

Théorie des groupes

1 Théorie des groupes

1.1 Théorèmes

Théorème.

Tout groupe cyclique fini est isomorphe à $\mathbf{Z}/n\mathbf{Z}$

Tout groupe cyclique infini est isomorphe à \mathbf{Z}

Théorème (Lagrange).

Soit G un groupe fini

$$H \leq G$$

$$|G| = |H| \times [G : H]$$

Corollaire.

Soit G un groupe fini

$$x \in G$$

L'ordre de x divise le cardinal de G

Corollaire.

Tout groupe d'ordre p premier est cyclique donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$

Théorème (Premier théorème d'isomorphisme).

Soit G, H deux groupes

$$\varphi: G \rightarrow H \text{ un morphisme}$$

Alors :

$$G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$$

Théorème (Deuxième théorème d'isomorphisme).

Soit G un groupe

$$H, K \leq G$$

On suppose que $H \leq N_G(K)$

Alors $HK \leq G$, $K \triangleleft HK$, $H \cap K \triangleleft H$ et :

$$H/(H \cap K) \cong HK/K$$

Théorème (Troisième théorème d'isomorphisme).

Soit G un groupe

$$H, K \triangleleft G \text{ et } H \leq K$$

Alors $K/H \triangleleft G/H$ et :

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

Remarque.

A chaque fois qu'il y a dans la conclusion H/K , c'est qu'il y a aussi $K \triangleleft H$ pour que H/K soit bien un groupe

Numéro	Hypothèses	Conclusion
1	$\varphi : G \rightarrow H$ un morphisme	$G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$
2	$K, H \leq G, H \leq N_G(K)$	$H/(H \cap K) \cong HK/K$
3	$K, H \triangleleft G, K \leq H$	$(G/K)/(H/K)$

Table 1: Les trois théorèmes d'isomorphismes

1.2 Actions de groupes

Definition.

Soit G un groupe

X un ensemble

Une action à gauche de G sur X , noté $G \curvearrowright X$ est une application $G \times X \rightarrow X$ qui satisfait :

i) $\forall x \in X, e \cdot x = x$

ii) $\forall x \in X, g_1, g_2 \in G, g_1(g_2 \cdot x) = (g_1 g_2) \cdot x$

Tout élément g de G définit une application $\sigma_g : X \rightarrow X$

$$x \rightarrow g \cdot x$$

Proposition.

Soit $G \curvearrowright X$ une action

i) $\forall g \in G, \sigma_g$ est une permutation de X

ii) $g \rightarrow \sigma_g$ est un morphisme de G dans S_X

iii) Si $\phi : G \rightarrow S_X$ est un morphisme, on peut définir une action $G \curvearrowright X : g \cdot x = \phi(g)(x)$

Une action $G \curvearrowright X$ est donc la même chose qu'un morphisme $G \rightarrow S_X$

Proposition.

Soit $G \curvearrowright X$ une action

i) Le noyau de l'action est le noyau du morphisme associé :

$$\{g \in G / \forall x \in X, g \cdot x = x\}$$

ii) Soit $x \in X$

Le stabilisateur de x , noté G_x est :

$G_x = \{g \in G / g \cdot x = x\}$ iii) L'action est dite fidèle si son noyau est triviale, donc si le morphisme ϕ associé est injectif. On a de plus :

$$\text{Ker}(\phi) = \bigcap_{x \in X} G_x$$

Proposition.

Soit $G \curvearrowright X$ une action

On définit sur X la relation $x \sim x'$ ssi $\exists g \in G, g \cdot x' = x$

\sim est une relation d'équivalence sur X

$$\forall x \in X, [x]_{\sim} = G \cdot x = g \cdot x / g \in G \text{ et } |G \cdot x| = [G : G_x]$$

$G \cdot x$ est appelée l'orbite de x

On dit que l'action est transitive lorsqu'il n'y a qu'une seule orbite

Definition.

Soit $G \curvearrowright X$ une action

$$Y \subset X$$

Y est dite G -invariante lorsque $\forall g \in G, \forall y \in Y, g \cdot y \in Y$

Théorème (Théorème de Cauchy).

Soit G un groupe fini

p un facteur premier de $|G|$

G contient un élément d'ordre p

Proposition.

