Théorie des groupes

Pierron Théo

ENS Ker Lann

Table des matières

Introduction

- Groupes en arithmétique (Galois) :
  Pour $P \in \mathbb{Z}[X]$, on dit que P est résoluble ssi on peut écrire ses racines en fonction de ses coefficients.
  À P, on associe son groupe de Galois G. La théorie de Galois repose sur P résoluble ssi G résoluble.
  Or G est résoluble si $\mathrm{Card}(G) \leqslant 24$ ie P est résoluble si $\deg P \leqslant 4$.
- Groupes en géométrie (Klein) :
  Une géométrie est composée d'un ensemble S de points et d'un groupe G de transformations de S.
  Dans une géométrie, on a des figures (parties de S) et des propriétés stables par G.
- Groupes en analyse :

  Théorème 0.1 *Un système différentiel hamiltonien (pendule, toupie, problème à trois corps,...) est intégrable ssi son groupe de Galois est presque commutatif.*

Chapitre 1

Groupes et sous-groupes

1.1 Groupes

1.1.1 Définitions

Définition 1.1 Un groupe G est un ensemble muni d'une loi de composition interne associative, possédant un neutre et inversible. On dit que G est abélien quand cette loi est commutative.

Définition 1.2 L'ordre d'un groupe G est son cardinal.

Proposition 1.1 Il y a unicité du neutre et de l'inverse.

Définition 1.3 On définit récursivement la puissance n^{e} de $g \in G$ par $g^n = gg^{n-1}$, $g^{-n} = (g^{-1})^n$ et $g^0 = e$.

1.1.2 Propriétés

Définition 1.4 On appelle translation à gauche l'application :

$$t_g : \begin{cases} G & \to & G \\ h & \mapsto & gh \end{cases}$$

qui est une bijection d'inverse $t_{g^{-1}}$.

Remarque 1.1 On obtient une nouvelle loi par transfert de structure : $h*k = t_g(t_{g^{-1}}(h)t_{g^{-1}}(k)) = hg^{-1}k$.

Proposition 1.2

$$\sigma : \begin{cases} G & \to & G \\ g & \mapsto & g^{-1} \end{cases}$$

est une bijection.

Remarque 1.2 On obtient aussi une nouvelle loi par transport de structure : $g * h = hg$ (groupe opposé).

Définition 1.5 (Tables de Cayley) Il s'agit d'une table de multiplication dans laquelle chaque élément de G ne doit apparaître qu'une seule fois par ligne et par colonne.

Exemple 1.1

- $G = \{1\}$

	1
1	1

- $G = 1, g$

	1	g
1	1	g
g	g	1

- $G = \{1, g, h\}$

	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

- $G = \{1, g, h, k\}$. S'il existe $g \neq h \neq 1$ tel que $gh = 1$:

	1	g	h	k
1	1	g	h	k
g	g	k	1	h
h	h	1	k	g
k	k	h	g	1

Si pour tout g, h, $gh \neq 1$:

	1	g	h	k
1	1	g	h	k
g	g	1	k	h
h	h	k	1	g
k	k	h	g	1

Proposition 1.3 $\text{Card}(GL_n(\mathbb{F}_q)) = \prod_{i=0}^{n-1}(q^n - q^i)$.

1.2 Sous-groupes

1.2.1 Définitions

Définition 1.6 Soit G un groupe. Un sous-groupe de G est une partie $H \subset G$ telle que :

- $1 \in H$
- $\forall (g, h) \in H^2$, $gh \in H$.
- $\forall g \in H$, $g^{-1} \in H$.

1.2.2 Propriétés

Définition 1.7 Un sous-groupe H de G est dit distingué (ou normal) ssi pour tout $h, g \in H \times G$, $ghg^{-1} \in H$.

On écrit parfois $H < G$ si H est un sous-groupe de G et $H \lhd G$ si H est en plus distingué.

Exemple 1.2

- Pour tout groupe G, $\{1\} \lhd G$ et $G \lhd G$.
- Pour tout espace vectoriel V, $SL(V) \lhd GL(V)$.
- $n\mathbb{Z} \lhd (\mathbb{Z}, +)$.

Remarque 1.3 Si G est abélien, tout sous-groupe de G est distingué.

THÉORÈME 1.1 *Si $(H_i)_{i\in I} < G$ alors $\bigcap_{i\in I} H_i < G$.*

Remarque 1.4 La distinction passe aussi à l'intersection.

Définition 1.8 Si $X \subset G$, il existe un plus petit sous-groupe de G contenant X appelé sous-groupe engendré par X et noté $\langle X \rangle$. C'est $\bigcap_{X\subset H<G} H$.

Définition 1.9 G est dit cyclique (ou monogène) ssi il existe $g \in G$ tel que $G = \langle g \rangle$.

Exemple 1.3 $(\mathbb{Z}/4\mathbb{Z}, +)$ est cyclique, de même que $(\mathbb{Z}/5\mathbb{Z}^*, \times)$.

THÉORÈME 1.2 *Si F est un corps fini, F^* est cyclique.*

1.3 Applications

1.3.1 Opérations élémentaires sur les matrices

Définition 1.10 Soit M une matrice. Il y a trois types d'opérations élémentaires :

- échanger les lignes L_i et L_j
- remplacer L_i par λL_i avec $\lambda \neq 0$
- remplacer L_i par $L_i + \lambda L_j$ avec $i \neq j$

Définition 1.11 Une matrice élémentaire est la matrice obtenue en effectuant une opération élémentaire sur I_n.

THÉORÈME 1.3 *Effectuer une opération élémentaire revient à multiplier à gauche par une matrice élémentaire.*

THÉORÈME 1.4 *Si $A \in GL_n(\mathbb{K})$, il existe $(E_i)_i$ un $p-$uplet de matrices élémentaires telles que $E_p \dots E_1 A = I_n$ ie $A = E_1^{-1} \dots E_p^{-1}$.*

Donc $GL_n(\mathbb{K})$ est engendré par les matrices élémentaires.

Exemple 1.4 $GL_2(\mathbb{Z}/2\mathbb{Z}) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$.

1.3.2 Mots

Définition 1.12 Un mot en $X \subset G$ est un élément $x_1 \dots x_n \in G$ avec $(x_i)_i \in X^n$ pas nécessairement distincts. On note $\mathcal{M}(X)$ cet ensemble.

Proposition 1.4 Si $X \subset G$, $\langle X \rangle = \mathcal{M}(X \cup X^{-1})$ avec $X^{-1} = \{x^{-1}, x \in X\}$.

Démonstration. On a $\langle X \rangle = \langle X \cup X^{-1} \rangle$ donc on peut supposer $X = X^{-1}$.

On doit montrer que $\mathcal{M}(X) = \langle X \rangle$ sachant $X = X^{-1}$.

$\mathcal{M}(X)$ est un sous-groupe de X qui contient X.

De plus, si $H < G$ contient X, pour tout $(x_1, \dots, x_n) \in X^n$, on a $(x_1, \dots, x_n) \in H^n$ et $x_1 \dots x_n \in H$ donc $\mathcal{M}(X) \subset H$.

Donc $\langle X \rangle = \mathcal{M}(X)$. ∎

Remarque 1.5 Dans le cas abélien, $\langle g_1, \dots, g_n \rangle = \mathbb{Z}g_1 + \dots + \mathbb{Z}g_n$.

Exemple 1.5 $n\mathbb{Z} = \langle n \rangle$.

Proposition 1.5 Si H est un sous-groupe de $\mathbb{Z}$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration.

- Les $n\mathbb{Z}$ sont clairement des sous-groupes de $\mathbb{Z}$.
- Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$.
  Sinon, $H \setminus \{0\} \neq \varnothing$ donc il existe $n \neq 0 \in H$.
  H est un groupe donc $|n| \in H$ donc on peut supposer $n \geqslant 0$. On pose ensuite $n_0 = \min\{n \in H, n > 0\}$.
  Tout élément de $n_0\mathbb{Z}$ est dans H.
  Réciproquement, si $x \in H$, $x = n_0 q + r$ avec $r < n_0$.
  On a alors $r \in H$ donc $r = 0$ donc $x \in n_0\mathbb{Z}$.
  Donc $H = n_0\mathbb{Z}$. ∎

Définition 1.13 L'ordre de $g \in G$ est l'ordre de $\langle g \rangle$.

Exemple 1.6 Dans $GL_2(\mathbb{Z}/2\mathbb{Z})$, il y a 1 élément d'ordre 1, 3 éléments d'ordre 2 et 2 éléments d'ordre 3.

1.3.3 Groupe diédral

Définition 1.14 Le groupe diédral D_n ($n \geqslant 3$) est le groupe des isométries du plan qui laissent (globalement) invariant le polynôme régulier $(A_0, \dots, A_{n-1})$, convexe, centré, orienté et normalisé à n côtés.

Proposition 1.6 D_n est d'ordre $2n$ et $D_n = \langle r, s\rangle$ où r est la rotation d'angle $\frac{2\pi}{n}$ et s la symétrie par rapport à l'axe des abscisses.

Démonstration.

- Les isométries sont affines donc préservent les barycentres donc O. Elles sont déterminées par leurs images de $\overrightarrow{OA_0}$ et $\overrightarrow{OA_1}$.
  Tout élément de D_n envoie A_0 sur A_k et A_i sur $A_{i+1 \bmod n}$ ou $A_{i-1 \bmod n}$.
  Donc D_n a au plus $2n$ éléments.
- r et s sont des éléments de D_n donc $\langle r, s\rangle \subset D_n$.
  Dans $\langle r, s\rangle$, il y a $2n$ éléments : $1, r, \ldots, r^{n-1}$ et $s, rs, \ldots, r^{n-1}s$ qui sont distincts deux à deux.
  Donc $D_n = \langle r, s\rangle$ et D_n est d'ordre $2n$. ■

1.3.4 Commutateurs, groupe dérivé

Définition 1.15

- Soit G un groupe. On appelle commutateur de $(g, h) \in G^2$ et on note $[g, h]$ le produit $ghg^{-1}h^{-1}$.
- Le groupe dérivé de G, noté $D(G)$ est le sous-groupe engendré par les commutateurs de G.

Remarque 1.6 Les commutateurs ne forment pas toujours un sous-groupe si G a au moins 96 éléments.

Proposition 1.7 $D(G) \lhd G$

Démonstration.

- On a $[g, h]^{-1} = [h, g]$ et $k[g, h]k^{-1} = [kgk^{-1}, khk^{-1}]$
- Si X est l'ensemble des commutateurs, $X^{-1} = X$ et $kXk^{-1} = X$ d'après le point précédent. ■

Remarque 1.7 $D(G) = \{1\}$ *ssi G est abélien.*

Exemple 1.7 $D(D_n)$ $[r^i, r^j] = \mathrm{Id}$, $[r^i s, r^j s] = (r^2)^{i-j}$, $[r^i s, r^j] = r^{-2j}$ et $[r^i, r^j s] = r^{2i}$. Donc $D(D_n) = \langle r^2\rangle$ (qui vaut aussi $\langle r\rangle$ si n impair).

Chapitre 2

Morphismes, isomorphismes

2.1 Définitions

Définition 2.1 Un morphisme de groupes (homomorphisme) entre deux groupes G et H est une application $\varphi : G \to H$ telle que pour tout $g, h \in G^2$, $\varphi(gh) = \varphi(g)\varphi(h)$.

φ est un isomorphisme ssi il est bijectif.

φ est un endomorphisme ssi $H = G$.

φ est un automorphisme ssi $H = G$ et φ bijectif.

Remarque 2.1 $\varphi(1) = \varphi(1.1) = \varphi(1).\varphi(1)$ *donc* $1 = \varphi(1)$.

$1 = \varphi(1) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ *donc* $\varphi(g)^{-1} = \varphi(g^{-1})$.

Plus généralement, $\varphi(g)^n = \varphi(g^n)$ *pour tout* $n \in \mathbb{Z}$.

Exemple 2.1

- Soit $H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in K \right\} < GL_2(K)$.

$$f : \begin{cases} H & \to & K \\ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} & \mapsto & a \end{cases}$$

  est un isomorphisme de groupes. En effet, la bijectivité est claire et $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$.

- ln et exp sont deux isomorphismes de groupe réciproques : $\mathbb{R}_*^+ \underset{\exp}{\overset{\ln}{\rightleftharpoons}} \mathbb{R}$
- Si G est un groupe,

$$.^{-1} : \begin{cases} G & \to & G \\ g & \mapsto & g^{-1} \end{cases}$$

n'est pas un automorphisme en général (pas un morphisme). Prendre par exemple G non commutatif.
En revanche,

$$.^{-1} : \begin{cases} G_{op} & \to & G \\ g & \mapsto & g^{-1} \end{cases}$$

est un automorphisme.

