

Groupes d'automorphismes de structures algébriques

Exercice : G est un groupe fini, de cardinal noté $|G|$. $|G|$ est donc appelé ordre de G . X est un ensemble, $n \in \mathbb{N}^*$ (avec indication contraire) On note Eq le corps $\mathbb{C}$ et q éléments, ou q est une puissance d'un nombre premier.

I. Cubes pour l'étude des groupes

1. Ordre d'un élément

Def 1 : Soit $g \in G$, on définit l'ordre de g , noté $o(g)$, par

$$o(g) = \min \{n \in \mathbb{N}^* : g^n = 1\}$$

Ex 1 : Dans $\mathbb{Z}/3\mathbb{Z}$, $o(1) = 2$

Ex 2 : Le sous-groupe engendré par g , noté $\langle g \rangle$, est un sous-groupe de G , et

$$o(g) = |\langle g \rangle|. \quad G \text{ étant fini, on a toujours } o(g) \leq |G|$$

Th 1 : Si $\sigma : G \rightarrow G$ est un isomorphisme, alors $\forall g \in G, o(g) = o(\sigma(g))$

Prop 1 : Si $g \in G, \varphi : \mathbb{Z} \rightarrow G, \text{ avec } \ker(\varphi) = o(g)\mathbb{Z},$
 $n \mapsto g^n \quad \langle g \rangle \cong \text{Im}(\varphi)$

Th 2 : (Théorème de Lagrange)

Soit $H \leq G$ un sous-groupe. Alors $|H| \mid |G|$. On pose $[G:H] = \frac{|G|}{|H|}$

Ex 3 : Si $g \in G, H = \langle g \rangle$, on a $[G:H] \mid |G|$

Ex 4 : $G = \langle i \rangle = \{1, -1, i, -i\}, H = \{1, -1\} \leq G,$
 $o(i) = 4 \mid 4 = |G|$

Cor 1 : Si $\exists g \in G, o(g) = n$, alors G est cyclique : $G = \langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$

Th 3 : Soit $g \in G, n \in \mathbb{Z}^*$

$$1) \quad o(g^n) = \frac{o(g)}{\text{pgcd}(o(g), n)}, \quad 2) \quad o(g^{-1}) = o(g)$$

Ex 5 : Si $gh = hg$, alors $o(gh) \mid \text{ppcm}(o(g), o(h))$
 Si $o(g) \mid o(h) = n$, alors $\langle g \rangle \cap \langle h \rangle = \{1\}$ et $o(gh) = o(g)o(h)$

Prop 1 : Soit $\langle gh \rangle$, l'hypothèse $gh = hg$ est impotente.

Ex 6 : Soit G_3 , si $\sigma = (12)$ et $\tau = (123)$, alors $\sigma\tau = (13) \neq (12) = \tau\sigma$
 $o(\sigma) = 2, o(\tau) = 3$ mais $o(\sigma\tau) \neq o(\sigma)o(\tau) = 6$ car dans S_3 aucun élément d'ordre 6.

2. Actions de groupes

Def 1 : On dit que G agit sur X (à gauche) si on note $G \times X \rightarrow X$ et satisfait à ce qui suit :

- 1) $\forall x \in X, 1_G \cdot x = x \quad \text{et} \quad (g \cdot h) \cdot x = g \cdot (h \cdot x)$
- 2) $\forall g \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x$

Ex 7 : (Action par conjugaison)

G agit sur G par conjugaison via $g \cdot x = gxg^{-1}$, et on a G en action libre et transitive. $\text{Im}(\sigma)$ est le groupe des automorphismes internes de G .

Def 2 : (Orbite)

Soit $x \in X$, on définit l'orbite de x sous l'action de G , notée O_x , par : $O_x = \{g \cdot x, g \in G\}$

Ex 8 : Pour l'action par conjugaison, les orbites sont appelées classes de conjugaison, on les note $C_g(G)$

Def 3 : (Stabilisateur)

On dit qu'une action $G \times X$ est libre si $\forall x \in X, x \neq 1_G \cdot x$ et qu'une action est transitive si $\forall x, y \in X, \exists g \in G, x = g \cdot y$

Prop 1 : $G \times X$ est libre si et seulement si $\forall x \in X, \text{Stab}_G(x) = \{1_G\}$

