx$, alors $\varphi_g \in \sigma_X$ et l'application $G \to \sigma_X,\ g \mapsto \varphi_g$ est un morphisme de groupes.
2. Soit $f : G \to \sigma_X$ est un morphisme de groupes. Alors il existe une unique action de G sur X tq :
$$g.x = (f(g))(x), \quad \forall g \in G, \forall x \in X$$
Comme le montre la proposition, on a une bijection naturelle entre l'ensemble des actions de G sur X et l'ensemble des morphismes de groupes de G vers σ_X

Démonstration

1. Pour tout $g \in G$, l'application φ_g est bijective de réciproque $\varphi_{g^{-1}}$ car :
$$\varphi_g \varphi_{g^{-1}}(x) = \varphi_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = ex = x$$
et de la même façon :
$$\varphi_{g^{-1}} \varphi_g(x) = ex = x$$
On a pour $g, h \in G$:
$$\varphi_{gh}(x) = (gh)(x) = g(hx) = \varphi_g \circ \varphi_h(x), \quad \forall x \in X$$
Donc l'application $g \mapsto \varphi_g$ est bien un morphisme de groupe $G \to \sigma_X$
2. On définit l'application $G \times X \to X$ par $g.x = (f(g))(x), \quad \forall g \in G, \forall x \in X$, vérifions qu'il s'agit d'une action.
$$ex = (f(e))x = Id_X(x) = x, \quad \forall x \in X$$
et
$$g(hx) = f(g(hx)) = f(g)(f(h)(x)) = (f(g) \circ f(h))(x) = f(gh)(x) = gh.x$$
pour tous $g, h \in G$ et tout $x \in X$

Définition

Soient G un groupe et X un ensemble. Une action à droite de G sur X est une application :
$$X \times G \to X,\ (x, g) \mapsto xg$$
telle que :

1. $x.e = x,\ \forall x \in X$
2. $x.(gh) = (xg).h,\ \forall g, h \in G,\ \forall x \in X$

Exemple

Soit $n \geq 1$, alors l'application :
$$\begin{array}{lll} M_n(\mathbb{R}) \times GL_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ (P, M) & \mapsto & MP \end{array}$$
est une action à droite de $GL_n(\mathbb{R})$ sur $M_n(\mathbb{R})$.

Remarque

Soit X un ensemble muni d'une action à droite d'un groupe G. On définit $g.x := x.g^{-1}$ $\forall g \in G$. C'est une action à gauche de G sur X car :

$$ex = xe^{-1} = xe = x$$

et

$$(gh)x = x.(gh)^{-1} = x(h^{-1}g^{-1}) = (xh^{-1})g^{-1} = (hx)g^{-1} = g(hx)$$

$\forall x \in X,\ \forall g, h \in G$.
On obtient ainsi une bijection entre les actions à droite de G sur X et les actions à gauche de G sur X.

2.3 Orbites et stabilisateurs

Soient G un groupe et X un G-ensemble.
Récupérer une photo du graphe.

Définition

Pour $x \in X$, l'orbite de x est :

$$G.x = \{gx | g \in G\}$$

Le stabilisateur de x est :

$$Stab_G(x) = G_x = \{g \in G | gx = x\}$$

Remarque

1. Soit $x \in X$. L'orbite $G.x$ contient $x = e.x$. Le stabilisateur G_x est un sous-groupe car $e.x = x$, et $g(hx) = gx = x$, $\forall g, h \in G_x$, et si $g \in G_x$ alors $g^{-1} \in G_x$ car $g^{-1}x = x \Leftrightarrow g(g^{-1}x) = gx \Leftrightarrow ex = x$.
2. On définit de façon analogue les orbites et stabilisateurs d'une action à droite.

Exemple

Soit $H \subseteq G$ un sous-groupe.

1. Pour l'action $H \times G \to G,\ (h, g) \mapsto hg$, l'orbite d'un $g \in G$ est Hg, la classe à gauche modulo H de g.
   Le stabilisateur de $g \in G$ est formé des $h \in H$ tq $hg = g \Leftrightarrow h = e$. Donc $Stab_H(g) = \{e\}$.