Proposition 2.1

- Si $\varphi : G \to H$ et $\psi : H \to K$ sont des morphismes de groupes, alors $\psi \circ \varphi : G \to K$ est un morphisme de groupes.
- Si $\varphi : G \to H$ est un isomorphisme de groupes, φ^{-1} aussi.

Démonstration.

- Soit $g, h \in G^2$, $\psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h))$.
- Soit $g', h' \in H^2$.

$$\varphi^{-1}(g'h') = \varphi^{-1}(g')\varphi^{-1}(h') \quad \text{ssi} \quad g'h' = \varphi(\varphi^{-1}(g')\varphi^{-1}(h'))$$

Or $\varphi(\varphi^{-1}(g')\varphi^{-1}(h')) = \varphi(\varphi^{-1}(g'))\varphi(\varphi^{-1}(h')) = g'h'$. ■

Définition 2.2 Le noyau d'un morphisme $\varphi : G \to H$ est $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{1_H\}) \subset G$.

L'image de φ est $\mathrm{Im}(\varphi) = \{\varphi(g), g \in G\} \subset H$.

2.2 Propriétés

Proposition 2.2 Soit φ un morphisme. Si $X \subset G$, $\langle \varphi(X) \rangle = \varphi(\langle X \rangle)$.

Démonstration. On a $\varphi(X^{-1}) = \varphi(X)^{-1}$ donc on peut supposer $X = X^{-1}$.

On montre alors $\varphi(\mathcal{M}(X)) = \mathcal{M}(\varphi(X))$, ce qui est clair car $\varphi(x_1 \dots x_n) = \varphi(x_1) \dots \varphi(x_n)$. ■

Proposition 2.3 Soit $\varphi : G \to H$ un morphisme. Alors $\mathrm{Im}(\varphi)$ est un sous-groupe de H et $\mathrm{Ker}(\varphi)$ un sous-groupe distingué de G.

Démonstration.

- La propriété précédente appliquée à $X = G$, on a $\mathrm{Im}(\varphi) = \varphi(\langle G \rangle) = \langle \varphi(G) \rangle$ est donc un sous-groupe).
- $\varphi(1) = 1$ donc $1 \in \mathrm{Ker}(\varphi)$
  Si $g \in \mathrm{Ker}(\varphi)$, $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$ donc $g^{-1} \in \mathrm{Ker}(\varphi)$.
  Si $g, h \in \mathrm{Ker}(\varphi)$ alors $\varphi(gh) = \varphi(g)\varphi(h) = 1$ donc $gh \in \mathrm{Ker}(\varphi)$.
  Si $g \in G$ et $h \in \mathrm{Ker}(\varphi)$, $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = 1$
  Donc $ghg^{-1} \in \mathrm{Ker}(\varphi)$. ■

Exemple 2.2 $SL_n(\mathbb{C})$ est un sous-groupe distingué de $GL_n(\mathbb{C})$ car c'est le noyau de det.

Remarque 2.2 Deux groupes sont isomorphes ssi il existe un isomorphisme entre eux. C'est équivalent à dire su'ils ont même tables de Cayley quitte à renommer les éléments.

Application : Soient G_1 et G_2 deux groupes isomorphes.

Les deux groupes ont même ordre et ont le même nombre d'éléments d'ordre k.

G_1 est cyclique ssi G_2 l'est. G_1 est commutatif ssi G_2 l'est.

À isomorphisme près, on a :

Ordre	Groupes
1	$\{0\}$
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, $\mathfrak{S}_3 \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \simeq D_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{F}_2^3$, $\mathbb{F}_2 \times \mathbb{Z}/4\mathbb{Z}$, D_4, Q_8
$\vdots$	$\vdots$

Remarque 2.3 Si $H < G$, l'application :

$$f : \begin{cases} H & \to & G \\ g & \mapsto & g \end{cases}$$

est un morphisme de groupes.

Proposition 2.4 Soit $\varphi : G \to H$ un morphisme de groupes.

φ est sujectif ssi $\mathrm{Im}(\varphi) = H$. φ est injectif ssi $\mathrm{Ker}(\varphi) = \{1\}$.

Démonstration. La première équivalence est immédiate (définition d'une surjection).

Si φ est injectif, soit $g \in \mathrm{Ker}(\varphi)$. $\varphi(g) = 1 = \varphi(1)$ donc $g = 1$. Donc $\mathrm{Ker}(\varphi) = \{1\}$.

Si $\mathrm{Ker}(\varphi) = \{1\}$, soit $g, h \in G^2$ tel que $\varphi(g) = \varphi(h)$.

On a $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} = 1$. Donc $gh^{-1} \in \mathrm{Ker}(\varphi)$ donc $gh^{-1} = 1$ et $g = h$. Donc φ est injectif. ∎

Proposition 2.5 Soit G un groupe.

- Si $\varphi : \mathbb{Z} \to G$ est un morphisme, il existe un unique $g \in G$ tel que $\varphi(n) = g^n$ pour tout $n \in \mathbb{Z}$.

- Si $g \in G$, il existe un unique $\varphi : \mathbb{Z} \to G$ tel que $\varphi(1) = g$. On a alors $\varphi(n) = g^n$ pour tout $n \in \mathbb{Z}$.

Démonstration.

- Il y a unicité car $\mathbb{Z}$ est monogène. Il suffit de fixer $\varphi(1)$ qui vaut, par définition, g.
  De plus ce morphisme existe car si on pose $g = \varphi(1)$, $\varphi(n) = \varphi(n.1) = \varphi(1)^n = g^n$.
- Il y a unicité car si $\varphi(1) = g$, les valeurs de φ sur $\mathbb{Z}$ sont fixées.
  Ce morphisme existe car $\varphi : n \mapsto g^n$ est bien un morphisme. ■

THÉORÈME 2.1 *Soit G un groupe et $g \in G$.*

- *Si g est d'ordre infini alors $\langle g \rangle$ est isomorphe à $\mathbb{Z}$ et*

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$$

  avec $g^i \neq g^j$ si $i \neq j$.
- *Si g est d'ordre fini n, alors $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ avec $g^i \neq g^j$ si $(i, j) \in [\![0, n-1]\!]^2$ avec $i \neq j$.*
  De plus, on a $g^k = 1$ ssi $n|k$.

Démonstration. On considère le morphisme :

$$\varphi : \begin{cases} \mathbb{Z} & \to & G \\ n & \mapsto & g^n \end{cases}$$

On a $\mathrm{Im}(\varphi) = \varphi(\langle 1 \rangle) = \langle \varphi(1) \rangle = \langle g \rangle$.

- Si φ est injective, φ induit un isomorphisme de $\mathbb{Z} \to \langle g \rangle$.
  On a alors $\langle g \rangle = \{g^i, i \in \mathbb{Z}\}$.
- Si φ n'est pas injective, $\mathrm{Ker}(\varphi) \neq \{0\}$. $\mathrm{Ker}(\varphi)$ est un sous-groupe de $\mathbb{Z}$ donc il existe $n \in \mathbb{N}^*$ tel que $\mathrm{Ker}(\varphi) = n\mathbb{Z}$.
  Pour tout $k \in \mathbb{Z}$, $k = nq + r$ avec $r \in [\![0, n-1]\!]$. On a alors $g^k = (g^n)^d g^r = g^r$ donc $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$.
  Si $g^i = g^j$ avec $0 \leqslant i \leqslant j \leqslant n-1$.
  $g^{j-i} = 1$ et $j - i < n$ donc $g^{j-i} \in \mathrm{Ker}(\varphi)$ donc $n|j-i$ donc $j = i$.
  Si $g^k = 1$, $g^r = 1 = g^0$ avec $r < n$ donc $r = 0$ et $n|k$. ■

Exemple 2.3 $G = \mathbb{C}^*$, $g = \mathrm{e}^{i\theta}$
Si $\theta = \pi\frac{m}{n}$ avec $\frac{m}{n}$ irréductible, g est d'ordre n si m est pair et $2n$ sinon.
Sinon, g est d'ordre infini.

Définition 2.3 Le centre d'un groupe G est $Z(G) = \{g \in G, \forall h \in G, gh = hg\}$.

Remarque 2.4 *G est commutatif ssi $G = Z(G)$ et $g \in Z(G)$* ssi $\forall h \in G, [g,h] = 1$.

Proposition 2.6 Soit G un groupe.

- L'ensemble $\mathrm{Aut}(G)$ des automorphismes de G est un sous-groupe de $(\mathfrak{S}(G), \cdot)$.
- Si $h \in G$, l'application :
$$\sigma_h : \begin{cases} G & \to & G \\ g & \mapsto & hgh^{-1} \end{cases}$$
est un automorphisme de G dit intérieur.
- L'ensemble des automorphismes intérieurs de G, noté $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.
- Enfin, l'application :
$$f : \begin{cases} G & \to & \mathrm{Int}(G) \\ h & \mapsto & \sigma_h \end{cases}$$
est un morphisme surjectif de noyau $Z(G)$. En particulier, $Z(G)$ est un sous-groupe distingué de G.

Démonstration.

- Id_G est un automorphisme et si φ et ψ sont des automorphismes, $\psi \circ \varphi$ et φ^{-1} en sont. Donc $\mathrm{Aut}(G) < \mathfrak{S}(G)$.
- $\sigma_h(g_1)\sigma_h(g_2) = hg_1h^{-1}hg_2h^{-1} = hg_1g_2h^{-1}$ donc σ_h est un morphisme d'inverse $\sigma_{h^{-1}}$. C'est donc un automorphisme.
- $f(h_1h_2)(g) = h_1h_2g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = f(h_1)(f(h_2)(g))$ et $f(1) = \mathrm{Id}$ donc f est $\mathrm{Int}(G) < \mathrm{Aut}(G)$.
  $(\varphi \circ \sigma_h \circ \varphi^{-1})(g) = \varphi(h\varphi^{-1}(g)h^{-1}) = \varphi(h)g\varphi^{-1}(h)) = \sigma_{\varphi(h)}(g)$.
  Donc $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$.
- Le point précédent assure que f est un morphisme surjectif (par définition de $\mathrm{Int}(G)$).
  $\sigma_h = \mathrm{Id}$ ssi pour tout $g \in G$, $hgh^{-1} = g$ ie ssi $h \in Z(G)$. Donc $\mathrm{Ker}(f) = Z(G)$ donc $Z(G) \lhd \mathrm{Int}(G)$. ∎

THÉORÈME 2.2 *Soit G un groupe cyclique d'ordre n fini.*
$\mathrm{Aut}(G)$ *est un groupe abélien d'ordre $\varphi(n)$ où φ est l'indicatrice d'Euler.*

Proposition 2.7 Si G est cyclique d'ordre n, $\mathrm{Aut}(G)$ est l'ensemble des :
$$\varphi_k : \begin{cases} G & \to & G \\ g & \mapsto & g^k \end{cases}$$
avec $k \in [\![1, n]\!]$ tel que $k \wedge n = 1$.

Démonstration.

- Comme G est cyclique, $G = \langle g \rangle$ avec $g \in G$. φ_k est bien un morphisme pour tout $k \in \mathbb{Z}$.
  Soit $\varphi : G \to G$ un morphisme. $\varphi(g) \in G$ donc $\varphi(g) = g^k$.
  On a alors $\varphi(g^i) = \varphi(g)^i = (g^k)^i = g^{ki} = (g^i)^k = \varphi_k(g^i)$ pour tout i donc $\varphi = \varphi_k$.
  Donc les seuls morphismes sont les φ_k.
- $\mathrm{Im}(\varphi_k) = \varphi_k(G) = \langle \varphi(g) \rangle = \langle g^k \rangle$.
  $\mathrm{Im}(\varphi_k) = G$ ssi l'ordre de g^k vaut n.

  $$\exists m < n, (g^k)^m = 1 \quad \text{ssi} \quad \exists m < n, n | km \quad \text{ssi} \quad n \wedge m \neq 1$$

  Par contraposée, l'ordre de g^k vaut n ssi $n \wedge k = 1$.
  Donc $\varphi_k \in \mathrm{Aut}(G) \quad \text{ssi} \quad n \wedge k = 1$.
  Il y a donc $\varphi(n)$ automorphismes. ■

Chapitre 3

Théorème de Lagrange

Introduction

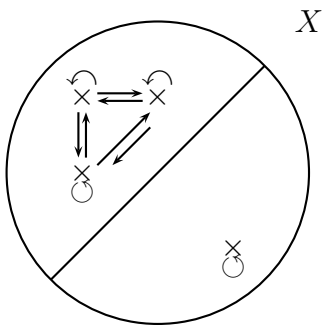
Définition 3.1 Un ensemble X est une collection d'éléments dans laquelle :

- l'ordre n'a pas d'importance : $\{1, 2\} = \{2, 1\}$
- les répétitions n'ont pas d'importance : $\{1, 1\} = \{1\}$

On note $|X|$ son nombre d'éléments (éventuellement infini).

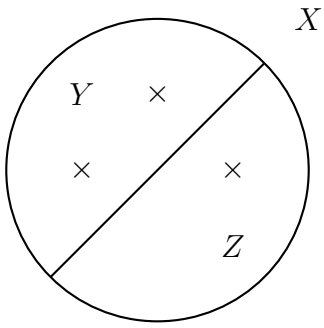
Définition 3.2 Une relation $\mathcal{R}$ dans un ensemble X est une relation d'équivalence ssi elle est réflexive, symétrique et transitive.

Une relation $\mathcal{R}$ dans un ensemble X est une relation d'ordre ssi elle est réflexive, antisymétrique et transitive.



Définition 3.3 Une partition d'un ensemble X est un ensemble P de parties de X tel que $\varnothing \notin P$, $\bigcup_{Y \in P} Y = X$ et $Y \cap Z \neq \varnothing \Rightarrow Y = Z$.

Il y a une surjection entre toute partition P de X et X (application



quotient) :

$$\pi : \begin{cases} X & \to & P \\ x & \mapsto & Y \quad \text{ssi} \quad x \in Y \end{cases}$$

À chaque relation d'équivalence, on peut associer une partition : $X/\mathcal{R} = \{\overline{x}, x \in X\}$.

De même, à chaque partition, on peut associer une relation d'équivalence par $x\mathcal{R}y \quad \text{ssi} \quad \exists Y \in P, (x,y) \in Y^2$.

On peut aussi associer une surjection à chaque partition et réciproquement.

3.1 Groupes, relations d'équivalence, indice

Définition 3.4 Soit G un groupe et H un sous-groupe. On définit une relation d'équivalence sur G par $g_1\mathcal{R}g_2 \quad \text{ssi} \quad \exists h \in H, g_2 = g_1 h$.

La classe de $g \in G$ est gH (classe à gauche)

Le quotient se note G/H.

Remarque 3.1 Si on applique ça à G^{op} et H^{op}, on obtient une autre relation dont les classes sont les classes à droite (Hg).

On note le quotient $H\backslash G = \{Hg, g \in G\}$.

On a $\forall g \in G, gH = Hg \quad \text{ssi} \quad G/H = H\backslash G \quad \text{ssi} \quad H \lhd G$.

Proposition 3.1 Si $H < G$ et $g \in G$ alors $|gH| = |Hg| = |H|$.

Démonstration. On montre que :

$$f : \begin{cases} H & \to & gH \\ h & \mapsto & gh \end{cases}$$

est bijective.

Elle est surjective par définition. De plus, si $gh_1 = gh_2$, alors $h_1 = h_2$.
Donc f est bijective. Donc $|H| = |gh|$. ■

Définition 3.5 Si $H < G$, l'indice de H dans G, noté $(G : H)$, vaut $|G/H|$

Exemple 3.1
- $G/\{1\} \simeq G$.
- $G/G \simeq \{1\}$.
- Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{k} = \{k + nq, q \in \mathbb{Z}\}$.

3.2 Théorèmes

Proposition 3.2 Tout sous-groupe d'indice 2 est distingué.

Démonstration. $|G/H| = 2$ donc $G/H = \{H, H^c\} = H\backslash G$. Donc H est distingué. ■

Exemple 3.2 Dans D_n, $\langle r \rangle$ est distingué.

$$D_n/\langle r \rangle = \{\{1, r, \ldots, r^{n-1}\}, \{s, sr, \ldots, sr^{n-1}\}\}$$

et $\langle r \rangle \ D_n = \{\{1, \ldots, r^{n-1}\}, \{s, rs, \ldots, r^{n-1}s\}\}$.

THÉORÈME 3.1 *Si $H < G$, $|G| = |H|(G : H)$.*

Démonstration. On a une injection de H dans G et une surjection de G dans G/H.

Donc $|H| \leqslant |G|$ et $|G| \geqslant |G/H|$.

On peut supposer $|H|$ et $|G/H|$ finis. On a alors $G/H = \{g_1H, \ldots, g_kH\}$. les (g_iH) ont $|H|$ éléments

On a $G = \bigcup_{1 \leqslant i \leqslant k} g_iH$. Comme les (g_iH) sont disjoints, $|G| = |G/H||H|$. ■

COROLLAIRE 3.1 DE LAGRANGE *L'ordre d'un sous-groupe divise le cardinal du groupe.*

COROLLAIRE 3.2 *Tout groupe d'ordre premier p est cyclique et tout élément différent de 1 en est un générateur.*

Démonstration. Soit $g \in G$. L'ordre de $\langle g \rangle$ divise p donc c'est $\{1\}$ ou G. ■

Chapitre 4

Actions d'un groupe sur un ensemble

Rappels sur le groupe symétrique

Définition 4.1 Pour tout ensemble X, on note $\mathfrak{S}(X)$ l'ensemble des bijections de X.

Remarque 4.1 *Si* $|X| = n$, $\mathfrak{S}(X) \simeq \mathfrak{S}_n$.

4.1 Actions de groupes

Définition 4.2 Une action (ou une opération) (à gauche) d'un groupe G sur un ensemble X est une application :

$$f : \begin{cases} G \times X & \to & X \\ (g, x) & \mapsto & gx \end{cases}$$

telle que $\forall x \in X$, $f(1, x) = x$ et $\forall (x, g, h) \in X \times G^2$, $f(gh, x) = f(g, f(h, x))$.

Exemple 4.1

- $\mathfrak{S}(X)$ opère sur X.
- Les isométries opèrent sur $\mathbb{R}^2$.
- $GL(V)$ opère sur V pour tout V espace vectoriel sur $\mathbb{K}$.

THÉORÈME 4.1 *Si* G *opère sur* X,

$$\varphi : \begin{cases} G & \to & \mathfrak{S}(X) \\ g & \mapsto & \sigma_g : \begin{cases} X & \to & X \\ x & \mapsto & gx \end{cases} \end{cases}$$

est un morphisme de groupes.

Si $\varphi : G \to \mathfrak{S}(X)$ est un morphisme de groupes, on a une action :

$$\psi : \begin{cases} G \times X & \to & X \\ (g,x) & \mapsto & \varphi(g)x \end{cases}$$

Démonstration.

- On a $\sigma_{gh}(x) = (gh)x$ et $\sigma_g(\sigma_h(x)) = \sigma_g(hx) = g(hx)$.
  Comme G opère sur X, $g(hx) = (gh)x$.
  De plus, $\sigma_1(x) = x$. Il faut montrer que $\sigma_g \in \mathfrak{S}(X)$.
  σ_g est bijective car $\sigma_g \circ \sigma_{g^{-1}} = \mathrm{Id}$ car G opère sur X. Donc φ est un morphisme.
- $(gh) \cdot x = \varphi(gh)(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) = g \cdot (h \cdot x)$
  Donc ψ est une action. ■

Définition 4.3 Une action à droite de G sur X est une action à gauche de G^{op} sur X :

$$f : \begin{cases} G \times X & \to & X \\ (g,x) & \mapsto & xg \end{cases}$$

tel que $x1 = x$ et $x(gh) = (xg)h$.

Proposition 4.1 Si $\varphi : G \to H$ est un morphisme de groupes et X muni d'une action de H, alors X est muni d'une action de G.

Démonstration. Il suffit de composer par φ un morphisme $\psi : H \to \mathfrak{S}(X)$ (théorème précédent). ■

Exemple 4.2

- $$\cdot^{-1} : \begin{cases} G & \to & G^{op} \\ g & \mapsto & g^{-1} \end{cases}$$
  transforme une action à droite en une action à gauche.
- Si $H < G$, toute action de G sur X induit une action de H sur X car l'injection canonique de H dans G est un morphisme.

COROLLAIRE 4.1 *Si X est un ensemble fini à n éléments, toute action de G sur X donne un morphisme $G \to \mathfrak{S}_n$. (et réciproquement)*

Définition 4.4 Soit G un groupe opérant sur un ensemble X. On définit, pour chaque $x \in X$, le stabilisateur de x, noté G_x, l'ensemble $\{g \in G, gx = x\} \subset G$.

L'orbite de x, notée $G.x = \{gx, g \in G\} \subset X$.

L'opération est dite transitive s'il existe une unique orbite (ie $\forall x, y \in X^2, \exists g \in G, gx = y$).

L'opération est libre si les stabilisateurs sont triviaux (ie $\forall (x, g) \in X \times G$, $gx = x \Rightarrow g = 1$).

Remarque 4.2 Pour tout x, $G_x < G$.

Proposition 4.2 Les orbites forment une partition de X. Ce sont les classes d'équivalences de :

$$x\mathcal{R}y \quad \text{ssi} \quad y = gx$$

On notera $G\backslash X$ l'ensemble quotient (et $X/G = G^{op}\backslash X$)

Démonstration. $x = 1x$ donc $x\mathcal{R}x$. Si $x\mathcal{R}y$, $y = gx$ donc $x = g^{-1}y$ donc $y\mathcal{R}x$.

Si $x\mathcal{R}y$ et $y\mathcal{R}z$, $y = gx$ et $z = hy$ donc $z = hgx$ et $x\mathcal{R}z$. ∎

Définition 4.5 Si G agit sur X et $H < G$, on dit qu'une partie Y de X est H-stable ssi $HY \subset Y$.

Exemple 4.3

- Si $Y = \{x\}$, on dit que x est fixe.
- Si $H = \langle g \rangle$, on dit que Y est g-stable.

Remarque 4.3 Si Y stable sous H, on obtient une action de H sur Y donné par :

$$f : \begin{cases} H \times Y & \to & Y \\ (h, y) & \mapsto & hy \end{cases}$$

Proposition 4.3 Si G agit sur X, $H < G$, $Y \subset X$, Y est H-stable ssi Y est une union d'orbites de X sous l'action de H

Proposition 4.4 Si G agit sur X et $\varphi : G \to \mathfrak{S}(X)$ le morphisme associé.

$$\mathrm{Ker}(\varphi) = \bigcap_{x \in X} G_x$$

Démonstration.

$$\begin{aligned} g \in \mathrm{Ker}(\varphi) \quad &\text{ssi} \quad \varphi(g) = \mathrm{Id} \quad \text{ssi} \quad \forall x \in X, gx = x \\ &\text{ssi} \quad \forall x, g \in G_x \quad \text{ssi} \quad g \in \bigcap_{x \in X} G_x \end{aligned}$$

∎

Définition 4.6 Una action est dite fidèle si le morphisme associé est injectif.

Remarque 4.4 Si les stabilisateurs sont triviaux, alors l'action est fidèle. La réciproque est fausse.

Exemple 4.4 G est l'ensemble des isométries du plan, $X = \mathbb{R}^2$, $X = D_n$ et $Y = \mathcal{P}_n$ (polygône régulier à n côtés).

L'action de D_n sur $\mathcal{P}_n$ est transitive ($\langle r \rangle$ agit transitivement), pas libre ($s \in (D_n)_{A_0}$) mais fidèle (pour $n \geqslant 3$) (une isométrie est affine et si elle fixe trois points non alignés de $\mathbb{R}^2$, elle est égale à Id).

En particulier $D_3 \simeq \mathfrak{S}_3$.

4.2 Opérations par translation

Définition 4.7 Pour tout groupe G, sa loi $\cdot$ est une action de G sur G à droite et à gauche. De plus $G\backslash G = G/G = \{1\}$.

Si $H < G$, $\cdot : G \times H \to G$ est un action à droite de H sur G.

Les orbites par l'action à droite de H sur G sont les classes à gauche gH.

Proposition 4.5 Soit $H < G$.

On a une action de G à gauche sur G/H donnée par :

$$f : \begin{cases} G \times G/H & \to & G/H \\ (g, g'H) & \mapsto & gg'H \end{cases}$$

Remarque 4.5 *Si $(G : H)$ est fini, on obtient un morphisme $G \to \mathfrak{S}_{(G:H)}$.*

Exemple 4.5 $G = GL_2(\mathbb{Z}/2\mathbb{Z} > H = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$.

$|H| = 2$ donc $(G : H) = 3$ et on obtient $G \to \mathfrak{S}_3$. L'action est fidèle donc $G \simeq \mathfrak{S}_3$.

Théorème 4.2 Cayley *Tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique.*

Démonstration. G agit à gauche sur G donc on a un morphisme φ de $G \to \mathfrak{S}(G)$. Or $\mathfrak{S}(G) \simeq \mathfrak{S}_{|G|}$

Ce morphisme est fidèle donc G est isomorphe à $\mathrm{Im}(\varphi) < \mathfrak{S}(G)$ donc isomorphe à un sous-groupe de $\mathfrak{S}_n$. ∎

4.3 Opérations par conjugaison

Définition 4.8 G agit sur G par conjugaison (à gauche) par :

$$f_g : \begin{cases} G \times G & \to & G \\ (g, h) & \mapsto & ghg^{-1} \end{cases}$$

Définition 4.9 La classe de h sous l'action par conjugaison de G est appelée classe de conjugaison de h. Le stabilisateur de h est appelé centralisateur : $Z_G(h) = \{g \in G, gh = hg\}$.

Exemple 4.6 $D_n = \langle r, s\rangle$.

$r^i r^j r^{-i} = r^j$, $(r^i s)r^j s r^{-i} = r^{-j}$, $r^i(r^j s)r^{-i} = r^{j+2i}s$ et $(r^i s)(r^j s)sr^{-i} = r^{2i-j}s$.

Donc les classes de conjugaison sont :

- pour n impair :

$$\{1\}, \{r, r^{n-1}\}, \ldots, \{r^{\frac{n-1}{2}}, r^{\frac{n+1}{2}}\}, \{s, rs, \ldots r^{n-1}s\}$$

- pour n pair :

$$\{1\}, \{r^{\frac{n}{2}}\}, \{r, r^{n-1}\}, \ldots, \{r^{\frac{n}{2}-1}, r^{\frac{n}{2}+1}\}, \{s, r^2 s, \ldots r^{\frac{n}{2}}s\}, \{rs, \ldots r^{\frac{n}{2}+1}s\}$$

Donc $Z(D_n) = \{1\}$ si n impair et $\{1, r^{\frac{n}{2}}\}$ si n pair.

De plus, $Z_{D_n}(r) = \langle r\rangle, \ldots$

Proposition 4.6 Soit G un groupe. $\mathrm{Aut}(G)$ agit sur les sous-groupes H de G par $\varphi \cdot H = \varphi(H)$.

Remarque 4.6

- $H \lhd G$ ssi $\mathrm{Int}(G) \subset \mathrm{Stab}_{\mathrm{Aut}(G)}(H)$
  En effet, $\mathrm{Int}(G) \subset \mathrm{Stab}_{\mathrm{Aut}(G)}(H)$ *ssi* $\forall g \in G, gHg^{-1} = H$ ssi $H \lhd G$.
- $K \lhd H \lhd G \not\Rightarrow K \lhd G$ *en général.*

Définition 4.10 Un sous-groupe H d'un groupe G est dit caractéristique ssi son stabilisateur sous l'action de $\mathrm{Aut}(G)$ est $\mathrm{Aut}(G)$.

Remarque 4.7 $H < G$ *caractéristique* $\Rightarrow H \lhd G$.

Exemple 4.7

- $D(G)$ est caractéristique.

$$\alpha([g,h]) = \alpha(ghg^{-1}h^{-1}) = \alpha(g)\alpha(h)\alpha(g)^{-1}\alpha(h)^{-1} = [\alpha(g), \alpha(h)]$$

  $D(G) = \langle X\rangle$ avec $X = \{[g,h], g, h \in G^2\}$.
  $\alpha(D(G)) = \langle \alpha(X)\rangle \subset \langle X\rangle = D(G)$.
  De même, $\alpha^{-1}(D(G)) \subset D(G)$ donc $\alpha(D(G)) = D(G)$.
- $Z(G)$ est caractéristique.

$$\alpha(g)h = \alpha(g\alpha^{-1}(h)) = \alpha(\alpha^{-1}(h)g) = h\alpha(g)$$

Proposition 4.7 Soient G un groupe et $K \lhd H \lhd G$.

Si K est caractéristique dans H, $K \lhd G$.

Si, de plus, H est caractéristique, K est caractéristique dans G.

Démonstration. Soit $\alpha \in \mathrm{Aut}(G)$ intérieur.

$\alpha(H) = H$ car $H \lhd G$. Donc α induit α' sur H.

Comme K est caractéristique dans H, $\alpha'(K) = K$. Or $\alpha(K) = \alpha'(K)$. Donc $\alpha(K) = K$. Donc $K \lhd G$.

Soit $\alpha \in \mathrm{Aut}(G)$ caractéristique.

$\alpha(H) = H$ car $H \lhd G$. Donc α induit α' sur H.

Comme K est caractéristique dans H, $\alpha'(K) = K$. Or $\alpha(K) = \alpha'(K)$. Donc $\alpha(K) = K$. Donc K est caractéristique dans G. ■

Remarque 4.8

- *α' n'est pas un automorphisme intérieur de H en général, même si α est intérieur sur G.*
- *Par composition avec*

$$\varphi : \begin{cases} G & \to & \mathrm{Aut}(G) \\ g & \mapsto & \sigma_g : \begin{cases} G & \to & G \\ h & \mapsto & ghg^{-1} \end{cases} \end{cases}$$

G agit sur ses sous-groupes par conjugaison.

Définition 4.11 Le normalisateur $N_G(H)$ est le stabilisateur de H sous l'action de G par conjugaison.

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

Remarque 4.9 *$N_G(H)$ est le plus grand sous-groupe de G dans lequel H est distingué.*

Chapitre 5

Groupes symétriques

5.1 Groupe des permutations

Définition 5.1 On note $\mathfrak{S}_n$ le groupe symétrique ie l'ensemble des permutations de $[\![1,n]\!]^{[\![1,n]\!]}$.

Proposition 5.1 $\mathrm{Card}(\mathfrak{S}_n) = n!$.

Notation :

$\sigma \in \mathfrak{S}_n$ s'écrit :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Exemple 5.1

- $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.
  On a $\sigma\rho = \mathrm{Id} = 1$.
- $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.
  $\sigma\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \rho\sigma$.

Remarque 5.1 *$\mathfrak{S}_3$ n'est pas commutatif.*

$\mathfrak{S}_n$ agit naturellement sur $[\![1,n]\!]$.

Les permutations qui fixent $[\![m+1,n]\!]$ forment un sous-groupe isomorphe à $\mathfrak{S}_m$.

Donc $\mathfrak{S}_n$ n'est pas abélien pour $n \geqslant 3$.

5.2 Cycles et support

Définition 5.2 Le support de $\sigma \in \mathfrak{S}_n$, noté $\text{supp}(\sigma)$, est le complémentaire de l'ensemble des points fixes de σ.

Proposition 5.2 Soient $\sigma, \rho \in \mathfrak{S}_n$.
$\text{supp}(\sigma\rho) \subset \text{supp}(\sigma) \cup \text{supp}(\rho)$ avec égalité ssi $\text{supp}(\sigma) \cap \text{supp}(\rho) = \varnothing$.
Dans ce cas, on a $\sigma\rho = \rho\sigma$.

Démonstration.

- Si $i \notin \text{supp}(G)$ et $i \notin \text{supp}(\rho)$, alors $(\sigma\rho)(i) = \sigma(\rho(i)) = \sigma(i) = i$.
  Donc $i \notin \text{supp}(\sigma\rho)$.
- Suppsons $\text{supp}(\sigma) \cap \sigma(\rho) = \varnothing$. Soit $i \in \text{supp}(\sigma)$.
  $(\sigma\rho)(i) = \sigma(i)$ car $i \in \text{supp}(\sigma) \subset \text{supp}(\rho)^c$.
  De même, si $i \in \text{supp}(\rho)$, $\rho(i) \in \text{supp}(\rho) \subset \text{supp}(\sigma)^c$. Donc $(\sigma\rho)(i) = \rho(i)$.
  Si $i \notin \text{supp}(\sigma)$ et $i \notin \text{supp}(\rho)$ alors $(\sigma\rho)(i) = \sigma(i) = i$.
  Les résultats en découlent. ■

Définition 5.3 Soient $(i_1, \ldots, i_l \in [\![1, n']\!]$ distincts avec $l \geqslant 2$. Alors, le l-cycle $(i_1, \ldots, i_l)$ est la permutation de $\mathfrak{S}_n$ de support $\{i_1, \ldots, i_l\}$ telle que $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, …, $\sigma(i_l) = i_1$.
l est la longueur du cycle.

Exemple 5.2

$$(142) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (421) \neq (124)$$

Remarque 5.2 Le support d'un cycle est l'unique orbite non triviale sous l'action du cycle.

Définition 5.4 Si G agit sur X et $g \in G$, on appelle action de g sur X l'action de $\langle g \rangle$ sur X.

Remarque 5.3 Un l-cycle est d'ordre l.

THÉORÈME 5.1 *Toute permutation s'écrit de manière unique comme produit de cycles à support disjoints.*

Démonstration.

! Supposons $\sigma = \gamma_1 \ldots \gamma_p$. On a $\text{supp}(\sigma) = \bigcup_{i=1}^{p} \text{supp}(\gamma_i)$ qui forment une partition de $\text{supp}(\sigma)$.
Donc $\gamma_i(i) = \sigma(i)$si $i \in \text{supp}(\gamma_i)$ et i sinon.
D'où l'unicité (car $\text{supp}(\gamma_j)$ est une orbite sous l'action de σ.

∃ On écrit $\text{supp}(\sigma) = \bigcup_{i=1}^{p} X_i$ avec $(X_i)_i$ formant la partition de $\text{supp}(\sigma)$ associée à l'action de G.
Soit X une orbite de $\text{supp}(G)$ sous l'action de σ et $i \in X$.
Soit l le plus petit entier tel que $\sigma^l(i) = i$. Par division euclidienne, on peut montrer que $\text{Card}(X) = l$ et $X = \{i, \sigma(i), \ldots, \sigma^{l-1}(i)\}$.
On pose $\gamma = (i, \sigma(i), \ldots, \sigma^{l-1}(x))$. γ et σ agissent de la même manière sur X.
On le fait pour chaque orbite X_j qui nous donne un γ_j. On a alors $\sigma = \gamma_1 \ldots \gamma_p$. ■

Exemple 5.3

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} = (124)(35)$$

Définition 5.5 Si $(X_i)_{i \in [\![1,p]\!]}$ est la partition de $[\![1, n]\!]$ sous $\sigma \in \mathfrak{S}_n$ avec $l_1 \geqslant l_2 \geqslant \ldots \geqslant l_p$ ($l_j = \text{Card}(X_j)$), on dit que $[l_1, \ldots, l_p]$ est le type de σ.

Remarque 5.4 On a alors $\sigma = \gamma_1 \ldots \gamma_r$ avec γ_i des cycles de longueur l_i pour i tel que $l_i \neq 1$.

Exemple 5.4 $(124) \in \mathfrak{S}_4$ est de type $[3, 1]$.

Proposition 5.3 Si σ est de type $[l_1, \ldots, l_r]$, alors $\text{Or}(\sigma) = \bigvee_{1 \leqslant i \leqslant r} l_i$.

Démonstration. On a $\sigma = \gamma_1 \ldots \gamma_r$ avec γ_i de longueur l_i.

$$\begin{aligned} \sigma^k = \text{Id} \quad &\text{ssi} \quad \forall i, \sigma^k(i) = i \\ &\text{ssi} \quad \forall i, j, \gamma_j^k(i) = i \\ &\text{ssi} \quad \forall j, \gamma_j^k = \text{Id} \end{aligned}$$

Donc $\text{Or}(\sigma) = \bigvee_{1 \leqslant i \leqslant r} \text{Or}(\gamma_i)$. ■

Proposition 5.4 Deux permutations sont conjuguées ssi elles ont même type.

Démonstration.

Lemme 5.1.1
$\omega \underbrace{(i_1, \ldots, i_l)}_{\gamma} \omega^{-1} = (\omega(i_1), \ldots, \omega(i_l)) = \gamma'$.

Démonstration. $(\omega\gamma\omega^{-1})(\omega(i_j)) = \omega(i_{j+1})$ et $(\omega\gamma\omega^{-1})(\omega(i_l)) = \omega(i_1)$.
Si $j \in \omega(\text{supp}(\gamma))$ alors $(\omega\gamma\omega^{-1})(j) = \gamma'(j)$.

Sinon, $\omega^{-1}(j) \notin \text{supp}(\gamma)$. On a alors $\gamma(\omega^{-1}(j)) = \omega^{-1}(j)$ et $(\omega\gamma\omega^{-1})(j) = j = \gamma'(j)$. ■

Si $\sigma \in \mathfrak{S}_n$ et $\sigma = \gamma_1 \dots \gamma_r$ sa décomposition.

$\omega\sigma\omega^{-1} = (\omega\gamma_1\omega^{-1}) \dots (\omega\gamma_r\omega^{-1})$ qui sont disjoints donc le type de σ est celui de $\omega\sigma\omega^{-1}$.

Réciproquement, si σ et ρ sont de type $[l_1, \dots, l_r]$.

Notons $(X_1, \dots, X_r)$ les orbites de σ et $(Y_1, \dots, Y_r)$ ceux de ρ.