Soit G un groupe

A un ensemble fini

$G \curvearrowright A$ une action transitive

$$H \triangleleft G$$

On note O_1, \dots, O_r les orbites de H sur A et on fixe $a \in O_1$

$$r = [G : HG_a]$$

Proposition (Formule de Burnside).

Soit G un groupe fini qui agit sur un ensemble fini X

On note Ω l'ensemble des orbites pour l'action $G \curvearrowright X$ de G sur X

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

1.2.1 Action par multiplication à gauche

Definition.

Soit G un groupe

$$G \curvearrowright G : g \cdot g' = gg'$$

Proposition.

Soit G un groupe

$$H \leq G$$

On pose $X = G/H$ et on définit $G \curvearrowright X : g \cdot xH = gxH$

i) L'action est transitive

ii) Le stabilisateur de H est H

iii) Le noyau de l'action est $\bigcap_{g \in G} gHg^{-1}$

Théorème (Théorème de Cayley).

Tout groupe est isomorphe à un sous-groupe du groupe symétrique

Si $|G| = n$, alors G est isomorphe à un sous-groupe de S_n

1.2.2 Action par conjugaison

Definition.

Soit G un groupe

$$G \curvearrowright G : g \cdot h = ghg^{-1}$$

Definition.

Deux éléments de G sont conjugués s'ils sont dans la même orbite par cette action

Les orbites s'appellent des classes de conjugaisons

Proposition.

Soit $x \in G$

$$C_G(x) = G_x$$

Proposition.

$$G \curvearrowright \mathcal{P}(G) : g \cdot S = gSg^{-1}$$

$$N_G(x) = \{g \in G, gS = Sg\}$$

$$N_G(\{x\}) = C_G(x)$$

Le nombre de conjugués d'une partie $S \subset G$ est $[G : N_G(S)]$

Si $x \in G$, le cardinal de la classe de conjugaison de x est $[G : C_G(x)]$

Proposition (Equation des classes).

Soit G un groupe fini

g_1, \dots, g_r les représentantes de classes de conjugaisons qui ne sont pas dans le centre

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$$

Théorème.

Soit p un nombre premier

G un groupe de cardinal $p^n, n \in \mathbb{N}^*$

Alors $Z(G)$ est non trivial

Corollaire.

Soit p un nombre premier

G un groupe de cardinal p^2

Alors G est abélien et $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Théorème (Théorème de Cauchy).

Soit G un groupe fini

p un facteur premier de $|G|$

G admet un sous-groupe d'ordre p

1.3 Théorèmes de Sylow

Definition.

Soit p un nombre premier

G un groupe

On dit qu'un groupe fini est un p -groupe si son ordre est une puissance de p

Un sous-groupe de G qui est un p -groupe s'appelle un p -sous-groupe de G

Si $|G| = p^\alpha m$ ou $p \nmid m$, un sous-groupe de G d'ordre p^α est appelé un sous-groupe de Sylow de G

$Syl_p(G) = \{H \leq G : H \text{ est un } p\text{-Sylow de } G\}$ et on pose $n_p(G) = |Syl_p(G)|$

Théorème.

Soit G un groupe fini de cardinal $p^\alpha m$ ou $p \nmid m$

1) $Syl_p(G) \neq \emptyset$

2) Si $Q \leq G$ est un p -sous-groupe et $P \leq G$ est un p -Sylow, alors :

$\exists g \in G/gQg^{-1} \leq P$

En particulier, tous les p -Sylow sont conjugués

3) $n_p \equiv 1[p]$ et $n_p|m$

Lemme.

Soit $P \in Syl_p(G)$

Si Q est un p -sous-groupe de G , alors $Q \cap N_G(P) = Q \cap P$

1.4 Produit direct et semi-direct

Definition.

Soit G_1, \dots, G_n des groupes

Le produit direct $G_1 \times \dots \times G_n$ muni de la loi définie par $(g_1, \dots, g_n) \cdot (g'_1, \dots, g'_n) = (g_1 g'_1, \dots, g_n g'_n)$ est un groupe

Proposition.

Soit G_1, G_2 deux groupes

On pose $G'_1 = \{(g, e_2)/g \in G_1\}$ et $G'_2 = \{(e_1, g)/g \in G_2\}$

1) G'_1 est un sous-groupe distingué de G isomorphe à G_1 et $G/G'_1 \cong G_2$

2) Si on identifie G_1 à G'_1 et G_2 à G'_2 , alors :

$\forall g_1 \in G_1, g_2 \in G_2, g_1 g_2 = g_2 g_1$

Remarque.

