Cadre : G désigne un groupe et H un sous-groupe de G.

I Action par conjugaison

1) G agit sur lui-même

Définition 1. On appelle isomorphisme intérieur tout automorphisme i_g donné, pour $g \in G$ par $i_g(h) = ghg^{-1}$ pour tout $h \in G$.

Proposition 2. *G agit sur lui-même par conjugaison en posant :*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g \cdot h = ghg^{-1} \end{array}$$

Définition 3. L'orbite $\left\{ghg^{-1} \,\middle|\, g \in G\right\}$ de $h \in G$ sous l'action de conjugaison par 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 $Stab_G(h) = \left\{g \in G \,\middle|\, ghg^{-1} = h\right\}$ de h s'appelle le centralisateur de h dans G.

Définition 4. Le centralisateur d'une partie A de G est donnée par $C_G(A) = \{g \in G \,|\, \forall a \in A, ga = ag\}$.

Remarque 5. *On rappelle que $Z(G) = \{g \in G \,|\, \forall h \in G, gh = hg\}$ est le centre de G. On a alors en particulier $Z(G) = C_G(G)$.*

Exemple 6. *La classe de conjugaison de e est $\{e\}$ et $C_G(e) = G$.*

2) G agit sur l'ensemble de ses sous-groupes

Proposition 7. *G agit sur l'ensemble de ses sous-groupes par conjugaison par $g \cdot H = gHg^{-1}$.*

Définition 8. On dit que H et gHg^{-1} sont conjugués. Le stabilisateur de H, noté $N_G(H)$ est appelé normalisateur de H dans G : $N_G(H) = \left\{g \in G \,\middle|\, gHg^{-1} = H\right\}$.

Proposition 9. *On suppose que G agit sur un ensemble X. Les stabilisateurs des éléments d'une même orbite sont tous conjugués. Plus précisément, on a, pour tout $x \in X$ et tout $g \in G$, $Stab_G(g \cdot x) = gStab_G(x)g^{-1}$.*

II Sous-groupe distingué et groupe quotient

1) Sous-groupe distingué

Définition 10. On dit que H est distingué dans G, noté $H \trianglelefteq G$, s'il est invariant par conjugaison, c'est-à-dire si :

$$\forall\, g \in G,\ \forall\, h \in H,\ ghg^{-1} \in H$$

Exemple 11. *On a toujours : $\{e\} \trianglelefteq G$, $G \trianglelefteq G$ et $Z(G) \trianglelefteq G$.*

Exemple 12. *Soit $n \in \mathbb{N}$, alors $\mathcal{SL}_n(\mathbb{R}) \trianglelefteq \mathcal{GL}_n(\mathbb{R})$.*

Définition 13. Un groupe G est dit simple s'il est non trivial et ne possède pas de sous-groupe distingué autre que $\{e\}$ et lui-même.

Proposition 14. *Soit I un ensemble et soient $H_i \trianglelefteq G$ pour tout $i \in I$. Alors $\bigcap_{i\in I} H_i \trianglelefteq G$.*

Proposition 15. *Soient $K \leqslant H \leqslant G$. Si $K \trianglelefteq G$, alors $K \trianglelefteq H$.*

Proposition 16. *Soit G' un groupe, H' un sous-groupe de G' et $\varphi : G \to G'$ un morphisme de groupes.*

(i) Si $H \trianglelefteq G$, alors $\varphi(H) \trianglelefteq \varphi(G)$.

(ii) Si φ est surjectif, alors $\varphi(H) \trianglelefteq G'$.

(iii) Si $H' \trianglelefteq G'$, alors $\varphi^{-1}(H') \trianglelefteq G$.

Proposition 17. *$H \trianglelefteq G$ si, et seulement si, H est un point fixe de l'action de G sur l'ensemble de ses sous-groupes par conjugaison. En particulier, $H \trianglelefteq G$ si, et seulement si, pour tout $g \in G$ on a $gHg^{-1} = H$.*

2) Classes d'équivalences

Théorème 18. *La relation "$g_1 \sim_H g_2 \ \Leftrightarrow\ \exists\, h \in H,\ g_1 = g_2 h$" définit une relation d'équivalence sur G dont les classes d'équivalences sont les sous-ensembles $gH = \{gh \,|\, h \in H\}$ où $g \in G$.*

Définition 19. Ces classes sont appelées classes à gauche de G modulo H. On appelle ensemble quotient de G par $\sim_H$, et on note G/H, l'ensemble des classes à gauche de G modulo H.

Définition 20. La quantité $[G : H] = |G/H|$ est l'indice de H dans G.

