Cours d'Algèbre et géométrie I

Bernhard Keller

écrit par Xavier Durand avec les graphes de Tristan François

11/09/2018 - 11/12/18

Table des matières

Chapitre 1

Groupes

1.1 Motivation

1.1.1 Éléments de symétrie

— 3 symétries orthogonales : $\sigma_A, \sigma_B, \sigma_C$
— 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 diédral.
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.

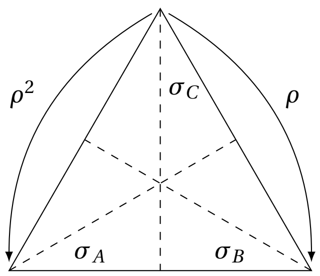


FIGURE 1.1 – Le groupe diédral D_3

1.2 Définition et premiers exemples

Définition 1.2.1
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 :*

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

Remarque 1.2.2

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 1.2.3
Un groupe G est abélien ou commutatif si xy=yx, pour tous $x, y \in G$.

Remarque 1.2.4
Souvent, on note + la loi de groupe d'un groupe abélien. On note alors 0, l'élément neutre et $-x$ l'élément inverse de $x \in G$.

Exemple 1.2.5

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. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ 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 $\mathfrak{S}_X$ 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 :

$$\mathfrak{S}_n = \mathfrak{S}_{\{1,2,\ldots,n\}} = \text{groupe de permutations de } \{1, \ldots, n\}$$

   Notons que $|\mathfrak{S}_n| = n!$.

Notation 1.2.6
Soit G un groupe. Soient $g \in G$ et $n \in \mathbb{N}$.
On note g^n, l'élément de G défini par récurrence :

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

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

Lemme 1.2.7
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 1.2.8
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 1.2.9
$G \times H$ muni de cette loi est le groupe produit de G par H.

Exercice 1.2.10
$G \times H$ est abélien ssi G et H sont abéliens.

1.3 Sous-groupe

Définition 1.3.1
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 1.3.2
On note $H \leq G$ lorsque H est un sous-groupe de G.

Lemme 1.3.3
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 $h_2^{-1} \in H$ (3.) et donc $h_1 h_2^{-1} \in H$ (2.).
"$\Leftarrow$" 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 1.3.4

1. Soit H un sous-groupe de G. Alors la loi de G induit une application $H \times H \to H$, $(h_1, h_2) \mapsto h_1 h_2$ (bien définie par 2.). 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 1.3.5

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 1.3.6

On appelle $Z(G)$ le centre de G.

Exemple 1.3.7

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

Exemple 1.3.8 (de sous-groupes (suite))

Soit $n \geq 1$. Les parties suivantes sont des sous-groupes de $GL_n(\mathbb{R})$:

— $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | \det A = 1\}$

— $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) | A^t A = I_n\}$

— $SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O_n(\mathbb{R})$

Notation 1.3.9

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

Remarque 1.3.10

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 1.3.11

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

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

Théoreme 1.3.12

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 $H = 0 \cdot \mathbb{Z}$. 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 $x = nq + r$, où $q, r \in \mathbb{Z}$ et $0 \leq r < n$.
   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 1.4.1

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 1.4.2

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

$$\langle S\rangle = \cap_{H \; sous-groupe \; tq \; H \supseteq S} H$$

On appelle $\langle S\rangle$ le sous-groupe engendré par S.

Remarque 1.4.3

$\langle S\rangle$ est le plus petit des sous-groupe contenant S.

Définition 1.4.4

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

Exemple 1.4.5

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

Lemme 1.4.6

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

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

Démonstration

Notons H le membre de droite. Clairement, H est un sous-groupe et contient S. Donc $H \supseteq \langle S\rangle$.
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 $H = \langle S\rangle$. □

1.5 Morphismes de groupes

Définition 1.5.1

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 1.5.2
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 $f(x^{-1}) = f(x)^{-1}$

Exemple 1.5.3

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

Théoreme 1.5.4
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 $n > 0$. □

Théoreme 1.5.5
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 1.5.6

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 :

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

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 1.5.7
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.

Exemple 1.5.8

1. On a des isomorphismes inverses l'un de l'autre (exp et ln)
2. Soit $\sigma \in \mathfrak{S}_2$ tq $\sigma(1) = 2$ et $\sigma(2) = 1$. On a un isomorphisme :

$$\begin{array}{lll} (\{\pm 1\}, \cdot) & \xrightarrow{\sim} & \mathfrak{S}_2 \\ 1 & \mapsto & Id \\ -1 & \mapsto & \sigma \end{array}$$

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 :

$$f : D_3 \xrightarrow{\sim} \mathfrak{S}_3$$

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

Définition 1.5.9
Soit G un groupe. Un automorphisme de G est un isomorphisme $f : G \to G$.
On note $\mathrm{Aut}(G)$ *l'ensemble des automorphismes de G. C'est un sous-groupe du groupe symétrique $\mathfrak{S}_G$ de l'ensemble G.*

Exemple 1.5.10
Pour tout $g \in G$, on a l'application de conjugaison par g :

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

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

Propriété 1.5.11

1. *L'application $G \to Aut(G)$, $g \mapsto c_g$ 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 1.5.12
Le noyau de f est :

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

L'image de f est :

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

.

Théoreme 1.5.13

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. □

Théoreme 1.5.14

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 :
$$x = y \cdot y^{-1}x \in G'$$
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 1.6.1
L'ordre de G est le cardinal $|G|$ de l'ensemble G.

Exemple 1.6.2

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

Notation 1.6.3
Pour $g \in G$, on pose $\langle g \rangle := \langle \{g\} \rangle$.

Propriété 1.6.4
Soit $g \in G$. On suppose qu'il existe $n \geq 1$ tq $g^n = e$.

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

Démonstration

1. " $\supseteq$ " est clair. Réciproquement, on sait que tout élément de $\langle g \rangle$ 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 :
$$\langle g \rangle = \{g^i | 0 \leq i \leq s-1\}$$
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 $s = |\langle g \rangle| = d$. □

Définition 1.6.5
Soit $g \in G$. Si $\langle g \rangle$ est infini, l'ordre de g est infini.
Si $\langle g \rangle$ est fini, l'ordre de g est le plus petit entier $d \geq 1$ tq $g^d = e$

Remarque 1.6.6

1. Donc on a que l'ordre de g est égal à l'ordre de $\langle g \rangle$
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 1.6.7
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 $\frac{ppcm(n,k)}{k}$

Théoreme 1.6.8 (Théorème de Lagrange)
Soit G un groupe fini. Alors, l'ordre de tout sous-groupe $G' \leq G$ divise l'ordre de G.

Corollaire 1.6.9
Soit G un groupe fini. Alors tout élément $g \in G$ est d'ordre fini et son ordre divise l'ordre de G.

Conséquence 1.6.10
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 $G = \langle g \rangle$. 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 : $H \to gH$, $h \mapsto gh$ et $gH \to H$, $x \mapsto g^{-1}x$.
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 $g = g \cdot e \in gH$, 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 $|G| = |H| \cdot |\{gH | g \in G\}|$. □

1.7 Les treillis de sous-groupes

Définition 1.7.1
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 1.7.2
Une relation R est une relation d'ordre ssi :

- *(réflexivité)* $\forall x \in X,\ xRx$
- *(antisymétrie)* $\forall x, y \in X\ (xRy\ et\ yRx) \Rightarrow x = y$
- *(transitivité)* $\forall x, y, z \in X\ (xRy\ et\ yRz) \Rightarrow xRz$

Définition 1.7.3
Un ensemble (X, R) muni d'une relation d'ordre s'appelle un ensemble ordonné.

Exemple 1.7.4
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 1.7.5
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 1.7.6
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 $\{x,y\}$.

Exemple 1.7.7

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 :
   $H,H' \in L(G)$ $sup(H,H') = \langle H,H' \rangle$ (groupe engendré par H et H'), et $inf(H,H') = H \cap H'$

Définition 1.7.8
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 $> x$.*

Exemple 1.7.9

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

$$\begin{tikzcd}
& \{1,2\} & \\
\{1\} \arrow[ur] & & \{2\} \arrow[ul] \\
& \emptyset \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

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

$$\begin{tikzcd}
& & 20 & \\
& 10 \arrow[ur] & & 4 \arrow[ul] \\
5 \arrow[ur] & & 2 \arrow[ul] \arrow[ur] & \\
& 1 \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

Lemme 1.7.10
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 $e : \mathbb{Z} \to \mathbb{U}_n,\ k \mapsto \zeta^k$.
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 1.7.11

1. Treillis de $\mathbb{U}_{20}$:
   D'après le lemme précédent, les sous-groupes de $\mathbb{U}_{20}$ sont $\langle \zeta^{20} \rangle$, $\langle \zeta^{10} \rangle$, $\langle \zeta^{5} \rangle$, $\langle \zeta^{4} \rangle$, $\langle \zeta^{2} \rangle$ et $\langle \zeta^{1} \rangle$:

$$\begin{tikzcd}
 & & \langle \zeta^1 \rangle & \\
 & \langle \zeta^2 \rangle \arrow[ur] & & \langle \zeta^5 \rangle \arrow[ul] \\
\langle \zeta^4 \rangle \arrow[ur] & & \langle \zeta^{10} \rangle \arrow[ul] \arrow[ur] & \\
 & \langle \zeta^{20} \rangle \arrow[ul] \arrow[ur] & &
\end{tikzcd}$$

FIGURE 1.2 – Diagramme de Hasse du groupe $\mathbb{U}_{20}$

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 :
   — $|H| = 1 \Rightarrow H = \{Id\}$
   — $|H| = 2 \Rightarrow H = \langle \sigma_A \rangle, \langle \sigma_B \rangle, \langle \sigma_C \rangle$
   — $|H| = 3 \Rightarrow H = \langle \rho \rangle = \langle \rho^2 \rangle$

$$\begin{tikzcd}
 & & \langle D_3 \rangle & & \\
 & & & & \langle \rho \rangle \arrow[ull] \\
 & \langle \tau_1 \rangle \arrow[uur] \arrow[r, dashed, no head] & \langle \tau_2 \rangle \arrow[uu] \arrow[r, dashed, no head] & \langle \tau_3 \rangle \arrow[uul] & \\
 & & \{Id\} \arrow[ul] \arrow[u] \arrow[ur] \arrow[uurr, bend right] & &
\end{tikzcd}$$

FIGURE 1.3 – Diagramme de Hasse du groupe diédral 3

   Ici, comme dans tous les diagrammes de Hasse de groupes à venir, les " - - - " représentent la relation de conjugaison par ρ.

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 :

— $|H| = 1 \Rightarrow H = \{Id\}$

— $|H| = 2 \Rightarrow H = \langle\rho^2\rangle, \langle\tau_1\rangle, \langle\tau_2\rangle, \langle\tau_3\rangle, \langle\tau_4\rangle$

— $|H| = 4 \Rightarrow H = \langle\rho\rangle, \langle\tau_1, \tau_3\rangle, \langle\tau_2, \tau_4\rangle$

$$
\begin{tikzcd}
 & & D_4 & & \\
 & \langle\tau_1,\tau_3\rangle \arrow[ur] & \langle\rho\rangle \arrow[u] & \langle\tau_2,\tau_4\rangle \arrow[ul] & \\
\langle\tau_1\rangle \arrow[ur] \arrow[r, dash, dashed] & \langle\tau_3\rangle \arrow[u] & \langle\rho^2\rangle \arrow[ul] \arrow[u] \arrow[ur] & \langle\tau_1\rangle \arrow[u] \arrow[r, dash, dashed] & \langle\tau_4\rangle \arrow[ul] \\
 & & \{e\} \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}
$$

FIGURE 1.4 – Diagramme de Hasse du groupe diédral D_4

Chapitre 2

Actions de groupes

2.1 Relations d'équivalence

Définition 2.1.1

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)* $\forall x, y, z \in X \; (xRy \; et \; yRz) \Rightarrow xRz$

Exemple 2.1.2

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 2.1.3

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 2.1.4

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 2.1.5

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. □

Théoreme 2.1.6
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 $x, y \in X, xRy \Rightarrow \pi(x) = \pi(y) \Rightarrow (\bar{f} \circ \pi)(x) = (\bar{f} \circ \pi)(y) \Rightarrow f(x) = f(y)$ □

Remarque 2.1.7
Lorsque f vérifie 1. du théorème, on dit que f passe au quotient par R et que $\bar{f}$ est induite par f.

Lemme 2.1.8
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, $f = \bar{f} \circ \pi$ est surjective, car $\bar{f}$ 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 2.1.9
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 2.2.1
Soient X un ensemble, G un groupe. Une action de G sur X est une application $\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \to & g \cdot x \end{array}$ *telle que :*

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

Définition 2.2.2
Un G-ensemble est un ensemble muni d'une action du groupe G.

Exemple 2.2.3

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 $\mathfrak{S}_n$ agit sur l'ensemble $X = \{1, \cdots, n\}$ par $\sigma \cdot x := \sigma(x),\ \forall \sigma \in \mathfrak{S}_n,\ \forall x \in X$.

   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 translation 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 $e \cdot x = e \cdot x \cdot e^{-1} = x, \forall x \in G$ et $(gh) \cdot x = ghx(gh)^{-1} g(hxh^{-1})g^{-1} = g(hx),\ \forall g, h \in G, \forall x \in G$).
   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 2.2.4
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 $\varphi_g \in \mathfrak{S}_X$ et l'application $G \to \mathfrak{S}_X\ g \mapsto \varphi_g$ est un morphisme de groupes.*

2. *Soit $f : G \to \mathfrak{S}_X$ est un morphisme de groupes. Alors il existe une unique action de G sur X tq :*

$$g \cdot x = (f(g))(x), \;\; \forall g \in G, \forall x \in X$$

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 $\mathfrak{S}_X$

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 $g, h \in G$:

$$\varphi_{gh}(x) = (gh)(x) = g(hx) = \varphi_g \circ \varphi_h(x), \;\; \forall x \in X$$

Donc l'application $g \mapsto \varphi_g$ est bien un morphisme de groupe $G \to \mathfrak{S}_X$

2. On définit l'application $G \times X \to X$ par $g \cdot x = (f(g))(x), \;\; \forall g \in G, \forall x \in X$, vérifions qu'il s'agit d'une action.

$$ex = (f(e))x = Id_X(x) = x, \;\; \forall x \in X$$

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 2.2.5

Soient G un groupe et X un ensemble. Une action à droite de G sur X est une application :

$$X \times G \to X, \; (x, g) \mapsto x \cdot g$$

telle que :

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

Exemple 2.2.6

Soit $n \geq 1$, alors l'application :

$$\begin{array}{lcl} M_n(\mathbb{R}) \times GL_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ (P, M) & \mapsto & MP \end{array}$$

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

Remarque 2.2.7

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

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

et

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

$\forall x \in X, \; \forall g, h \in G$.
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.