Le résultat est vrai avec un nombre fini de facteurs

Théorème.

Soit G un groupe

$H, K \leq G$

Supposons que :

1) $H, K \triangleleft G$

2) $H \cap K = \{e\}$

Alors $HK \cong H \times K$

En particulier, H et K commutent

Remarque.

Pour n groupes H_1, \dots, H_n tels que :

$H_1, \dots, H_n \triangleleft G, \forall i \neq j, H_i \cap H_j = \{e\}$

Alors :

$H_1 \dots H_n \cong H_1 \times \dots \times H_n$

Théorème (Théorème chinois).

Soit $n_1, \dots, n_k \in \mathbf{N}$ tels que $\forall i \neq j, \text{PGCD}(n_i, n_j) = 1$

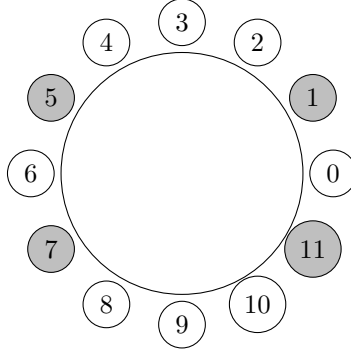
Alors : $\mathbf{Z}/n_1 \dots n_k \mathbf{Z} \cong \mathbf{Z}/n_1 \mathbf{Z} \times \dots \times \mathbf{Z}/n_k \mathbf{Z}$

2 Groupes usuels

2.1 Groupe $(\mathbf{Z}/n\mathbf{Z}, +)$

$\mathbf{Z}/n\mathbf{Z} = \{ \bar{x} : x \in [0, n-1] \}$

Groupe abélien, cyclique engendré par tout élément \bar{x} tel que $x \wedge n = 1$



2.2 Groupe symétrique

Definition. Le groupe symétrique (S_n, o) est le groupe des permutations de $[1, n]$

Definition.

On appelle support de σ l'ensemble des points non fixes de σ : $\text{supp}(\sigma) = \{n \in [1, n] / \sigma(n) \neq n\}$

Remarque.

$x \in \text{supp}(\sigma) \Rightarrow \sigma(x) \in \text{supp}(\sigma)$

Lemme.

Soit $\sigma, \tau \in S_n$ Si $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$, alors : $\sigma\tau = \tau\sigma$

Lemme.

L'ordre d'un k -cycle est de k

Théorème.

Toute permutation est décomposable en produit de cycles à supports disjoints

Proposition.

Tout cycle est décomposable en produit de transpositions

Proposition.

$S_n = \langle \{(ii+1)/i \in [1, n-1]\} \rangle$

$S_n = \langle (12...n), (12) \rangle$

Definition.

Soit $\sigma \in S_n$

On dit que i, j est une inversion pour σ lorsque $i < j$ et $\sigma(i) > \sigma(j)$

On note $N(\sigma)$ le nombre d'inversions pour σ

Definition.

La signature d'une permutation $\sigma \in S_n$, noté $\epsilon(\sigma)$ est :

$\epsilon(\sigma) = (-1)^{N(\sigma)}$

Proposition.

$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$

Proposition.

ϵ est un morphisme surjectif $\epsilon((a_1, \dots, a_k)) = (-1)^{k+1}$

Definition.

Une permutation de signature 1 est dite paire

Une permutation de signature -1 est dite impaire

Proposition (Conjugaison dans S_n).

Soit $\sigma, \tau \in S_n$

On pose $\sigma = (a_{11}a_{12}...a_{1k_1})...(a_{m1}a_{m2}...a_{mk_m})$ la décomposition de σ en produit de cycles à supports disjoints

$\tau\sigma\tau^{-1} = (\tau(a_{11})...\tau(a_{1k_1}))...(\tau(a_{m1})...\tau(a_{mk_m}))$

Definition.

Soit $\sigma \in S_n$

On note n_1, \dots, n_r la suite croissante des longueurs des cycles apparaissant dans la décomposition de σ en produit de cycles à supports disjoints

Une partition de $[1, n]$ est une suite $1 \leq n_1 \leq n_r \leq n$ avec $n = \sum_{i=1}^r n_i$

Proposition.

Deux permutation sont conjugués dans S_n si et seulement si elles ont le même type

Le nombre de classes de conjugaisons dans S_n est le nombre de partitions de $[1, n]$

2.3 Groupe diédral

Le groupe diédral $D_{2n}, n \geq 3$ est le groupe de symétrie du n-gone régulier

$$D_{2n} \leq S_n$$

On définit sur $[1, n]$ la relation binaire R_n défini par : $iR_n j$ ssi $|j - i| = 1$ ou $i=1$ et $j=n$ ou $i=n$ et $j=1$

Definition.

$$D_{2n} = \{\sigma \in S_n / \forall i, j \in [1, n], iR_n j \Leftrightarrow \sigma(i)R_n \sigma(j)\}$$

$r = (1 \ 2 \ \dots \ n)$ est la rotation d'angle $\frac{2\pi}{n}$ s est la réflexion par rapport à la droite qui passe par 1

$$s = \begin{cases} (2n)(3n-1)\dots(\frac{n}{2}\frac{n}{2}+1) & \text{si } n \text{ est pair} \\ (2n)(3n-1)\dots(\frac{n+1}{2}\frac{n+3}{2}) & \text{si } n \text{ est impair} \end{cases} \quad \text{ord}(r)=n \text{ et } \text{ord}(s)=2 \quad |D_{2n}| = 2n \quad D_{2n} = \{e, r, r^2, \dots, r^{n-1}, s, rs, \dots\}$$

2.4 Groupe alternée

Le groupe alterné est le groupe des permutations paires, on le note A_n , on a donc $A_n = \text{Ker}(\epsilon)$

$$A_n \triangleleft S_n$$

$$\text{card}(A_n) = \frac{n!}{2}$$

A_n est engendré par les 3-cycles

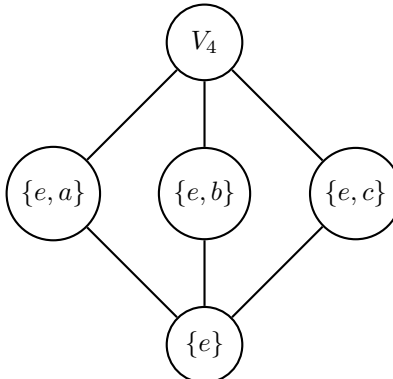
A_n est simple pour $n \geq 5$

3 Exemples de groupes de petits cardinal**3.1 Groupe de Klein**

C'est un groupe de cardinal 4 caractérisé par le fait que les trois éléments différents du neutre sont d'ordre deux et le produit de deux de ces éléments distincts donne le troisième. On le note V_4 . C'est un groupe abélien et le plus petit groupe non cyclique.

