Conjugaison dans un groupe. Exemples, sous-groupes normaux et groupes quotient

103

Soit G groupe de neutre 1, E un ensemble et $n \in \mathbb{N}^*$.

I] Notion de conjugaison

1] Action par conjugaison

Définition 1 : On dit que G agit à gauche sur E s'il existe un morphisme de groupes $\varphi : G \to \mathfrak{S}(E)$, $g \mapsto [x \mapsto g.x]$.

Si $E = G$ et $g.x = gxg^{-1}$, alors on dit que G agit sur lui-même par conjugaison et le morphisme φ est noté Int.

On note $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G et $Z(G) := \ker(\mathrm{Int})$.

Remarque 2 : L'action par conjugaison devient triviale dès que G est abélien. Il s'agit d'un outil pour décrire les groupes non-abéliens.

Exemple 3 : (1) $GL_n(\mathbb{R})$ agit par conjugaison sur $\mathcal{M}_n(\mathbb{R})$.
(2) G agit sur tout sous-groupe distingué H par conjugaison.

2] Classes de conjugaison, stabilisateurs et équation aux classes

Définition 4 : Soit G opérant sur lui-même par conjugaison et soit $x \in G$. L'orbite de x : $\mathrm{Orb}(x) = \{g.x \mid g \in G\}$ est appelée classe de conjugaison de x. Deux éléments de G sont conjugués s'ils appartiennent à la même classe de conjugaison.

Exemples 5 : (1) Les renversements sont conjugués dans $SO_3(\mathbb{R})$
(2) Les cycles d'ordre $p \in [\![1; n]\!]$ sont conjugués dans S_n.
(3) Les transvections sont conjuguées dans $GL(E)$.

Définition 6 : Soit G opérant sur lui-même par conjugaison et soit $x \in G$. Le stabilisateur de x est : $\mathrm{Stab}(x) = \{g \in G \mid gxg^{-1} = x\}$.

Théorème 7 : Soit G opérant sur E, $x \in E$ et $\varphi_x : G/\mathrm{Stab}(x) \to \mathrm{Orb}(x)$, $g\,\mathrm{Stab}(x) \mapsto g.x$.
Alors : φ_x est bien définie et bijective.
De plus, si G est fini, $|\mathrm{Orb}(x)| = \dfrac{|G|}{|\mathrm{Stab}(x)|}$

Théorème 8 : (équation aux classes) Soit G agissant sur E.
Alors : $|E| = \sum_{i=1}^{r} |\mathrm{Orb}(x_i)| = \sum_{i=1}^{r} \dfrac{|G|}{|\mathrm{Stab}(x_i)|}$ avec $\mathrm{Orb}(x_1), \dots, \mathrm{Orb}(x_r)$ toutes les orbites deux à deux distinctes de E.

3] p-groupes et leur structure

Définition 9 : Soit p premier. On appelle p-groupe tout groupe de cardinal p^α avec $\alpha \in \mathbb{N}^*$.

Proposition 10 : Soit p premier et G un p-groupe agissant sur E.
Alors : $|E^G| \equiv |E| \bmod(p)$ avec $E^G = \{x \in E \mid \mathrm{Orb}(x) = \{x\}\}$.

Remarque 11 : Si $E = G$, et G agit sur G, alors $E^G = Z(G)$ et on a alors $|Z(G)| = |G| \bmod(p)$.

Application 12 : Soit p premier et G un p-groupe.
Alors $Z(G) \neq \{1\}$

Application 13 : Tout groupe d'ordre p^2, avec p premier, est abélien.

Remarque 14 : (1) Si G d'ordre p^2 a un élément d'ordre p^2, alors : G est cyclique isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.
(2) Si tous ses éléments sont d'ordre p, alors G isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.

II] Ensemble quotient et structure de groupe

1] Notion de sous-groupe normal

Définition 15 : Soit H un sous-groupe ~~normal~~ de G ($H < G$). On dit que H est normal si pour tout $h \in H$, tout $g \in G$, $ghg^{-1} \in H$.
On note $H \lhd G$.

Remarque 16 : Ceci revient à dire que H est stable par tout automorphisme intérieur (i.e. pour tout $g \in G$, $\mathrm{Int}(g)(H) \subset H$).

Exemples 17 : (1) $\{1\}$ et G sont toujours distingués dans G.
(2) Soit $H_1 \lhd G$ et $H_2 < G$. Alors $H_1 \cap H_2 \lhd G$.
(3) Soit G groupe abélien. Alors tous ses sous-groupes sont normaux.

Contrexemple 18 : La réciproque n'est pas vraie en général. $\mathbb{H}$ a tous ses sous-groupes normaux mais $\mathbb{H}$ non-abélien.

Proposition 19 : Soit G, G' deux groupes et $\varphi : G \to G'$ morphisme.
Alors : $\ker(\varphi)$ est un sous-groupe normal de G.

[Rom] I.6
[Rom] I.6
[Rom] I.6
[Rom] I.1
[Rom]

Exemples 20 : (1) Pour tout $n \in \mathbb{N}^*$, $A_n = \ker(\varepsilon) \triangleleft S_n$.
(2) $SL(E) \triangleleft GL(E)$.

2] Groupe quotient

Théorème 21 : Soit H sous-groupe de G.
Alors $H \triangleleft G$ ssi il existe une unique structure de groupe sur l'ensemble quotient G/H telle que $\pi_H : G \to G/H$ soit un morphisme de groupes.

Proposition 22 : Soit H sous-groupe normal de G.
Alors : Les sous-groupes de G/H sont de la forme K/H avec K un sous-groupe de G qui contient H.

Exemple 23 : Les sous-groupes de $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$ sont les μ_d avec $d \mid n$.

Application 24 : Pour tout $n \geq 2$, $n = \sum_{d \mid n}^{} \varphi(d)$ avec $\varphi(d) = |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ord}(x) = d\}|$

Théorème 25 : (1er théorème d'isomorphisme) Soit G, G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes.
Alors : il existe un isomorphisme $\tilde{\varphi} : G/\ker(\varphi) \xrightarrow{\sim} \mathrm{Im}(\varphi)$

Application 26 : Un groupe cyclique G d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 27 : (1) $\mathrm{Int}(G) \simeq G/Z(G)$
(2) Pour tout $n \in \mathbb{N}^*$, $GL_n(\mathbb{C})/SL(\mathbb{C}) \simeq \mathbb{C}^*$.

Théorème 28 : (2ème théorème d'isomorphisme) Soit K, H deux sous-groupes de G tels que $K \subset N_G(H) := \{g \in G \mid gHg^{-1} = H\}$
Alors : $KH = HK$ est un sous-groupe de G, H est normal dans KH, $K \cap H$ est normal dans K et $KH/H \simeq K/K \cap H$

Exemple 29 : $S_4/V_4 \simeq S_3$

Théorème 30 : (3ème théorème d'isomorphisme) Soit $K \subset H \subset G$ groupes tels que $H \triangleleft G$ et $K \triangleleft G$
Alors : $\frac{G/K}{H/K} \simeq G/H$

Exemple 31 : $\frac{\mathbb{Z}/10\mathbb{Z}}{2\mathbb{Z}/10\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z}$

III] Simplicité et théorèmes de Sylow

1] Groupes simples

Définition 32 : Un groupe $G \neq \{1\}$ est dit simple si ses seuls sous-groupes normaux sont $\{1\}$ et G.

Exemple 33 : (1) $\mathbb{Z}/p\mathbb{Z}$ est simple ssi p est premier
(2) Pour $n \geq 5$, A_n est simple.

Contexemple 34 : A_4 n'est pas simple car $V_4 \triangleleft A_4$

Exemple 35 : (admis) Parmi les groupes simples non-cycliques, il y a les A_n pour $n \geq 5$ et les $PSL_n(\mathbb{F}_q)$ pour $n \geq 2$ et $q \geq 4$.

2] Théorèmes de Sylow

Définition 36 : Soit G groupe de cardinal $n = p^\alpha m$ avec p premier, $p \nmid m$. On appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

Exemple 37 : $P = \{(a_{ij}) \in GL_n(\mathbb{F}_p) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}$ est un p-sous-groupe de Sylow de $GL_n(\mathbb{F}_p)$.

Théorème 38 : (de Sylow) Soit G groupe fini et $p \mid |G|$ avec p premier.
Alors : G contient au moins un p-sous-groupe de Sylow.

Corollaire 39 : Soit G groupe tel que $|G| = p^\alpha m$ avec p premier et $p \nmid m$.
Alors : pour tout $i \leq \alpha$, G contient des sous-groupes d'ordre p^i.

Théorèmes 40 : (de Sylow bis) Soit G groupe de cardinal $|G| = p^\alpha m$.
Alors : (1) Si H est un sous-groupe de G et un p-groupe, alors il existe un p-Sylow S tel que $H \subset S$.
(2) Les p-Sylow sont tous conjugués
(3) $n_p \equiv 1 \bmod(p)$ et $n_p \mid m$ avec n_p le nombre de p-Sylows.

Application 41 : Soit S un p-Sylow de G
Alors : $S \triangleleft G$ ssi S est l'unique p-Sylow de G ssi $n_p = 1$

3] Applications des théorèmes de Sylow

Application 42 : Un groupe d'ordre 63 n'est pas simple.

Propositions 43 : (1) Un groupe d'ordre pq avec p et q premiers n'est pas simple.
(2) Un groupe d'ordre p^2q avec p et q premiers n'est pas simple.

I.1 I.5 [Rom] II III [Ulm] IV I.2 [Per] [Ulm] V.3 I.5 [Per] IX [Ulm]

IV] Sous-groupes normaux remarquables et application à l'action par conjugaison

1) Centre d'un groupe

Définition 44 : On rappelle que le centre de G est :

$$Z(G) := \ker(\mathrm{Int}) = \{g \in G \mid \forall h \in G,\ gh = hg\}$$

Proposition 45 : $Z(G) \lhd G$ et $\mathrm{Int}(G) \simeq \frac{G}{Z(G)}$

Exemple 46 : (1) Si G est abélien, alors $Z(G) = G$

(2) $\forall n \geq 3,\ Z(S_n) = \{1\}$

(3) $Z(\mathbb{H}_8) = \{-1; 1\}$ avec $\mathbb{H}_8$ les quaternions

(4) $Z(\mathbb{H}) = \mathbb{R}$ avec $\mathbb{H}$ l'algèbre des quaternions

Théorème 47 : (de Dixon) Soit G groupe non-abélien fini.

Alors : la probabilité $p(G)$ pour que deux éléments de G (tirés au hasard uniformément, indépendamment) commutent vérifie : $p(G) \leq \frac{5}{8}$

Application 48 : Soit $\mathbb{D}_8$ le groupe diédral à 8 éléments

Alors : $p(\mathbb{D}_8) = \frac{5}{8}$

2) Groupe dérivé d'un groupe

Définition 49 : Le groupe dérivé $D(G)$ de G est :

$$D(G) = \{xyx^{-1}y^{-1} \mid x, y \in G\}$$

Proposition 50 : $D(G) \lhd G$

Exemples 51 : (1) Si G est abélien, alors $D(G) = 1$

(2) Si $G = S_3$, alors $D(G) = \{1; \sigma; \sigma^2\}$ avec $\sigma \neq 1$

(3) Si $G = \mathbb{H}_8$, alors : $D(G) = \{-1; 1\}$

(4) Si $G = A_5$, alors $D(G) = A_5$

Proposition 52 : $\frac{G}{D(G)}$ est abélien et c'est le plus grand quotient abélien de G. Ceci caractérise $D(G)$.

3) Application à $SO_3(\mathbb{R})$

Définition 53 : Un corps gauche est un anneau (unitaire, associatif) non-réduit à un élément dans lequel l'ensemble des éléments non-nuls est un groupe pour la multiplication.

Théorème 54 : (de Wedderburn) Tout corps gauche fini est commutatif.

Contrexemple 55 : L'hypothèse de finitude est vitale. L'algèbre des quaternions $\mathbb{H}$ est un corps gauche non-fini et non-commutatif.

Lemme 56 : La sphère unité S^{n-1} de $\mathbb{R}^n$ est connexe par arcs.

En particulier, $Sp(1) = \{q \in \mathbb{H} \mid N(q) = 1\}$ est connexe par arcs.

Théorème 57 : $SO_3(\mathbb{R})$ est engendré par les retournements

Théorème 58 : $SO_3(\mathbb{R})$ est isomorphe à $\frac{Sp(1)}{\{\pm 1\}}$

I.3 [Per] — I.3 [Per] — [Les] — I.3 [Per] — III.4 [Per] — [Isom]

Références :

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi

[Ulm] Théorie des groupes - Ulmer

[Per] Cours d'algèbre - Perrin

[Les] 131 développements pour l'oral - Lesesure

[Isen] L'oral à l'agrégation de mathématiques - Isenmann