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

Tout groupe G sera noté multiplicativement.

I Principe de conjugaison

[Ulm21]

I.1 Opération d'un groupe par conjugaison

Soit G un groupe.

Prop 1. G opère sur lui-même par l'action : $G\times G \to G$, $(g,h) \mapsto g\cdot h = ghg^{-1}$. On l'appelle action par conjugaison.

Cor 2. Soit $g \in G$. L'application $h \mapsto ghg^{-1}$ est un automorphisme de G, appelé automorphisme intérieur de G. On note $\mathrm{Int}(G) \leq (\mathrm{Aut}(G), \circ)$ le groupe des automorphismes intérieurs de G.

Déf 3. Soit $h \in G$. L'orbite $G\cdot h = \{ghg^{-1} : g \in G\}$ sous l'action de conjugaison de G sur lui-même s'appelle la classe de conjugaison de h. Deux éléments de G qui appartiennent à la même classe de conjugaison sont dits conjugués. Le stabilisateur $\mathrm{Stab}_G(h) = \{g \in G : ghg^{-1} = h\}$ de h s'appelle le centralisateur de h dans G, noté $Z_G(h)$.

Prop 4. Soit $Z(G) = \{h : \forall g \in G,\ gh = hg\}$ le centre du groupe. Alors $h \in Z(G)$, si et seulement si, $Z_G(h) = G$. De plus, pour tout $h \in Z(G)$, pour tout $g \in G$, $ghg^{-1} \in Z(G)$.

Cor 5. Soit $g \in G$. Alors $g \in Z(G)$, si et seulement si, sa classe de conjugaison est réduite à un seul élément. Ainsi, $Z(G)$ est l'union des classes de conjugaison de taille 1.

Ex 6. Soit $n \geq 3$, les classes de conjugaison du groupe diédral D_n, d'ordre $2n$, où $D_n =< r, s >$ avec $r^n = e$, $s^2 = e$ et $srs = r^{-1}$, sont :

1. Pour n impair, $\{e\}, \{r^i, r^{-i}\}$ pour $i \in \{1,\dots,\frac{n-1}{2}\}$, $\{r^i s : i \in \{1,\dots,n\}\}$. D'où $Z(D_n) = \{e\}$.
2. Pour n pair : $\{e\}, \{r^{\frac{n}{2}}\}, \{r^i, r^{-i}\}$ pour $i \in \{1,\dots,\frac{n}{2}\}$ et $\{r^{2i+1}s : i \in \{1,\dots,\frac{n}{2}\}\}$. D'où $Z(D_n) = \{e, r^{\frac{n}{2}}\} <$

Notation 7. On note $\mathscr{L}(G) = \{H : H \leq G\}$ l'ensemble des sous-groupes de G.

Prop 8. $\mathrm{Int}(G)$ agit sur $\mathscr{L}(G)$ par : $\forall \alpha_g \in \mathrm{Int}(G)$, $\forall H \in \mathscr{L}(G)$, $\alpha_g \cdot H = \alpha_g(H) = gHg^{-1}$.

Déf 9. Deux sous-groupes de G sont dits conjugués s'ils appartiennent à la même orbite pour cette action.

Prop 10. Soit X un ensemble non vide sur lequel G agit. Alors les stabilisateurs des éléments d'une même orbite sont tous conjugués. Entre autre, ils sont isomorphes.

I.2 Application au groupe des permutations

Soit $n \geq 2$, $\mathfrak{S}_n$ le groupe symétrique.

Déf 11. On appelle type d'une permutation $\sigma \in \mathfrak{S}_n$, et on note $[l_1,\dots,l_m]$, la liste des cardinaux l_i des orbites dans $\{1,\dots,n\}$ de l'action du groupe $<\sigma>$ sur $\{1,\dots,n\}$, rangée en ordre croissant.

Ex 12. La permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} \in \mathfrak{S}_6$

a pour type $[3,2,1]$.

Thm 13. Deux permutations σ et $\rho \in \mathfrak{S}_n$ sont conjuguées dans $\mathfrak{S}_n$, si et seulement si, elles sont de même type. Entre autre, pour $\sigma \in \mathfrak{S}_n$, et tout cycle $(i_1 \cdots i_m) \in \mathfrak{S}_n$, $\sigma(i_1 \cdots i_m)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_m))$

Ex 14. Les permutations $\begin{pmatrix} 1 & 6 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}$ et $\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 & 5 \end{pmatrix}$ sont conjuguées.

I.3 Conjugaison matricielle

Soit $n \geq 1$ et $\mathbb{K}$ un corps.

