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

1. Conjugaison dans un sous-groupe

1.1. L'action par conjugaison

1. Définition. Soit G un groupe. Alors la relation
$$g \cdot h \coloneqq ghg^{-1}$$
définie une action du groupe G sur lui-même, appelée l'*action par conjugaison*. L'orbite d'un élément est sa *classe de conjugaisons*. Deux éléments d'une même classe de conjugaisons sont dits *conjugués*. Le stabilisateur d'un élément $h \in G$ est noté $\mathrm{Z}_G(h)$.

2. Remarque. Dans un groupe abélien G, les classes de conjugaisons sont réduites à un élément : pour un élément $h \in G$, on a $\mathrm{Z}_G(h) = \{h\}$.

3. Exemple. Dans le groupe symétrique $\mathfrak{S}_3$, les permutations (1 2 3) et (1 3 2) sont conjugués puisque $(1\ 3\ 2) = (2\ 3)^{-1}(1\ 2\ 3)(2\ 3)$.

4. Définition. Le *centre* d'un groupe G est le sous-groupe
$$\mathrm{Z}(G) \coloneqq \{h \in G \mid \forall h \in G,\ ghg^{-1} = h\}.$$

5. Remarque. Pour un élément $h \in G$, on a $h \in \mathrm{Z}(G) \Leftrightarrow G = \mathrm{Z}_G(h)$.

6. Définition. Un *automorphisme intérieur* est un morphisme de la forme
$$\left|\begin{array}{l} G \longrightarrow G, \\ x \longmapsto gxg^{-1} \end{array}\right.$$
pour un élément $g \in G$. On note $\mathrm{Int}(G)$ le groupe des morphismes intérieurs.

7. Application *(théorème de Wedderburn).* Tout corps fini, non supposé commutatif, est commutatif.

1.2. Exemples de classes de conjugaisons

8. Lemme *(principe de transfert).* Soient $\sigma \coloneqq (a_1\ \cdots\ a_k) \in \mathfrak{S}_n$ un k-cyclique et $\tau \in \mathfrak{S}_n$ une permutation. Alors
$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \cdots\ \tau(a_k)).$$

9. Proposition. Dans le groupe $\mathfrak{S}_n$, les k-cycles sont conjugués.

10. Corollaire. Deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si leurs décompositions en produit de cycles à supports disjoints ont le même nombre de k-cycles pour tout $k \in \{2, \dots, n\}$.

11. Exemple. Les permutations (1 2)(3 4) et (1 3) ne sont pas conjugués dans $\mathfrak{S}_4$.

12. Lemme. Le groupe $\mathfrak{A}_n$ agit $n-2$-transitivement sur l'ensemble $\{1, \dots, n\}$.

13. Proposition. Si $n \geqslant 5$, les 3-cycles de $\mathfrak{S}_n$ sont conjugués dans $\mathfrak{A}_n$.

14. Définition. Soit K un corps. Deux matrices de $\mathrm{GL}_n(K)$ sont *semblables* si elles sont conjuguées dans $\mathrm{GL}_n(K)$.

15. Théorème *(Frobenius).* Deux matrices de $\mathrm{GL}_n(K)$ sont semblables si et seulement si elles ont les mêmes invariantes de similitude.

16. Exemple. Les matrices
$$\begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 1 & & \\ & 0 & & \\ & & 0 & 1 \\ & & & 0 \end{pmatrix}$$
ne sont pas semblables.

2. Sous-groupes distingués et groupes quotients

2.1. Sous-groupes distingués

17. Définition. Un sous-groupe H de G est *distingué* dans G si
$$\forall g \in G,\ \forall h \in H, \qquad ghg^{-1} \in H.$$
On note alors $H \triangleleft G$.

18. Exemple. Le groupe G et le groupe trivial $\{1\}$ sont distingué dans G. Le centre $\mathrm{Z}(G)$ est distingué dans G.

19. Remarque. Lorsque le groupe G est abélien, tout ses sous-groupes sont distingués.

20. Proposition. Soit H un sous-groupe de G. Alors les points sont équivalents :
- il est distingué ;
- pour tout élément $g \in G$, on a $gH = Hg$;
- pour tout élément $g \in G$, on a $gHg^{-1} \subset H$.

21. Proposition. Soit $f : G \longrightarrow H$ un morphisme de groupes. Alors son noyau $\mathrm{Ker}\, f$ est distingué dans G.

22. Exemple. Le groupe alterné $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$ et le groupe spécial orthogonal $\mathrm{SO}(E)$ d'un espace euclidien E est distingué dans le groupe orthogonal $\mathrm{O}(E)$.

23. Proposition. Le groupe dérivé
$$\mathrm{D}(G) \coloneqq \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$$
est un sous-groupe distingué de G.

2.2. Groupes quotients et théorèmes d'isomorphisme

24. Définition. Soit H un sous-groupe de G. On définit la relation $\sim$ sur G par
$$x \sim y \quad \Longleftrightarrow \quad xy^{-1} \in H.$$
L'ensemble des ces orbites est notée $G/H \coloneqq G/\sim$ et appelée le *quotient* de G par H.