Ex 9 : S_n agit transitivement sur $\{1, \dots, n\}$

Th 4 : A une action $G \times X$ correspond la donnée d'un morphisme

$$\gamma : G \rightarrow S_X = \{ \text{bijections de } X \}$$

Def 4 : (Action fidèle)

On dit que l'action $G \times X$ est fidèle si γ est injectif

Ex 10 : (Transitive à gauche)

$$G \rightarrow G \quad \text{est fidèle} \\ h \mapsto gh$$

Def 5 : (Stabilisateur)

Soit $x \in X$. On définit le stabilisateur de x par $\text{Stab}_G(x) = \{g \in G : g \cdot x = x\}$

Prop 2 : Soit $x \in X, \text{Stab}_G(x) \leq G$ (c'est un sous-groupe)

Ex 11 : S_n agit transitivement sur $\{1, \dots, n\}$ et $\text{Stab}_1(S_n) \cong S_{n-1}$

Prop 3 : Soit $x \in X, |O_x| = [G : \text{Stab}_G(x)]$

Th 5 : (Equation aux cosets)

$$\text{Soit } O_{x_1}, \dots, O_{x_r} \text{ les orbites de } G \times X \text{ pour } |X| = \sum_{i=1}^r |O_{x_i}|$$

Th 6 : (Formule de Burnside)

$$\text{Le nombre d'orbites est } \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|, \quad \text{Fix}(g) = \{x \in X : g \cdot x = x\}$$

Ex 12 : On peut se rendre d'un coin en rouge et en vert. Il y a 3 manières différentes de colorier les arêtes du cube.

Th. 20. (Théorème de Cauchy)

Soit p un nombre premier tel que $p \mid |G|$. Alors $\exists g \in G, g^p = 1$.

Prop. 21. Caractéristique du groupe d'ordre S est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^S$.

3 - Sous-groupes remarquables

Def. 22. On dit qu'un sous-groupe H de G est normal ou distingué si :

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H$$

Ex. 23. $\langle \mathbb{Z}/2\mathbb{Z} \rangle, G \trianglelefteq G$

Prop. 24. Si $H \leq G$ et $[G:H] = 2$, alors $H \trianglelefteq G$.

Def. 25. (Centre)

On définit le centre de G par : $Z(G) = \{h \in G : \forall g \in G, gh = hg\}$, on dit que G est abélien si $Z(G) = G$.

Ex. 26. $Z(G) \trianglelefteq G$

Prop. 27. Tout groupe d'ordre p^2 , où p premier, est abélien.

Def. 28. (Commutateur de groupe d'ordre)

Soient $x, y \in G$, on définit la commutateur de x et y par $[x, y] = xyx^{-1}y^{-1}$.

On définit le groupe d'ordre de G par $D(G) = \langle [x, y], x, y \in G \rangle$.

Prop. 29. G est abélien $\iff D(G) = \{1\}$.

Ex. 30. $D(S_3) = A_3$

Th. 31. Si $H \trianglelefteq G$, alors le quotient G/H est muni d'une structure de groupe, dans le cas où $(gh)(h^{-1}g^{-1}) = (gh)H$, et si G/H est un groupe, alors $H \trianglelefteq G$.

$$\text{Ex. 32. } \frac{S_3}{A_3} \cong \mathbb{Z}/2\mathbb{Z}$$

Prop. 33. $\frac{G}{N}$ est abélien si $D(G) \subset N$, en particulier $\frac{G}{D(G)}$ est abélien, c'est l'abélianisé de G .

II - Groupes abéliens finis

1 - Groupes cycliques

Def. 34. On dit que G est cyclique si $G = \langle g \rangle$ ($g \in G$), G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où n est un générateur de G .

Ex. 35. $(\mathbb{Z}/n\mathbb{Z}, +) = \langle 1 \rangle$, c'est un groupe cyclique.

Prop. 36. Si G est cyclique d'ordre n et $G \cong \mathbb{Z}/n\mathbb{Z}$ via l'isomorphisme

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \xrightarrow{\varphi} G, \text{ où } \varphi \text{ est un générateur de } G$$

Prop. 37. Le nombre de générateurs de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est donné par $\varphi(n)$ (fonction d'Euler) où $\varphi(n) = \#\{k \in \mathbb{Z}/n\mathbb{Z} : \gcd(k, n) = 1\}$.

Ex. 38. $\varphi(6) = |\{1, 5\}| = 2$, il y a deux générateurs de $\frac{\mathbb{Z}}{6\mathbb{Z}}$, 1 et 5 .

Prop. 39. Deux groupes cycliques d'ordre n sont isomorphes si et seulement si n est le même nombre.

Prop. 40. $\text{Aut}(\frac{\mathbb{Z}}{n\mathbb{Z}}) \cong \varphi(n)$, $\text{Aut}(\frac{\mathbb{Z}}{n\mathbb{Z}}) = \{x \mapsto ax, \gcd(a, n) = 1\}$.

Prop. 41. Si p est premier, et si $|G| = p$, alors $G \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$, G est simple.

Prop. 42. Les sous-groupes de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont de la forme $\frac{\mathbb{Z}}{d\mathbb{Z}}$, où $d \mid n$.

Th. 32. (Lemme chinois)

Si $m, n \in \mathbb{N}^*$, $\gcd(m, n) = 1$, on a alors une isomorphisme : $\frac{\mathbb{Z}}{(mn)\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$.

Ex. 39. (Le système de congruences)

Le système de congruences $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{2} \end{cases}$ admet pour solution $\begin{cases} x \equiv 3 \pmod{10} \end{cases}$, $x \in \mathbb{Z}$.

2 - Caractérisation des groupes abéliens finis

Th. 33. (Théorème de structure des groupes abéliens finis)

Si G est un groupe abélien fini, alors $\exists q_1, \dots, q_r \in \mathbb{N}^*$. Via Th. 32, $G \cong \frac{\mathbb{Z}}{q_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{q_r\mathbb{Z}}$, où $q_1 \dots q_r = |G|$.

Ex. 36. Si $|G| = 36 = 2^2 \cdot 3^2$, 6 éléments, alors $G \cong \frac{\mathbb{Z}}{36\mathbb{Z}}$, $G \cong \frac{\mathbb{Z}}{12\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$, $G \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{18\mathbb{Z}}$ ou $G \cong (\frac{\mathbb{Z}}{2\mathbb{Z}})^2 \times \frac{\mathbb{Z}}{9\mathbb{Z}}$.

III - Exemples de groupes non abéliens finis

1 - Le groupe symétrique d'ordre n

Def. 37. $S_n = \{\text{permutations de } \{1, \dots, n\}\} = \{\text{permutations de } [n]\mathbb{Z}\}$, où $n \in \mathbb{N}$, $\sigma = (1 \dots n)$ est un cycle si $\sigma(1) = 2, \sigma(2) = 3, \dots, \sigma(n-1) = n, \sigma(n) = 1$, on note $\sigma = (1 \dots n)$.

Prop. 38. $(S_n, \circ)$ est un groupe d'ordre $n!$.

Ex. 39. Prenons S_3 , $\sigma = (1 \ 2 \ 3)$, $\tau = (1 \ 2)$, $\sigma \circ \tau = (1 \ 3 \ 2)$.

Th. 34. (Engendrement) de S_n

(i) $S_n = \langle (1 \ 2), (1 \ 2 \ 3), \dots, (1 \ 2 \dots n) \rangle$ (ii) $S_n = \langle (1 \ 2), (1 \ 2 \dots n) \rangle$

(iii) $S_n = \langle (1 \ 2), (1 \ 2 \dots n-1) \rangle$ (iv) $S_n = \langle (1 \ 2), (1 \ 2 \dots n) \rangle$

Def. 41. (Support) Soit $\sigma \in S_n$, $\text{Supp}(\sigma) = \{i \in [n] : \sigma(i) \neq i\}$.

Ex. 42. Si $(1 \ 2 \ 3) \in S_3$, alors $\text{Supp}((1 \ 2 \ 3)) = \{1, 2, 3\}$.

Prop. 43. Si $\sigma, \tau \in S_n$, $\text{Supp}(\sigma) \cap \text{Supp}(\tau) = \emptyset$, alors $\sigma \circ \tau = \tau \circ \sigma$.

Ex. 44. Toute permutation de décomposition en cycles à support disjoint.