Prop 15. $GL_n(\mathbb{K})$ agit par conjugaison sur $M_n(\mathbb{K})$: $\forall P \in GL_n(\mathbb{K})$, $\forall M \in M_n(\mathbb{K})$, $P \cdot M = PMP^{-1}$.

Déf 16. On appelle classe de similitude l'orbite d'une matrice de $M_n(\mathbb{K})$ pour cette action. Deux matrices dans la même classe de similitude sont dites semblables.

Déf 17. Une matrice $A \in M_n(\mathbb{K})$ est diagonalisable, resp. trigonalisable, si elle est semblables à une matrice diagonale, resp. triangulaire supérieure.

Rq 18. La conjugaison permet alors de transformer un élément en un autre "plus simple à manipuler".

Prop 19. Si deux matrices sont semblables, alors elles ont même rang, même déterminant, même trace et même polynôme caractéristique.

C-ex 20. La réciproque est fausse : considérer $\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}$ et $\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix} \in M_3(\mathbb{C})$.

Thm 21 (Décomposition de Frobenius)**.** Soit $A \in M_n(\mathbb{K})$. Il existe une unique famille de polynômes unitaire non constants $P_1, \dots, P_s$ de $\mathbb{K}[X]$ tels que l'on ait la décomposition suivante, dite de Frobenius :

1. $P_s \mid \dots \mid P_1$
2. $E = \bigoplus_{i=1}^{s} \mathbb{K}[A] \cdot x_i$, où $\mu_{u,x_i} = P_i$.

Où $\mathbb{K}[A] \cdot x = \{P(A)x : P \in \mathbb{K}[X]\}$ et $\mu_{A,x}$ le polynôme minimal local de A en $x \in \mathbb{K}^n$.

Thm 22 (Invariant total)**.** Deux matrices sont semblables, si et seulement si, elles admettent la même famille de polynômes dans la décomposition de Frobenius. Entre autre, si famille de polynômes est $P_s \mid \dots \mid P_1$, la matrice est semblable à la matrice diagonale par blocs formée des $(C_{P_1}, \dots, C_{P_s})$, où C_P désigne la matrice compagnon associée au polynôme P.

II Sous-groupes distingués et groupes quotients

II.1 Généralités

[Rom21] Soit G un groupe.

Notation 23. Soit H une partie non vide de G. On note alors pour tout $g \in G$, $gH = \{gh : h \in H\}$ et $Hg = \{hg : h \in H\}$. Si G est abélien, $gH = Hg$ pour tout $g \in G$.

Thm 24. Pour tout sous-groupe H de G. Pour tout $g_1, g_2 \in G$, $g_1 \sim g_2$ si et seulement si $g_1^{-1} g_2 \in H$, est une relation d'équivalence.

Prop 25. Soit $g \in G$ et $\overline{g}$ sa classe d'équivalence. Alors $h \in \overline{g}$, si et seulement si, $h \in gH$.

Déf 26. L'ensemble de ces classes d'équivalences est noté G/H, appelé ensemble des classes à gauche modulo H. Entre autre, $G/H = \{\overline{g} : g \in G\} = \{gH : g \in G\}$.

Prop 27. Si $H \leq G$, l'ensemble des classes à gauche modulo H deux à deux distincts forme une partition de G.

Déf 28. Si $H \leq G$, le cardinal de l'ensemble G/H est note $[G : H]$ et on l'appelle indice de H dans G.

Thm 29 (Lagrange)**.** Si G est un groupe fini d'ordre $n \geq 2$, et H est un sous-groupe de G. Pour tout $g \in G$, $|gH| = |H|$ et $|G| = [G : H]|H|$. Entre autre, $|H| \mid n$.

Cor 30. Si G est fini, pour tout $x \in G$, l'ordre de x dans G divise $|G|$.

Déf 31. On dit qu'un sous-groupe H de G est distingué, si $gH = Hg$ pour tout $g \in G$

Ex 32.
1. Si l'on note e le neutre de G, $\{e\}$ et G sont des sous-groupes distingués de G.
2. L'intersection de deux sous-groupes distingués de G, est distingué.
3. Si G est abélien, alors tous ses sous-groupes sont distingués
4. Soit $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ le groupe symétrique et $\mathcal{A}_n$ le groupe alterné. Alors $\mathcal{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$

Thm 33. Soient G, G' deux groupes et φ un morphisme de groupes de G dans G'. Alors $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué de G.

Prop 34. $Z(G)$ est un sous-groupe distingué dans G. De plus, c'est un groupe abélien.

Thm 35. Un sous-groupe H de G est distingué, si et seulement si, il existe une unique structure de groupe sur G/H telle que la surjection canonique $\pi : G \to G/H$ soit un morphisme de groupes surjectif.

