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

Soit $(G, \cdot)$ un groupe et H un sous groupe de G.

1 Conjugaison dans un groupe

1.1 Conjugaison

Définition 1. Deux éléments $g_1, g_2 \in G$ sont dits conjugués lorsqu'il existe $h \in G$ tel que $hg_1h^{-1} = g_2$.
La conjugaison est une action de groupe $\varphi : G \times G \to G\ ;\ (g,h) \mapsto ghg^{-1}$, l'orbite d'un élément $h \in G$ définie par $\{ghg^{-1} | g \in G\} := cc(h)$ est appelée classe de conjugaison et son stabilisateur $\{g \in G | ghg^{-1} = h\} := Z_G(h)$ est appelé centralisateur de h.

Lemme 2. *Soit $g \in G$, l'application $Int_g : G \to G\ ;\ x \mapsto gxg^{-1}$ est un automorphisme de G et l'application $Int : G \to Aut(G)\ ;\ gInt_g$ est un morphisme de groupe.*

Exemple 3.
1. Soit $x \in G$, alors $cc(x) = \{x\} \iff x \in Z(G)$.
2. Soit E un $\mathbb{K}$espace vectoriel de dimension finie, deux éléments $u, v \in GL(E)$ sont conjugués si et seulement si il existe deux bases $\mathcal{B}$ et $\mathcal{B}'$ telles que $Mat_{\mathcal{B}}(u) = Mat_{\mathcal{B}'}(v)$.

1.2 Sous groupes distingués

Définition 4. On dit que H est distingué dans G lorsque pour tout $h \in H$ et tout $g \in G$ on a $ghg^{-1} \in H$. On notera $H \lhd G$.

Exemple 5. Si G est abélien tout sous groupe est distingué. Les sous groupes $\{1_G\}$ et G sont toujours distingués.

Proposition 6. *Soit $f : G \to G'$ un morphisme de groupe, alors* $\ker(f) \lhd G$.

Exemple 7. Soit E un $\mathbb{K}$espace vectoriel de dimension finie, alors $SL(E) \lhd GL(E)$ car c'est le noyau du déterminant qui est un morphisme $GL(E) \to \mathbb{K}^\times$.
Pour tout $n \geqslant 2$ le groupe alterné $\mathcal{A}_n \lhd \mathcal{S}_n$ comme noyau du morphisme de signature $\mathcal{S}_n \to \{-1, 1\}$.

Définition 8. On dit que G est simple lorsque $G \neq \{1_G\}$ et que $\{1_G\}$ et G sont les seuls sous groupes distingués de G.

Exemple 9. Pour $n \geqslant 3$ le groupe $\mathcal{S}_n$ n'est pas simple. Les groupes abéliens simple sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Proposition 10. *Les conditions suivantes sont équivalentes :*
1. *$H \lhd G$,*
2. *$gHg^{-1} = H$ pour tout $g \in G$,*
3. *$gH = Hg$ pour out $g \in G$.*

Proposition 11. *Soit $K \subset H \subset G$ des sous groupes de G. Si $K \lhd G$ alors $K \lhd H$.*

2 Groupes quotients

2.1 Prérequis

Définition 12. On appelle ensemble des classes à gauche de G modulo H l'ensemble $G/H = \{gH | g \in G\}$ des classes d'équivalences de la relation $g_1 \sim_H g_2$ définie par $\exists h \in H, g_1 = hg_2$.

Définition 13. On appelle indice de G dans H noté $[G : H] := |G/H|$ le cardinal de l'ensemble quotient.

Proposition 14. *Si $[G : H] = 2$ alors $H \lhd G$.*

Théorème 15. *Soit H un sous groupe de G, leurs cardinaux sont liés par la formule $|G| = |H|[G : H]$.*

Théorème 16. *(Lagrange) Soit G un groupe fini et H un sous groupe de G. Alors l'ordre de H divise l'ordre de G, en particulier l'ordre d'un élément de G divise toujours l'ordre de G.*

2.2 Groupes quotient

Théorème 17. *Un sous groupe H est distingué dans G si et seulement si la formule $g_1H * g_2H = (g_1g_2)H$ définit une loi de groupe sur l'ensemble quotient G/H telle que la surjection canonique définie par $\pi : G \twoheadrightarrow G/H \ ; \ g \mapsto gH$ soit un morphisme de groupe.*
Ces propriétés déterminent la loi de manière unique et le groupe $(G/H, *)$ est appelé groupe quotient de G par H.
Si $H \lhd G$ alors $\pi : G \twoheadrightarrow G/H$ est un morphisme surjectif de noyau H. Si de plus G est fini on a $[G : H] = |G/H| = \frac{|G|}{|H|}$

Théorème 18. *(Prolongement) Soient G et G' deux groupes, $H \lhd G$, $\pi : G \twoheadrightarrow G/H$ le morphisme canonique et $\varphi : G \to G'$ un morphisme de groupe. Les assertions suivantes sont équivalentes :*

1. *$H \subset \ker(\varphi)$,*
2. *$\varphi(H) = \{1_{G'}\}$,*
3. *Il existe un unique morphisme de groupe $\overline{\varphi} : G/H \to G'$ tel que $\varphi = \overline{\varphi} \circ \pi$.*

Si c'est le cas le morphisme $\overline{\varphi}$ est unique, défini par $\overline{\varphi}(gH) = \varphi(g)$, son image est celle de φ et son noyau est $\ker(\varphi)/H$.

Théorème 19. *(1er théorème d'isomorphisme) Soient G et G' des groupes et $\varphi : G \to G'$ un morphisme de groupe. Alors il existe un isomorphisme $G/\ker(\varphi) \cong Im(\varphi)$ défini par $\overline{\varphi} : G/\ker(\varphi) \twoheadrightarrow Im(\varphi) \ ; \ g\ker(\varphi) \to \varphi(g)$.*

Exemple 20. Le morphisme det : $GL_n(\mathbb{C}) \to \mathbb{C}^*$ est surjectif de noyau $SL_n(\mathbb{C})$. Ainsi $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \cong \mathbb{C}^*$.

Théorème 21. *(3e théorème d'isomorphisme) Soit $K \subset H \subset G$ des groupes. Si $H \lhd G$ et $K \lhd G$ alors $(G/K)/(H/K) \cong G/H$.*

Exemple 22. Comme $10\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$ et que l'on peut construire un morphisme $\varphi : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ surjectif de noyau $2\mathbb{Z}/10\mathbb{Z}$. Il existe un isomorphisme $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

3 Applications de la conjugaison

3.1 Groupes symétriques et alternés

Définition 23. Pour tout entier $n \in \mathbb{N}^*$ l'ensemble $\mathcal{S}_n$ des permutations de $\{1, \dots, n\}$ est un groupe pour la loi de composition des applications. Il est fini d'ordre $|\mathcal{S}_n| = n!$.

Proposition 24. *Soit $n \in \mathbb{N}^*$ et $\rho, \tau \in \mathcal{S}_n$. On a toujours $supp(\tau\rho) \subset supp(\tau) \cup supp(\rho)$. Si $supp(\tau) \cap supp(\rho) = \varnothing$ alors il y a égalité.*

Proposition 25. *Les cycles à support disjoint commutent*

Théorème 26. *Tout élément $\sigma \in \mathcal{S}_n$ possède une unique décomposition en produit de cycle à support disjoint (à ordre près).*

Définition 27. On appelle type d'une permutation $\sigma \in \mathcal{S}_n$ noté $[l_1, \dots, l_m]$ la liste rangé dans l'ordre croissant des longueurs des cycles dans la décomposition de cycle à support disjoint.

Proposition 28. *Une permutation $\sigma \in \mathcal{S}_n$ de type $[l_1, \dots, l_m]$ a pour ordre $ppcm(l_1, \dots, l_m)$.*

Théorème 29. *Deux permutations sont conjuguées dans $\mathcal{S}_n$ si et seulement si elles sont de même type. En particulier pour $\omega, (i_1, \dots, i_l) \in \mathcal{S}_n$ on a $\omega(i_1, \dots, i_l)\omega^{-1} = (\omega(i_1), \dots, \omega(i_l))$.*

Lemme 30. *Tout cycle d'ordre l de $\mathcal{S}_n$ peut s'écrire comme produit de $l-1$ transposition.*

Corollaire 31. *Le groupe $\mathcal{S}_n$ est engendré par les transpositions.*

Définition 32. On appelle signature de $\sigma \in \mathcal{S}_n$ noté $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j} \in \{-1, 1\}$. C'est un morphisme de groupe.