2. Pour l'action à droite :
   $$G \times H \to G,\ (g, h) \mapsto gh$$
   l'orbite de $g \in G$ est la classe à droite gH. En outre, $Stab_H(g) = \{e\}$

Propriété - Définition

Soit $\sim$ la relation sur X tq :

$$x \sim y \Leftrightarrow y \in G_x$$

Alors $\sim$ est une relation d'équivalence sur X appelée la relation d'équivalence associée à l'action de G sur X.

Démonstration

On vérifie que $\sim$ est :
— réflexive : $x \sim x$ car $x = ex$
— symétrique : $x \sim y \sim y \sim x$ car $y = gx \Leftrightarrow g^{-1}y = x$
— transitive : Si $x \sim y$ et $y \sim z$, alors $x \sim z$ car si $y = gx$ et $z = hy$, alors $z = hy = h(gx) = (hg)x$

Remarque

Pour tout $x \in X$, la classe d'équivalence de x est égale à l'orbite $G.x$.

Définition

Le quotient de X par G est l'ensemble $G\backslash X := X/\sim$ formé des orbites de G dans X.

Remarque

On définit de façon analogue la relation d'équivalence et l'ensemble quotient d'une action à droite de G sur X.
L'ensemble quotient est alors noté X/G.

Propriété

L'ensemble des orbites est une partition de X.

Démonstration

En effet, ce sont des classes d'équivalence pour une relation d'équivalence.

Définition

Soit X un G-ensemble non-vide.
L'action de G sur X est :

— transitive s'il n'y a qu'une seule orbite
— fidèle si $\forall g \in G$, on a :

$$gx = x,\ \forall x \in X \Rightarrow g = e$$

— libre si tous les stabilisateurs sont triviaux ($Stab_G(x) = \{e\},\ \forall x \in X$).

Remarque

1. On définit de façon analogue les notions correspondantes pour les actions à droite.
2. L'action de G sur X est transitive ssi $G\backslash X$ est un singleton.
3. L'action de G sur X est fidèle ssi le morphisme associé $G \to \sigma_X$ a pour noyau $\{e\}$, c'est à dire ssi $G \to \sigma_X$ est injectif.

Exemple

1. Pour tout sous-groupe H de G, l'action de H sur G par translations à gauche (ou à droite) est libre (car $Stab_H(g) = \{h \in H | hg = g\} = \{e\}$), donc fidèle.
   Elle est transitive ssi $H = G$ (s'il n'y a qu'une seule orbite, elle est égale à G, donc G est l'orbite sous H de e mais cette orbite est $H.e = H$)
2. Soit $n \geq 1$. Considérons l'action :

   $$GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n,\ (g, v) \mapsto gv$$

   L'orbite d'un vecteur $v \neq 0$ est $\mathbb{R}^n\backslash\{0\}$ (en effet si $v1, ...v_n$ est une base tq $v_1 = v$ et $w_1, ..., w_n$ est une base tq $w_1 = w \neq 0$, il existe un unique $g \in GL_n(\mathbb{R})$ tq $g(v_i) = w_i$, $\forall i$, en particulier $gv = w$).
   L'orbite de $v = 0$ est $\{0\}$.
   Il y a donc exactement 2 orbites : $\mathbb{R}^n\backslash\{0\}$ et $\{0\}$.
   Donc l'action n'est pas transitive.
   Elle est fidèle (car si $gv = v\ \forall v$, alors $ge_i = e_i$, pour $i \in [|1, n|]$ et $g = Id$).
   Elle n'est pas libre car $Stab_{GL_n(\mathbb{R})}(0) = GL_n(\mathbb{R})$
3. L'action $GL_n(\mathbb{R}) \times \mathbb{R}^n* \to \mathbb{R}^n*,\ (g, v) \mapsto gv$ est transitive, fidèle et non libre. En effet, $Stab_{GL_n(\mathbb{R})}(e_1) = [e_1, *, *, ..., *]$ avec * des vecteurs quelconques.