Théorème 21 (Lagrange)**.** *Si G est fini, $|G| = |H||G/H| = |H|[G : H]$. En particulier, l'ordre d'un élément $g \in G$ divise l'ordre de G*

Proposition 22. *Un sous-groupe d'indice 2 est toujours distingué.*

3) Groupe quotient

Théorème 23. *On a $H \trianglelefteq G$ si, et seulement si, $(g_1H)*(g_2H) = (g_1g_2)H$ définit une loi de groupe $*$ sur G/H telle que l'application canonique $\pi : G \to G/H$ définit par $\pi(g) = gH$ soit un morphisme de groupes.*

Définition 24. Le groupe $(G/H, *)$ est le groupe quotient de G par H.

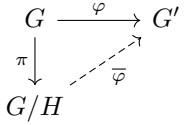
Exemple 25. *Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z} \trianglelefteq \mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ est un groupe.*

Corollaire 26. *$H \trianglelefteq G$ si, et seulement si, H est le noyau d'un morphisme de groupe.*

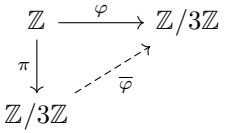
Théorème 27 (Propriété universelle du quotient)**.** *On suppose que $H \trianglelefteq G$. Soient $\pi : G \to G/H$ le morphisme canonique et $\varphi : G \to G'$ un morphisme de groupe. Les assertions suivantes sont équivalentes :*

(i) $H \subseteq \mathrm{Ker}(\varphi)$

(ii) Il existe un unique morphisme de groupe $\overline{\varphi} : G/H \to G'$ tel que le diagramme ci-contre soit commutatif.



Exemple 28. *En prenant $G = \mathbb{Z}$, $H = 6\mathbb{Z}$, $G' = \mathbb{Z}/3\mathbb{Z}$ et $\varphi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ le morphisme canonique, on a le diagramme commutatif ci-contre, car $6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathrm{Ker}(\varphi)$.*



Théorème 29 (Premier théorème d'isomorphie)**.** *Soit $\varphi : G \to G'$ un morphisme de groupe. Alors $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.*

Exemple 30. *Le morphisme de groupe* det : $\mathcal{GL}_n(\mathbb{C}) \to \mathbb{C}^\star$ *donne* $\mathcal{GL}_n(\mathbb{C})/\mathcal{SL}_n(\mathbb{C}) \cong \mathbb{C}^\star$.

Application 31. *Un groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

4) Théorèmes de Sylow

Définition 32. On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Un p-Sylow est un sous-groupe de G d'ordre p^α.

Exemple 33. *$|GL_n(\mathbb{F}_p)| = p^\alpha m$, où $\alpha = \frac{n(n-1)}{2}$ et $p \nmid m$, et $\{(a_{i,j}) \,|\, a_{i,j} = 0$ si $i > j, a_{i,i} = 1\} \subset GL_n(\mathbb{F}_p)$ est un p-Sylow.*

Lemme 34. *On suppose G fini d'ordre $p^\alpha m$, où $p \nmid m$. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Lemme 35. *Soit G un p-groupe agissant sur X. On note X^G l'ensemble des points fixes de X par G. Alors $|X| \equiv |X^G| \mod p$.*

Théorème 36 (Sylow)**.** *On suppose G fini d'ordre $n = p^\alpha m$, où $p \nmid m$.*

(i) L'ensemble $Syl_p(G)$ des p-Sylow de G est non vide.

(ii) Tous les p-Sylow sont conjugués.

(iii) $|Syl_p(G)| \equiv 1 \mod p$ et $|Syl_p(G)| \mid m$.

Corollaire 37. *Soit $S \in Syl_p(G)$, alors : $S \trianglelefteq G \Leftrightarrow |Syl_p(G)| = 1$.*

Exemple 38. *Un groupe d'ordre 63 possède un sous-groupe distingué.*

III Exemples de sous-groupes distingués et de groupes quotients

1) Groupe symétrique

Classes de conjugaison

Théorème 39. *Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit de cycles à supports disjoints. Ils correspondent aux orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$.*

Définition 40. On appelle type de $\sigma \in \mathfrak{S}_n$, notée $[l_1, \ldots, l_m]$, la liste des cardinaux des orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ dans l'ordre décroissant.

Exemple 41. *Les types possibles d'une permutation de $\mathfrak{S}_5$ sont :* $[1,1,1,1,1]$, $[2,1,1,1]$, $[2,2,1]$, $[3,1,1]$, $[3,2]$, $[4,1]$ *et* $[5]$.