Table de multiplication du groupe de Klein V_4

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

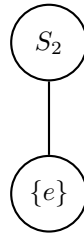


3.2 $S_n, n \in \{2, 3, 4\}$

3.2.1 S_2

Groupe commutatif

$$S_2 = \{e, (12)\}$$

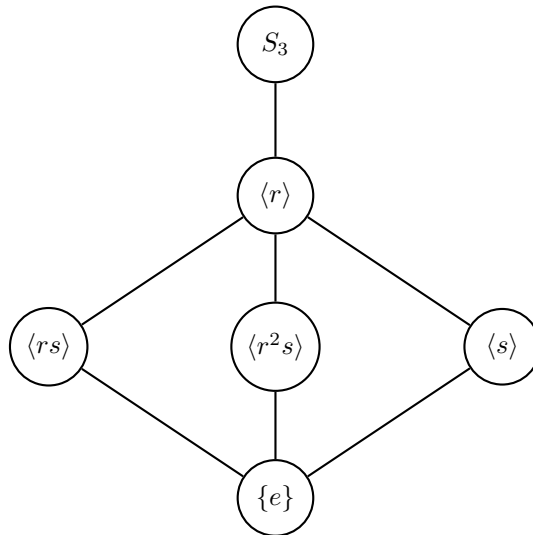


3.2.2 S_3

Plus petit groupe non abélien

$$S_3 = \{e, (123), (132), (12), (13), (23)\}$$

$S_3 = D_6$, groupe de symétrie du triangle équilatéral



3.2.3 S_4

3.3 $D_{2n}, n \in \{3, 4\}$

3.3.1 D_6

$$D_6 = S_3$$

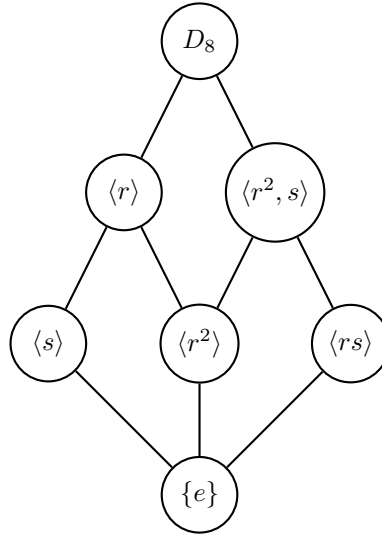
3.3.2 D_8

Groupe de symétrie du carré

On montre avec un contre-exemple dans ce groupe que $K \triangleleft H \triangleleft G$ n'implique pas nécessairement $K \triangleleft G$:

$$\{e, (13)(24)\} \triangleleft \{e, (13), (24), (13)(24)\} \triangleleft D_8 \text{ mais } \{e, (13)(24)\} \not\triangleleft D_8$$

Remarque : $\{e, (13), (24), (13)(24)\}$ est le groupe de Klein



3.4 Q_8

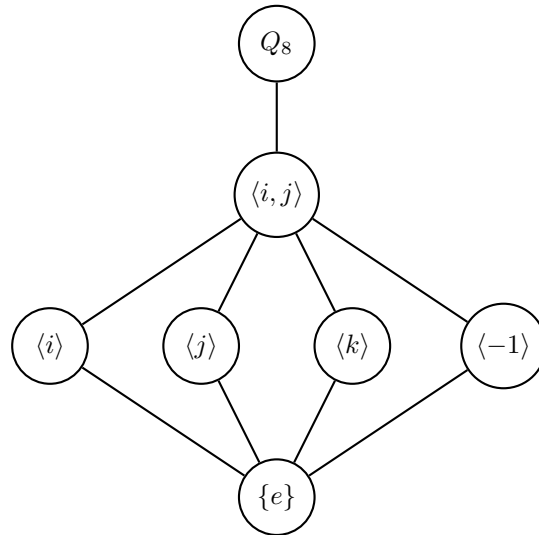
Sous-groupe de $GL_2(\mathbf{C})$

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

En notant 1 la matrice identité :

$$\langle I, J \rangle = \{\pm 1, \pm I, \pm J, \pm K\}$$

Plus petit groupe dont tous les sous-groupes sont distingués



4 Liste des groupes de cardinal 1 à 26

$ G $	#	liste des groupes à isomorphisme près
4	2	$C_4, D_2 \cong C_2 \times C_2$
6	2	$C_6, D_3 \cong \mathfrak{S}_3 \cong C_3 \rtimes C_2$
8	5	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, Q_8, D_4 \cong C_4 \rtimes C_2$
9	2	$C_9, C_3 \times C_3$
10	2	$C_{10}, D_5 \cong C_5 \rtimes C_2$
12	5	$C_{12}, C_2 \times C_6, D_6 \cong C_6 \rtimes C_2 \cong C_2 \times \mathfrak{S}_3,$ $\mathfrak{A}_4 \cong (C_2 \times C_2) \rtimes C_3, C_3 \rtimes C_4$
14	2	$C_{14}, D_7 \cong C_7 \rtimes C_2$
15	1	C_{15}
16	14	...
18	5	$C_{18}, C_3 \times C_6, D_9, C_3 \times \mathfrak{S}_3, (C_3 \times C_3) \rtimes C_2$
20	5	$C_{20}, C_2 \times C_{10}, C_5 \rtimes_{\varphi_1} C_4, C_5 \rtimes_{\varphi_2} C_4,$ $D_{10} \cong C_{10} \rtimes C_2 \cong C_5 \rtimes (C_2 \times C_2)$
21	2	$C_{21}, C_7 \rtimes C_3$
22	2	$C_{22}, D_{11} \cong C_{11} \rtimes C_2$
24	15
25	2	$C_{25}, C_5 \times C_5$
26	2	$C_{26}, D_{13} \cong C_{13} \rtimes C_2$

Figure 1: Enter Caption