25. Définition. L'*indice* d'un sous-groupe H de G est l'entier $[G : H] \coloneqq |G/H|$.

26. Proposition. Soit H un sous-groupe d'un groupe fini G. Alors
$$|G| = [G : H] \times |H|.$$

27. Proposition. Un sous-groupe d'indice 2 est distingué

28. Lemme. Soit H un sous-groupe distingué de G. Soient $x, x', y, y' \in G$ quatre éléments tels que $x \sim x'$ et $y \sim y'$. Alors $xx' \sim yy'$.

29. Corollaire. Un sous-groupe est distingué si et seulement s'il s'agit du noyau d'un morphisme.

30. Théorème. Soit H un sous-groupe distingué de G. Alors le quotient G/H est muni d'une structure de groupe.
31. Exemple. Les quotients $\mathbf{Z}/n\mathbf{Z}$ avec $n \in \mathbf{N}^*$ sont des groupes.
32. Application. Le discriminant d'une forme quadratique non dégénéré sur un corps K est un élément du groupe $K^\times/K^{\times 2}$
33. Remarque. Avec cette définition, la projection canonique $\pi\colon G \longrightarrow G/H$ est alors un morphisme de groupes.
34. Théorème *(premier théorème d'isomorphisme)*. Soit $f\colon G \longrightarrow H$ un morphisme de groupes. Alors les groupes $G/\operatorname{Ker} f$ et $\operatorname{Im} f$ sont isomorphes.
35. Exemple. Les groupes $\mathbf{U} \coloneqq \{z \in \mathbf{C} \mid |z| = 1\}$ et $\mathbf{R}/2\pi\mathbf{Z}$ sont isomorphes.
36. Théorème *(deuxième théorème d'isomorphisme)*. Soient H un sous-groupe distingué de G et K un sous-groupe de G. Alors il existe un isomorphisme

$$\frac{K}{H \cap K} \simeq \frac{HK}{H}.$$

37. Théorème *(troisième théorème d'isomorphisme)*. Soient H et K deux sous-groupes distingués de G tels que $H \subset K$. Alors il existe un isomorphisme

$$\frac{G}{K} \simeq \frac{G/H}{K/H}.$$

3. Groupes simples et p-groupes

3.1. Les groupes simples

38. Définition. Un groupe est *simple* s'il n'est pas trivial et si ses seuls sous-groupes distingués sont lui-même et le groupe trivial.
39. Exemple. Pour $n \in \mathbf{N}^*$, le groupe $\mathbf{Z}/n\mathbf{Z}$ est simple si et seulement si l'entier n est premier.
40. Proposition. Les seuls sous-groupes abéliens simples sont les groupes $\mathbf{Z}/p\mathbf{Z}$ pour un nombre premier p.
41. Théorème. Soit K un corps. Alors le quotient $\mathrm{PSL}_n(K) \coloneqq \mathrm{SL}_n(K)/\operatorname{Z}(\mathrm{SL}_n(K))$ est un groupe simple si $K \notin \{\mathbf{F}_2, \mathbf{F}_3\}$ et $n = 2$.
42. Lemme. Le groupe $\mathfrak{A}_5$ est simple.
43. Théorème. Soit $n \geqslant 5$ un entier. Alors le groupe $\mathfrak{A}_n$ est simple.
44. Corollaire. Pour tout entier $n \geqslant 5$, on a $\operatorname{D}(\mathfrak{A}_n) = \mathfrak{A}_n$ et, pour tout entier $n \geqslant 2$, on a $\operatorname{D}(\mathfrak{S}_n) = \mathfrak{A}_n$.
45. Corollaire. Pour tout entier $n \geqslant 5$, le seul sous-groupe propre et non trivial du groupe $\mathfrak{S}_n$ est le groupe $\mathfrak{A}_n$.

3.2. Les p-groupes et le théorème de Sylow

46. Définition. Soit p un nombre premier. Un *p-groupe* est un groupe fini dont le cardinal est une puissance de l'entier p.
47. Proposition. Le centre d'un p-groupe non trivial est non trivial.
48. Définition. Soient G un groupe fini de cardinal n et p un diviseur premier de l'entier n. On note $n = p^\alpha m$ avec $p \nmid m$. Un *p-sous-groupe de Sylow* de G est un sous-groupe de cardinal p^α.
49. Exemple. Un p-sous-groupe de Sylow du groupe $\mathrm{GL}_n(\mathbf{F}_p)$ est le groupe des matrices triangulaires supérieures dont les coefficients de la diagonale valent 1.
50. Théorème *(Sylow)*. Soient G un groupe fini et p un diviseur de son ordre. Alors le groupe G contient au moins un p-sous-groupe de Sylow.
51. Théorème *(Sylow)*. Soient G un groupe fini de cardinal n et p un diviseur premier de l'entier n. On note $n = p^\alpha m$ avec $p \nmid m$. Alors
- pour tout sous-groupe $H \subset G$, il existe un p-sous-groupe de Sylow $S \subset G$ tel que $H \subset S$;
- les p-sous-groupes de Sylow sont conjugués ;
- le nombre de p-sous-groupes de Sylow vérifie $k \equiv 1 \mod p$ et $k \mid |G|$

52. Corollaire. Soit S un p-sous-groupe de Sylow de G. Alors il est distingué si et seulement s'il est l'unique p-sous-groupe de Sylow de G.
53. Application. Un groupe d'ordre 63 n'est pas simple.

[1] Josette Calais. *Éléments de théorie des groupes*. 3e édition. Presses Universitaires de France, 1998.
[2] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.
[3] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.