Définition 2.3.1
Pour $x \in X$, l'orbite de x est :

$$G \cdot x = \{g \cdot x | g \in G\}$$

Le stabilisateur de x est :

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

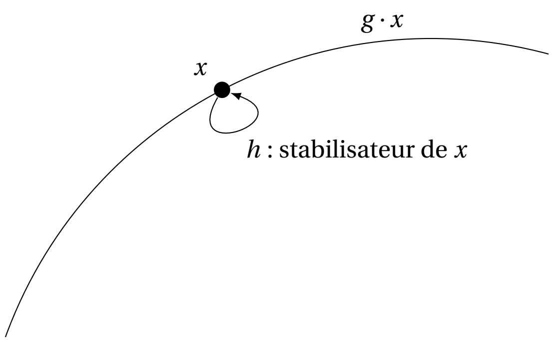


FIGURE 2.1 – Orbite de x sous G

Remarque 2.3.2

1. Soit $x \in X$. L'orbite $G \cdot x$ contient $x = e \cdot x$. Le stabilisateur G_x est un sous-groupe car $e \cdot x = x$, 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 2.3.3
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 2.3.4
Soit $\sim$ la relation sur X tq :

$$x \sim y \Leftrightarrow y \in G \cdot x$$

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 2.3.5
Pour tout $x \in X$, la classe d'équivalence de x est égale à l'orbite $G \cdot x$.

Définition 2.3.6
Le quotient de X par G est l'ensemble $G\backslash X := X/\sim$ formé des orbites de G dans X.

Remarque 2.3.7
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 2.3.8
L'ensemble des orbites est une partition de X.

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

Définition 2.3.9
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 2.3.10
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 $G \to \mathfrak{S}_X$ a pour noyau $\{e\}$, c'est à dire ssi $G \to \mathfrak{S}_X$ est injectif.

Exemple 2.3.11
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 $H \cdot e = H$)
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 $\mathbb{R}^n \setminus \{0\}$ (en effet si $v_1, \dots v_n$ est une base tq $v_1 = v$ et $w_1, \dots, w_n$ 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 : $\mathbb{R}^n \setminus \{0\}$ 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 $GL_n(\mathbb{R}) \times (\mathbb{R}^n \setminus \{0\}) \to (\mathbb{R}^n \setminus \{0\})$, $(g, v) \mapsto gv$ est transitive, fidèle et non libre. En effet, $Stab_{GL_n(\mathbb{R})}(e_1) = [e_1, *, *, ..., *]$ avec $*$ des vecteurs quelconques.
4. Soit $C = \{(x_1, x_2, x_3) \in \mathbb{R} | \forall i \text{ on a } x_i = \pm 1\}$ l'ensemble des sommets d'un cube de $\mathbb{R}^3$ centré 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).

Théoreme 2.4.1
Soit $x \in X$. Soit $\pi : G \to G/Stab_G(x)$ la projection canonique.
Il existe une et une seule application :
$$\varphi : G/Stab_G(x) \to G \cdot x$$
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 :
$$(gh)x = g(hx) = gx \qquad h \in Stab_G(x)$$
Donc l'application $\tilde{\varphi} : G \to G \cdot x$ 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, $\tilde{\varphi} : G \to G \cdot x$ induit $\varphi : G/H \to G \cdot x$. 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 2.4.2
L'ensemble $G/Stab_G(x)$ est un G-ensemble pour l'action naturelle :
$$g \cdot \pi(g') := \pi(gg'), \qquad \forall g, g' \in G$$
où $\pi : G \to G/Stab_G(x)$ est la projection canonique. La bijection canonique $G/Stab_G(x) \xrightarrow{\sim} G \cdot x$ 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 2.4.3
On suppose G et X finis.

1. *Pour tout* $x \in X$, *on a* $|G\cdot x| = \frac{|G|}{|Stab_G(x)|}$. *En particulier,* $|G\cdot x|$ *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 2.4.4
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 2.4.5
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 $|G\cdot x|$ est un diviseur > 1 de $|G|$.
Donc p divise $|G\cdot x|$. D'où :

Corollaire 2.4.6
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

Théoreme 2.4.7 (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 :

$$\begin{aligned} & g_1 g_2 ... g_p = e \\ \Rightarrow\ & g_2 ... g_p = g_1^{-1} \\ \Rightarrow\ & g_2 ... g_p g_1 = e \end{aligned}$$

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 $(e, ..., e)$. $\square$

Chapitre 3

Groupes symétriques

3.1 Définition et premières propriétés

Rappel

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

$$\mathfrak{S}_n := \mathfrak{S}_{\{1,2,\dots,n\}} \qquad\qquad n \geq 1$$

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

Remarque 3.1.1
Si E et F sont deux ensembles et $\varphi : E \to F$, une bijection, on a un isomorphisme de groupes :

$$\mathfrak{S}_E \to \mathfrak{S}_F,\ f \mapsto \varphi \circ f \circ \varphi^{-1}$$

En particulier, l'étude de $\mathfrak{S}_E$ pour un ensemble fini de cardinal n se ramène à celle de $\mathfrak{S}_n$.

Notation 3.1.2
Si $\sigma \in \mathfrak{S}_n$, on le décrit à l'aide du tableau :

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

Remarque 3.1.3

1. Le groupe $\mathfrak{S}_n$ agit sur $\{1,\dots,n\}$ par :

$$\sigma.i = \sigma(i), \qquad \forall i \in \{1,\dots,n\}, \forall \sigma \in \mathfrak{S}_n$$

2. Cette action est fidèle et transitive
3. Pour tout $i \in \{1,\dots,n\}$, la stabilisateur de i dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{\{1,2,\dots,n\}\setminus\{i\}}$

Définition 3.1.4
Soit $\sigma \in \mathfrak{S}_n$. Le support de σ est l'ensemble :

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

Propriété 3.1.5

1. *Deux permutations à supports disjoints commutent*
2. *Les groupes symétriques $\mathfrak{S}_1$ et $\mathfrak{S}_2$ sont abéliens. Pour $n \geq 3$, le centre de $\mathfrak{S}_n$ est trivial.*

Démonstration

On peut et on va supposer $n \geq 3$.

1. Soient $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ 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 $i \notin supp(\sigma_2)$ 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 $\sigma \in \mathfrak{S}_n \backslash \{Id\}$.
   Soient $i \in \{1, ..., n\}$ tq $\sigma(i) \neq i$ et $k \in \{1, ..., n\} \backslash \{i, \sigma(i)\}$.
   Soit τ la permutation tq :
   $$\tau(\sigma(i)) = k,\ \tau(k) = \sigma(i),\ \tau(j) = j,\ \forall j \notin \{k, \sigma(i)\}$$
   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 3.1.6

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 :

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

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 3.1.7

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 $\mathfrak{S}_n$.
2. Pour tout $\tau \in \mathfrak{S}_n$, 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 3.1.8

1. $$\mathfrak{S}_2=\{e,(12)\}$$

2. $$\mathfrak{S}_3=\{e,(12),(13),(23),(123),(132)\}$$

3. $\mathfrak{S}_4$={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)}

Théoreme 3.1.9

Soit $\sigma\in\mathfrak{S}_n$.

1. *Il existe un entier naturel k et des cycles $c_1,...,c_k$ de $\mathfrak{S}_n$ 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 $\tau\in\mathfrak{S}_k$ tq $c'_i=c_{\tau(i)}$, $\forall 1\leq i\leq k$.

Idée de la démonstration : On fait agir le groupe $\langle\sigma\rangle\subseteq\mathfrak{S}_n$ sur $\{1,...,n\}$. Les orbites nous fournissent les cycles c_i, $1\leq i\leq k$.

Exemple 3.1.10

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

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

Démonstration

On fait agir le sous-groupe $\langle\sigma\rangle$ engendré par σ dans $\mathfrak{S}_n$ sur l'ensemble $\{1,...,n\}$.
Sous cette action, l'ensemble $\{1,...,n\}$ se décompose en orbites disjointes 2 à 2. Les orbites ponctuelles sont exactement les points fixes de σ.
Soient $\Omega_1,...,\Omega_r$ les orbites non ponctuelles.
Le sous-groupe $\langle\sigma\rangle$ permute cycliquement les éléments de chaque Ω_i. Soit $a_{i_1},...,a_{i_{l_i}}$ une énumération des éléments de Ω_i tq :

$$\sigma(a_{i_j})\begin{cases}a_{i_{j+1}} & 1\leq j\leq l_i-1\\ a_{i_1} & j=l_i\end{cases}$$

Soit $c_i=(a_{i_1},...,a_{i_{l_i}})$, alors l'action de c_i et de σ sur l'orbite Ω_i est la même.
Donc l'action de σ et de $c_1c_2...c_r$ sur $\{1,...,n\}$ est la même.
Donc $\sigma=c_1...c_r$. $\square$

Terminologie

1. Avec les hypothèses et les notations du théorème, on dit que l'égalité $\sigma = c_1 ... c_r$ est la décomposition de σ en **produit de cycles à supports disjoints**.
2. Si σ et σ' sont deux permutations, on dit que σ et σ' sont du **même type** si pour tout entier $2 \leq l \leq n$, le nombre de l-cycles dans la décomposition de σ en produit de cycles à support disjoints est égal au nombre de l-cycles dans la décomposition de σ' en produit de cycles à support disjoints .

Exemple 3.1.11
(12)(34)(567) est du même type que (123)(45)(67).

Corollaire 3.1.12
Pour tout $n \geq 1$, $\mathfrak{S}_n$ est engendré par l'ensemble de ses transpositions.

Démonstration
En effet, $\mathfrak{S}_n$ est engendré par ses cycles et chaque cycle est produit de transpositions, comme on l'a vu.□

Exercice 3.1.13
Monter que $\mathfrak{S}_n$ est même engendré par les $n-1$ transpositions :

$$(1\ 2), (2\ 3), ..., (n-1\ n)$$

.

Corollaire 3.1.14
Soient $n \geq 1$ et $\sigma \in \mathfrak{S}_n$, alors l'ordre de σ est le PPCM des longueurs des cycles apparaissant dans la décomposition de σ en produit de cycles à support disjoints .

Exemple 3.1.15
$ord((1\ 2)(2\ 3)(4\ 5\ 6)) = PPCM(2, 2, 3) = 6$

Corollaire 3.1.16
Soient $n \geq 1$ et $\sigma, \sigma' \in \mathfrak{S}_n$, alors on a une équivalence entre :

1. *σ et σ' sont du même type.*
2. *σ et σ' sont conjugués.*

Démonstration
Cela provient du fait que pour un cycle $(a_1, ..., a_l)$ et une permutation $\tau \in \mathfrak{S}_n$, on a :

$$\tau \circ (a_1, ..., a_l) \circ \tau^{-1} = (\tau(a_1), ..., \tau(a_l))$$

□

Exemple 3.1.17
$\sigma = (1\ 2)(3\ 4)(5\ 6\ 7)$ et $\sigma' = (1\ 2\ 3)(4\ 5)(6\ 7)$ sont conjugués par :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \end{pmatrix}$$

Remarque 3.1.18
Deux permutations conjuguées ont même ordre (et même signature, voir ci-dessous).

3.2 La signature

Soit $n \geq 1$. Le groupe symétrique $\mathfrak{S}_n$ agit sur l'ensemble $\mathbb{Z}[X_i,...,X_n]$ des polynômes en $X_1,...,X_n$ à coefficients entiers par :

$$(\sigma\ P)(X_1,...,X_n) := P(X_{\sigma(1)},...,X_{\sigma(n)})$$

(clairement, $Id.P = P$ et $\sigma(\tau\ P) = (\sigma\ \tau)P, \forall \sigma, \tau \in \mathfrak{S}_n$ et $\forall P \in \mathbb{Z}[X_i,...,X_n]$).

Soit

$$\Delta_n := \prod_{i<j}(X_i - X_j) \in \mathbb{Z}[X_i,...,X_n]$$

Par exemple, on a $\Delta_2 = X_1 - X_2$, $\Delta_3 = (X_1 - X_2)(X_1 - X_3)(X_2 - X_3)$.
Toute permutation σ envoie un $X_i - X_j$ sur $X_{\sigma(i)} - X_{\sigma(j)}$ et on a $\sigma(i) < \sigma(j)$ ou $\sigma(j) < \sigma(i)$ si $i < j$.
Donc σ envoie un facteur $X_i - X_j$ de Δ_n soit sur un autre facteur de Δ_n soit sur l'opposé d'un autre facteur de Δ_n. Donc :

$$\sigma\Delta_n = \pm\Delta_n, \ \ \forall \sigma \in \mathfrak{S}_n$$

Définition 3.2.1
*La **signature** $\epsilon(\sigma)$ de $\sigma \in \mathfrak{S}_n$ est l'unique nombre $\epsilon(\sigma) \in \{1,-1\}$ tq :*

$$\epsilon(\sigma)\Delta_n = \sigma\Delta_n$$

Exemple 3.2.2

1. $\sigma = (12) \in \sigma_2 : \sigma(X_1 - X_2) = X_2 - X_1 = -(X_1 - X_2) \Rightarrow \epsilon(\sigma) = -1$
2. $\sigma = (123) \in \sigma_3 : \sigma((X_1 - X_2)(X_1 - X_3)(X_2 - X_3)) = (X_2 - X_3)(X_2 - X_1)(X_3 - X_1) = (-1)(-1)\Delta_3 = \Delta_3 \Rightarrow \epsilon(\sigma) = 1$

Propriété 3.2.3

1. *La signature est un morphisme de groupes*

$$\epsilon : \mathfrak{S}_n \to (\{1,-1\},\cdot)$$

2. *Toute transposition est de signature -1. Tout cycle de longueur l est de signature $(-1)^{l-1}$*

Démonstration

1. résulte du fait que $\mathfrak{S}_n$ agit sur $\mathbb{Z}[X_i,...,X_n]$. En effet, pour $\sigma,\tau \in \mathfrak{S}_n$, on a :

$$\epsilon(\sigma\tau).\Delta_n = (\sigma\tau)\Delta_n = \epsilon(\tau)\epsilon(\sigma)\Delta_n$$

et donc $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau), \forall \sigma,\tau \in \mathfrak{S}_n$.

2. Soit $\sigma \in \mathfrak{S}_n$. Une **inversion** de σ est un couple (u,v) de nombres dans $\{1,...,n\}$ tq $u < v$ mais $\sigma(u) > \sigma(v)$. Clairement, on a $\epsilon(\sigma) = (-1)^t$, où t est le nombre d'inversions de σ. Soit maintenant $\sigma = (i\,j)$, où $1 \leq i < j \leq n$.
Les inversions de σ sont :
   - (u,j) pour $i < u < j$
   - (i,u) pour $i < u < j$
   - (i,j)

   Le nombre des inversions de σ est donc :

$$2(j - i + 1) + 1$$

Donc $\epsilon(\sigma) = -1$.
Donc toute transposition est de signature -1.
Comme un l-cycle c est produit de $l-1$ transposition, par 1), on a $\epsilon(c) = (-1)^{l-1}$ □

Remarque 3.2.4

Soient $n \geq 2$, et $\sigma \in \mathfrak{S}_n$.

1. On dit que σ est **paire** (respectivement **impaire**) si $\epsilon(\sigma) = 1$ (respectivement $\epsilon(\sigma) = -1$)
2. σ est pair (resp impair) ssi σ est produit de nombre pair (resp impair) de transpositions.
3. Soient $l_1, ..., l_r$ les cardinaux des orbites $\Omega_1, ..., \Omega_r$ de $\langle\sigma\rangle$ dans $\{1, ..., n\}$ (y compris les orbites ponctuelles), alors on a :

$$\epsilon(\sigma) = \epsilon(c_1...c_r) = (-1)^{l_1-1}...(-1)^{l_n-1} = (-1)^{(\sum l_i)-r} = (-1)^{n-r}$$

Définition 3.2.5

*Soit $n \geq 1$. On appelle n-ième **groupe alterné** le noyau $\mathscr{A}_n$ de la signature $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$.*

Remarque 3.2.6

On verra que $|\mathscr{A}_n| = \frac{n!}{2}$

Exemple 3.2.7

1. $\sigma_2 = \{e, (12)\}$ $\mathscr{A} = \{e\}$
2. $\sigma_3 = \{e, (12), (13), (23), (123), (132)\}$ $\mathscr{A}_3 = \{e, (123), (132)\}$
3. $|\sigma_4| = 24$, on a $\mathscr{A}_4 = \{e, (123), (132), (234), (243), (134), (143), (124), (142), (12)(34), (13)(24), (14)(23)\}$

Chapitre 4

Sous-groupes distingués, groupes quotients

4.1 Sous-groupes distingués

Soient G un groupe et H un sous-groupe de G.

Notation 4.1.1
Pour $g \in H$, on note $gHg^{-1} = \{ghg^{-1} | h \in H\}$. C'est un sous-groupe en tant qu'image de H par l'automorphisme de conjugaison (= automorphisme intérieur)

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

Propriété 4.1.2
Les conditions suivantes sont équivalentes :

1. $\forall g \in G$, *on a* $gH = Hg$
2. $\forall g \in G$, *on a* $gHg^{-1} = H$
3. $\forall g \in G$, *on a* $gHg^{-1} \subseteq H$

Démonstration
Clairement 1) $\Leftrightarrow$ 2) et 2) $\Rightarrow$ 3). Montrons que 3) $\Rightarrow$ 2) :
Soit $x \in G$, alors pour $g = x^{-1}$, on a :

$$H \supseteq gHg^{-1} = x^{-1}H(x^{-1})^{-1} = x^{-1}Hx$$

et donc $xHx^{-1} \supseteq H$. □

Définition 4.1.3
*H est **distingué** (ou **normal**) dans G ssi, pour tout $g \in G$, on a $gHg^{-1} = H$. On écrit alors $H \lhd G$.*

Définition 4.1.4
*Soit un groupe G et H un sous-groupe. Le **normalisateur** de H dans G est :*

$$N_G(H) = \{g \in G | gHg^{-1} = H\}$$

Remarque 4.1.5
$N_G(H)$ est un sous-groupe de G contenant H. H est distingué dans $N_G(H)$ et $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est distingué.
H est distingué dans G ssi $N_G(H) = G$

Définition 4.1.6
*L'**indice** de H dans G est* $[G:H] = |G/H| = \dfrac{|G|}{|H|}$ *si* $|G|$ *et* $|H|$ *sont finis.*

Exemple 4.1.7

1. $\{e\} = H \Rightarrow gHg^{-1} = \{gg^{-1}\} = \{e\}$. Donc $\{e\} \lhd G$. On a $G \lhd G$ et $Z(G) \lhd G$
2. Si G est **abélien**, alors $c_g = Id_G$, $\forall g \in G$, donc $H \lhd G$ pour tout sous-groupe H de G.
3. Si H est **d'indice 2** dans G ($|G/H| = 2$) alors $G = H \cup gH = H \cup Hg$ et $gH = Hg$, H est distingué dans G.

Lemme 4.1.8
Si $f : G \to K$ est un morphisme de groupes, alors $Ker(f)$ est distingué dans G.

Démonstration
Soient $x \in Ker(f)$ et $g \in G$. On a :

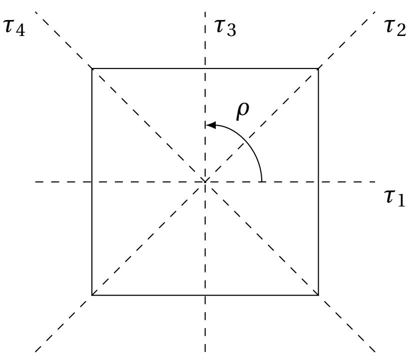
$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)ef(g)^{-1} = e$$

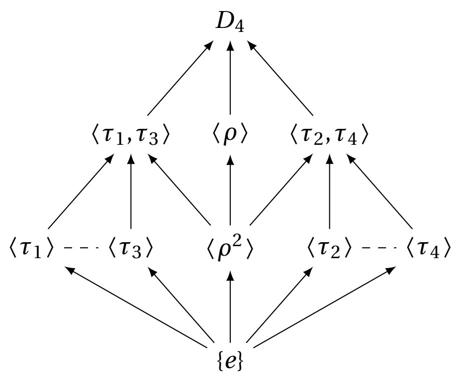
Donc $g\ Ker(f)\ g^{-1} \subseteq Ker(f), \forall g \in G$ et $Ker(f) \lhd G$. □

Remarque 4.1.9
$Im(f) \subseteq K$ n'est pas distingué en général. Par exemple, si $f : G \to K$ est l'inclusion d'un sous-groupe non distingué, alors $Im(f) = G \subseteq K$ n'est pas distingué.

Exemple 4.1.10

1. $\mathscr{A}_n \lhd \mathfrak{S}_n$ car $\mathscr{A}_n = Ker(\epsilon)$
2. $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$ car $SL_n(\mathbb{R}) = Ker(det)$
3. $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$, $SU_n(\mathbb{C}) \lhd U_n(\mathbb{C})$ par la même raison.
4. Quels sont les sous-groupes distingués de $D_4 = \{e, \tau_1, \tau_2, \tau_3, \tau_4, \rho, \rho^2, \rho^3\}$





Notons σ_D la symétrie orthogonale par rapport à une droite D et f une isométrie. Alors :

$$f \circ \sigma_D \circ f^{-1} = \sigma_{f(D)}$$

Donc D_4, $\{e\}$, $\langle \tau_1, \tau_3 \rangle$, $\langle \tau_2, \tau_4 \rangle$, $\langle \rho \rangle$, $\langle \rho^2 \rangle$ sont distingués et $\langle \tau_1 \rangle$, $\langle \tau_3 \rangle$, $\langle \tau_2 \rangle$ et $\langle \tau_4 \rangle$ ne sont pas distingués. On a $N_{D_4}(\langle \tau_1 \rangle) = \langle \tau_1, \tau_3 \rangle$, $N_{D_4}(\langle \tau_2 \rangle) = \langle \tau_2, \tau_4 \rangle$.

Remarque 4.1.11

1. Dans les treillis des sous-groupes , on a l'action de conjugaison de G sur l'ensemble des sous-groupes par conjugaison.

Les orbites ponctuelles sont les sous-groupes distingués, cad les sous-groupes qui ne sont pas liés par une action de ρ à d'autres sous-groupes .
Les orbites non ponctuelles sont les paquets de sous-groupes reliés par une action de ρ.
Le stabilisateur d'un sous-groupe H est l'ensemble des g tq $gHg^{-1} = H$, donc c'est le normalisateur de H dans G.
L'isomorphisme $G/Stab_G(x) \xrightarrow{\sim} G \cdot x$ dit que l'indice du normalisateur $N_G(H)$ est égal au cardinal de l'orbite de H sous l'action de conjugaison.

2. Un groupe G est **simple** si $G \neq \{e\}$ et ses seuls sous-groupes distingués sont $\{e\}$ et G.
On verra plus tard que $\mathscr{A}_n$ est simple pour $n \geq 5$. Cela est lié au fait que l'équation du n-ième degré n'est pas résoluble par des radicaux pour $n \geq 5$ (voir $M1$).

4.2 Groupes quotients

Soient G un groupe et $H \leq G$ un sous-groupe . On note $\pi : G \to G/H,\ g \mapsto gH$ la bijection canonique.

Rappel

- π est surjective
- $\forall g \in G$, on a $\pi(g) = gH$
- Pour $g, g' \in G$, on a $\pi(g) = \pi(g')$ ssi $\exists h \in H$ tq $g' = gh$

Théoreme 4.2.1
On suppose que $H \lhd G$.
Il existe une unique loi de composition interne $*$ sur G/H tq $(G/H, *)$ soit un groupe et

$$\pi : G \to G/H$$

un morphisme de groupes.

Démonstration
Soient $\alpha, \beta \in G/H$. Soient $x, y \in G$ tq $\pi(x) = \alpha$ et $\pi(y) = \beta$.
On définit

$$\alpha * \beta = \pi(x) * \pi(y) = \pi(xy)$$

et c'est la seule possibilité car π doit être un morphisme de groupes.
Il faut vérifier que $\alpha * \beta$ est bien défini.
Soient $x', y' \in G$ tq $\pi(x') = \alpha$ et $\pi(y') = \beta$.
Il existe $h, k \in H$ tq $x' = xh$ et $y' = yk$. On a :

$$\pi(x'y') = \pi(xhyk) = \pi(xyy^{-1}hyk) = \pi(xy)$$

Ce qui montre que $\pi(xy)$ ne dépend que du choix des représentants x et y de α et β.
Montrons l'associativité : Soient $\pi(x), \pi(y), \pi(z)$ dans G/H. On a :

$$\begin{aligned} (\pi(x)\pi(y))\pi(z) &= \pi(xy)\pi(z) \\ &= \pi(xyz) \\ &= \pi(x)(\pi(y)\pi(z)) \end{aligned}$$

$\pi(e)$ est neutre car :

$$\pi(x)\pi(e) = \pi(xe) = \pi(x) = \pi(ex) = \pi(e)\pi(x)$$

et $\pi(x^{-1})$ est inverse de $\pi(x),\ \forall x \in G$, car :

$$\pi(x)\pi(x^{-1}) = \pi(xx^{-1}) = \pi(e) = \pi(x^{-1}x) = \pi(x^{-1}x) = \pi(x^{-1})\pi(x)$$

□

Remarque 4.2.2

1. On suppose que $H \lhd G$. Alors la loi de composition sur G/H vérifie :
   — $H = \ker(\pi : G \to G/H)$
   — $eH = H$ est l'élément neutre
   — $\forall x, y \in G : xH * yH = xyH$
2. Supposons que $H \leq G$ et G/H a une structure de groupe telle que $\pi : G \to G/H$ est un morphisme. Alors $H = \ker(\pi)$ est forcément distingué dans G.

Définition 4.2.3

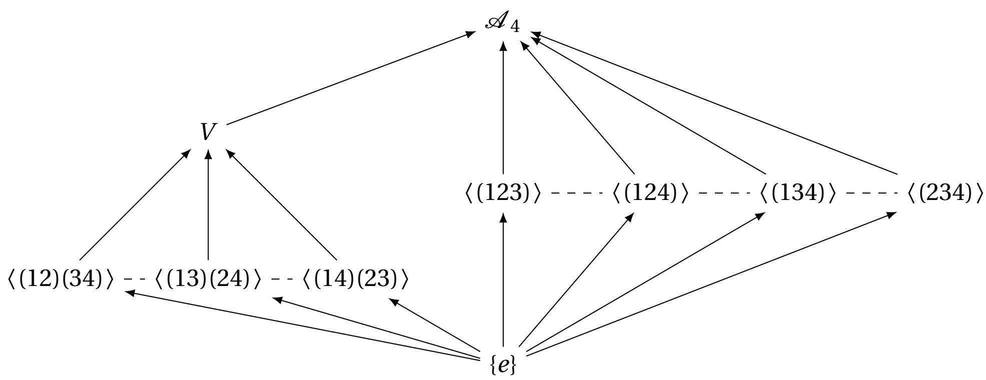
*Supposons que $H \lhd G$. Le groupe G/H du théorème 4.2.1 est le **groupe quotient** de G par H.*

Corollaire 4.2.4

Les sous-groupes distingués de G sont exactement les noyaux des morphismes de groupes $G \underset{\varphi}{\to} K$ de domaine G.

Exemple 4.2.5

1. Si E est un espace vectoriel sur $\mathbb{R}$ et F un sous espace vectoriel alors $(F, +)$ est un sous-groupe distingué de $(E, +)$ (qui est commutatif).
   Alors E/F devient un espace vectoriel pour la multiplication par les scalaires définie par $\lambda\cdot(v+F) = \lambda v + F$
   Si $F' \subseteq E$ est un supplémentaire de F ($E = F' \oplus F$), alors la composition :
   $$F' \hookrightarrow E \to E/F$$
   est un isomorphisme d'espaces vectoriels (exo !).
   En particulier, si $\dim E < \infty$, alors :
   $$\dim E/F = \dim E - \dim F$$
2. Soit $V = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. C'est un sous-groupe de $\mathscr{A}_4$.
   Alors V est distingué dans $\mathscr{A}_4$ et le quotient $\mathscr{A}_4/V$ est d'ordre $12/4 = 3$.
   Donc $\mathscr{A}_4/V$ est isomorphe à $\mathbb{U}_3$.
   Il est instructif de voir la position de V dans le treillis des sous-groupes de $\mathscr{A}_4$.



   On a : $N_{\mathscr{A}_4}(\langle(1\ 2)(3\ 4)\rangle) = V$ est d'indice 3 dans $\mathscr{A}_4$ et cet indice est égal au nombre de sous-groupes conjugués à $\langle(1\ 2)(3\ 4)\rangle$.
   $N_{\mathscr{A}_4}(\langle(1\ 2\ 3)\rangle) = \langle(1\ 2\ 3)\rangle$ est d'indice 4 dans $\mathscr{A}_4$ et cet indice est égal au nombre de sous-groupes conjugués à $\langle(1\ 2\ 3)\rangle$.

4.3 Passage au quotient des morphismes de groupes

Théoreme 4.3.1 (Propriété universelle du groupe quotient)
Soit $f : G \to K$ un morphisme de groupes . Soit $H \lhd G$. On suppose que $H \subseteq \ker(f)$.
Alors il existe un unique morphisme de groupes

$$\bar{f} : G/H \to K$$

tq $f = \bar{f} \circ \pi$

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & K \\ & G/H \arrow[ur, dashed, "\exists \bar{f}"'] & \end{tikzcd}$$

Terminologie
On dit que $\bar{f}$ est obtenu à partir de f par passage au quotient par H, ou que $\bar{f}$ est induit par f.

Remarque 4.3.2
On a $Im(\bar{f}) = Im(f)$ et $\ker(\bar{f}) = \pi(\ker f)$

Démonstration (Théorème 4.3.1)
Comme π est surjectif, $\bar{f}$ est unique. On définit pour $x \in G$,

$$\bar{f}(\pi(x)) = f(x)$$

On doit vérifier que si $\pi(x) = \pi(x')$, alors $f(x) = f(x')$. En effet, il existe $h \in H$ tq $x' = xh$ et on a donc :

$$f(x') = f(xh) = f(x)f(h) = f(x)$$

car $f(h) \in \ker f$.
Vérifions que $\bar{f}$ est bien un morphisme :
On a pour $x, y \in G$:

$$\begin{array}{rcl} \bar{f}(\pi(x)\pi(y)) & = & \bar{f}(\pi(xy)) \\ & = & f(xy) \\ & = & f(x)f(y) \\ & = & \bar{f}(\pi(x))\bar{f}(\pi(y)) \end{array}$$

□

Théoreme 4.3.3 (Premier théorème d'isomorphisme)
Soit $f : G \to K$ un morphisme de groupes , alors f induit un isomorphisme de groupes de $G/\ker(f)$ sur $Im(f)$.
En particulier, si f est surjectif, alors f induit un isomorphisme

$$G/\ker(f) \xrightarrow{\sim} K$$

$$\begin{tikzcd} G \arrow[rrr, "f"] \arrow[dr, "\pi"'] & & & K \\ & G/\ker(f) \arrow[r, "\sim"] & Im(f) \arrow[ur, hook] & \end{tikzcd}$$

Démonstration
$\bar{f}$ est bien définie par la propriété universelle du groupe quotient (théorème 4.3.1). Clairement, $\bar{f}$ est surjectif.
Montrons que $\bar{f}$ est injectif : si on a $\bar{f}(\pi(x)) = \bar{f}(\pi(x'))$, alors $f(x) = f(x')$, donc $x^{-1}x' \in \ker(f)$ et donc $\pi(x) = \pi(x')$ dans $G/\ker(f)$. □

Remarque 4.3.4
Ce théorème est important car il relie le groupe quotient, qui a priori est difficile à comprendre, avec un sous-groupe , qui est plus facile à comprendre.

Exemple 4.3.5
1. Soit $f : \mathbb{Z} \to \mathbb{U}_n,\ k \mapsto e^{\frac{2\pi ik}{n}}$, alors f est surjectif de noyau $n\mathbb{Z} \subseteq \mathbb{Z}$.
   Donc f induit un isomorphisme $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{U}_n$.
2. Soit $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$ la signature, alors ϵ est surjectif de noyau $\mathscr{A}_n$.
   Donc ϵ induit un isomorphisme
   $$\mathfrak{S}_n/\mathscr{A}_n \xrightarrow{\sim} \{\pm 1\}$$
   En particulier, on a $|\mathscr{A}_n| = \frac{1}{2}(n!)$.

Lemme 4.3.6
Soient G un groupe fini et p le plus petit diviseur premier de $|G|$.
Soit $H \subseteq G$ un sous-groupe d'indice p. Alors H est distingué.

Remarque 4.3.7
Pour $p = 2$, on retrouve le fait qu'un sous-groupe d'indice 2 est toujours distingué.

Démonstration
Faisons agir G sur G/H par translation à gauche :
$$g.xH := gxH,\ \forall g \in G, \forall x \in G$$
Comme $|G/H| = p$, cela définit un morphisme de groupes $f : G \to \mathfrak{S}_p$. Ce morphisme est non trivial car l'action est transitive.
Notons K son image. Alors $|K|$ divise à la fois $|G|$ et $|\sigma_p| = p!$. Donc il divise $pgcd(|G|, p!) = p$. Donc $|K| = p$.
Comme $G/\ker(f) \xrightarrow{\sim} K$, l'indice de $\ker(f)$ dans G est p. Or les éléments de $\ker(f)$ laissent fixe eH. Donc $\ker(f) \subseteq H$. Comme les deux sont d'indice p dans G, ils sont égaux et $H = \ker(f)$ est distingué. □

Théoreme 4.3.8 (Deuxième théorème d'isomorphisme)
Soient G un groupe, H un sous-groupe distingué et $K \subseteq G$ un sous-groupe . Alors $HK = \{hk | h \in H, k \in K\}$ est un sous-groupe de G et on a un isomorphisme de groupes
$$K/H \cap K \xrightarrow{\sim} HK/H$$

Exemple 4.3.9
Si F, G sont des sous espaces vectoriels d'un espace vectoriel E, on a
$$F/F \cap G \xrightarrow{\sim} F + G/F$$

Démonstration
Montrons que HK est un sous-groupe :
$e = e \cdot e \in HK$. Si $x, x' \in H$ et $y, y' \in K$, on a :
$$(xy)^{-1} = y^{-1}x^{-1} = y^{-1}x^{-1}yy^{-1} \in HK$$

et

$$xyx'y' = xyx'y^{-1}yy' \in HK$$

La composée

$$K \hookrightarrow HK \twoheadrightarrow HK/H$$

est un morphisme de groupes surjectif dont le noyau est $K \cap H$. Par le premier théorème d'isomorphisme , on obtient l'isomorphisme $K/H \cap K \xrightarrow{\sim} HK/H$. □

Théoreme 4.3.10 (Troisième théorème d'isomorphisme)
Soient $H \subseteq K$ deux sous-groupes distingués d'un groupe G. Alors, on a

$$G/K \xrightarrow{\sim} (G/H)\big/(K/H)$$

Démonstration
La composée des surjections canoniques

$$G \twoheadrightarrow G/H \twoheadrightarrow (G/H)\big/(K/H)$$

est un morphisme de groupes surjectif de noyau K. Le premier théorème d'isomorphisme nous donne l'isomorphisme

$$G/K \to (G/H)\big/(K/H)$$

□

Remarque 4.3.11
En particulier, si G et K sont finis et $f : G \to K$ est un morphisme de groupes, alors l'ordre de l'image de f divise à la fois $|G|$ et $|K|$

Exemple 4.3.12
Soit $n \geq 1$ un entier. Soit K un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Alors $K = d\mathbb{Z}/n\mathbb{Z}$ pour un diviseur d de n. On a

$$\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}\big/d\mathbb{Z}/n\mathbb{Z}$$

Chapitre 5

Sous-groupes de Sylow

5.1 Définition et exemples

Motivation

Le théorème de Lagrange affirme que si H est un sous-groupe de G, alors l'ordre de H est un diviseur de l'ordre de G. On peut se demander si réciproquement, pour tout diviseur d de l'ordre de G, il existe un sous-groupe d'ordre d.

Ceci est faux, par exemple $\mathscr{A}_4$ est d'ordre 12 et n'admet pas de sous-groupe d'ordre 6.

Néanmoins, nous allons voir que si d est une **puissance maximale d'un nombre premier** divisant l'ordre du groupe G, il existe toujours un sous-groupe d'ordre d. Ces sous-groupes sont les **sous-groupes de Sylow**.

Soit G un groupe fini. soit n son ordre. Soit p un diviseur premier de n. On a donc $n = p^\alpha \cdot m$, où α est un entier ≥ 1, et m n'est pas divisible par p.

Définition 5.1.1

*Un **p-sous-groupe de Sylow** (ou p-Sylow) est un sous-groupe P d'ordre p^α de G.*

Remarque 5.1.2

On montrera que pour tout diviseur premier p de $|G| = n$, il **existe** un p-Sylow, et que tous les p-Sylow sont **conjugués**.

Exemple 5.1.3

1. $G = D_3 = \{Id, \sigma_A, \sigma_B, \sigma_C, \rho, \rho^2\}$

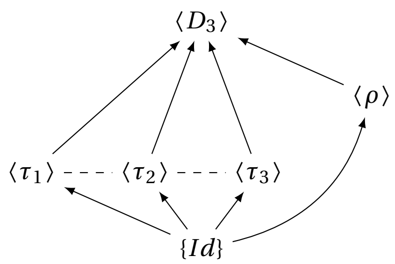


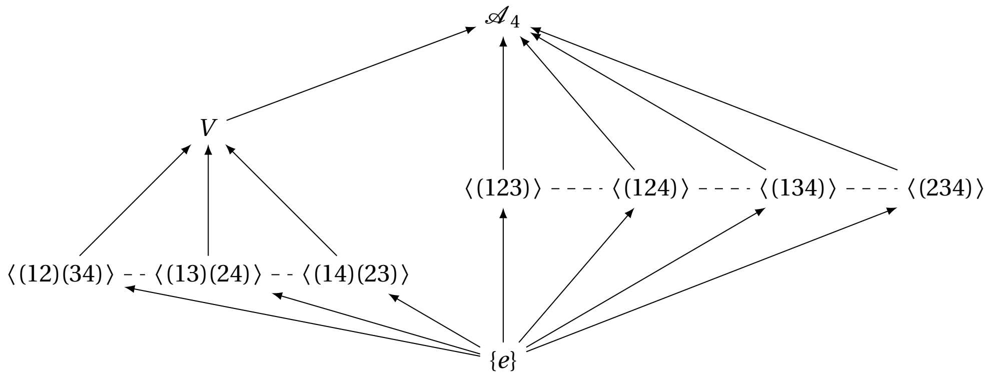
FIGURE 5.1 – Diagramme de Hasse du groupe diédral 3

On a $|D_3| = 2 \times 3$.

D_3 admet trois 2-Sylow $\langle \tau_1 \rangle$, $\langle \tau_2 \rangle$, $\langle \tau_3 \rangle$. Ils sont tous conjugués.

D_3 admet un unique 3-Sylow $\langle \rho \rangle$. Il est distingué.

2. $G = \mathscr{A}_4$



$|\mathscr{A}_4| = 12 = 4 \times 3$ et $V = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. $\mathscr{A}_4$ admet V pour unique 2-Sylow (on l'appelle le sous-groupe de Klein V). Il est distingué.
$\mathscr{A}_4$ admet quatre 3-Sylow $\langle (1\,2\,3) \rangle$, $\langle (1\,2\,4) \rangle$, $\langle (1\,3\,4) \rangle$, $\langle (2\,3\,4) \rangle$. Ils sont tous conjugués.

3. $G = \mathbb{U}_{12}$. On a $|G| = 12 = 2^2 \times 3$
Les 2-Sylow sont d'ordre 4. Il y en a un seul : $\mathbb{U}_4 < \mathbb{U}_{12}$
Les 3-Sylow sont d'ordre 3. Il y en a un seul : $\mathbb{U}_3 < \mathbb{U}_{12}$.

4. $G = \mathfrak{S}_4$. On a $|\mathfrak{S}_4| = 24 = 2^3 \times 3$.
Les 2-Sylow sont les sous-groupes d'ordre 8. Soit σ un 4-cycle de $\mathfrak{S}_4$.
Soient $a, b, c, d \in \{1, 2, 3, 4\}$ tel que $\sigma = (a\ b\ c\ d)$
Alors $P = \langle \sigma, (a\ c) \rangle$ est un 2-Sylow de $\mathfrak{S}_4$ constitué de :
   — Id
   — les transpositions $(a\ c)$ et $(b\ d)$
   — les 3 doubles transpositions :
$$(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)$$
   — les deux 4-cycles : σ et
$$\begin{aligned} \sigma^{-1} &= (a\ b\ c\ d) \\ &= (a\ c)\sigma(a\ c)^{-1} \\ &= (b\ d)\sigma(b\ d)^{-1} \end{aligned}$$
Notons que P n'est pas distingué dans $\mathfrak{S}_4$.
Les 3-Sylow de $\mathfrak{S}_4$ sont les sous-groupes d'ordre 3.
Ils sont tous de la forme $\langle c \rangle$, où c est un 3-cycle (exercice : compter le nombre de 3-cycles et le nombre de sous-groupe d'ordre 3). Ils sont tous conjugués.

5. $G = \mathfrak{S}_5$. On a $|G| = 120 = 2^3 \times 3 \times 5$
Les 2-Sylow de $\mathfrak{S}_3$ sont les sous-groupes d'ordre 8.
Les 3-Sylow sont les sous-groupes d'ordre 3. Donc ils sont tous de la forme $\langle c \rangle$, où c est un 3-cycle.
Les 5-Sylow sont les sous-groupes d'ordre 5. Ils sont tous de la forme $\langle c \rangle$, où c est un 5-cycle.

6. $G = D_4$. On a $|G| = 8 = 2^3$. Il y a un unique 2-Sylow, à savoir D_4 lui-même.

Le prochain but est de montrer qu'il existe toujours des p-Sylow.

5.2 Digression arithmétique

Définition 5.2.1
*Un **anneau** est un triplet* $(A,+,\bullet)$*, où* $(A,+)$ *est un groupe abélien et*

$$\bullet : A \times A \longrightarrow A$$

un loi telle que :

1. *est associative :* $(ab)c = a(bc), \quad \forall a,b,c \in A$
2. *admet un élément neutre 1 :* $1.a = a = a \cdot 1, \quad \forall a \in A$
3. *est distributive à gauche et à droite par " + " :*

$$(a+b)c = ac+bc \qquad \textit{et} \qquad a(b+c) = ab+ac, \quad a,b,c \in A$$

*L'anneau A est **commutatif** si* $ab = ba, \quad \forall a,b \in A$

Exemple 5.2.2

1. $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ sont des anneaux commutatifs.
2. $M_2(\mathbb{R})$ est un anneau non commutatif
3. Soit $n \geq 1$ un entier. Alors $\mathbb{Z}/n\mathbb{Z}$ est un anneau pour l'addition habituelle et la multiplication définie par
$$\overline{a}\cdot\overline{b} = \overline{ab}, \quad \overline{a},\overline{b} \in \mathbb{Z}/n\mathbb{Z}$$
où $\overline{a} = a + n\mathbb{Z}$
4. Si A est un anneau commutatif, alors
$$\begin{aligned} A[X] :&= \{\text{polynômes en } X \text{ à coefficients dans } A\} \\ &= \left\{ \sum_{k=1}^{n} a_k X^k \middle| n \in \mathbb{N}, a_k \in A, \forall k \right\} \end{aligned}$$
est un anneau commutatif pour l'addition et la multiplication naturelles des polynômes.

Soit p un nombre premier.

Lemme 5.2.3
Dans $(\mathbb{Z}/p\mathbb{Z})[X]$*, on a* $(P+Q)^p = P^p + Q^p, \quad \forall P,Q \in (\mathbb{Z}/p\mathbb{Z})[X]$

Démonstration
Par le binôme de Newton (valable dans tout anneau commutatif), on a

$$(P+Q)^p = P^p + Q^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot P^k \cdot Q^{p-k}$$

Il suffit de montrer que p divise $\binom{p}{k}$ pour $1 \leq k \leq p-1$.
Or on a :

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

et p divise le numérateur mais pas le dénominateur. □

Lemme 5.2.4
Si s, m sont des entiers naturelles tel que p ne divise pas s, alors $\binom{s.p^m}{p^m}$ *est congru à s modulo p.*

Démonstration
La quantité $\binom{s.p^m}{p^m}$ modulo p est le coefficient de X^{p^m} dans le développement du binôme

$$(X+1)^{p^m} \in \mathbb{Z}/p\mathbb{Z}[X]$$

Or, on a :
$$(X+1)^{s.p^m} = \left((X+1)^{p^m}\right)^s \underset{\text{lemme 5.2.3}}{=} (X^{p^m}+1^{p^m})^s = 1 + s\cdot X^{p^m} + \dots$$
□

5.3 Les théorèmes de Sylow

Soit G un groupe fini et $n = |G|$. Soit p un nombre premier qui divise n. Écrivons $n = s\cdot p^m$, où p ne divise pas s ($i.e$ p^m est la puissance maximale de p qui divise n). Alors, par définition, les p-Sylow de G sont les sous-groupes d'ordre p^m.

Théoreme 5.3.1 (Premier théorème de Sylow)
Il existe au moins un p-Sylow dans G.

Démonstration
Soit S l'ensemble des parties de G ayant p^n éléments.
On a :
$$|S| = \binom{s\cdot p^n}{p^n} \underbrace{\equiv}_{\text{lemme 2}} s \neq 0 \mod p$$
La translation à gauche par un élément de G transforme une partie à p^n éléments en une partie à p^n éléments (car $l_g : G \to G,\ g' \mapsto gg'$ est bijective de réciproque $l_{g^{-1}}$). On a donc une action par translations à gauche :
$$G\times S \to S,\ (g,E) \mapsto gE = \{gs \mid s \in E\}$$
L'équation aux classes associées est
$$|S| = \sum_{O \text{ orbite}} |O|$$
Comme $|S| = \binom{sp^n}{p^n} \equiv s \mod p$ n'est pas divisible par p au moins l'une des orbites est de cardinal non divisible par p. Prenons un élément A d'une telle orbite et considérons son stabilisateur $H = \mathrm{Stab}_G(A)$. On va montrer que H est un p-Sylow, c'est à dire $|H| = p^n$. Comme on a :

$$|G/H| = |G\cdot A|\ et\ |G| = |H|\cdot|G\cdot A|$$

et p ne divise pas $|G\cdot A|$, p^n doit diviser $|H|$.
De l'autre côté, on a $h\cdot A = A$ pour tout $h \in H$. Donc l'action de H par translation à gauche laisse stable A et A est réunion de H-orbites $H\cdot a$, $a \in A$.
Or $|H\cdot a| = |H|$ car $H\cdot a$ est en bijection avec H via la translation à droite par a^{-1}. Donc $|H|$ divise $|A| = p^n$.
Finalement, on obtient bien que $|H| = p^n$. □

Théoreme 5.3.2 (Deuxième théorème de Sylow)
Soit K un sous-groupe de G et soit H un p-Sylow de G. Alors il existe un conjugué H' de H tel que $H'\cap K$ est un p-Sylow de K.

Corollaire 5.3.3
1. *Si $K \leq G$ est un p-sous-groupe, alors K est contenu dans un p-Sylow de G.*

2. *Les p-Sylow de G sont tous conjugués.*

Démonstration (Démonstration du corollaire)

1. Le deuxième théorème nous fournit un p-Sylow H' de G tel que $K \cap H'$ est un p-Sylow de K. Comme K est un p-groupe, on a $K = K \cap H'$, autrement dit : $K \subset H'$

2. Soient K et H deux p-Sylow de G. Par le deuxième théorème, il existe un conjugué H' de H tel que $H' \cap K$ est un p-Sylow de K. Or K est un p-groupe. Donc $H' \cap K = K$ et $K \subset H'$. Or K et H' sont tous les deux d'ordre p^m. Donc $K = H'$ est bien conjugué à H.

Démonstration (Démonstration du deuxième théorème de Sylow)

On a un sous-groupe $K \leq G$ et un p-Sylow $H \subseteq G$, et on doit montrer qu'on peut conjuguer H en un p-Sylow H' tq $H' \cap K$ est un p-Sylow de K.

Soit S l'ensemble des classes G/H. On aura besoin des faits suivants : G opère transitivement sur G/H (par translation à gauche : $g \cdot xH = gxH$) et H est le stabilisateur de l'un des points de S, à savoir : $s = eH$.
Donc le stabilisateur de as, $a \in G$ est : aHa^{-1} (si G agit sur X et $x \in X$ et $g \in G$, alors $Stab_G(gx) = gStab_G(x)g^{-1}$ comme on le vérifie facilement. La conjugaison $h \mapsto ghg^{-1}$ donne la bijection).
Nous restreignons l'action de G sur S à K. Comme H est un p-Sylow, le cardinal de $|S| = |G/H| = |G|/|H| = sp^m/p^m = s$ n'est pas divisible par p.
Donc le cardinal d'au moins l'une des K-orbites, disons O, n'est pas divisible par p.
Supposons que O est l'orbite du point as pour un $s \in G$.
Soit $H' = aHa^{-1}$ le stabilisateur de as pour l'action de G. Alors le stabilisateur de as pour l'action restreinte à K est clairement $K \cap H'$ et l'indice $[K : H' \cap K]$ est $|O|$, qui n'est pas divisible par p. En outre, $K \cap H'$ est un p-groupe en tant que sous-groupe de H' (qui est un p-groupe car conjugué de H). Donc $H' \cap K$ est un p-groupe.
Il s'ensuit que $H' \cap K$ est bien un p-Sylow de K. □

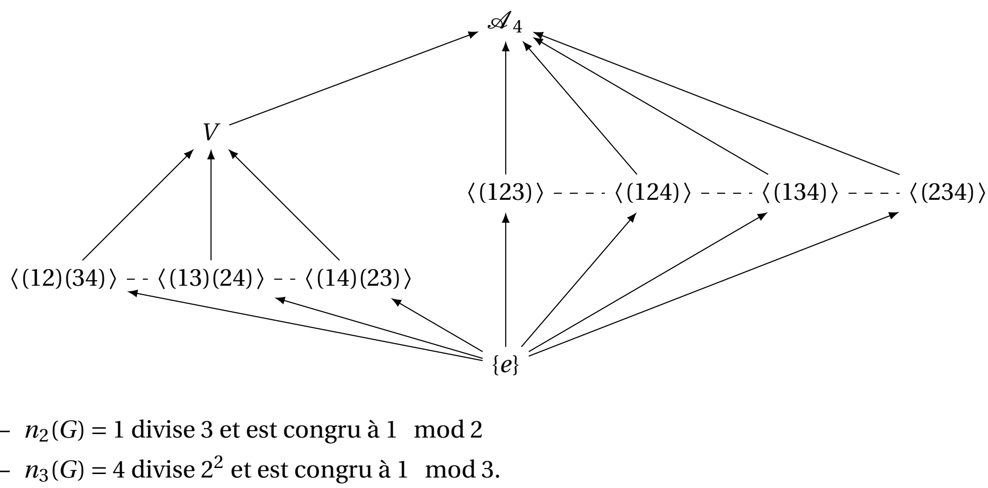
Théoreme 5.3.4 (Troisième théorème de Sylow)

Soit $n_p(G)$ le nombre de p-Sylow de G.
Alors $n_p(G)$ divise s et est congru à $1 \mod p$.

Exemple 5.3.5

1. $G = D_3$, $|G| = G = 2 \times 3$
   — $n_2(G) = 3$ divise bien $s = 3$ et est congru à $1 \mod 2$
   — $n_3(G) = 1$ divise bien $s = 2$ et est congru à $1 \mod 3$

2. $G = \mathscr{A}_4$, $|G| = 12 = 2^2 \times 3$



   — $n_2(G) = 1$ divise 3 et est congru à $1 \mod 2$
   — $n_3(G) = 4$ divise 2^2 et est congru à $1 \mod 3$.

Démonstration (Démonstration du troisième théorème de Sylow)
Par le corollaire, les p-Sylow de G sont tous conjugués à l'un d'entre eux, disons H. Soit $N = N_G(H)$ le normalisateur de H. Alors N est le stabilisateur de H dans l'action de G par conjugaison sur les p-Sylow.
Donc $n_p(G) = [G : N]$ est le cardinal de l'orbite de H.
Comme $H \subseteq N$, $[G : N]$ divise $[G : H] = s$
Pour montrer que $n_p(G) \equiv 1 \mod p$, on décompose l'ensemble des p-Sylow $\left\{H_1, H_2, \ldots, H_{n_p(G)}\right\}$ en orbite sous l'action de conjugaison par $H = H_1$.
Une orbite ponctuelle est formée d'un seul sous-groupe H_i ssi H est contenu dans le normalisateur N_i de H_i. Si c'est le cas, alors H_i et H sont tous les deux des p-Sylow de N_i. Donc ils sont conjugués par un élément de N_i. Or H_i est distingué dans N_i, donc $H = H_i$.
Donc il n'existe qu'une seule orbite ponctuelle sous l'action de H sur les p-Sylow, à savoir $\{H\} = \{H_1\}$.
Les cardinaux des autres orbites divisent $|H|$, donc sont des multiples de p. Il s'ensuit que $n_p(G) \equiv 1 \mod p$. $\square$

Exemple 5.3.6
Soit G un groupe d'ordre 15. On va montrer que G est cyclique.
On a $|G| = 15 = 3 \times 5$
$n_3(G)$ divise 5 et est congru à $1 \mod 3$, donc $n_3(G) = 1$ et G admet un unique 3-Sylow P, qui est donc distingué (car pour $g \in G$, le conjugué gPg^{-1} est encore un $3 - Sylow$ et donc $gPg^{-1} = P$) et d'ordre 3.
$n_5(G)$ divise 3 et est congru à 1 modulo 5. Donc $n_5(G) = 1$. Donc G admet un unique 5-Sylow Q qui forcément est distingué.
On a $P \cap Q = \{e\}$ car $|P \cap Q|$ divise à la fois $|P| = 3$ et $|Q| = 5$.
On a $P \cong \mathbb{U}_3$ et $Q \cong \mathbb{U}_5$ car 3 et 5 sont premiers.
Pour $x \in P$ et $y \in Q$, on a $xy = yx$, car le commutateur $xyx^{-1}y^{-1}$ appartient à la fois à P et à Q car P et Q sont distingués.
Donc on a un morphisme de groupes bien défini :

$$\varphi : P \times Q \to G,\ (x, y) \mapsto xy$$

Son noyau est formé des (x, y) tq $xy = e \Leftrightarrow x = y^{-1}$.
Donc $\ker(\varphi) = \{e\}$. Donc φ est injectif. Comme $|P \times Q| = 15 = |G|$, φ est aussi surjectif.
Donc φ est un isomorphisme

$$G \simeq P \times Q \simeq \mathbb{U}_3 \times \mathbb{U}_5 \cong \mathbb{U}_{15} \quad \text{car pgcd}(3, 5) = 1$$

Chapitre 6

Théorèmes de classification

6.1 Un outil : le produit semi-direct

Définition 6.1.1

Soient G un groupe et $N \lhd G$ un sous-groupe distingué. Un ***complément*** *de N dans G est un sous-groupe $K < G$ tel que*

$$K \cap N = \{e\} \quad \textit{et} \quad K \cdot N = G$$

Remarque 6.1.2

Notons que comme N est distingué, $K \cdot N$ est un sous-groupe et en fait égal à $N \cdot K$.

Exemple 6.1.3

1. Rappelons-nous le treillis des sous-groupes de D_3

$$\begin{tikzcd}
 & \langle D_3 \rangle & & \\
 & & & \langle \rho \rangle \arrow[ull] \\
\langle \tau_1 \rangle \arrow[uur] \arrow[r, dashed, no head] & \langle \tau_2 \rangle \arrow[uu] \arrow[r, dashed, no head] & \langle \tau_3 \rangle \arrow[uul] & \\
 & \{Id\} \arrow[ul] \arrow[u] \arrow[ur] \arrow[uurr, bend right] & &
\end{tikzcd}$$

   Le sous-groupe $N = \langle \rho \rangle$ est distingué et chacun des $\langle \tau_i \rangle$, où τ_i est la i-ème symétrie, est un complément.

2. Plus généralement, dans $G = D_n$, le sous-groupe des rotations $N = \langle \rho \rangle$ est distingué et chaque sous-groupe $K = \langle \tau \rangle$, où τ est une symétrie, est un complément.

3. Si E est un espace vectoriel et $F \subset E$ un sous-espace, alors tout supplémentaire G (i.e. $E = F \oplus G$) est un complément du sous-groupe $N = F$ de $G = E$.

Remarque 6.1.4

Soient G un groupe, $N \lhd G$ et K un complément. Alors par le deuxième théorème d'isomorphisme, on a

$$G/N = KN\big/N \cong K\big/N \cap K = K$$

Donc si K_1 et K_2 sont deux compléments, alors $K_1 \cong K_2$.

Définition 6.1.5
Soient G un groupe, N un sous-groupe distingué et K un complément de N.
*Alors G est **le produit semi-direct interne** de N par K, en symboles :* $G = N \overset{i}{\rtimes} K$

Exemple 6.1.6
$D_n = \langle \rho \rangle \overset{i}{\rtimes} \langle \tau \rangle$, où ρ engendre le sous-groupe des rotations et τ est une symétrie quelconque.

6.2 Produit semi-direct externe

Rappel
Si G est un groupe. $\mathrm{Aut}(G)$ désigne le groupe des automorphismes de G, i.e. des morphismes de groupes bijectifs $\varphi : G \xrightarrow{\sim} G$.

Définition 6.2.1
Soient K et N des groupes et

$$u : K \to \mathrm{Aut}(N),\ k \mapsto u_k$$

*un morphisme de groupes. Le **produit semi-direct externe** $N \underset{u}{\rtimes} K$ est l'ensemble $N \times K$, muni de la loi définie par* $(n,k)\cdot(n',k') = \big(n\cdot u_k(n'), k\cdot k'\big), \quad \forall n, n' \in N,\ \forall k, k' \in K$

Remarque 6.2.2
Si u est trivial (i.e. $u_k = \mathrm{Id}_N,\ \forall k \in K$), alors le produit semi-direct externe se réduit au produit direct : $N \underset{u}{\rtimes} K = N \times K$

Lemme 6.2.3
1. *$N \underset{u}{\rtimes} K$ est un groupe*
2. *$N \underset{u}{\rtimes} K$ est le produit semi-direct interne de son sous-groupe distingué $N \times \{e\}$ par le complément $\{e\} \times K$.*

Démonstration
1. Montrons l'associativité de la multiplication :

$$\begin{aligned}\big((n,k),(n',k')\big)\cdot(n'',k'') &= \big(n\cdot u_k(n'), k\cdot k'\big)\cdot(n'',k'') \\ &= \big(n\cdot u_k(n')\cdot u_{k\cdot k'}(n''), k\cdot k'\cdot k''\big) \\ &= \big(n\cdot u_k(n')\cdot u_k\cdot u_{k'}\cdot(n''), k\cdot k'\cdot k''\big)\end{aligned}$$

$$\begin{aligned}(n,k)\cdot\big((n',k'),(n'',k'')\big) &= (n,k)\cdot\big(n'\cdot u_{k'}(n''), k'\cdot k''\big) \\ &= \big(n\cdot u_k\big(n'\cdot u_{k'}(n'')\big), k\cdot k'\cdot k''\big) \\ &= \big(n\cdot u_k(n')\cdot u_k\big(u_{k'}(n'')\big), k\cdot k'\cdot k''\big)\end{aligned}$$

Montrons que (e,e) est un élément neutre :

$$\begin{aligned}(n,k)(e,e) &= (nu_K(e), ke)\\ &= (ne, ke) = (n,k)\end{aligned}$$

$$\begin{aligned}(e,e)(n,k) &= (eu_K(n), ek)\\ &= (e\,\mathrm{Id}_N(n), ek)\\ &= (n,k)\\ & n\in N,\ k\in K\end{aligned}$$

Montrons que $\left(u_{K^{-1}}(n^{-1}), k^{-1}\right)$ est l'inverse de $(n,k) \in N \underset{u}{\rtimes} K$

$$\begin{aligned}\left(u_{K^{-1}}(n^{-1}\right)(n,k) &= \left(u_{K^{-1}}(n^{-1})\cdot u_{K^{-1}}(n), k^{-1}k\right)\\ &= \left(u_{K^{-1}}(n^{-1}\cdot n), k^{-1}k\right) = (e,e)\end{aligned}$$

$$\begin{aligned}(n,k)\left(u_{K^{-1}}(n^{-1}, k^{-1}\right) &= \left(n\cdot u_K\left(u_{K^{-1}}(n^{-1})\right), kk^{-1}\right)\\ &= \left(nu_{KK^{-1}}(n^{-1}), kk^{-1}\right)\\ &= \left(n\,\mathrm{Id}(n^{-1}, e\right) = (e,e)\end{aligned}$$

2. Montrons que $N\times\{e\}$ est distingué dans $N \underset{u}{\rtimes} K$:

$$\begin{aligned}(n,k)(n',e)\left(u_{K^{-1}}(n^{-1}), k^{-1}\right) &= \left(nu_K(n'), k\right)(u_{K^{-1}}(n^{-1}), k^{-1})\\ &= \left(n\cdot u_K(n')\cdot u_K\left(u_{K^{-1}}(n^{-1})\right), kk^{-1}\right)\\ &= \left(n\cdot u_K(n')n^{-1}, e\right) \in N\times\{e\}\end{aligned}$$

Il est clair que $\left(N\times\{e\}\right)\cap\left(\{e\}\times K\right) = \{e\}\times\{e\} = e_{N \underset{u}{\rtimes} K}$
Montrons que $\left(N\times\{e\}\right)\cdot\left(\{e\}\times K\right) = N \underset{u}{\rtimes} K$

$$(n,e)\cdot(e,k) = (nu_e(e), ek) = (n,k)$$

pour $n\in N,\ k\in K$ □

Lemme 6.2.4
Supposons que $G = N \overset{i}{\rtimes} K$. *Soit*

$$u : K \to \mathrm{Aut}(N), \quad k \mapsto (n \mapsto knk^{-1})$$

Alors on a un isomorphisme canonique :

$$\varphi : N \underset{u}{\rtimes} K \xrightarrow{\sim} N \overset{i}{\rtimes} K = G, \quad (n,k)\mapsto nk$$

Exemple 6.2.5
On a $D_n = \underbrace{\langle\rho\rangle}_{N} \overset{i}{\rtimes} \underbrace{\langle\tau\rangle}_{K}$, où ρ engendre le sous-groupe des rotations et τ est une symétrie.
On a $\tau\rho\tau^{-1} = \rho^{-1}$. Donc si :

$$u : \langle\tau\rangle \to \mathrm{Aut}(\langle\rho\rangle), \quad \tau \mapsto (\rho^l \mapsto \rho^{-l})$$

Alors : $D_n \xleftarrow{\sim} \langle\rho\rangle \underset{u}{\rtimes} \langle\tau\rangle$
Notons qu'on a $\langle\rho\rangle \simeq \mathbb{Z}/n\mathbb{Z}, \quad \langle\tau\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ et donc

$$D_n \xleftarrow{\sim} \mathbb{Z}/n\mathbb{Z} \underset{u}{\rtimes} \mathbb{Z}/2\mathbb{Z}$$

où

$$u : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad \bar{1} \mapsto (\overline{a} \mapsto -\overline{a})$$

Démonstration (Démo du lemme)
Vérifions que φ est un morphisme

$$\begin{aligned}
\varphi\big((n,k),(n',k')\big) &= \varphi\big((nu_K(n'),kk'\big) \\
&= n \cdot u_K(n')kk' \\
&= nkn'k^{-1}kk' \\
&= nkn'k' \\
&= \varphi\big((n,k)\big) \cdot \varphi\big((n',k')\big)
\end{aligned}$$

où $n, n' \in N, \quad k, k' \in K$. Clairement φ est surjectif. Le noyau de φ est formé des couples (n,k) tel que $nk = e$, i.e. $n = k^{-1} \in N \cap K = \{e\}$. □

6.3 Les groupes d'automorphismes des groupes cycliques

Définition 6.3.1
*Soit A un anneau. Un élément de $a \in A$ est **inversible** s'il existe $a \in A$ tel que $aa' = 1 = a'a$.*
On note A^* l'ensemble des éléments inversibles.

Remarque 6.3.2
A^* est un groupe pour la multiplication.

Exemple 6.3.3

1. $M_n(\mathbb{R})^* = Gl_n(\mathbb{R})$

2. On a :

$$\begin{aligned}
(\mathbb{Z}/n\mathbb{Z})^* &= \left\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \,\middle|\, \exists \overline{a'} \quad \text{tel que} \quad \overline{a}\overline{a'} = \overline{1}\right\} \\
&= \left\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \,\middle|\, \exists a', k \in \mathbb{Z} \quad \text{tel que} \quad a'a + kn = 1\right\} \quad \text{identité de Bézout} \\
&= \left\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \,\middle|\, \mathrm{pgcd}(a,n) = 1\right\}
\end{aligned}$$

En particulier, si p est un nombre premier, on a :

$$(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\} \qquad \text{est d'ordre } p-1$$

On peut montrer qu'en fait $(\mathbb{Z}/p\mathbb{Z})^*$ est **cyclique** d'ordre $p-1$

Définition 6.3.4
*Un **corps commutatif** est un anneau commutatif A où $1 \neq 0$ et tout élément non nul est inversible.*

Exemple 6.3.5
Si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Les anneaux $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps. L'anneau $\mathbb{Z}$ n'est pas un corps car $\mathbb{Z}^* = \{1, -1\}$.

Théoreme 6.3.6
Si K est un corps commutatif fini (i.e K n'a qu'un nombre fini d'éléments), alors $K^* = K \setminus \{0\}$ est cyclique.
En particulier, si p est premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique d'ordre $p-1$.

Remarque 6.3.7
Si A est un anneau, on a un morphisme naturel

$$A^* \to \operatorname{Aut}\big((A,+)\big), \quad a \mapsto (b \mapsto ab)$$

En effet, on a $a(b+b') = ab + ab'$ et $(aa')b = a(a'b), \quad \forall a, a' \in A^*, \forall b, b' \in A$

Lemme 6.3.8
Le morphisme naturel

$$\begin{aligned} f : (\mathbb{Z}/n\mathbb{Z})^* &\to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ \bar{a} &\mapsto (\bar{b} \mapsto \bar{a}\bar{b}) \end{aligned}$$

est un isomorphisme. En particulier, si p est premier, alors $\operatorname{Aut}(\mathbb{Z}/p\mathbb{Z})$ *est cyclique d'ordre* $p-1$.

Démonstration
Clairement f est un morphisme.
f est injectif car $\bar{b} \mapsto \bar{a}\bar{b}$ est l'identité ssi $\bar{a} \cdot 1 = 1$
Montrons que f est surjectif. Soit $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ un automorphisme. Alors $\varphi(\overline{1})$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$
Or cela signifie que $\varphi(\overline{1}) = \overline{a}$ pour un $a \in \mathbb{Z}$ tel que $\operatorname{pgcd}(a,n) = 1$
Pour $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$, on a :

$$\begin{aligned} \varphi(\overline{b}) &= \varphi(\underbrace{1+1+\ldots+1}_{b}) \\ &= \underbrace{\varphi(1)+\varphi(1)+\ldots+\varphi(1)}_{b} \\ &= \overline{a}+\ldots+\overline{a} \\ &= \overline{a}.\overline{b} \\ &= \big(f(\overline{a})\big)(\overline{b}) \end{aligned}$$

Donc $\varphi = f(\bar{a})$ □

6.4 Classification des groupes d'ordre pq, p < q premiers

Théoreme 6.4.1
Soient $p < q$ premiers et G un groupe d'ordre pq. Alors ou bien G est cyclique ou bien isomorphe à un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_u \mathbb{Z}/p\mathbb{Z}$ pour un $u : \mathbb{Z}/p\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ non trivial.

Remarque 6.4.2
Comme $\operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique d'ordre $q-1$, il existe un

$$u : \mathbb{Z}/p\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$$

non trivial ssi $\mathbb{Z}/(q-1)\mathbb{Z}$ admet un sous-groupe d'ordre p
ssi p divise $q-1$ ssi $q \equiv 1 \mod p$. Donc pour $p < q$:

— $q \neq 1 \mod p \Rightarrow$ tout groupe d'ordre pq est cyclique.
— $q \equiv 1 \mod p \Rightarrow$ tout groupe d'ordre pq est ou bien cyclique ou bien un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_u \mathbb{Z}/p\mathbb{Z}$

C'est le cas par exemple pour $pq = 21$ car $7 \equiv 1 \mod 3$.

Exemple 6.4.3 (Exemple d'application)
Un groupe d'ordre $6 = 2 \times 3$ est ou bien cyclique ou bien isomorphe à

$$\mathbb{Z}/3 \underset{u}{\rtimes} \mathbb{Z}/2 \simeq D_3 \simeq \mathfrak{S}_3, \quad D_3 \text{ permute les sommets au triangle}$$

Donc à isomorphisme près, $\mathbb{Z}/6$ et $D_3 \simeq \mathfrak{S}_3$ sont les seuls groupes d'ordre 6.
Soit G un groupe d'ordre $15 = 3 \times 5$. On a $5 \neq 1 \mod 3$. Donc par le théorème, G est cyclique.

Démonstration
Le premier théorème de Sylow nous affirme l'existence d'au moins un sous-groupe P d'ordre p et d'au moins un sous-groupe Q d'ordre q. Tous deux sont cycliques et isomorphes à $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ respectivement. Remarquons que comme $\mathrm{pgcd}(p, q) = 1$, on a $P \cap Q = \{e\}$
Enfin P et Q engendrent le sous-groupe G, seul sous-groupe contenant strictement P et Q.
Le 3ème théorème de Sylow nous indique si $n_q(G)$ est le nombre de q-Sylow de G, alors $n_q(G)$ divise p est est congru à 1 modulo q.
Puisque $p < q$, la seule possibilité est $n_q(G) = 1$. Ainsi G admet Q pour q-Sylow unique et Q est donc distingué dans G.
Nous avons donc

$$\begin{aligned} G &= Q \cdot P = Q \overset{i}{\rtimes} P \\ &\simeq Q \underset{u}{\rtimes} P \\ &\simeq \mathbb{Z}/q\mathbb{Z} \underset{u}{\rtimes} \mathbb{Z}/p\mathbb{Z} \end{aligned}$$

Pour un $u : \mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/q) \simeq \mathbb{Z}/(q-1)$.
Si u est trivial, alors

$$\mathbb{Z}/q\mathbb{Z} \underset{u}{\rtimes} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$$

□

6.5 Classification des groupes d'ordre p^2, p premier

Soit p un nombre premier.

Lemme 6.5.1
Si G est un p-groupe (i.e. $|G|$ est une puissance de p), alors le centre $Z(G)$ est non trivial.

Démonstration
Écrivons l'équation aux classes pour l'action de conjugaison de G sur lui-même :

$$|G| = |Z(G)| + \sum_{O \text{ orbite non ponctuelle}} |O|$$

Les points fixes (= orbites ponctuelles) de cette action sont exactement les éléments du centre et les orbites non ponctuelles sont toutes de cardinal une puissance $\geq p$ de p.
Donc $|Z(G)|$ est congru à 0 modulo p, et comme $e \in Z(G)$, l'ordre de $Z(G)$ est au moins p. □

Lemme 6.5.2
Tout groupe d'ordre p^2 est abélien.

Remarque 6.5.3
Il existe des groupes d'ordre p^3 qui ne sont pas abéliens, par exemple D_4 qui est d'ordre 8.

Démonstration

Soit G un groupe d'ordre p^2. On va montrer que pour tout $x \in G$, le centralisateur

$$\mathbb{Z}_G(x) = \{y \in G \big| xy = yx\}$$

est le groupe G tout entier.
Soit $x \in G$. Si $x \in Z(G)$, alors $Z_G(x) = G$ comme annoncé.
Supposons donc que $x \notin Z(G)$. Alors $Z_G(x)$ est strictement plus grand que $Z(G)$ car il contient $Z(G)$ et en plus l'élément x. Or les ordres de $Z(G)$ et $Z_G(x)$ divisent p^2 et d'après le lemme précédent, l'ordre de $Z(G)$ est $\geq p$. Donc $|Z_G(x)| > p$ et divise $p^2 = |G|$. La seule possibilité est $|Z_G(x)| = p^2$ et $Z_G(x) = G$. □

Théoreme 6.5.4

Tout groupe d'ordre p^2 est ou bien cyclique isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou bien isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Démonstration

Comme l'ordre d'un élément divise p^2, deux cas sont possibles :

— 1er cas : Il existe un élément d'ordre p^2 et $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ est cyclique.

— 2ème cas : Tout élément autre que e est d'ordre p.

Soient x et y deux éléments d'ordre p et H_1 et H_2 les sous-groupes qu'ils engendrent.
On peut choisir y de telle façon qu'il ne soit pas une puissance de x.
Alors comme $y \notin H_1$, le sous-groupe $H_1 \cap H_2$ est strictement plus petit que H_2 qui est d'ordre p.
Donc $H_1 \cap H_2 = \{e\}$. De plus, H_1 et H_2 sont distingués dans G qui est abélien.
Puisque $y \notin H_1$, le groupe $H_1 H_2$ est strictement plus grand que H_1 et son ordre divise p^2.
Donc $H_1 \cdot H_2 = G$ et on a un isomorphisme $\mathbb{Z}/p \times \mathbb{Z}/p \simeq H_1 \times H_2 \xrightarrow{\sim} G$. □

6.6 Classification des groupes d'ordre 12

Théoreme 6.6.1

Tout groupe d'ordre 12 est isomorphe à l'un des uniques groupes suivants :

- $\mathbb{Z}/3 \times \mathbb{Z}/4$
- $\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$
- $\mathscr{A}_4$
- D_6
- $\tilde{\mathfrak{S}_3} := \mathbb{Z}/3 \rtimes_u \mathbb{Z}/4$, *$u$ non trivial*

Remarque 6.6.2

Notons que $\mathbb{Z}/3 \times \mathbb{Z}/4 \cong \mathbb{Z}/12$ et $\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \cong \mathbb{Z}/6 \times \mathbb{Z}/2$. Ce sont les seuls sous-groupes abéliens d'ordre 12 à isomorphisme près.
Le morphisme $u : \mathbb{Z}/4 \to \mathrm{Aut}(\mathbb{Z}/3) \cong \mathbb{Z}/2$ est l'**unique** morphisme **non trivial**.
Le groupe $\tilde{\mathfrak{S}_3}$ contient le sous-groupe $N = \langle(\bar{0}, \bar{2})\rangle \cong \mathbb{Z}/2$ qui est distingué dans $\tilde{\mathfrak{S}_3}$.
Le quotient $\tilde{\mathfrak{S}_3}/N$ est isomorphe à $\mathbb{Z}/3 \rtimes \mathbb{Z}/2 \cong \mathfrak{S}_3$. On a donc ce qu'on appelle une **suite exacte** :

$$\{e\} \to \mathbb{Z}/2 \xrightarrow{i} \tilde{\mathfrak{S}_3} \xrightarrow{p} \mathfrak{S}_3 \to \{e\}$$

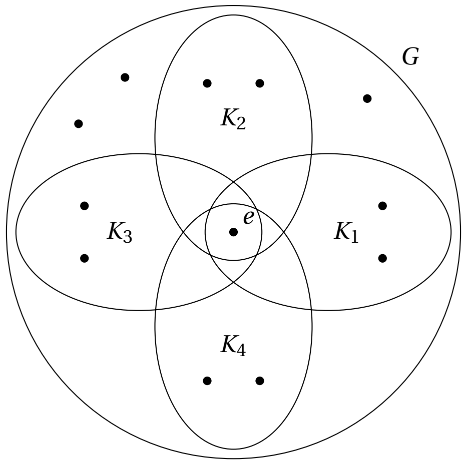
i.e i est injectif, p est surjectif et $\ker(p) = Im(i)$

Démonstration (Théorème)

Soit G un groupe d'ordre $12 = 3 \times 2^2$. Soit H un 2-Sylow de G (il est d'ordre 4) et soit K un 3-Sylow de G (il est d'ordre 3). D'après le 3ème théorème de Sylow, le nombre $n_2(G)$ divise 3 et est congru à 1 modulo 2. Donc $n_2(G) \in \{1, 3\}$. De même, le nombre $n_3(G)$ divise 4 et est congru à 1 modulo 3. En outre, $K \cong \mathbb{Z}/3$. Donc $n_3(G) \in \{1, 4\}$. En outre, H est d'ordre 4 et donc isomorphe à $\mathbb{Z}/4$ ou à $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Lemme 6.6.3
L'un au moins parmi les groupes H et K est distingué dans G.

Démonstration
Supposons que K n'est pas distingué. Alors K a 4 sous-groupes conjugués $K = K_1, K_2, K_3, K_4$.
Puisque $|K_i| = 3$, $\forall i$, l'intersection de deux quelconques de ces sous-groupes est réduite à l'identité. En comptant les éléments de G, on voit que seuls 3 éléments de G ne sont dans aucun des sous-groupes K_i.



Le 2-Sylow H est d'ordre 4 et $H \cap K_i = \{e\}$, $\forall i$.
Donc H est formé de e et de ces 3 éléments. Donc H est unique et par conséquent distingué. □

HK est un sous-groupe de G. Puisque $H \cap K = \{e\}$, chaque élément de HK a une **unique** expression comme produit hk, $h \in H$, $k \in K$. Puisque $|G| = 12$, on a $G = HK$.

— 1er cas : H et K sont tous les deux distingués.
Dans ce cas, on a $hk = kh$, pour tous $h \in H$, $k \in K$, car

$$hkh^{-1}k^{-1} \in H \cap K = \{e\}$$

avec $hkh^{-1} \in K$, $k^{-1} \in K, khk^{-1} \in H$, $h \in H$
Donc on a un isomorphisme $H \times K \xrightarrow{\sim} HK = G$, $(h,k) \mapsto hk$ et donc $G \simeq \mathbb{Z}/4 \times \mathbb{Z}/3$ ou $G \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3$, suivant que $H \cong \mathbb{Z}/4$ ou $H \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

Remarque 6.6.4
On verra que ce sont les seuls groupes abéliens d'ordre 12.

— 2ème cas : H est distingué mais K ne l'est pas.
Il y a donc 4 3-Sylow conjugués K_1, K_2, K_3, K_4. G agit par conjugaison sur cet ensemble X de 4 sous-groupes conjugués.
À cette action est associé un morphisme de groupes

$$\phi : G \longrightarrow \mathfrak{S}_4$$

On va montrer que ϕ induit un isomorphisme de G sur $\mathscr{A}_4 \subseteq \mathfrak{S}_4$. Le stabilisateur de K_i pour l'action de conjugaison est le normalisateur $N_G(K_i)$, qui contient K_i. Le cardinal de l'orbite est 4 et c'est aussi l'indice de $N_G(K_i)$ dans G (le cardinal d'une orbite est l'indice du stabilisateur de tout point de l'orbite).
Donc $N_G(K_i)$ est d'ordre 3 et $N_G(K_i) = K_i$. L'intersection des $N_G(K_i)$ est l'intersection des K_i, c'est-à-dire $\{e\}$.

Donc

$$\mathrm{Ker}(\phi) = \bigcap_{i=1}^{4} N_G(K_i) = \{e\}$$

ϕ est injectif et G est isomorphe à $Im(\phi)$
Puisque G a 4 sous-groupes d'ordre 3, il contient 8 éléments d'ordre 3 et ces 8 éléments engendrent G. Si x est d'ordre 3, $\phi(x)$ est d'ordre 3 donc un 3-cycle donc une permutation paire.
Donc $Im(\phi) \in \mathscr{A}_4$, et comme les deux sont d'ordre 12, on a $Im(\phi) = \mathscr{A}_4$

— 3ème cas : K est distingué mais H ne l'est pas
Dans ce cas, on a $G = K \overset{i}{\rtimes} H \simeq K \underset{u}{\rtimes} H$ pour un morphisme $u : H \longrightarrow \mathrm{Aut}(K)$ à déterminer.
Comme $K \simeq \mathbb{Z}/3$, on a $\mathrm{Aut}(K) \simeq \mathbb{Z}/2$, et il reste à voir comment les éléments de H agissent sur K par conjugaison (c'est cette action qui donne u). Supposons que H est cyclique engendré par x. Soit y un générateur de K. Comme G n'est pas abélien, on a $xy \neq yx$ et donc $xyx^{-1} = y^2$ (car y et y^2 sont les seuls générateurs de $K \cong \mathbb{Z}/3$). Donc $u : \underset{\mathbb{Z}/4}{H} \longrightarrow \underset{\mathbb{Z}/2}{\mathrm{Aut}(K)}$ est l'unique morphisme non trivial et on a $G \simeq \mathbb{Z}/3 \underset{u}{\rtimes} \mathbb{Z}/4 = \tilde{\mathfrak{S}}_3$.
La dernière possibilité est que $H \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. H contient 3 éléments d'ordre 2.
Puisque K n'a que deux automorphismes et H est d'ordre 4, il existe un élément $w \in H$ autre que l'identité qui agit trivialement sur K : $wyw^{-1} = y$.
Puisque G n'est pas abélien, il y a aussi un élément $v \in H$, qui agit non trivialement : $vyv^{-1} = y^2$.
Alors on a

$$H = \{e, v, w, vw\}$$

et $v^2 = w^2 = e$ et $vw = wv$.
L'élément $x = wy$ est d'ordre 6 et

$$vxv^{-1} = vwyv^{-1} = wy^2 = y^2 w = x^{-1}$$

On a donc x est d'ordre 6, v est d'ordre 2 et $vxv^{-1} = x^{-1}$, d'où un isomorphisme :

$$D_6 \xrightarrow{\sim} G$$
$$\rho \mapsto x$$
$$\tau \mapsto v$$

□

6.7 Classification des groupes abéliens finis

Notations dans les groupes abéliens

1. Soit A un groupe abélien. Soit $a \in A$. Pour $n \in \mathbb{N}$, on note $na = a + \ldots + a$ (cela correspond à g^n dans un groupe noté multiplicativement). On note $(-n)a = -na$ pour $n \in \mathbb{N}$. L'**ordre** de a est le plus petit entier $n \geq 1$, tq $na = 0$, respectivement $+\infty$ s'il existe pas de tel entier. On a $ma = 0$ ssi m est multiple de l'ordre de a. Si a est d'ordre n, on a un unique morphisme de groupes injectif :

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow A, \bar{k} \mapsto ka$$

   Son image est le sous-groupe $\langle a \rangle$ engendré par a.
2. Si A et B sont deux groupes abéliens, on note $A \oplus B := A \times B$ (somme directe externe).
   Si A est un groupe abélien et $B, C \subseteq A$ des sous-groupes on note $A = B \oplus C$ (somme directe interne) si $A = B + C$ et $B \cap C = \{0\}$ (i.e C est un complément de B dans A).

3. Si A est un groupe abélien et $A_1, \ldots, A_n$ des sous-groupes , on note $A = A_1 \oplus \ldots \oplus A_n$ si tout $a \in A$ s'écrit de façon unique sous la forme :

$$a = a_1 + \ldots + a_n$$

   pour des $a_i \in A_i$, $1 \leq i \leq n$. De façon équivalente :
   (a) $A = A_1 + \ldots + A_n$
   (b) $A_i \cap (A_1 + \ldots + \hat{A}_i + \ldots + A_n) = \{0\}$ ($\hat{A}_i$ = on omet A_i) pour tout $1 \leq i \leq n$.

Décomposition en p-Sylow

Remarque 6.7.1

Si A est abélien fini, tout sous-groupe est distingué. Donc A admet un **unique** p-Sylow noté A_p pour tout nombre premier p.

Théoreme 6.7.2

Soit A un groupe abélien fini. Alors A est la somme directe de ses p-Sylow. Autrement dit, on a :

$$A = A_{p_1} \oplus \ldots \oplus A_{p_k}$$

où les p_i sont les diviseurs premiers de $|A|$.

Exemple 6.7.3

$$\begin{aligned} \mathbb{Z}/12 &= (\mathbb{Z}/12)_2 \oplus (\mathbb{Z}/12)_3 \\ &\cong \mathbb{Z}/4 \oplus \mathbb{Z}/3 \end{aligned}$$

Démonstration

Par récurrence sur $|A|$. Si $|A| = 1$, alors $A = \{0\}$ et il n'y a rien à démontrer. Supposons $|A| > 1$.
Soit p un diviseur premier de $|A|$. Écrivons $|A| = p^e s$ où p ne divise pas s.
Décrivons $A_p \subseteq A$. On a :

$$\begin{aligned} p^e a = 0 \quad &\Leftrightarrow \quad \text{l'ordre de } a \text{ divise } p^e \\ &\Leftrightarrow \quad \langle a \rangle \text{ est un } p\text{-groupe} \\ &\Leftrightarrow \quad \langle a \rangle \subseteq A_p \text{ (car } A_p \text{ est le } \textbf{seul } p\text{-Sylow de } A) \\ &\Leftrightarrow \quad a \in A_p \end{aligned}$$

Donc $A_p = \{a \in A | p^e a = 0\}$. Posons $A_s := \{a \in A | sa = 0\}$. Montrons que $A = A_p \oplus A_s$.
Soit

$$1 = up^e + vs \quad , u, v \in \mathbb{Z}$$

est une identité de Bézout. Soit $a \in A_p \cap A_s$. Alors :

$$a = 1 \cdot a = (up^e + vs) \cdot a = up^e a + vsa = 0$$

Soit $a \in A$. On a $a = 1 \cdot a = up^e a + vsa$ et :

$$\begin{aligned} s(up^e a) = usp^e a = 0 \Rightarrow up^e a \in A_s \\ p^e(vsa) = vp^e sa = 0 \Rightarrow vsa \in A_p \end{aligned}$$

Par l'hypothèse de récurrence, on a :

$$A_s = (A_s)_{p_2} \oplus \ldots \oplus (A_s)_{p_k}$$

où les p_i sont les diviseurs premiers de $|A|$ autres que p. Et on a :

$$\begin{aligned} (A_s)_{p_i} &= \{a \in A_s | p_i^{e_i} a = 0\}, \text{ où } s = p_i^{e_i} s_i, \ p_i \text{ ne divise pas } s_i \\ &= \{a \in A | p_i^{e_i} a = 0\}, \text{ où } |A| = p_i^{e_i} p^e s, p_i \text{ ne divise pas } p^e s \\ &= A_{p_i} \end{aligned}$$

Donc $A = A_p \oplus \ldots \oplus A_{p_k}$ □

6.7.1 Classification des p-groupes abéliens

Remarque 6.7.4

On va montrer que tout p-groupe abélien est isomorphe à une somme directe de groupes $\mathbb{Z}/p^m$, $m \in \mathbb{N}$.

Lemme 6.7.5

Soit A un p-groupe abélien. Soit $a \in A$ un élément d'ordre maximal. Soit $\pi : A \to A/\langle a \rangle$ la projection canonique. Alors il existe $c \in A$ tel que $\pi(c) = b$ et tq c a même ordre que b.

Démonstration

Notons $ord(x)$ l'ordre d'un élément x. Soit $c' \in A$ tq $\pi(c') = b$.
Soit $k = ord(b)$. Alors $ord(c') \cdot b = ord(c')\pi(c') = \pi(ord(c')c') = \pi(0) = 0$. Donc $ord(c')$ est un multiple de $ord(b) = k$. Disons $ord(c') = kl$. Comme a est d'ordre maximal,$ord(c') = kl$ divise $ord(a)$. Disons $ord(a) = klm$. On a :

$$\pi(kc') = k\pi(c') = k \cdot b = 0$$

Donc $kc' = ia$ pour un $i \in \mathbb{N}$. On a $lia = lk \cdot c' = 0$. Donc li est divisible par $klm = ord(a)$ et i est divisible par km. Disons $i = jkm$. Posons $c = c' - jma$.
Alors $\pi(c) = \pi(c') = b$ et $k \cdot c = k(c' - jma) = kc' - kjma = kc' - ia = 0$. Donc k divise $ord(c)$.
Mais $ord(c)$ divise $ord(\pi(c)) = ord(b) = k$.
Donc $ord(c) = k = ord(b)$. □

Théoreme 6.7.6

Soit A un p-groupe abélien. Alors, on a :

$$A \cong \mathbb{Z}/p^{m_1} \oplus \ldots \oplus \mathbb{Z}/p^{m_k}$$

pour un unique $k \in \mathbb{N}$ et des $m_i \geq 1$ uniques à permutation près.

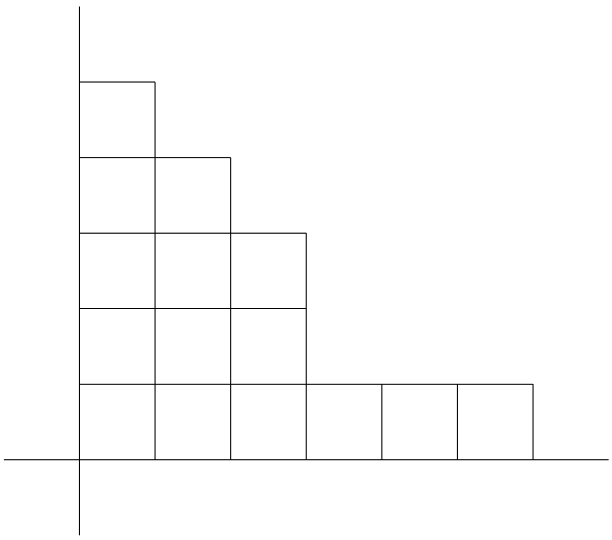
Définition 6.7.7

*Le **diagramme de Young** associé à A est un diagramme formé de k lignes chacune à m_i cases, où l'on a ordonné les m_i tels que $m_1 \geq m_2 \geq \ldots \geq m_k$.*

Exemple 6.7.8

diagramme de Young associé à $6 \geq 3 \geq 3 \geq 2 \geq 1$ respectivement au groupe :

$$\mathbb{Z}/p^6 \oplus \mathbb{Z}/p^3 \oplus \mathbb{Z}/p^3 \oplus \mathbb{Z}/p^2 \oplus \mathbb{Z}/p$$



Démonstration

Unicité : On va montrer que A détermine son diagramme de Young. Considérons le noyau de la multiplication par p^r :

$$\begin{aligned} p^k : \mathbb{Z}/p^m &\to \mathbb{Z}/p^m \\ \bar{k} &\mapsto p^r \bar{k} \end{aligned}$$

Si $r \geq m$, alors le noyau est $\mathbb{Z}/p^m$ tout entier.
Si $r < m$, alors le noyau est le sous-groupe engendré par $\overline{p^{m-r}}$. Dans ce cas, il est donc d'ordre p^r.
Donc :

$$|\ker(p^r : \mathbb{Z}/p^m \to \mathbb{Z}/p^m)| = \begin{cases} p^m & si\ r \geq m \\ p^r & si\ r \leq m \end{cases}$$

Chapitre 7

Un peu de géométrie affine

7.1 Espaces affines

Soit K un corps (par ex. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$)

Définition 7.1.1
*Un **espace affine** sur K est un triplet (ε, E, ϕ), où*
- *ε est un ensemble non vide*
- *E est un $\mathbb{K}$-espace vectoriel*
- *$\phi : \varepsilon \times E \longrightarrow \varepsilon$ est une action libre et transitive du groupe $(E, +)$ sur l'ensemble ε.*

Remarque 7.1.2
Dans la situation de la définition, on dit aussi que ε est un espace affine de **direction** E.
Les éléments de ε sont appelés **points**, ceux de E **vecteurs**.

Exemple 7.1.3
Soit E un $\mathbb{K}$-espace vectoriel. On pose $\varepsilon = E$, et on note ϕ l'action de $(E, +)$, sur $\varepsilon = E$ par translation.
Alors ε est un espace affine de direction E.

Notation 7.1.4
Soit ε un espace affine de direction E. On note :

$$\phi(P, v) = P + v, \qquad \forall P \in \varepsilon, \forall v \in E$$

Remarque 7.1.5
Pour tous $P, Q \in \varepsilon$, et $v, w \in E$, on a :
- $P + 0 = P$
- $(P + v) + w = P(v + w)$
- $\exists u \in E$ tel que $Q = P + u$

Notation 7.1.6
Pour tous $P, Q \in \varepsilon$, on note $\vec{PQ}$ l'unique vecteur tel que

$$Q = P + \vec{PQ}$$

Remarque 7.1.7
Pour tous $P, Q, R \in \varepsilon$ et $u, v \in E$, on a

- $\vec{PQ} = 0 \quad \Leftrightarrow \quad P = Q$
- $\vec{PQ} = u \quad \Leftrightarrow \quad P + u = Q$
- $\vec{PQ} + \vec{QR} = \vec{PR}$
  (relation de Chasles)
- $P + u = Q + v \quad \Leftrightarrow \quad \vec{PQ} = u - v$

7.2 Sous-espaces affines

Soit ε un espace affine de direction E.

Définition 7.2.1

Un sous-espace affine de ε est une partie $\mathscr{F} \in \varepsilon$ telle qu'il existe un point $P \in \varepsilon$ et sous-espace vectoriel $F \subset E$ tel que

$$\mathscr{F} = \{P + v \big| v \in F\} = P + F$$

Exemple 7.2.2

1. $\mathscr{F} = \varepsilon$ est un sous-espace affine ($F = E$)
2. Pour $P \in \varepsilon$, $\mathscr{F} = \{P\}$ est un sous-espace affine ($F = \{0\}$)

Remarque 7.2.3

Soient $P \in \varepsilon$ et $F \subset E$ un sous-espace vectoriel.
Posons $\mathscr{F} = P + F$.

1. On a $F = \{\vec{QR} \big| Q, R \in \mathscr{F}\}$
   Donc F est uniquement déterminé par $\mathscr{F}$
2. $\forall Q \in \varepsilon \qquad Q \in \mathscr{F} \quad \Leftrightarrow \quad \vec{PQ} \in F$
3. $\forall Q \in \mathscr{F} \qquad \mathscr{F} = Q + F$
4. $\forall u \in E \qquad u \in F \quad \Leftrightarrow \quad P + u \in \mathscr{F}$

Définition 7.2.4

Soit $\mathscr{F} \in \varepsilon$ un sous-espace affine

1. *l'unique sous-espace vectoriel F de E pour lequel il existe $P \in \varepsilon$ tel que $\mathscr{F} = P + F$ est appelé la **direction** de $\mathscr{F}$ et parfois noté $\vec{\mathscr{F}}$*
2. *On appelle **dimension** de $\mathscr{F}$ la dimension de F*
3. *Si $\dim(\mathscr{F}) = 1$ (resp. 2), on dit que $\mathscr{F}$ est une **droite affine** (resp. un **plan affine**) de ε*

Exemple 7.2.5

1. On suppose que $\dim(E) = 2$. Soit e_1, e_2 une base de E. soit $P \in \varepsilon$ et soit $u \in E \setminus \{0\}$.
   Soit $\mathbb{D}$ la droite affine $P + \mathrm{Vect}(u)$. On a
   $$\forall M \in \varepsilon : \qquad M \in \mathbb{D} \Leftrightarrow \det_{(e_1,e_2)}(u, \vec{PM}) = 0$$
2. On suppose que $\dim(E) = 3$. Soit e_1, e_2, e_3 une base de E. Soit $P \in \varepsilon$ et soient $u, v \in E$ linéairement indépendants.
   On note $\mathscr{P}$ de plan affine $P + \mathrm{Vect}(u, v)$.
   On a :
   $$\forall M \in \varepsilon \qquad \det_{(e_1,e_2,e_3)}(u, v, \vec{PM}) = 0$$

Remarque 7.2.6

1. Soit $\mathscr{F}$ un sous-espace affine de direction F.
   De façon naturelle, $\mathscr{F}$ est lui-même un espace affine de direction F.

2. ε est l'unique sous-espace affine de direction E

3. Les sous-espaces affines de direction $\{0\}$ sont exactement les singletons de ε

Exemple 7.2.7

1. $\left\{(x,y,z)\in\mathbb{K}^3 \,\middle|\, x+y+z=1\right\}$ est un sous-espace affine de $\varepsilon=\mathbb{K}^3$.
C'est un plan de direction
$$\left\{(x,y,z)\in\mathbb{K}^3 \,\middle|\, x+y+z=0\right\}$$

2. Soit $n\in\mathbb{N}$. Alors $\mathscr{F}=\left\{(x_1,\ldots,x_{n+1})\in\mathbb{K}^{n+1} \,\middle|\, x_1+\ldots+x_{n+1}=1\right\}$ est un sous-espace affine de $\varepsilon=\mathbb{K}^{n+1}$ de dimension n et de direction
$$F=\left\{(x_1,\ldots,x_{n+1})\in\mathbb{K}^{n+1} \,\middle|\, x_1+\ldots+x_{n+1}=0\right\}$$

3. Soit V un $\mathbb{K}$-espace vectoriel. Soit $f:V\longrightarrow\mathbb{K}$ une forme linéaire non nulle. Alors
$$\mathscr{F}=\left\{v\in V \,\middle|\, f(v)=1\right\}$$
est un sous-espace affine de $\varepsilon=V$ de direction $\mathrm{Ker}(f)\subset E=V$. Si $\dim(V)<\infty$, $\mathscr{F}$ est de dimension $\dim(V)=1$. On dit que $\mathscr{F}$ est un **hyperplan affine** dans $\varepsilon=V$.

Définition 7.2.8

Deux sous-espaces affines sont ***parallèles*** *si leurs directions sont égales.*

Remarque 7.2.9

1. Deux sous-espaces affines parallèles ont même dimension

2. Soient $\mathscr{F}$ et $\mathscr{G}$ deux sous-espaces affines F G.
Si $\mathscr{F}\subset\mathscr{G}$, alors $F\subset G$. Si de plus : $F=G$, alors $\mathscr{F}=\mathscr{G}$

Lemme 7.2.10

Soit $(\mathscr{F}_i)_{i\in I}$ une famille de sous-espaces affines. Soit F_i la direction de $\mathscr{F}_i$.
Si $\bigcap\limits_{i\in I}\mathscr{F}_i$ est non vide, alors c'est un sous-espace affine de direction $\bigcap\limits_{i\in I}F_i$.

Démonstration

Supposons que $P\in\bigcap\limits_{i\in I}F_i$. On a :
$$\begin{aligned} u\in\bigcap_{i\in I}F_i &\Leftrightarrow \mathscr{F}_i,\ \forall i\in I\\ &\Leftrightarrow P+u\in\bigcap_{i\in I}\mathscr{F}_i \end{aligned}$$

Donc $\bigcap\limits_{i\in I}\mathscr{F}_i=P+\bigcap\limits_{i\in I}F_i$ □

Lemme 7.2.11

Soient deux sous-espaces affines $\mathscr{F}$ et $\mathscr{G}$ de directions F et G. Si $E=F+G$, alors $\mathscr{F}$ $cap\mathscr{G}$ est non vide et donc c'est un sous-espace affine de direction $F\cap G$. Si de plus $E=F\oplus G$, alors $\mathscr{F}\cap\mathscr{G}$ est un singleton.

Démonstration

Soient $P\in\mathscr{F}$ et $Q\in\mathscr{G}$
Comme $E=F+G$, le vecteur $\vec{PQ}$ s'écrit
$$\vec{PQ}=u+v,\quad u\in F,\ v\in G$$

Alors le point

$$P + u = Q - v$$

appartient à $\mathscr{F} \cap \mathscr{G}$. Si $E = F \oplus G$, alors la direction de $\mathscr{F} \cap \mathscr{G}$ est $E \cap F = \{0\}$, donc $\mathscr{F} \cap \mathscr{G}$ est un singleton.$\square$

Exemple 7.2.12

Soit un système à m équations linéaires à n inconnues, et à coefficients dans $\mathbb{K}$? Soit $\mathscr{F}_i$, $1 \leq i \leq m$, l'ensemble des solutions de la i-ème équation. Supposons $\mathscr{F}_i \neq \emptyset$, $\forall i$.
Alors $\mathscr{F}_i$ est un sous-espace affine de direction F_i, l'espace des solutions de l'équation homogène associée. L'ensemble $\mathscr{F}$ des solutions du système est l'intersection $\bigcap_{i=1}^m \mathscr{F}_i$.
S'il est non vide, c'est un sous-espace affine de $\mathbb{K}^n$ de direction $\mathscr{F} = \bigcap_{i=1}^m \mathscr{F}_i$ l'espace des solutions du système homogène associé.

Conséquence 7.2.13 (en petit dimension)

1. *On suppose que ε est un plan affine. Soient $\mathbb{D}, \mathbb{D}'$ des droites* ***distinctes*** *de ε de directions D, D'*
   Alors une et une seule des assertions suivantes est vrai :
   - *$\mathbb{D}$ et $\mathbb{D}'$ sont parallèles et disjointes*
   - *$\mathbb{D} \cap \mathbb{D}'$ est un singleton*

2. *On suppose que ε est de dimension 3.*
   Soient $\mathbb{D}$ et $\mathbb{D}'$ des droites affines ***distinctes*** *de ε de direction D et D'.*
   Alors une seule des assertions est vrai :
   - *$\mathbb{D}$ et $\mathbb{D}'$ sont disjointes*
   - *$\mathbb{D} \cap \mathbb{D}'$ est un singleton*

3. *On suppose que ε est de dimension 3. Soit $\mathbb{D}$ une droite affine de direction D. Soit $\mathscr{P}$ un plan affine de direction P.*
   Alors une et une seule des assertions suivantes est vraie :
   - *$\mathbb{D} \subset \mathscr{P}$* *(et alors $D \subset P$)*
   - *$\mathbb{D} \cap \mathscr{P}$ est vide* *(et alors $D \subset P$)*
   - *$\mathbb{D} \cap \mathscr{P}$ est un singleton.*

4. *On suppose que ε est de dimension 3. Soient $\mathscr{P}$ et $\mathscr{P}'$ des plans affines* ***distinctes*** *de direction P et P'. Alors une et une seule des assertions suivantes est vraie :*
   - *$\mathscr{P}$ et $\mathscr{P}'$ sont parallèles et disjoints.*
   - *$\mathscr{P} \cap \mathscr{P}'$ est une droite affine de direction $P \cap P'$*

7.3 Applications affines

Soit ε un espace affine de direction E.

Définition 7.3.1

Soit $\mathscr{F}$ un espace affine de direction F
Une application $f : \varepsilon \to \mathscr{F}$ est ***affine****.*