Théorème 42. *Deux permutation de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.*

Groupe alterné

Proposition 43. *$\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$. De plus, $\mathfrak{S}_n/\mathfrak{A}_n \cong \{\pm 1\}$.*

Lemme 44. *$\mathfrak{A}_n$ est $n-2$ fois transitif sur $[\![1, n]\!]$: si on a $a_1, \ldots, a_{n-2} \in [\![1, n]\!]$ distincts et $b_1, \ldots, b_{n-2} \in [\![1, n]\!]$ distincts, il existe $\sigma \in \mathfrak{A}_n$ tel que $\sigma(a_i) = b_i$ pour tout $i \in [\![1, n-2]\!]$.*

Proposition 45. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Proposition 46. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Théorème 47. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

2) Sous-groupe dérivé, groupe résoluble

Définition 48. Soient $g_1, g_2 \in G$. On appelle commutateur de g_1 et g_2 la quantité $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$. On appelle groupe dérivé de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs.

Exemple 49. *Si G est abélien, on a $D(G) = \{e\}$.*

Proposition 50. *Pour $g_1, g_2, h \in G$, on a :*

$$[g_1, g_2]^{-1} = [g_2, g_1] \quad et \quad h[g_1, g_2]h^{-1} = [hg_1h^{-1}, hg_2h^{-1}]$$

Proposition 51. $D(G) \trianglelefteq G$

Théorème 52. *$G/D(G)$ est abélien. De plus, $D(G) \subseteq H$ si, et seulement si, $H \trianglelefteq G$ et G/H est abélien.*

Définition 53. $G/D(G)$ est appelé l'abélianisé de G.

Définition 54. On définit la suite dérivée de G par :

$$G^{(0)} = G \quad \text{et} \quad \forall i \in \mathbb{N},\ G^{(i+1)} = D(G^{(i)}) = D^{i+1}(G)$$

S'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$, G est dit résoluble.

Remarque 55. *G est résoluble si, et seulement si, la suite $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots$ est stationnaire en $\{e\}$. Le quotient de deux termes consécutifs est toujours abélien.*

Exemple 56. *(i) Tout groupe abélien est résoluble.*

(ii) Un groupe simple non abélien n'est jamais résoluble.

IV Théorie des représentations

Soit G un groupe d'ordre n et V un $\mathbb{C}$-espace vectoriel de dimension d.

Définition 57. Une représentation linéaire de G est un morphisme $\rho : G \to \mathcal{GL}(V)$. On appelle caractère de ρ la fonction $g \mapsto \mathrm{tr}(\rho(g))$.

Définition 58. Soit $\rho : G \to \mathcal{GL}(V)$ une représentation linéaire de G. On dit qu'elle est irréductible si V n'est pas réduit à $\{0\}$ et si aucun sous-espace vectoriel non trivial de V n'est stable par G. Le caractère associé une telle représentation est dit irréductible.

Remarque 59. *Se donner une représentation de G dans V revient à se donner une action de groupes de G sur V en posant $\rho(g)(x) = g \cdot x$.*

Exemple 60. *$\rho : g \mapsto Id_V$ est une représentation de G sur V.*

Définition 61. Soient $\varphi, \psi : G \to \mathbb{C}$ deux fonctions. On pose :

$$(\varphi|\psi) = \frac{1}{|G|} \sum_{t \in G} \varphi(t)\overline{\psi(t)}$$

$(.|.)$ est un produit scalaire.

Théorème 62. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur G.*

Théorème 63. *Le nombre des représentations irréductibles de G (à isomorphisme près) est égal au nombre classes de conjugaison de G.*

Théorème 64. *Soit $\mathcal{T}$ un tétraèdre régulier de l'espace affine euclidien de dimension 3. Le groupe* $\mathrm{Isom}(\mathcal{T})$ *des isométries préservant $\mathcal{T}$ est isomorphe à $\mathfrak{S}_4$.*

Application 65. *La table de caractères de $\mathfrak{S}_4$ est :*

$\mathfrak{S}_4$	Id	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1	1	1	1	1	1
ε	1	-1	1	1	-1
χ	3	1	-1	0	-1
$\varepsilon\chi$	3	-1	-1	0	1
θ	2	0	2	-1	0

Développements

- Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (45,47) [Per96]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (64,65) [Ser70]

Références

[Ulm12] F. Ulmer. *Théorie des groupes.* Ellipses
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[CG13] P. Caldero et J. Germoni. *Histoires Hédonistes de Groupes et de Géométries 1.* Calvage et Mounet
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann