103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

On considère G un groupe noté multiplicativement et e son élément neutre.

1. Conjugaison dans un groupe.

1.1. Classes de conjugaison.

Proposition-Définition 1. Le groupe G agit sur lui-même par l'action suivante, appelée **action de conjugaison** :

$$\begin{array}{ccc} G \times G & \to & G \\ (g,h) & \mapsto & ghg^{-1} \end{array}.$$

Définition 2. Les orbites de l'action de conjugaison sont appelées **classes de conjugaison**.
Deux éléments de G sont dits **conjugués** s'ils appartiennent à la même classe de conjugaison.

Proposition 3. Les classes de conjugaison forment une partition de G.

Exemple 4. Dans $\mathcal{S}_n$, les cycles de même longueur sont conjugués.

Définition. On appelle **centre** de G l'ensemble :
$Z(G) := \{g \in G \mid \forall h \in G\ gh = hg\}$.

Proposition 5. L'application $g \mapsto (h \mapsto ghg^{-1})$ est un morphisme de G sur $\mathcal{S}(G)$ et son noyau est $Z(G)$, le centre de G.

Définition 6. On note $\mathrm{Int}(G)$ l'image du morphisme précédent. Ses éléments sont appelés **automorphismes intérieurs** de G.

Proposition 7. Un élément $g \in G$ appartient à $Z(G)$ ssi la classe de conjugaison de g est réduite à un seul élément. Autrement dit, $Z(G)$ est l'union des classes de conjugaison de taille 1 de G.

Exemple 8. Dans un groupe abélien, toutes les classes de conjugaison sont de taille 1, il y a autant de classes de conjugaison que d'éléments dans G et le stabilisateur de tout élément de G par l'action de conjugaison est G.

Proposition 9. G agit sur l'ensemble de ses sous-groupes par l'action définie par $g.H := gHg^{-1}$ pour $g \in G$ et H un sous-groupe de G.

Définition 10. Soit H un sous-groupe de G. L'orbite de H par l'action précédente est appelée **classe de conjugaison** de H. Deux sous-groupes de G sont dits **conjugués** s'ils appartiennent à la même classe de conjugaison.

Exemple 11. Dans $\mathrm{GL}_2(\mathbf{R})$, le sous-groupe engendré par $\begin{pmatrix} 1 & 0 \\ 0 & 1/2 \end{pmatrix}$ et le sous-groupe engendré par $\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$ sont conjugués.

1.2. Sous-groupes distingués.

Définition 12. On dit qu'un sous-groupe H de G est **dinstingué** ou normal (dans G), et l'on note $H \triangleleft G$, si la classe de conjugaison de H est réduite à H, autrement dit si

$$\forall g \in G \quad gHg^{-1} = H.$$

Remarque 13. On peut remplacer l'égalité par une inclusion dans l'un ou l'autre sens.

Exemple 14. Le sous-groupe trivial et G sont distingués dans G.
Le centre d'un groupe est distingué.
Dans un groupe abélien, tout sous-groupe est distingué.

Proposition 15. Le noyau d'un morphisme de groupes est distingué.

Application 16. Soient $n \in \mathbf{N}^*$ et $\mathbf{K}$ un corps. On a :

$$\mathrm{SL}_n(\mathbf{K}) \triangleleft \mathrm{GL}_n(\mathbf{K}), \quad \mathcal{SO}_n(\mathbf{R}) \triangleleft \mathcal{O}_n(\mathbf{R}), \quad \mathcal{SU}_n(\mathbf{C}) \triangleleft \mathcal{U}_n(\mathbf{C}).$$

Définition 17. On dit qu'un groupe est **simple** s'il n'est pas trivial et si ses seuls sous-groupes distingués sont le sous-groupe trivial et lui-même.

Exemple 18. $\mathcal{S}_2$ et $\mathcal{A}_3$ sont simples.
$\mathbf{Z}$ et $\mathrm{GL}_n(\mathbf{K})$ (avec $n \in \mathbf{N}^*$ et $\mathbf{K}$ un corps) ne sont pas simples.
Pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est simple ssi n est premier.

2. Groupes quotients

2.1. Définition et exemples

Définition 19. Soit H un sous-groupe de G. On définit sur G la relation $\sim$ par $x \sim y \iff x^{-1}y \in H$ qui est une relation d'équivalence.
Ses classes d'équivalence sont appelées les **classes à gauche** modulo H :

$$\forall x \in G, \quad \overline{x} := xH = \{xh\,;\, h \in H\}\,.$$

L'ensemble des classes à gauche modulo H, noté G/H, est appelé G **quotienté par** H.

Définition 20. Soit H un sous-groupe de G. L'application $\pi : G \to G/H$ qui à un élément de G lui associe sa classe à gauche modulo H est appelée **projection canonique** sur H.

Remarque 21. On définit de manière analogue les classes à droite modulo H. Ne nombre de classes à gauche est égal au nombre de classes à droite.