Def 61: (signature) $E: S_n \rightarrow \{-1, 1\}$

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

Prop 62: $E: S_n \rightarrow \{-1, 1\}$ est morphisme de groupe

Def 63: (Groupe alterné) $A_n = \{\sigma \in S_n, E(\sigma) = 1\} \subset \text{Ker}(E)$

Prop 64: Si $n \geq 3$, $A_n = \langle 3\text{-cycles} \rangle = \langle (1, 2, 3), (1, 2, 4), \dots, (1, 2, n) \rangle$

Lemma 65: Le nombre de permutations à support dans n -cycle de longueur n , est $(n-1)!$

(Ex: $(1, 2, \dots, n)$ est égal à $\frac{n!}{n}$)

Th 90: $\forall n \geq 5$, A_n est simple

DIPT 1

Cor 91: $\forall n \geq 5$, $D(S_n) = A_n$, $D(A_n) = A_n$

Ex 72: $D(A_4) = \{id, (1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4)\} \cong V_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$

2- Quelques groupes de matrices sur les corps finis

Def 73: $GL_n(F_q) = \{M \in M_n(F_q) \mid \exists N \in M_n(F_q), MN = NM = I_n\}$ (Groupe linéaire)

$SL_n(F_q) = \{M \in GL_n(F_q) \mid \det(M) = 1\}$ (Groupe spécial linéaire)

Def 74: $M \in GL_n(F_q)$ est une matrice si $IPSG_n(F_q) = PGL_n(F_q)$

et est une dérivée $\Rightarrow IPSG_n(F_q) = PSL_n(F_q)$

Th 93: La matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ engendre $GL_2(F_q)$

Ex 75: Les transformations de dérivations engendrent $GL_n(F_q)$

Th 94: $S(n, q) \neq \{2, 2\}$, $D(GL_n(F_q)) = SL_n(F_q)$ et $S(n, q) \neq \{4, 4\}$, $D(SL_n(F_q)) = SL_n(F_q)$

Prop 95: $|GL_n(F_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$

Def 76: $IPSG_n(F_q) = \frac{GL_n(F_q)}{\langle \lambda I_n, \lambda \in F_q^* \rangle}$ (Groupe projectif linéaire)

(a) $IPSG_n(F_q) = \frac{SL_n(F_q)}{\langle \lambda I_n, \lambda \in F_q^* \rangle}$ (Groupe projectif spécial linéaire)

Th 96: $S(n, q) \neq \{2, 2\}, \{4, 4\}$, $IPSG_n(F_q)$ est simple

Prop 97: (Tous morphismes acceptables)

(i) $IPSG_2(F_2) \cong S_3$, (ii) $IPSG_2(F_3) \cong S_4$, (iii) $IPSG_2(F_4) \cong A_5$

3- Groupe d'homotopie possédant une figure

Def 82: Soit $A \subset \mathbb{R}^n$ une partie finie. On pose

$Isot(A) = \{g = f \circ a, f \in O_n(\mathbb{R}), a \in \mathbb{R}^n, g(A) = A\}$ (Groupe d'homotopie affine de A)

$Isot^+(A) = \{g = f \circ a, f \in SO_n(\mathbb{R}), a \in \mathbb{R}^n, g(A) = A\}$ (Groupe d'homotopie affine positive de A)

Ex 83: Si T est un triangle quelconque, alors $Isot(T) \cong \mathbb{Z}/2\mathbb{Z}$, et $Isot^+(T) \cong \mathbb{Z}/2\mathbb{Z}$

Prop 84: Soit $P_n \subset \mathbb{R}^2$ le polygone régulier à n côtés. On a alors

$Isot(P_n) = D_n = \langle \sigma, \tau : \sigma^n = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$ (Groupe diédral), et $Isot^+(P_n) = \frac{\mathbb{Z}}{n\mathbb{Z}}$

Ex 85: P_3 correspond au triangle équilatéral, et $Isot(P_3) = S_3$

$Isot^+(P_3) = A_3 \cong \frac{\mathbb{Z}}{3\mathbb{Z}}$

Prop 86: Soit A une partie finie de $\mathbb{R}^3$ qui admette une norme de symétrie. Soit n

est un morphisme. $Isot(A) \cong Isot(A) \times \frac{\mathbb{Z}}{2\mathbb{Z}}$

$$g \mapsto \begin{pmatrix} g & 1 \\ 0 & 1 \end{pmatrix} : g \in Isot(A) \quad \text{et} \quad \tau \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : \tau \in Isot(A)$$

Th 97: (Groupe d'homotopie du tétraèdre et du cube)