Proposition 33. *Si $\#(\sigma)$ désigne un nombre de transposition qui apparaît dans une décomposition de σ en produit de transposition. Alors $\varepsilon(\sigma) = (-1)^{\#(\sigma)}$.*
Si σ est de type $[l_1, \dots, l_m]$ alors $\varepsilon(\sigma) = (-1)^{l_1 + \dots + l_m - m}$.

Définition 34. Le noyau de ε est un sous-groupe distingué de $\mathcal{S}_n$ appelé groupe alterné noté $\mathcal{A}_n$.

Proposition 35. *Le groupe $\mathcal{A}_n$ est un sous groupe d'indice 2 de $\mathcal{S}_n$ qui contient $\frac{n!}{2}$ éléments.*

Proposition 36. *Pour $n \geqslant 5$ les 3 cycles sont conjugués dans le groupe alterné $\mathcal{A}_n$.*

Proposition 37. *Le produit de 2 transpositions est un produit de 3 cycles.*

Proposition 38. *Le groupe alterné $\mathcal{A}_n$ est engendré par les 3 cycles.*

Théorème 39. *Pour $n = 3$ et $n \geqslant 5$ le groupe $\mathcal{A}_n$ est simple.*

3.2 Les p-Groupes [ROM17]

Définition 40. Si p est un nombre premier, on appelle p-groupe tout groupe G de cardinal p^α où $\alpha \in \mathbb{N}$.

Théorème 41. *Soit $(G, \cdot)$ un groupe fini opérant sur un ensemble fini E, en notant $G \cdot x_1, \ldots, G \cdot x_r$ toutes les orbites deux à deux distinctes on : $|E| = \sum_{i=1}^{r} |G \cdot x_i| = \sum_{i=1}^{r} \frac{|G|}{|Stab_G(x_i)|}$*

Corollaire 42. *Si p est premier et $(G, \cdot)$ un p-groupe opérant sur un ensemble fini E, on a alors $|E^G| \equiv |E| \mod p$.*

Théorème 43. *Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.*

Théorème 44. *Tout groupe d'ordre p^2 avec p premier est commutatif.*

Corollaire 45. *Tout groupe d'ordre p^2 avec p premier est soit isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

DEV1 : An est simple 37, 38 et 39
DEV2 : Classification des groupes d'ordre $\mathbf{p^2}$ 42, 43, 44 et 45

Références

[BER18] Grégory BERHUY : Algèbre : Le grand combat. Calvague Mounet, 2018.

[ROM17] Jean Etienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Superieur, 2017.

[ULM12] Félix ULMER : Théorie des groupes. Ellipses, 2012.

Rapport du jury :
Dans un premier temps, la notion de conjugaison dans un groupe introduite brièvement doit être développée et illustrée dans des situations variées. On doit proposer des situations où la conjugaison aide à résoudre certains problèmes (par exemple, en transformant un élément en un autre plus simple à manipuler). On peut aussi illustrer et utiliser le principe du transport par conjugaison voulant que hgh-1 ait la même nature géométrique que g. Ensuite, il est attendu de développer l'intérêt de la notion de sous-groupe distingué en particulier en regard de la structure de groupe obtenue par quotient d'un groupe, le lien entre sous-groupe distingué et noyau de morphisme de groupes, ainsi que la factorisation d'un morphisme de groupe au travers d'un tel quotient. Il est indispensable de proposer quelques résultats bien choisis mettant en évidence l'utilisation de ces notions : citons par exemple le lien entre les sous-groupes de l'un et de l'autre et la caractérisation interne des produits directs. L'examen de la simplicité de certains groupes peut être proposé. Comme indiqué dans le sujet, il est demandé de présenter des exemples pertinents utilisés pour obtenir des résultats significatifs. De tels exemples sont nombreux en théorie des groupes mais il est souhaitable d'en proposer dans d'autres domaines, comme en arithmétique, en géométrie et en algèbre linéaire. Pour aller plus loin, les candidates et candidats peuvent poursuivre en illustrant ces notions en théorie des représentations des groupes finis (classes de conjugaison et nombre de représentations irréductibles, treillis des sous-groupes distingués lu dans la table de caractères, etc.). La notion de produit semi-direct et les théorèmes de Sylow débordent du programme. Il est possible de les évoquer, mais en veillant à les illustrer par des exemples et des applications.