Proposition 22. Soit H un sous-groupe de G. On a :

$$H \triangleleft G \iff \forall x \in G, xH = Hx \iff \forall x \in G, xH \subset Hx \iff \forall x \in G, xH \supset Hx$$

Définition 23. S'il est fini, le nombre de classes à gauche modulo H est appelé **indice de** H **dans** G et est noté $[G : H]$.

Exemple 24. Soit $n \in \mathbf{N}^*$. Considérons le groupe $(\mathbf{Z}, +)$ et $n\mathbf{Z}$ l'un de ses sous-groupes. La relation d'équivalence précédente est alors la relation de congruence modulo n et la classe à gauche d'un entier $x \in \mathbf{Z}$ est $x + n\mathbf{Z}$.
On a en outre, $[\mathbf{Z} : n\mathbf{Z}] = |\mathbf{Z}/n\mathbf{Z}| = n$.

Proposition 25. Tout sous-goupe d'indice 2 est distingué.

Théorème 26 : Lagrange. Supposons G fini et soit H un sous-groupe de G. Alors $|G| = [G : H] \times |H|$. En particulier, $|H|$ divise $|G|$.

Application 27. Supposons G fini. Soit $x \in G$, $G.x$ la classe de conjugaison de x dans G et G_x le stabilisateur de x. Alors $|G| = |G.x| \times |G_x|$. En particulier, le cardinal d'une classe de conjugaison divise le cardinal du groupe.

Proposition-Définition 28. Soit $H \triangleleft G$. Alors la loi $(\overline{x}, \overline{y}) \mapsto \overline{xy}$ définit une loi de composition interne sur G/H, de neutre $\overline{e}$ et lui confère une structure de groupe. G/H est alors appelé le **groupe quotient de** G **par** H.
De plus, la projection canonique $\pi : G \to G/H$ est un morphisme de groupes surjectif, de noyau H.

Théorème 29. Soit H un sous-groupe de G. Alors $H \triangleleft G$ ssi il existe une unique structure de groupe sur G/H telle que la projection canonique $\pi : G \to G/H$ soit un morphisme de groupes.

Exemple 30. Soit $n \in \mathbf{N}^*$. Le groupe $\mathbf{Z}/n\mathbf{Z}$ des classes de congruence modulo n est le quotient de $\mathbf{Z}$ par le sous-groupe $n\mathbf{Z}$.

Proposition 31. Soit $H \triangleleft G$. La projection canonique $\pi : G \to G/H$ induit une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de G/H.

2.2. Théorèmes d'isomorphisme

Théorème 32 : Factorisation. Soit $H \triangleleft G$ et $\varphi : G \to G_1$ un morphisme de groupes tel que $H \subset \operatorname{Ker}\varphi$.
Alors il existe un unique morphisme de groupes $\overline{\varphi} : G/H \to G_1$ tel que $\varphi = \overline{\varphi} \circ \pi$, défini pour tout $\overline{x} \in G/H$ par $\overline{\varphi}(\overline{x}) := \varphi(x)$.

Théorème 33 : 1er théorème d'isomorphisme. Soit $\varphi : G \to G_1$ un morphisme de groupes. Alors $G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$.

Exemple 34.

- ⋆ On a $\mathbf{C}^*/\mathbf{U} \simeq \mathbf{R}_+^*$ via $\varphi : z \mapsto |z|$.
- ⋆ On a $\mathbf{R}/2\pi\mathbf{Z} \simeq \mathbf{U}$ via $\varphi : \theta \mapsto \mathrm{e}^{\mathrm{i}\theta}$.
- ⋆ On a $G/Z(G) \simeq \operatorname{Int}(G)$ via le morphisme de la Proposition 4.
- ⋆ Soit $n \in \mathbf{N}^*$ et $\mathbf{K}$ un corps. On a, via le morphisme $M \mapsto \det M$:

$$\mathrm{GL}_n(\mathbf{K})/\mathrm{SL}_n(\mathbf{K}) \simeq \mathbf{K}^*, \quad \mathcal{O}_n(\mathbf{R})/\mathcal{SO}_n(\mathbf{R}) \simeq \mathbf{U}_2, \quad \mathcal{U}_n(\mathbf{C})/\mathcal{SU}_n(\mathbf{C}) \simeq \mathbf{U}.$$

Application 35. Soit $n \in \mathbf{N}^*$ et G un groupe cyclique d'ordre n. Alors $G \simeq \mathbf{Z}/n\mathbf{Z}$.

Corollaire 36. Soit $\varphi : G \to G_1$ un morphisme de groupes. Si G est fini, alors $|G| = |\operatorname{Ker}\varphi| \times |\operatorname{Im}\varphi|$.

Théorème 37 : 2e théorème d'isomorphisme. Considérons H et K des sous-groupes de G tels que $H \triangleleft G$. Alors HK et KH sont des sous-groupes de G. En outre, $H \triangleleft HK$, $H \cap K \triangleleft K$ et $(HK)/H \simeq K/(H \cap K)$.

Exemple 38. On a $12\mathbf{Z} \cap 20\mathbf{Z} = (12 \vee 20)\mathbf{Z} = 60\mathbf{Z}$ et $12\mathbf{Z} + 20\mathbf{Z} = (12 \wedge 20)\mathbf{Z} = 4\mathbf{Z}$. Ainsi, $4\mathbf{Z}/12\mathbf{Z} \simeq 20\mathbf{Z}/60\mathbf{Z}$.

Théorème 39 : 3e théorème d'isomorphisme. Soit H et K des sous-groupes distingués de G tels que $K \subset H$.
Alors $K \triangleleft H$, $H/K \triangleleft G/K$ et $(G/K)/(H/K) \simeq G/H$.

Exemple 40. Comme $10\mathbf{Z} \subset 2\mathbf{Z} \subset \mathbf{Z}$, on a $(\mathbf{Z}/10\mathbf{Z})/(2\mathbf{Z}/10\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z}$.

3. Applications

3.1. p-groupes

Soit p un nombre premier.

Définition 41. On dit que G est un p-groupe s'il existe un entier $\alpha \geq 1$ tel que $|G| = p^\alpha$.

Théorème 42. Un groupe d'ordre p est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

Proposition 43. [DEV 1] Si G est un p-groupe, alors $Z(G) \neq \{e\}$.

Lemme 44. [DEV 1] Si $G/Z(G)$ est monogène, alors G est abélien.

Théorème 45. [DEV 1] Un groupe d'ordre p^2 est abélien et est soit isomorphe à $\mathbf{Z}/p^2\mathbf{Z}$, soit isomorphe à $(\mathbf{Z}/p\mathbf{Z})^2$.

3.2. Groupe symétrique et groupe alterné

Soit $n \in \mathbf{N}^*$.

Proposition 46. Considérons $(a_1 \cdots a_k) \in \mathcal{S}_n$ un k-cycle et $\sigma \in \mathcal{S}_n$. Alors

$$\sigma \circ (a_1 \cdots a_k) \circ \sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k)).$$

Ainsi, la classe de conjugaison d'un cycle dans $\mathcal{S}_n$ est l'ensemble des cycles de même longueur.

Proposition 47. Le centre de $\mathcal{S}_n$ vaut $\mathcal{S}_n$ si $n \leq 2$ et est trivial sinon.

Proposition 48. Deux permutations sont conjuguées dans $\mathcal{S}_n$ ssi les longueurs des cycles apparaissant dans leur décomposition en produit de cycles à supports disjoints sont les mêmes (à l'ordre près).

Corollaire 49. Le nombre de classes de conjugaison de $\mathcal{S}_n$ est égal au nombre de partitions de $[\![1, n]\!]$.

Définition 50. La signature ε est l'unique morphisme de groupes non trivial de $(\mathcal{S}_n, \circ)$ dans $(\{\pm 1\}, \times)$. Son noyau $\mathcal{A}_n$ est appelé groupe alterné.

Proposition 51. La signature est invariante par conjugaison.

Proposition 52. Le groupe alterné $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$, d'indice 2 et son centre vaut $\mathcal{A}_n$ si $n \leq 3$ et est trivial sinon.

Lemme 53. Si $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Théorème 54. Si $n = 3$ ou si $n \geq 5$, alors $\mathcal{A}_n$ est simple.

Remarque 55. $\mathcal{A}_4$ n'est pas simple car le sous-groupe engendré par les produits de 2 transpositions à supports disjoints est distingué dans $\mathcal{A}_4$.

Théorème 56. Si $n \geq 5$, les seuls sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{Id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

Lemme 57. [DEV 2] Soit φ un automorphisme de $\mathcal{S}_n$. Si φ envoie les transpositions sur les transpositions, alors $\varphi \in \mathrm{Int}(\mathcal{S}_n)$.

Théorème 58. [DEV 2] Si $n \neq 6$, les automorphismes de $\mathcal{S}_n$ sont tous intérieurs.

3.3. Matrices semblables

Soit $n \in \mathbf{N}^*$ et $\mathbf{K}$ un corps.

Définition 59. On appelle **action par conjugaison** de $\mathrm{GL}_n(\mathbf{K})$ sur $\mathcal{M}_n(\mathbf{K})$ l'action définie par $P.A := PAP^{-1}$ pour $P \in \mathrm{GL}_n(\mathbf{K})$ et $A \in \mathcal{M}_n(\mathbf{K})$.
Les orbites de cette action sont appelées **classes de similitude**.

Définition 60. On dit que deux matrices de $\mathcal{M}_n(\mathbf{K})$ sont **semblables** si elles appartiennent à la même classe de similitude.

Proposition 61. Deux matrices semblables sont équivalentes. La réciproque est fausse.

Proposition 62. Deux matrices semblables ont même rang, même déterminant, même trace, même polynôme caractéristique et même polynôme minimal. Ces données sont appelées **invariants de similitude**.

Remarque 63. La réciproque est fausse. En général, partager certains invariants de similitude ne suffit pas à assurer la similitude de deux matrices.

Contre-exemple 64. Les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont même déterminant, même trace et même polynôme caractéristique mais ne sont pas semblables.

Définition 65. Une matrice est diagonalisable (resp. trigonalisable) ssi sa classe de similitude contient une matrice diagonale (resp. triangulaire supérieure).