Soit $A_4 \subset \mathbb{R}^3$ le tétraèdre régulier et soit $C_6 \subset \mathbb{R}^3$ le cube. On a alors

(i) $Isot(A_4) = S_4$ et $Isot^+(A_4) = A_4$

DIPT 2

(ii) $Isot(C_6) = \mathbb{Z} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ et $Isot^+(C_6) = \mathbb{Z}$ (cf. Ex 2)

4- Représentations de groupe

Def 87: V est un $\mathbb{C}$ -espace vectoriel de dimension finie

Def 88: Une représentation linéaire de G est la donnée d'un $\mathbb{C}$ -espace vectoriel V et d'un morphisme $\rho: G \rightarrow GL(V)$. On appelle degré de ρ la dimension de V . Une sous-représentation est la donnée de $\rho(g) \in W \subset V$, sous-espace

invariant, $\forall g \in G$. ρ est dite irréductible si on a toujours $W = \{0\}$ ou V

Def 89: Soit $\rho: G \rightarrow GL(V)$ une représentation linéaire. Le caractère de ρ est la fonction $\chi_\rho: G \rightarrow \mathbb{C}$

$g \mapsto \text{Tr}[\rho(g)]$. χ_ρ est dite irréductible si ρ est irréductible

$g \mapsto \text{Tr}[\rho(g)]$. χ_ρ est dite irréductible si ρ est irréductible

$g \mapsto \text{Tr}[\rho(g)]$. χ_ρ est dite irréductible si ρ est irréductible

$g \mapsto \text{Tr}[\rho(g)]$. χ_ρ est dite irréductible si ρ est irréductible

$g \mapsto \text{Tr}[\rho(g)]$. χ_ρ est dite irréductible si ρ est irréductible

Ex 90: χ_ρ est invariante sous la classe de conjugaison de G

Th 98: Soit $\text{Irr}(G)$ l'ensemble des caractères irréductibles de G :

$$(i) \sum_{\chi \in \text{Irr}(G)} \chi^2 = |G| \quad (ii) \forall g \neq 1_G, \sum_{\chi \in \text{Irr}(G)} \chi(g) \chi(1) = 0$$

$$(iii) \exists \chi, \chi' \in \text{Irr}(G), \langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi'(g)} = \begin{cases} 1 & \text{si } \chi = \chi' \\ 0 & \text{sinon} \end{cases}$$

Prop 92: Table de caractères de S_3

(cf. Fig 3)

Prop 93: $\{g \in G : \chi(g) = \chi(1)\}$ est un sous-groupe normal de G , où $\chi \in \text{Irr}(G)$

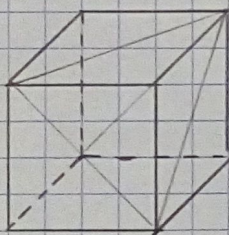
Prop 94: Soit la table de caractères de S_3 , on vérifie bien que les

sous-groupes distingués sont $\{1, 2\}$, A_3 et V_4

Annexe :

$ G $	6	$ G $	6	$ G $	6
1	$\{1\}$	4	$\frac{\mathbb{Z}}{4\mathbb{Z}}, V_4$	7	$\frac{\mathbb{Z}}{7\mathbb{Z}}$
2	$\frac{\mathbb{Z}}{2\mathbb{Z}}$	5	$\frac{\mathbb{Z}}{5\mathbb{Z}}$		
3	$\frac{\mathbb{Z}}{3\mathbb{Z}}$	6	$\frac{\mathbb{Z}}{6\mathbb{Z}}, S_3$		

(Classification des groupes d'ordre ≤ 6) (Fig 1)
isomorphisme près



$= C_6$
 $= \Delta_6$

Le cube et le tétraèdre (Fig 2)

$ G $	1	6	6	3	6
χ	Id	(...)	(...)	(...)(...)	(...)
Id	1	1	1	1	1
E	1	-1	-1	-1	-1
Isos(Qu)	3	1	0	-1	-1
$\in$ Isos(Qu)	3	-1	0	-1	-1
δ	2	0	-1	2	0

Table de caractères de S_4 (Fig 3)

Références :

F. Ulmer, Théorie des groupes

D. Perrin, Cours d'algèbre

P. Collet, J. Benmoun, Nouveaux thèmes heuristiques de groupes et de géométrie

Tome second.