4. Soit $C = \{(x_1, x_2, x_3) \in \mathbb{R} | \forall i \text{ on a } x_1 = \pm 1\}$ l'ensemble des sommets d'un cube de $\mathbb{R}^3$ contré en l'origine. Soit $G = \{g \in O_3(\mathbb{R}) | g(C) = C\}$ (O_n est l'ensemble des matrices orthogonales de taille $n \times n$).
L'action :
$$G \times C \to C, (g, x) \mapsto gx$$
est transitive (combiner des rotations et des symétries).
Elle est fidèle (les vecteurs $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$ forment une base de $\mathbb{R}^3$).
Elle n'est pas libre (la rotation d'angle $\frac{2\pi}{3}$ et d'axe $\mathbb{R} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ est dans G et dans le stabilisateur de $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$).

2.4 Aspects numériques

Soit G un groupe et soit X un G-ensemble (ensemble muni d'une action de G).

Théorème

Soit $x \in X$. Soit $\pi : G \to G/Stab_G(x)$ la projection canonique.
Il existe une et une seule application :

$$\varphi : G/Stab_G(x) \to G.x$$

telle que $\varphi \circ \pi(g) = gx$ pour tout $g \in G$.
Cette application est bijective.

Démonstration

Soit $H = Stab_G(x)$. Comme π est surjective, l'application φ, si elle existe, est unique.
Soient $g \in G$ et $h \in H$. On a :

$$(gh)x = g(hx) = gx \qquad\qquad h \in Stab_G(x)$$

Donc l'application $\tilde{\varphi} : G \to G.x$ vérifie$\tilde{\varphi}(gh) = \tilde{\varphi}(g), \forall h \in H, \forall g \in G$.
Donc $\tilde{\varphi}(g)$ ne dépend que de la classe $gH \in G/H$. Par passage au quotient par H, $\tilde{\varphi} : G \to G.x$ induit $\varphi : G/H \to G.x$. Clairement, φ est surjective.
Supposons que $g_1, g_2 \in G$ sont tels que $\varphi(g_1) = \varphi(g_2)$. Alors $g_1 x = g_2 x$, donc $x = g_1^{-1} g_2 x$ et $g_1^{-1} g_2 \in H$ et $g_2 \in g_1 H$. Donc on a $g_2 H = g_1 H$, ou $\pi(g_1) = \pi(g_2)$.
Cela montre que φ est injective.

Remarque

L'ensemble $G/Stab_G(x)$ est un G-ensemble pour l'action naturelle :

$$g.\pi(g') := \pi(gg'), \qquad\qquad \forall g, g' \in G$$

où $\pi : G \to G/Stab_G(x)$ est la projection canonique. La bijection canonique $G/Stab_G(x) \xrightarrow{\sim} G.x$ est en fait un isomorphisme de G-ensembles.
En particulier, tout G-ensemble transitif est isomorphe à un G-ensemble de la forme G/H pour un sous-groupe H de G.

Corollaire

On suppose G et X finis.

1. Pour tout $x \in G$, on a $|G.x| = \frac{|G|}{|Stab_G(x)|}$. En particulier, $|G.x|$ divise $|G|$.
2. Choisissons un élément x_i dans chaque orbite, $1 \leq i \leq n$. On a :

$$|X| = \sum_{i=1}^{n} \frac{|G|}{|Stab_G(x_i)|}$$

Remarque

Ces égalités sont appelées **équations aux classes**.

2.4.1 Applications

Application 1

Soit p un nombre premier. Supposons que G est un p-groupe, c'est à dire son ordre est une puissance de p.

Définition

Un élément x d'un G-ensemble X est un point fixe si $gx = x \ \forall g \in G$.

Soient G un p-groupe, et X un G-ensemble fini.
Si $x \in X$ n'est pas un point fixe, le cardinal de l'orbite $|G.x|$ est un diviseur > 1 de $|G|$.
Donc p divise $|G.x|$. D'où :

Corollaire

Si G est un p-groupe et X un G-ensemble fini, alors :

$$|X| \equiv |X^G| \ mod \ p$$

où X^G est l'ensemble des points fixes de G dans X.

Application 2

Théorème de Cauchy

Soient G un groupe fini et p un nombre premier qui divise $|G|$, alors G contient un élément d'ordre p.

Démonstration (d'après John McKay)

Soit :

$$X = \{(g_1, ..., g_p) \in G^p | g_1 g_2 .... g_p = e\}$$

Notons que :

$$g_1 g_2 ... g_p = e$$
$$\Rightarrow g_2 ... g_p = g_1^{-1}$$
$$\Rightarrow g_2 ... g_p g_1 = e$$

Donc X est stable par permutation cyclique des composantes. Donc le groupe cyclique $H = \mathbb{U}_p$ agit sur X par :

$$\zeta(g_1, g_2 ... g_p) := (g_2 ... g_p g_1)$$

où $\zeta = e^{\frac{2\pi i}{p}}$.
Les points fixes sont les $(g, ..., g) \in G^p$ tq $g^p = e$. Cela veut dire que ou bien $g = e$ ou bien g est un élément d'ordre p.
Par le corollaire précédent, on a :

$$|X^H| = |X| \ mod \ p$$

Or X est de cardinal $|G|^{p-1}$ (l'application $X \to G^{p-1}$, $(g_1, ..., g_p) \mapsto (g_2, ..., g_p)$ est bijective). Donc :

$$|X^H| = 0 \ mod \ p$$

Il existe donc au moins un point fixe autre que $(e, ..., e)$.

Chapitre 3

Groupes symétriques

3.1 Définition et premières propriétés

Rappel

Si E est un ensemble, le groupe symétrique σ_E est le groupe des bijections $f : E \to E$ avec la composition des applications pour loi. On note :

$$\sigma_n := \sigma_{\{1,2,...,n\}} \qquad n \geq 1$$

et on l'appelle le n-ième groupe symétrique. Il est d'ordre $n!$.

Remarque

Si E et F sont deux ensembles et $\varphi : E \to F$, une bijection, on a un isomorphisme de groupes :

$$\sigma_E \to \sigma_F,\ f \mapsto \varphi \circ f \circ \varphi^{-1}$$

En particulier, l'étude de σ_E pour un ensemble fini de cardinal n se ramène à celle de σ_n.

Notation

Si $\sigma \in \sigma_n$, on le décrit à l'aide du tableau :

$$\begin{array}{cccc} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{array}$$

Remarque

1. Le groupe σ_n agit sur $\{1, ..., n\}$ par :
$$\sigma.i = \sigma(i), \qquad \forall i \in \{1, ..., n\}, \forall \sigma \in \sigma_n$$
2. Cette action est fidèle et transitive
3. Pour tout $i \in \{1, ..., n\}$, la stabilisateur de i dans σ_n est isomorphe à $\sigma_{\{1,2,...,n\}\setminus\{i\}}$

Définition

Soit $\sigma \in \sigma_n$. Le support de σ est l'ensemble :

$$supp(\sigma) = \{i \in \{1, ..., n\} | \sigma(i) \neq i\}$$

Propriété

1. Deux permutations à supports disjoints commutent
2. Les groupes symétriques σ_1 et σ_2 sont abéliens. Pour $n \geq 3$, la centre de σ_n est trivial.

Démonstration

1. On peut et on va supposer $n \geq 3$. Soient $\sigma_1, \sigma_2 \in \sigma_n$ tq $supp(\sigma_1) \cap supp(\sigma_2) = \emptyset$.
   Si l'une parmi σ_1 et σ_2 est l'identité, elles commutent bien.
   Supposons $supp(\sigma_1)$ et $supp(\sigma_2)$ non vides ($\sigma_i \neq Id\ \forall i$).
   Soit $i \in supp(\sigma_1)$, alors $i \in supp(\sigma_2)$ et $\sigma_1(i) \notin supp(\sigma_2)$. Donc :
   $$\sigma_1 \circ \sigma_2(i) = \sigma_1(i)$$
   $$\sigma_2 \circ \sigma_1(i) = \sigma_1(i)$$
   De même, pour $i \in supp(\sigma_2)$, on a :
   $$\sigma_1 \circ \sigma_2(i) = \sigma_2(i)$$
   $$\sigma_2 \circ \sigma_1(i) = \sigma_2(i)$$
   D'autre part, si $i \notin supp(\sigma_1) \cup supp(\sigma_2)$, alors $\sigma_1 \circ \sigma_2(i) = i = \sigma_2 \circ \sigma_1(i)$.
   On conclut que $\sigma_1 \circ \sigma_2(i) = \sigma_2 \circ \sigma_1(i)$
2. Soit $\sigma \in \sigma_n \backslash \{Id\}$.
   Soient $i \in \{1, ..., n\}$ tq $\sigma(i) \neq i$ et $k \in \{1, ..., n\} \backslash \{i, \sigma(i)\}$.
   Soit τ la permutation tq :
   $$\tau(\sigma(i)) = k,\ \tau(k) = \sigma(i),\ \tau(j) = j,\ \forall j \notin \{i, \sigma(i)\}$$
   Montrons que $\tau \circ \sigma \neq \sigma \circ \tau$. En effet :
   $$\tau \circ \sigma(i) = k$$
   $$\sigma \circ \tau(i) = \sigma(i) \neq k$$

3.1.1 Transpositions et cycles

Définition

Soit $n \geq 2$ et soit $2 \leq l \leq n$. Soit $(a_1, ..., a_l)$ une suite d'éléments 2 à 2 distincts de $\{1, ..., n\}$. On note encore $(a_1, ..., a_l)$ la permutation définition par :

$$\begin{array}{ll} x \mapsto x & \forall x \in \{1, ..., n\} \backslash \{a_1, ..., a_l\} \\ a_i \mapsto a_{i+1} & \forall 1 \leq i \leq l-1 \\ a_l \mapsto a_1 & \end{array}$$

Une telle permutation est appelée l-cycle (ou cycle). Sa longueur est l.
Si $l = 2$, elle est appelée la transposition de a_1 et a_2

Remarque

Soit $\sigma = (a_1, ..., a_l)$ un l-cycle.

1. Soit $i \in \{1, ..., l-1\}$, alors $\sigma^i(a_1) = a_{1+i}$. Plus généralement, on a :
   $$\sigma^i(a_j) = \begin{cases} a_{j+i} & 1 \leq j \leq l-i \\ a_{j+i-l} & l-i+1 \leq j \leq l \end{cases}$$
   Le cycle est d'ordre l dans σ_n.
2. Pour tout $\tau \in \sigma_n$, on a :
   $$\tau \circ (a_1, ..., a_l) \circ \tau^{-1} = (\tau(a_1), ..., \tau(a_l))$$
3. $$(a_1, ..., a_n) = (a_1, a_2) \circ ... \circ (a_{l-2}, a_{l-1}) \circ (a_{l-1}, a_l)$$
   Le l-cycle est produit de $l - -1$ transpositions.
4. $$(a_1, ..., a_n) = (a_2, ..., a_n, a_1)$$
5. Soit τ_1 et τ_2 deux transpositions à support disjoint, alors $\tau_1\tau_2 = \tau_2\tau_1$ (qui est d'ordre 2) est appelé une **double transposition**.

Exemple

1. $$\sigma_2 = \{e, (12)\}$$

2. $$\sigma_3 = \{e, (12), (13), (23), (123), (132)\}$$

3. σ_4={e, (12), (13), (23), (14), (24), (34),
(12)(34), (13)(24), (14)(23),
(123), (132), (124),(142),(134),(143),(234),(243),
(1234),(1243),(1324),(1342),(1423),(1432)}

Théorème

Soit $\sigma \in \sigma_n$.

1. Il existe un entier naturel k et des cycles $c_1, ..., c_k$ de σ_n à supports disjoints 2 à 2 tq :

$$\sigma = c_1 ... c_k$$

2. Si s est un entier naturel et $c'_1, ..., c'_s$ des cycles à supports disjoints 2 à 2 tq :

$$\sigma = c'_1 ... c'_s$$

alors $k = s$ et il existe une permutation $\tau \in \sigma_k$ tq $c'_i = c_{\tau(i)}$, $\forall 1 \leq i \leq k$

Idée de la démonstration : On fait agir le groupe $< \sigma > \subseteq \sigma_n$ sur $\{1, ..., n\}$. Les orbites nous fournissent les cycles c_i, $1 \leq i \leq k$

Exemple

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 6 & 7 & 9 & 4 & 5 & 10 & 2 & 3 & 12 & 13 & 8 & 11 & 1 & 14 \end{pmatrix}$$

$\sigma = (1\ 6\ 10\ 13)(2\ 7)(3\ 9\ 12\ 11\ 8)$ est une décomposition en produit de cycles à supports disjoints 2 à 2 de $\sigma \in \sigma_{14}$.