Thm 36 (Premier théorème d'isomorphisme)**.** Soient G, G' deux groupes, et $\varphi : G \to G'$ un morphisme de groupes. Il existe un unique isomorphisme de groupes $\overline{\varphi} : G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$ tel que $\varphi = \overline{\varphi} \circ \pi$, où π désigne la surjection canonique de G dans $G/\mathrm{Ker}(\varphi)$.

Cor 37. Si G et G' sont finis, alors $|G| = |\operatorname{Ker}\varphi||\operatorname{Im}\varphi|$

Déf 38. On dit qu'un groupe $G \neq \{e\}$ est simple si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Ex 39. 1. $(\mathbb{Z}/p\mathbb{Z})$ est simple, si et seulement, p est premier.

2. $\mathcal{A}_4$ n'est pas simple.

II.2 Exemple du groupe affine

On considère un espace vectoriel sur $\mathbb{R}$ de dimension finie n, noté E, et un ensemble $\mathcal{E}$ non vide.

Déf 40. $\mathcal{E}$ est un espace affine associé à E si $(E,+)$ agit de façon simplement transitive sur $\mathcal{E}$. Si E est de dimension n, on dit que $\mathcal{E}$ est de dimension n. On appelle vecteur tout élément de E et point tout élément de $\mathcal{E}$.

Notation 41. $\forall \overrightarrow{u} \in E,\ \forall M \in \mathcal{E},\ \overrightarrow{u} \cdot M =: M + \overrightarrow{u}$. On note $\overrightarrow{AB}$ le vecteur $\overrightarrow{u}$ tel que $A = B + \overrightarrow{u}$.

Déf 42. On dit qu'une application $f : \mathcal{E} \to \mathcal{E}$ est une application affine s'il existe un point A de $\mathcal{E}$, et un endomorphisme l de E vérifiant :

$$\forall M \in \mathcal{E},\ \overrightarrow{f(A)f(M)} = l(\overrightarrow{AM})$$

Prop 43. $\exists! l \in \mathscr{L}(E),\ \forall M, P \in \mathcal{E},\ \overrightarrow{f(P)f(M)} = l(\overrightarrow{PM})$. On appelle l l'application linéaire associée à f. On la note $\overrightarrow{f}$.

Notation 44. On note $GA(\mathcal{E})$ l'ensemble des applications affines bijectives de $\mathcal{E}$ dans $\mathcal{E}$.

Thm 45. $(GA(\mathcal{E}), \circ)$ est un groupe. On l'appelle groupe affine de $\mathcal{E}$.

Déf 46. Soit $\overrightarrow{u} \in E$. On appelle translation de vecteur $\overrightarrow{u}$ l'application $t_{\vec{u}} : \mathcal{E} \to \mathcal{E}$, qui à M associe l'unique point M' tel que $\overrightarrow{MM'} = \overrightarrow{u}$.

Prop 47. L'ensemble des translations de $\mathcal{E}$ est un sous-groupe commutatif de $(GA(\mathcal{E}), \circ)$, noté $T(\mathcal{E})$.

Thm 48. L'application $L : \begin{cases} GA(\mathcal{E}) & \longrightarrow & GL(E) \\ f & \longmapsto & \overrightarrow{f} \end{cases}$ est un morphisme de groupe surjectif, de noyau $T(\mathcal{E})$.

Cor 49. $T(\mathcal{E})$ est distingué dans $GA(\mathcal{E})$, et $GA(\mathcal{E})/T(\mathcal{E}) \simeq GL(E)$.

Cor 50. Pour tout $f \in GA(\mathcal{E})$, pour tout $\overrightarrow{u} \in E$, $f \circ t_{\vec{u}} \circ f^{-1} = t_{\vec{f}(\vec{u})}$.

Prop 51. L'ensemble $\mathcal{H}(\mathcal{E}) = \{f \in GA(\mathcal{E}) : \overrightarrow{f} \in \mathrm{Id}_E\,\mathbb{R}\}$, appelé groupe des homothéties ou translations, est un sous-groupe distingué de $GA(\mathcal{E})$.

Notation 52. Une homothétie de centre O et de rapport λ est notée $h_{O,\lambda}$

Cor 53. Soit $O \in \mathcal{E}$, $\lambda \in \mathbb{R}$. Pour tout $f \in GA(\mathcal{E})$, $f \circ h_{O,\lambda} \circ f^{-1} = h_{f(O),\lambda}$

III Applications

III.1 Application aux études des p-Sylow

[Per96] [Ulm21] Soit G un groupe fini.

Déf 54. Si G est fini, de cardinal $n := p^\alpha m$, où $p \nmid m$. On appelle p-sous-groupe de Sylow de G un sous-groupe de G de cardinal p^α.

Rq 55. Dire que S est un p-sous-groupe de Sylow de G revient à dire que S est un p-groupe tel que $[G : S]$ est premier à p.

Ex 56 (DEV 1)**.** Soient $\mathbb{F}_p$ le corps fini à p éléments et $n \in \mathbb{N}^*$. Alors l'ensemble des matrices triangulaires supérieurs strictes est un p-sous-groupe de Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 57 (DEV 1)**.** Si G est fini, d'ordre $|G| = n = p^\alpha m$, $p \nmid m$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H

Thm 58 (DEV 1 - Premier théorème de Sylow)**.** Si G est fini, et $p \mid |G|$, alors G contient au moins un p-sous-groupe de Sylow.

Ex 59. Un groupe G d'ordre 36 possède au moins un 3-Sylow S. Celui-ci est de cardinal 9 et d'indice 4 dans G.

Cor 60. Si $|G| = p^\alpha m$, $p \nmid m$, G contient des sous-groupes d'ordre p^i, pour $0 \leq i \leq \alpha$.

Thm 61 (DEV 1 - Deuxième théorème de Sylow)**.** Si $|G| = p^\alpha m$, $p \nmid m$, alors si l'on note n_p le nombre de p-Sylow de G :

1. Si $H \leq G$ est un p-groupe, il existe un p-Sylow S de G contenant H.

2. Les p-Sylow sont tous conjugués.
3. $n_p \equiv 1 \pmod p$. Entre autre, $n_p \mid m$.

Cor 62. Si S est un p-Sylow de G, alors S est distingué dans G, si et seulement si, il est l'unique p-Sylow de G.

App 63. Un groupe d'ordre 200 n'est pas simple.

App 64. Soit G un groupe d'ordre 340. Alors G possède un sous-groupe distingué d'ordre 85.

III.2 Quaternions et SO_3, SO_4

[CG17]

Déf 65. On appelle corps des quaternions, et l'on note $\mathbb{H}$ l'algèbre de dimension 4 sur le corps des réels, ayant pour base $(\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k})$, dans laquelle la multiplication est définie par :

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \text{ et } \mathbf{ijk} = -1.$$

Notation 66. On note $SU_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) : |a|^2 + |b|^2 = 1 \right\}$.

Prop 67. $SU_2(\mathbb{C})$ est un sous-groupe de $GL_2(\mathbb{C})$, homéomorphe avec $\mathbb{S}^3$.

Thm 68. $\mathbb{H} \simeq \mathbb{R}_+^* I_2 \times SU_2(\mathbb{C}) \cup \{0\}$. On notera alors $\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) : a, b \in \mathbb{C} \right\} \subseteq GL_2(\mathbb{C})$.

Notation 69.
1. Si $x, y, z, t \in \mathbb{R}$, et si l'on note $a = x + iy$, $b = z + it$, un élément de $\mathbb{H}$ s'écrit $h = x\mathbf{1} + y\mathbf{i} + z\mathbf{j} + t\mathbf{k} = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$.
2. On note $\overline{h} = x\mathbf{1} - y\mathbf{i} - z\mathbf{j} - t\mathbf{k}$ le conjugué de h.
3. On note $N(h) = \det h = |a|^2 + |b|^2 = x^2 + y^2 + z^2 + t^2$.
4. On note $\mathbb{I} = \mathrm{Vect}_{\mathbb{R}}(\mathbf{i}, \mathbf{j}, \mathbf{k})$.

Prop 70 (DEV 2)**.** $SU_2(\mathbb{C})$ agit par conjugaison sur $\mathbb{H}$. Une telle action induit une application linéaire, continue et qui conserve la norme.

Thm 71 (DEV 2)**.** Il existe deux isomorphismes de groupes :
1. $SU_2(\mathbb{C})/\{\pm I_2\} \simeq SO_3(\mathbb{R})$.
2. $SU_2(\mathbb{C}) \times SU_2(\mathbb{C})/\{(I_2, I_2), (-I_2, -I_2)\} \simeq SO_4(\mathbb{R})$.

Bibliographie

[CG17] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, tome second*. Calvage et Mounet, 2017.

[Per96] Daniel Perrin. *Cours d'algèbre*. ellipses, 1996.

[Rom21] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation : Algèbre et géométrie*. 2e éd. De Boeck Supérieur, 2021.

[Ulm21] Felix Ulmer. *Théorie des groupes*. 2021.