On a donc $|X_j| = |Y_j| = l_j$. Pour chaque j, soit $i_j \in X_j$ et $k_j \in Y_j$ on définit ω par $\omega(\sigma^t(i_j)) = \rho^t(k_j)$ pour $t \in [\![1, l_j]\!]$.

On vérifie que $\omega\sigma\omega^{-1} = \rho$. ■

Exemple 5.5 Dans $\mathfrak{S}_4$, il y a 4 types possibles :

types	nombre de permutations
$[1,1,1,1]$	1
$[2,1,1]$	6
$[2,2]$	3
$[3,1]$	8
$[4]$	6

5.3 Générateurs et signature

Proposition 5.5 $\mathfrak{S}_n$ est engendré par les transpositions.

Démonstration. Tout cycle est un produit de transpositions : $(i_1, \dots, i_l) = (i_1, i_2) \dots (i_{l-1}, i_l)$ et les cycles engendrent $\mathfrak{S}_n$. ■

Remarque 5.5 Autre démonstration : par récurrence, $n = 1$ débile.

Si $\sigma(n) = n$, $\sigma \in \mathfrak{S}_{n-1}$ donc l'hypothèse de récurrence conclut. Si $\sigma(n) = k \neq n$, $\rho = (k, n)\sigma$ vérifie $\rho(n) = n$ et le cas précédent conclut à $\sigma = (k, n)\rho = (k, n)\prod_{i=1}^{p} \tau_i = \prod_{i=1}^{p+1} \tau_i$.

Proposition 5.6 $\mathfrak{S}_n$ est engendré par les $\{(1\,i), i \in [\![1, n]\!]\}$.

Démonstration. Pour tout i, j, $(ij) = (1j)(1i)(1j)$. D'où le résultat. ■

Définition 5.6 On note $\mathscr{P}_n$ l'ensemble des paires d'éléments de $[\![1, n]\!]$.

Si $\sigma \in \mathfrak{S}_n$, on pose :

$$\varepsilon(\sigma) = \prod_{\{i,j\} \in \mathscr{P}_n} \frac{\sigma(i) - \sigma(j)}{i - j} = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Remarque 5.6

- $\{i,j\} = \{j,i\}$ *et* $\{i,i\} \notin \mathscr{P}_n$ *alors que* $(i,j) \neq (j,i)$ *et* (i,i) *est un couple.*
- $\mathscr{P}_n$ *est muni d'une action de* $\mathfrak{S}_n$ *par* $\sigma(\{i,j\}) = \{\sigma(i), \sigma(j)\}$.
- *Par conséquent, on a :*

$$\varepsilon(\sigma) = \frac{\prod_{i<j} \sigma(i) - \sigma(j)}{\prod_{\sigma(i)<\sigma(j)} \sigma(i) - \sigma(j)} = (-1)^{\underbrace{\text{Card}\{(i,j), i<j \text{ et } \sigma(i)>\sigma(j)\}}_{\text{nombre d'inversions}}}$$

  et $\varepsilon(\mathfrak{S}_n) = \{1, -1\}$.
- $\varepsilon(k,l) = -1$.

Proposition 5.7

- $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ est un morphisme de groupes.
- Si σ est produit d'un nombre pair de transpositions, $\varepsilon(\sigma) = 1$ et -1 sinon.
- Si $\gamma_1 \dots \gamma_p$ est la décomposition de σ en l_i-cycles à support disjoints, $\varepsilon(\sigma) = \prod_{i=1}^{p} (-1)^{l_i - 1}$.

Démonstration.

- On a :

$$\begin{aligned}
\varepsilon(\sigma\rho) &= \prod_{\{i,j\} \in \mathscr{P}_n} \frac{\sigma(\rho(i)) - \sigma(\rho(j))}{i-j} \\
&= \prod_{\{i,j\} \in \mathscr{P}_n} \frac{\sigma(\rho(i)) - \sigma(\rho(j))}{\rho(i) - \rho(j)} \times \prod_{\{i,j\} \in \mathscr{P}_n} \frac{\rho(i) - \rho(j)}{i-j} \\
&= \prod_{\{i,j\} \in \mathscr{P}_n} \frac{\sigma(i) - \sigma(j)}{i-j} \times \prod_{\{i,j\} \in \mathscr{P}_n} \frac{\rho(i) - \rho(j)}{i-j} \\
&= \varepsilon(\sigma)\varepsilon(\rho)
\end{aligned}$$

- Clair par le point précédent et la remarque ci-dessus.
- Clair par les points précédents et par la décomposition de tout cycle en produit de transpositions : $(i_1, \dots, i_l) = (i_1, i_2) \dots (i_{l-1}, i_l)$. ■

5.4 Groupe alterné

5.4.1 Définition

Définition 5.7 Le noyau de la sigmature $\varepsilon : \mathfrak{S}_n \to \{1, -1\}$ est le groupe alterné $\mathfrak{A}_n$.

Proposition 5.8 $\mathfrak{A}_n \lhd \mathfrak{S}_n$ et $\text{Card}(\mathfrak{A}_n) = \frac{n!}{2}$.

Démonstration. $\mathfrak{S}_n = \mathfrak{A}_n \cup (1\,2)\mathfrak{A}_n$ donc $\text{Card}(\mathfrak{A}_n) = \frac{n!}{2}$. ■

Exemple 5.6

- $\mathfrak{A}_2 = \{1\}$.
- $\mathfrak{A}_3 = \{\text{Id}, (132), (123)\}$.
- $$\mathfrak{A}_4 = \{\text{Id}, (12)(34), (13)(24), (14)(23), (123), \\ (132), (124), (142), (234), (243), (134), (143)\}$$

5.4.2 Sous-groupes

Ordre	Sous-groupe
1	$\{1\}$
2	$\langle(12)(34)\rangle, \langle(13)(24)\rangle, \langle(14)(23)\rangle$
3	$\langle(123)\rangle, \langle(124)\rangle, \langle(234)\rangle, \langle(134)\rangle$
4	$\{1, (12)(34), (13)(24), (14)(23)\}$ [1]
6	Il n'y en a pas
12	$\{1\}$

Proposition 5.9 $\mathfrak{A}_n$ est engendré par les 3-cycles, et aussi par les cycles de la forme $(1\,i\,j)$.

Démonstration. On sait que $(1\,i\,j) = (1\,j)(1\,i)$ et que les $\{(1\,i)(1\,j), (i,j) \in [\![1,n]\!]^2\}$ engendrent $\mathfrak{A}_n$. ■

5.5 Simplicité

Définition 5.8 Un groupe G est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et G.

Exemple 5.7

- $\mathbb{Z}/p\mathbb{Z}$ avec p premier est simple.
- $\mathbb{Z}/4\mathbb{Z}$ n'est pas simple.
- $\mathfrak{S}_n$, D_n et $\mathfrak{A}_4$ ne sont pas simples.

THÉORÈME 5.2 *Pour tout $n \geqslant 5$, $\mathfrak{A}_n$ est simple.*

Démonstration. Soit N un sous-groupe distingué de $\mathfrak{A}_n$ tel que $N \neq \mathfrak{A}_n$.

- Supposons que N contienne un cycle de la forme $(i\,j\,k) = \sigma$.
  Si $\sigma' = (i'\,j'\,k')$ est un 3-cycle, il existe $\rho \in \mathfrak{S}_n$ tel que $\sigma' = \rho\sigma\rho^{-1}$ car ils ont même type.
  Si $\rho \in \mathfrak{A}_n$, $\sigma' \in N$ donc N contient tout les 3-cycles donc $N = \mathfrak{A}_n$ donc contradiction.
  Sinon, $\rho \notin \mathfrak{A}_n$, on remplace ρ par $\rho(l\,m) \in \mathfrak{A}_n$ avec i, j, k, l, m distincts (possible car $n \geqslant 5$). D'où une contradiction par le cas précédent.
  Donc il n'y a pas de cycles d'ordre 3 dans N.
- Soit $\sigma \in N$ qui s'écrit $\sigma = (i_1 \dots i_p)\gamma_2 \dots \gamma_m$ avec $p \geqslant 4$.
  On conjugue avec $(i_1, i_2, i_3) \in \mathfrak{A}_n$ et on a $\sigma' = (i_2\,i_3\,i_1 \dots\, i_p)\gamma_2 \dots \gamma_m \in N$.
  Donc, comme N est un groupe, $\sigma'\sigma^{-1} = (i_2\,i_4\,i_1) \in N$. D'où la contradiction.
  Donc tous les cycles dans la décomposition de $\sigma \in N$ sont de longueur 2 ou 3.
- Si σ est de type $[3, 2, \dots, 2]$, σ^2 est de type $[3, 1, \dots, 1]$ donc contradiction.
  Il reste donc les permutations associées aux types $[3, \dots, 3]$ et $[1, \dots, 1]$.
- Type $[3, \dots, 3]$: soit $\sigma = (i_1\,i_2\,i3)(i'_1\,i'_2\,i'_3)\gamma_3 \dots \gamma_p$.
  On conjugue avec $(i'_1\,i'_2\,i_3)$ et on a $\sigma' = (i_1\,i_2\,i'_1)(i'_2\,i_3\,i'_3)\gamma_3 \dots \gamma_p$ et on obtient un cycle à plus de quatre éléments dans $\sigma\sigma'$. D'où une contradiction.
- Type $[2, \dots, 2]$: $\sigma = (i_1\,i_2)(i_3\,i_4)$
  On conjugue avec $(i_1\,i_5\,i_2)$ et on trouve $\sigma' = (i_5\,i_1)(i_3\,i_4)$ et $\sigma'\sigma = (i_2\,i_5\,i_1)$, d'où une contradiction.
- Cas où $\sigma = (i_1\,i_2)(i_3\,i_4)(i_5\,i_6)\gamma_4 \dots \gamma_m$.
  On conjugue avec $(i_5\,i_4)(i_3\,i_2)$ et on a $\sigma' = (i_1\,i_3)(i_2\,i_5)(i_4\,i_6)\gamma_4 \dots \gamma_m$ et $\sigma'\sigma = (i_1\,i_5\,i_4) \dots$ d'où une contradiction. OUF ! ! ! ∎

Proposition 5.10

- Les groupes commutatifs simples sont les groupes cycliques d'ordre p avec p premier.
- Il n'y a aucun groupe simple non abélien à moins de 60 éléments.
- À isomorphisme près, il n'y a qu'un seul groupe simple de cardinal compris entre 60 et 360 : c'est $PSL_2(\mathbb{Z}/7\mathbb{Z}) = SL_2(\mathbb{Z}/7\mathbb{Z})/\mu_2(\mathbb{Z}/7\mathbb{Z})$ avec $\mu_2(\mathbb{Z}/7\mathbb{Z}) = \{a \in \mathbb{Z}/7\mathbb{Z}, a^2 = 1\}$.7
- Le premier groupe de Mathieu (7920 éléments) noté M_1 est :

$$\langle (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11), (3\,7\,11\,8)(4\,10\,5\,6)\rangle \subset \mathfrak{S}_{11}$$

  est simple.

Exemple 5.8 En notant $PSL_n(q) = PSL_n(\mathbb{Z}/q\mathbb{Z})$, on a

$$\mathfrak{A}_5 \simeq PSL_2(4) \simeq PSL_2(5)$$

$$PSL_2(7) \simeq PSL_3(2) \text{ et } \mathfrak{A}_6 \simeq PSL_2(9)$$

Chapitre 6

Groupes quotients

Proposition 6.1

$$\begin{aligned} H \lhd G \quad &\text{ssi} \quad G/H = H\backslash G \\ &\text{ssi} \quad \forall g \in G, gH = Hg \\ &\text{ssi} \quad H \text{ stable sous } \mathrm{Int}(G) \\ &\text{ssi} \quad H \text{ est réunion de classes de } G \end{aligned}$$

Théorème 6.1 *Soit $H < G$.*
$H \lhd G$ ssi il existe une structure de groupe sur G/H telle que l'application :

$$\pi : \begin{cases} G & \to & G/H \\ g & \mapsto & gH \end{cases}$$

soit un morphisme de groupe. Celle-ci est alors unique et π est un morphisme surjectif de noyau H.

Démonstration.
$\Leftarrow$ Si G/H est muni d'une structure de groupe telle que π soit un morphisme. On aura alors

$$gH \cdot g'H = \pi(g)\pi(g') = \pi(gg') = gg'H$$

D'où l'unicité. La surjectivité est connue. De plus,

$$g \in \mathrm{Ker}(\pi) \quad \text{ssi} \quad \pi(g) = H \quad \text{ssi} \quad gH = H \quad \text{ssi} \quad g \in H$$

Donc $H = \mathrm{Ker}(\pi)$ donc est distingué.
$\Rightarrow$ Si $H \lhd G$, $gHg'H = gg'H$ car $g'H = Hg'$.
Donc $(gH, g'H) \mapsto gg'H$ est bien définie et fait de G/H un groupe. De plus, π est bien un morphisme. ∎

Définition 6.1 Si $H \lhd G$ et $g \in G$, on note $\overline{g} = \overline{g}^H = gH = Hg$.

Exemple 6.1

- $\mathfrak{A}_n \lhd \mathfrak{S}_n$ et $\mathfrak{S}_n/\mathfrak{A}_n = \{\mathfrak{A}_n, (1\,2)\mathfrak{A}_n\}$.
- $V_4 \lhd \mathfrak{A}_4$ et $V_4 \lhd \mathfrak{S}_4$.

$$\mathfrak{A}_4/V_4 = \{\overline{1}, \overline{(123)}, \overline{132}\}$$

$$\mathfrak{S}_4/V_4 = \{\overline{1}, \overline{(123)}, \overline{(132)}, \overline{(12)}, \overline{(14)}, \overline{(13)}\}$$

COROLLAIRE 6.1 *Un sous-groupe est distingué ssi c'est le noyau d'un morphisme.*

THÉORÈME 6.2 *Soit G un groupe.*

- *$G^{ab} = G/D(G)$ est un groupe abélien.*
- *Soit $H < G$. $D(G) \subset H$ ssi $H \lhd G$ et G/H abélien.*

Démonstration. Le deuxième point implique le premier donc on montre le deuxième.

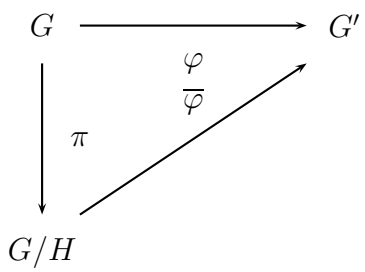
$\Leftarrow$ On suppose $H \lhd G$ et on note $\pi : g \mapsto \overline{g}$.
$\overline{[g,h]} = [\overline{g}, \overline{h}]$ car π est un morphisme. Donc $[g,h] \in H$ ssi $\overline{[g,h]} = 0$ ssi $[\overline{g}, \overline{h}] = 0$.
Donc $D(G) \subset H$ ssi $\forall (g,h), [\overline{g}, \overline{h}] = 0$ ssi G/H abélien.

$\Rightarrow$ Il reste à montrer que $D(G) \subset H$ ssi $H \lhd G$.
Soit $(g,h) \in G \times H$. $[g,h] \in D(G) \subset H$ donc $ghg^{-1}h \in H$ donc $ghg^{-1} \in H$. ∎

THÉORÈME 6.3 (PROPRIÉTÉ UNIVERSELLE DU QUOTIENT) *Soit $\varphi : G \to G'$ un morphisme et $H \lhd G$. $H \subset \mathrm{Ker}(\varphi)$ ssi il existe un morphisme $\overline{\varphi} : G/H \to G'$ tel que $\varphi = \overline{\varphi} \circ \pi$.*

Remarque 6.1

- *$\overline{\varphi}$ est l'unique morphisme vérifiant cette propriété.*
- *On écrit :*



- $\mathrm{Ker}(\overline{\varphi}) = \mathrm{Ker}(\varphi)/H$.
- *$\overline{\varphi}$ est injective ssi $H = \mathrm{Ker}(\varphi)$.*
- *$H < K < G$ et $H \lhd G$ implique $H \lhd K$.*

Démonstration.
$\Leftarrow$ Soit $h \in H$.
$\varphi(h) = \overline{\varphi}(\overline{h}) = \overline{\varphi}(\overline{1}) = 1$ donc $h \in \mathrm{Ker}(\varphi)$. Donc $H \subset \mathrm{Ker}(\varphi)$.
$\Rightarrow$ On définit $\overline{\varphi}(\overline{g}) = \varphi(g)$.
Il faut montrer que c'est bien défini. Si $\overline{g} = \overline{g'}$, $g^{-1}g' \in H \subset \mathrm{Ker}(\varphi)$ donc $\varphi(g) = \varphi(g')$.
Le reste est vraie par définition. ■

THÉORÈME 6.4 *Soit $\varphi : G \to G'$ un morphisme de groupes.*

$$\psi : \begin{cases} G/\mathrm{Ker}(\varphi) & \to & \mathrm{Im}(\varphi) \\ \overline{g} & \mapsto & \varphi(g) \end{cases}$$

est un isomorphisme et c'est le seul.

Démonstration. φ est à valeurs dans $\mathrm{Im}(\varphi)$ donc on a un morphisme surjectif $G \to \mathrm{Im}(\varphi)$. Son noyau est $\mathrm{Ker}(\varphi)$ donc il existe un morphisme injectif de $G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(G)$ qui reste surjectif. ■

COROLLAIRE 6.2 *Tout groupe cyclique est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 6.2
- $G/Z(G) \simeq \mathrm{Int}(G)$ car

$$\varphi : \begin{cases} G & \to & \mathrm{Aut}(G) \\ & & \\ g & \mapsto & \sigma_g : \begin{cases} G & \to & G \\ h & \mapsto & ghg^{-1} \end{cases} \end{cases}$$

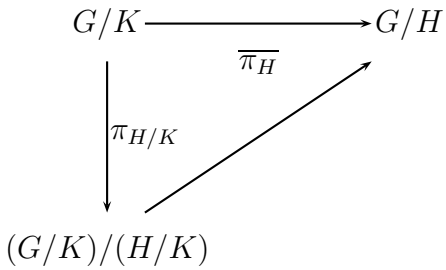
  a pour noyau $Z(G)$ et pour image $\mathrm{Int}(G)$.
- $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \simeq \mathbb{C}^*$. (considérer det)
- $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$ (considérer ε)

THÉORÈME 6.5 *Soit $K < H < G$ avec $K \lhd G$ et $H \lhd G$.*

$$(G/K)/(H/K) \simeq G/H$$

Démonstration. Il suffit de considérer le graphe suivant :

■



Définition 6.2 Soit X un ensemble et $\mathcal{M}(X \cup X^{-1})$ l'ensemble des mots sur X. On définit une relation d'équivalence $\sim$ sur cet ensemble en contractant les produits xx^{-1} et $x^{-1}x$.

On note $\mathscr{F}(X) = \mathcal{M}(X \cup X^{-1})/\sim$ le quotient. $\mathscr{F}(X)$ est le groupe libre sur X

Proposition 6.2 C'est un groupe.

Proposition 6.3 Soit G un groupe, $Y \subset G$ et X en ensemble quelconque.

Pour tout $f : X \to Y$, il existe un unique morphisme $\varphi : \mathscr{F}(X) \to G$ tel que $\varphi(x) = f(x)$ pour tout $x \in X$.

Si f est surjective et $G = \langle Y \rangle$, φ est surjective.

Remarque 6.2 *Si φ est surjective, $G \simeq \mathscr{F}(X)/\operatorname{Ker}(\varphi)$.*

Exemple 6.3 Pour $X = \{x, y\}$, $R = \langle , x^n, y^2, xyxy \rangle$, $\mathscr{F}(X)/R \simeq D_n$.

Chapitre 7

Formule des classes

Proposition 7.1 Si G agit sur X, pour tout $x \in X$,

$$\varphi : \begin{cases} G/G_x & \to & Gx \\ gG_x & \mapsto & gx \end{cases}$$

est une bijection.

Démonstration. La surjectivité est claire.

Soit $g, g' \in G$.

$$gx = g'x \quad \text{ssi} \quad x = g^{-1}g'x \quad \text{ssi} \quad g^{-1}g' \in G_x \quad \text{ssi} \quad g'G_x = gG_x$$

D'où l'injectivité et la bonne définition. ∎

Remarque 7.1 Si x et x' sont dans la même orbite, leurs stabilisateurs sont conjugués et $|G_x| = |G_{x'}|$.

En effet, si $x' = gx$, on a :

$$\begin{aligned} h \in G_{x'} \quad &\text{ssi} \quad hx' = x' \quad \text{ssi} \quad hgx = gx \quad \text{ssi} \quad g^{-1}hgx = x \\ &\text{ssi} \quad g^{-1}hg \in G_x \quad \text{ssi} \quad h \in gG_xg^{-1} \end{aligned}$$

Corollaire 7.1 $|G| = |Gx||G_x|$

Démonstration. Clair par le théorème avant Lagrange et par la proposition précédente. ∎

Exemple 7.1 Quels sont les groupes finis avec exactement deux classes de conjugaison ?

Soit G un tel groupe.

La classe de 1 est $\{1\}$ donc l'autre classe est $G \setminus \{1\}$. Donc $|G| - 1$ divise $|G|$ et donc $|G| = 2$.

COROLLAIRE 7.2 (FORMULE DES CLASSES) *Soit G fini agissant sur X et $(x_1, \dots, x_r) \in X$ un élément dans chaque orbite.*

On a $|X| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$.

Démonstration. On a $X = \bigcup_{i=1}^{r} Gx_i$ qui est disjointe donc $|X| = \sum_{i=1}^{r} |Gx_i| = \sum_{i=1}^{r} \frac{|G|}{|G_{x_i}|}$ par la proposition. ∎

Définition 7.1 On note $X^G = \{x \in X, \forall g \in G, gx = x\}$, $X^g = X^{\langle g \rangle} = \{x \in X, gx = x\}$ et $G\backslash X$ l'ensemble des orbites sous l'action de G.

Proposition 7.2 On a $|G\backslash X| = \sum_{g \in G} \frac{|X^g|}{|G|}$

Démonstration. On a :

$$\begin{aligned}
\sum_{g \in G} |X^g| &= \text{Card}(\{(g, x) \in G \times X, gx = x\}) \\
&= \sum_{x \in X} |G_x| \\
&= \sum_{i=1}^{r} \sum_{x \in Gx_i} |G_x| \\
&= \sum_{i=1}^{r} |G_{x_i}||Gx_i| \\
&= \sum_{i=1}^{r} |G| \\
&= |G||G\backslash X|
\end{aligned}$$

Définition 7.2 Soit p premier. Un p-groupe fini est un groupe dont l'ordre est une puissance de p.

Remarque 7.2 Tout groupe abélien fini est somme de p-groupes abéliens finis.

Proposition 7.3 Si un p-groupe fini agit sur un ensemble X, $|X^G| \equiv |X| \mod p$.

Démonstration. On a par la formule des classes :

$$|X| = \sum_{i=1}^{r} |Gx_i| = \sum_{\substack{i=1 \\ |Gx_i|=1}}^{r} |Gx_i| + \sum_{\substack{i=1 \\ p \text{ divise } |Gx_i|}}^{r} |Gx_i| \equiv \sum_{\substack{i=1 \\ |Gx_i|=1}}^{r} |Gx_i| = |X^G|$$

∎

THÉORÈME 7.1 DE CAUCHY *Si G est un groupe fini d'ordre n et p premier divisant n alors il existe un élément d'ordre p dans G.*

Démonstration. On fait agir $\mathfrak{S}_p$ sur G^p par

$$(\sigma, (g_1, \dots, g_p)) \mapsto (g_{\sigma(1)}, \dots, g_{\sigma(n)})$$

On se limite au sous-groupe $\langle\gamma\rangle \in \mathfrak{S}_p$ avec $\gamma = (1\,2\,3\dots p)$.
Posons $X = \{(g_1, \dots, g_p) \in G^p, g_1 \dots g_p = 1\} \subset G^p$.
X est stable sous l'action de $\langle\gamma\rangle$.
On a de plus $|\langle\gamma\rangle| = p$ et $|X| = |G|^{p-1} = n^{p-1}$.
Donc, comme $p|n$, $p||X|$ donc $p||X^\gamma|$ car $|X^\gamma| \equiv |X| \mod p$.
Donc, comme $X^\gamma \neq \varnothing$ (contient $(1\,1\dots1)$), il existe $(g_1, \dots, g_p) \in X^\gamma$ avec au moins un des g_i différent de 1.
On a donc $(g_2, g_3, \dots, g_p, g_1) = (g_1, \dots, g_p)$ donc $g_1 = g_2 = \dots = g_p$.
Donc $(g_1, \dots, g_1) \in X$ donc $g_1^p = 1$. ■

Proposition 7.4
- Le centre d'un p-groupe fini non trivial est non trivial.
- Si G est un p-groupe fini simple, $|G| = 1$ ou $|G| = p$.

Démonstration.
- On fait agir G sur lui-mêm par conjugaison.
  On a $|Z(G)| \equiv |G| \mod p$.
  Si $Z(G) = \{1\}$, $|G| \equiv 1 \mod p$. Comme $p||G|$, $|G| = 1$ donc $G = \{1\}$.
- On a $Z(G) \lhd G$. Si G est simple, on a $Z(G) = G$ ou $Z(G) = 1$.
  Si $Z(G) = G$, G est abélien. Si $G \neq \{1\}$, comme G est un p-groupe, $p||G|$ donc il existe un élément g d'ordre p.
  Alors $\langle g\rangle \lhd G$. Donc $G = \langle g\rangle$ et $|G| = p$.
  Si $Z(G) = \{1\}$, $G = \{1\}$ par le point précédent. ■

Proposition 7.5 Un groupe d'ordre p^2 est abélien.

Remarque 7.3 Les groupes d'ordre p aussi.

Démonstration. Soit G un groupe d'ordre p^2 et $g \in G$.
Si $g \in Z(G)$, $Z_G(g) = G$.
Sinon, $g \in Z_G(g)$ et $Z(G) \subset Z_G(g)$ donc $|Z_G(g)| > p$ car $Z(G)$ est non trivial.
Or $|Z_G(g)||p^2$ donc $Z_G(g) = G$.
Donc $Z_G(g) = G$ pour tout $g \in G$, ce qui conclut. ■

Proposition 7.6 Soit G est un p-groupe et $H < G$.
Si $J \neq G$ alors $H \neq N_G(H)$.

Démonstration. On suppose qu'il existe un p-groupe G fini et un sous-group H de G avec $H \neq G$ et $N_G(H) = H$.

On prend G tel que $|G|$ minimal.

On a $Z(G) \subset N_G(H) = H$.

On pose $G' = G/Z(G)$ et $H' = H/Z(G)$.

H' est un sous-groupe de G', $H' \neq G'$ et $|G'| < |G|$ car $Z(G) \neq \{1\}$.

De plus, $N_{G'}(H') = N_G(H)/Z(G) = H/Z(G) = H'$. D'où la contradiction. ∎

Chapitre 8

Produits directs et semi-directs

8.1 Produit direct

8.1.1 Définitions

THÉORÈME 8.1 *Si H et K sont deux groupes, il existe une unique structure de groupe sur $H \times K$ telle que les projections soient des morphismes.*

Démonstration. Unicité : Clair
Existence : le premier truc qui vous passe par la tête marche[1] ■

Définition 8.1 $H \times K$ est le produit direct de H et K.

8.1.2 Propriétés

Proposition 8.1 (universelle) Étant donnés deux morphismes de groupes $\varphi : G \to H$ et $\psi : G \to K$, il existe un unique morphisme $\theta : G \to H \times K$ qui redonne ϕ et ψ après composition avec les projections.

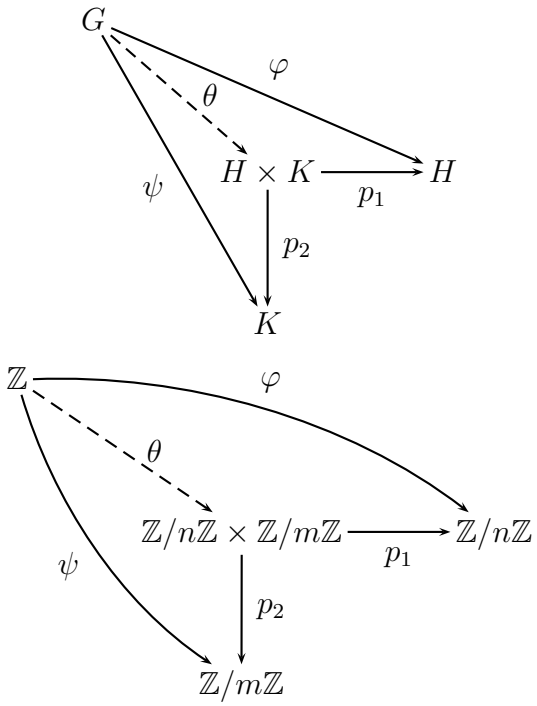
Démonstration. Il suffit de considérer : ■

Exemple 8.1 D'où le théorème chinois : $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$.

Remarque 8.1 *On peut définir $\prod_{i \in I} G_i$ de la même façon. Il est abélien si les G_i le sont.*

THÉORÈME 8.2 *Soient H et K deux sous-groupes d'un groupe G.*
- *Si $K \subset N_G(H)$, alors HK est un sous-groupe de G et $HK = KH$.*
- *Si $H \cap K = \{1\}$, l'application $(h, k) \mapsto hk$ est injective.*

1. encore faudrait-il que quelque chose passe...



- *Si $H \subset N_G(K)$, $K \subset N_G(H)$ et $H \cap G = \{1\}$, alors $(h,k) \to hk$ est un morphisme qui induit un isomorphisme de $H \times K \to HK$. (considérer les commutateurs)*

Démonstration. Clair ∎

Exemple 8.2 $K = \langle (1\,2) \rangle$, $H = \mathfrak{A}_3$ et $G = \mathfrak{S}_3$.
$H \cap K = \{1\}$, $H \lhd G$ et $HK = G$. Mais $H \not\subset N_G(K)$ car

$$1 \neq (1\,2\,3)(1\,2)(1\,3\,2) = (1\,3) \neq (1\,2)$$

Et ça marche pas : $(\sigma, \tau) \mapsto \sigma\tau$ n'est pas un morphisme. Seulement une bijection.

8.1.3 Applications

COROLLAIRE 8.1 *Tout groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou bien à $(\mathbb{Z}p/2\mathbb{Z})^2$.*

Démonstration. Tout groupe d'ordre 4 est d'ordre p^2 avec $p = 2$ donc il est abélien.

Si G est cyclique, alors $G \simeq \mathbb{Z}/4\mathbb{Z}$.

Sinon, tous les éléments sont d'ordre 1 ou 2. Donc il y a trois éléments d'ordre 2 : g, h et k.

On a $\langle g\rangle \cap \langle h\rangle = \{1\}$ donc $G \simeq \langle g\rangle \times \langle h\rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2$. ∎

Proposition 8.2 Si G est un sous-groupe d'ordre 6 alors $G \simeq \mathbb{Z}/6\mathbb{Z}$ ou $G \simeq \mathfrak{S}_3$.

Démonstration. Par Cauchy, il existe un élément d'ordre 2 qui engendre H et un élément d'ordre 3 qui engendre K.

On a $K \lhd G$ car il est d'indice 2. On a bien sur $H \cap K = \{1\}$ par Lagrange.

Si $H \lhd G$, $G \simeq H \times K \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$.

Sinon, il y a trois éléments d'ordre 2. G agit par cojugaison sur les groupes engendrés par ces trois éléments.

On a donc un morphisme φ de $G \to \mathfrak{S}_3$. Montrons que $\mathrm{Ker}(\varphi) = \{1\}$. On aura alors φ bijectif.

Or $\mathrm{Ker}(\varphi) = \bigcap_{ordre(g)=2} N_G(g) = \bigcap_{ordre(g)=2} \langle g\rangle = \{1\}$. ∎

Remarque 8.2 Le nombre de conjugués d'un sous-groupe H dans un groupe G divise $(G : H)$. En effet, c'est le nombre d'orbites de H sous l'action par conjugaison de G ie $(G : N_G(H))$ par la formule des classes.

8.2 Produit semi-direct

8.2.1 Définitions

THÉORÈME 8.3 *Soient Q et N deux groupes et $\varphi : Q \to \mathrm{Aut}(N)$ un morphisme.*

La formule $(n_1, q_1)(n_2, q_2) = (n_1\varphi(q_1)(n_1), q_1q_2)$ définit une structure de groupe sur $N \times Q$.

Définition 8.2 Le groupe obtenu, noté $N \rtimes_\varphi Q$ est le produit semi-direct de N par Q le long de φ.

Remarque 8.3 On aura un morphisme surjectif $N \rtimes_\varphi Q \to Q$ dont le noyau est N.

Démonstration. On a $(1,1)(n,q) = (\varphi(1)(n), q) = (n,q)$ et $(n,q)(1,1) = (n\varphi(q)(1), q) = (n,q)$.

$(n,q)(n',q') = (1,1)$ ssi $q' = q^{-1}$ et $n' = \varphi(q^{-1})(n^{-1})$.

L'associativité marche aussi. ∎

THÉORÈME 8.4 *Soient N et Q deux sous-groupes de G avec $N \lhd G$ et $N \cap Q = \{1\}$.*

NQ est un sous-groupe de G et l'application :

$$\times : \begin{cases} N \rtimes_\varphi Q & \to & G \\ (n,q) & \mapsto & nq \end{cases}$$

avec $\varphi(q)(n) = qnq^{-1}$ induit un isomorphisme avec NQ.

Démonstration. On a $NQ < G$ et $N \rtimes_\varphi Q \to G$ est injective.

$\varphi(q)$ est un automorphisme de N car $N \lhd G$ et que $q \mapsto \varphi(q)$ est un morphisme.

De plus, $(n_1, q_1)(n_2, q_2) = n_1 q_1 n_2 q_1^{-1} q_1 q_2 = n_1 \varphi(q_1)(n_2) q_2$. ∎

Exemple 8.3

- $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.
  $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{F}_3^*$.
  Si φ est trivial, ça fait le produit direct des deux ie $\mathbb{Z}/6\mathbb{Z}$.
  Sinon, ça fait D_3 car $\varphi(0) = \mathrm{Id}$ et $\varphi(1)(1) = 2$ et $\varphi(1)(2) = 1$ et on peut faire correspondre r à $(1,0)$ et s à $(0,1)$.
- $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
  Le seul morphisme φ est le morphisme trivial donc ça fait $\mathbb{Z}/6\mathbb{Z}$.

Remarque 8.4 *Si $NQ = G$ et G fini, on a $N \rtimes_\varphi Q \simeq G$ et $|N||Q| = |G|$*

THÉORÈME 8.5 *Soit $\varphi : G \to G'$ un morphisme de groupes et $N = \mathrm{Ker}(\varphi)$.*

- *Si $K < G$, $\varphi^{-1}(\varphi(K)) = NK = KN$.*
- *Si $K' < G'$, $\varphi(\varphi^{-1}(K')) = K' \cap \mathrm{Im}(\varphi)$.*
- *φ et φ^{-1} induisent des bijections réciproques entre l'ensemble des sous-groupes de G contenant $\mathrm{Ker}(\varphi)$ et les sous-groupes de $\mathrm{Im}(\varphi)$.*
- *Lorsque φ est surjective, cette bijection préserve les sous-groupes distingués.*

Remarque 8.5 *$K \lhd G \not\Rightarrow \varphi(K) \lhd G'$ en général. Par exemple, $K = \langle (1\,2) \rangle$, $G = K$, $G' = \mathfrak{S}_3$ et $\varphi = \mathrm{Id}$.*

Démonstration.

- On a :

$$\begin{aligned} g \in \varphi^{-1}(\varphi(K)) \quad &\text{ssi} \quad \varphi(g) \in \varphi(K) \\ &\text{ssi} \quad \exists h \in K, \varphi(g) = \varphi(h) \\ &\text{ssi} \quad \exists h \in K, \varphi(gh^{-1}) = 1 \\ &\text{ssi} \quad \exists h \in K, gh^{-1} \in N \\ &\text{ssi} \quad g \in NK \end{aligned}$$

De même pour KN.

- On a :

$$\begin{array}{rll} g' \in \varphi(\varphi^{-1}(K')) & \text{ssi} & \exists g \in \varphi^{-1}(K'), g' = \varphi(g) \\ & \text{ssi} & \exists g' \in K' \cap \mathrm{Im}(\varphi) \end{array}$$

- Si $N \subset K$, alors $\varphi^{-1}(\varphi(K)) = NK = K$.
  Si $K' < \mathrm{Im}(\varphi)$, $\varphi(\varphi^{-1}(K')) = K' \cap \mathrm{Im}(\varphi) = K'$.
- Si $K' \lhd G'$, on regarde $\overline{\varphi} = \varphi \circ \pi$ avec π la surjection canonique de G' dans G'/H'.
  $g \in \mathrm{Ker}(\overline{\varphi})$ ssi $\overline{\varphi}(g) = 0$ ssi $\varphi(g) \in K'$ ssi $g \in \varphi^{-1}(K')$.
  Donc $\varphi^{-1}(K') = \mathrm{Ker}(\overline{\varphi}) \lhd G$.
  Si $K \lhd G$ et φ surjective, $\varphi(K) \lhd G'$.
  Soit $h \in K$ et $g' \in G'$. Comme φ est surjectif, $g' = \varphi(g)$ avec $g \in G$.
  On a $g'\varphi(h)g'^{-1} = \varphi(ghg^{-1}) \in \varphi(K)$. ■

Remarque 8.6 *Quels sont les sous-groupes de $\mathbb{Z}/10\mathbb{Z}$?*
Ce sont ceux de $\mathbb{Z}$ qui contiennent $10\mathbb{Z}$ ie $p\mathbb{Z}$ avec $p \in \{1, 2, 5, 10\}$.
Donc les sous-groupes en question sont $\{0\}$, $\mathbb{Z}/10\mathbb{Z}$, $2\mathbb{Z}/10\mathbb{Z}$ et $5\mathbb{Z}/10\mathbb{Z}$.

Corollaire 8.2 *Soit G un groupe cyclique d'ordre n et d un diviseur de n. Il existe un unique sous-groupe de G cyclique d'ordre d.*

Démonstration. Le problème est stable par isomorphisme donc on peut supposer $G = \mathbb{Z}/n\mathbb{Z}$. On a $n = md$.
Dans $\mathbb{Z}/n\mathbb{Z}$, les sous-groupes d'ordre d sont exactement ceux d'indice m.
Ce sont les sous-groupes d'indice m de $\mathbb{Z}$ contenant $n\mathbb{Z}$.
Or il y en n'a qu'un seul : $m\mathbb{Z}$. Ce qui conclut. ■

Théorème 8.6 (Deuxième théorème d'isomorphisme) *Soient H et K deux sous-groupes de G tels que $K \subset N_G(H)$.*
On a $HK/H \simeq K/(K \cap H)$.

Démonstration. On a $K \subset N_G(H)$ et $H \subset N_G(H)$ donc $HK \subset N_G(H)$ car $N_G(H)$ est un groupe.
Donc $H \lhd HK$.
Notons π la surjection canonique de $HK \to HK/H$. Posons $\varphi : K \to HK/H$ l'injection canonique de K dans HK composée avec π.
On a φ surjective de noyau $H \cap K$ donc $K/(H \cap K) \simeq HK/K$. ■

Corollaire 8.3 *Si G est de plus fini, $|HK||H \cap K| = |H||K|$.*

8.3 Suites exactes

Définition 8.3 On appelle suite exacte une suite de morphismes φ_i tels que $\mathrm{Ker}(\varphi_i) = \mathrm{Im}(\varphi_{i-1})$.

On dit qu'elle est courte ssi il existe i tel que φ_i est injective et φ_{i+1} est surjective.

Exemple 8.4 $1 \to \mathrm{Ker}(\varphi) \to G \to \mathrm{Im}(\varphi) \to 1$.

$1 \to G_1 \to G_1 \times G_2 \to G_2 \to 1$

Si $G = N \rtimes_\varphi Q$, $1 \to N \to G \to Q \to 1$ en est une.

Définition 8.4 On appelle scindage d'une suite exacte courte un morphisme σ tel que $\pi \circ \sigma = \mathrm{Id}$ avec π un morphisme surjectif de la suite.

Proposition 8.3 G est un produit semi direct ssi il existe un scindage.

Exemple 8.5

- $Q_8 \not\simeq D_4$ car Q_8 n'est pas un produit semi-direct (tout sous-groupe non trivial de Q_8 contient le centre $\{\pm I\}$) alors que D_4 si, c'est $\langle r \rangle \langle s \rangle$.
- $V_4 \lhd \mathfrak{S}_4$, $\mathfrak{S}_3 < \mathfrak{S}_4$ et $V_4 \cap \mathfrak{S}_4 = \{\mathrm{Id}\}$.
  De plus $|V_4||\mathfrak{S}_3| = |\mathfrak{S}_4|$ et $\mathfrak{S}_4 \simeq V_4 \rtimes \mathfrak{S}_3 = V_4\mathfrak{S}_3$.
  Et $\mathfrak{S}_4/V_4 = V_4\mathfrak{S}_3/V_4 \simeq \mathfrak{S}_3/(\mathfrak{S}_3 \cap V_4) \simeq \mathfrak{S}_3/\{1\} \simeq \mathfrak{S}_3$.

Chapitre 9

Théorèmes de Sylow

Définition 9.1 Soit G un groupe fini et p un nombre premier. Un p-Sylow de G est un p-sous-groupe maximal pour l'inclusion.

Proposition 9.1 $D < G$ est un p-Sylow ssi D est un p-groupe et si $D < H < G$ avec H un p-groupe, alors $D = H$.

Proposition 9.2 Soit G un groupe et p premier.

L'intersection de tous les p-Sylow de G est caractéristique.

Si N est un p-sous-groupe distingué de G alors N est inclus dans cette intersection.

Démonstration. Si P est un p-Sylow de G et $\sigma : G \to G$ un automorphisme, alors $\sigma(P)$ est un p-Sylow de G.

On a donc, pour $\sigma \in \mathrm{Aut}(G)$, $\sigma\left(\bigcap_{p\text{-Sylow}} P\right) = \bigcap_{p\text{-Sylow}} \sigma(P) \subset \bigcap_{p\text{-Sylow}} P$ et il y a égalité car les cardinaux sont égaux.

Si N est distingué et P un p-Sylow, NP est un sous-groupe donc $|NP| = \frac{|N||P|}{|N \cap P|}$ donc $|NP|$ est une puissance de p

Donc NP est un p-groupe qui contient P donc $NP = P$ et $N \subset P$. ∎

Exemple 9.1 Dans $\mathfrak{S}_4$ de cardinal $24 = 2^3 \times 3$, il y a quatre 3-Sylow (les sous-groupes engendrés par les cycles) et trois 2-Sylow : $\langle (1\,j), V_4 \rangle$ avec $j \in \{2, 3, 4\}$.

Définition 9.2 Un p-sous-groupe P d'un groupe fini G est dit p-clos ssi il contient tous les éléments d'ordre une puissance de p.

Remarque 9.1

- *L'existence n'est pas assurée.*
- *On a l'unicité si on a l'existence.*
- *S'il existe, c'est l'unique p-Sylow de G.*

COROLLAIRE 9.1 *Soit G un groupe fini, p premier.*
Soit $P < G$. P est p-clos ssi P est un p-Sylow distingué.
Dans ce cas, l'ordre de P est la plus grande puissance de p qui divise $|G|$.

Démonstration.
- $\Rightarrow$ P est un p-Sylow, son conjugué aussi donc comme P est l'unique p-Sylow, P est distingué.
- $\Leftarrow$ Si P est un p-Sylow distingué, il est contenu dans tous les autres p-Sylow car il est distingué et par maximalité, il est égal aux autres. P est donc l'unique p-Sylow et donc il est p-clos.
- On a $|G| = p^e m$ avec $p \wedge m = 1$ et on veut montrer $|P| = 2^e$.
  Par Lagrange, il suffit de montrer $p \not| |G/P|$.
  Si $p||G/P|$, par Cauchy, il existe $H' < G/P$ d'ordre p. Mais on a une bijection entre les sous-groupes de G/P et ceux de G qui contiennent P.
  Donc il existe un unique $H < G$ tel que $P \subset H$ qui correspond à H'.
  Les théorèmes d'isomorphismes donnent $(H : P) = |H'|$ donc $p = (H : P)$ donc H est un p-groupe par Lagrange.
  Donc $H = P$ et $p = 1$. ■

THÉORÈME 9.1 DE SYLOW *Soit G un groupe fini et p premier. On écrit $|G| = p^e m$ avec $p \wedge m = 1$. Notons n_p le nombre de p-Sylow de G.*
- *Les p-Sylow sont les sous-groupes d'ordre p^e.*
- *Tous les p-Sylow sont conjugués et $n_p = (G : N_G(P))$*
- *$n_p \equiv 1 \mod p$ et $n_p | m$.*

Remarque 9.2 En général, $(G : N_G(H))$ est le cardinal de l'orbite de H sous l'action par conjugaison de G. C'est donc le nombre de conjugués distincts de H dans G.

Démonstration.
2 Soient P et P' deux p-Sylow de G.
On sait que G agit sur $G/N_G(P) = X$ et on peut regarder la restriction de l'action à P'.
Comme P' est un p-groupe, on a $|X^{P'}| \equiv |X| \mod p$.
De plus on a :

$$\begin{aligned} gN_G(P) \in X^{P'} \quad &\text{ssi} \quad \forall h \in P', hgN_G(P) = gN_G(P) \\ &\text{ssi} \quad \forall h \in P', g^{-1}hgN_G(P) = N_G(P) \\ &\text{ssi} \quad g^{-1}P'gN_G(P) = N_G(P) \\ &\text{ssi} \quad g^{-1}P'g \subset N_G(P) \\ &\text{ssi} \quad g^{-1}P'g \subset P \end{aligned}$$

- Si $P' = P$, $gN_G(P) \in X^P$ ssi $g^{-1}Pg \subset P$ ssi $g \in N_G(P)$.
  Donc $X^P = \{N_G(P)\}$ donc $|X| \equiv |X^P| \equiv 1 \mod p$.
- Si $P \neq P'$, on a $|X^{P'}| \equiv |X| \equiv 1 \mod p$ donc $|X^{P'}| \neq 0$ et $X^{P'} \neq \varnothing$.
  $g^{-1}P'g \subset P$ et comme P et P' jouent des rôles symétriques, P et P' sont conjugués. On a donc le deuxième point.

1 et 3 On a $|G| = (G : P)|P| = (G : N_G(P))(N_G(P) : P)|P|$.
$(N_G(P) : P) \not\equiv 0 \mod p$ et $(G : N_G(P)) = n_p \equiv 1 \mod p$.
En effet, P est un p-Sylow de $N_G(P)$ et $P \lhd N_G(P)$.
Donc P est p-clos dans $N_G(P)$ donc $p \not| (N_G(P) : P)$ donc $(N_G(P) : P) \not\equiv 0 \mod p$.
On a donc $(G : P) = m$ et $|P| = p^e$. ∎

Exemple 9.2 Tout groupe G d'ordre 15 est cyclique.
$n_3 \equiv 1 \mod 3$ et $n_3|5$ donc $n_3 = 1$. De même, $n_5 = 1$.
Donc on a un 3-Sylow H et un 5-Sylow K distingués.
$H \cap K = \{1\}$ car son ordre doit diviser 3 et 5.
On a $G \simeq H \times K \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$.

COROLLAIRE 9.2 *Si P est un p-Sylow et H un p-sous-groupe.*
Il existe g tel qie $H \subset gPg^{-1}$.

THÉORÈME 9.2 *Il existe un unique groupe simple d'ordre 60 (à isomorphisme près).*

Démonstration. Soit G un groupe simple d'ordre 60.

Soit H un sous-groupe d'indice k dans G. On fait agir G sur G/H pour obtenir un morphisme $\varphi : G \to \mathfrak{S}_k$.

On a $\mathrm{Ker}(\varphi) \lhd F$ donc $\mathrm{Ker}(\varphi) = \{1\}$ ou $\mathrm{Ker}(\varphi) = G$.

Mais si $\mathrm{Ker}(\varphi) = \{1\}$, φ est injectif donc $k! \geqslant 60$ donc $k \geqslant 5$ et si $\mathrm{Ker}(\varphi) = \{G\}$, pour tout $g \in G$, $gH = H$ donc $G = H$ et $k = 1$.

Supposons $k = 5$. On a un isomorphisme entre G et H qui est d'indice 2 dans $\mathfrak{S}_5$ donc $H = \mathfrak{A}_5$.

Supposons que pour tout $H < G$, on ait $(G : H) \geqslant 6$. On applique les théorèmes de Sylow : $n_2 \geqslant 6$, $n_2 \equiv 1 \mod 2$ et $n_2|30$ donc $n_2 = 15$.

De même, $n_3 = 10$ et $n_5 = 6$. Il y a donc $24 = 6(5-1)$ éléments d'ordre 5 et $20 = 10(3-1)$ éléments d'ordre 3.

Soient $P \neq Q$ des 2-Sylow de G et $K = P \cap Q$. Si $K \neq \{1\}$, on pose $H = \langle P, Q\rangle$.

Comme ils sont d'ordre 4, ils sont abéliens donc $K \lhd P$ et $K \lhd Q$ donc $K \lhd \langle P, Q\rangle$.

Donc H n'est pas simple donc $H \neq G$ donc $(G : H) > 5$. Donc $H = P$.

Donc contradiction avec $P \neq Q$. Donc $K = \{1\}$ et on a 45 éléments d'ordre 2 ou 4. Donc $|G| \geqslant 24+20+45+1 > 60$ et on a une contradiction. ∎

Remarque 9.3 $\mathfrak{A}_n$ *est le seul espace d'indice* 2 *dans* $\mathfrak{S}_n$ *car* ε *est le seul morphisme non trivial de* $\mathfrak{S}_n$ *dans* $\{\pm 1\}$.

Si $N < \mathfrak{S}_n$ *est d'indice* 2, $N = \mathrm{Ker}(\pi) = \mathrm{Ker}(\varepsilon) = \mathfrak{A}_n$ *avec* π *la surjection canonique dans* $\mathfrak{S}_n/N$.

