Cadre : G est un groupe, H un sous-groupe de G, et X un ensemble.

I Définitions et premières propriétés

1) Ordre d'un groupe

Définition 1. G est fini si son cardinal est fini. On appelle ordre de G son cardinal, noté $|G| = \mathrm{Card}(G)$.

Théorème 2 (Lagrange)**.** *L'ordre de H est fini et divise $|G|$.*

Définition 3. Si G est fini, l'indice de H dans G est $|G/H|$, noté $[G : H]$.

Remarque 4. *$|G| = [G : H]|H|$, un sous-groupe d'indice 2 est distingué.*

Proposition 5. *Deux groupes finis isomorphes ont même ordre.*

Exemple 6. *Soit $f : G \to G'$ un morphisme, alors $|G| = |\operatorname{Ker} f||\operatorname{Im} f|$.*

Proposition 7. *L'intersection de sous-groupes est un sous-groupe.*

Définition 8. Pour $A \subset G$, le sous-groupe engendré par A, noté $\langle A \rangle$ est le plus petit sous-groupe de G contenant A. C'est l'intersection de tous les sous-groupes de G contenant A.

Définition 9. L'ordre de $a \in G$ est l'ordre de $\langle a \rangle$.

Exemple 10. *$\overline{2}$ est d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.*

Proposition 11. *Soit $a \in G$ d'ordre p, alors $a^q = e \Leftrightarrow p \mid q$.*

Proposition 12. *L'ordre de tout élément de G divise n.*

Corollaire 13. $\forall\, a \in G,\ a^n = e$

Remarque 14. *L'ordre de $a \in G$ est le plus petit $k \in \mathbb{N}^\star$ tel que $a^k = e$.*

2) Action de groupe

Définition 15. Une action de groupes est la donnée d'une application $G \times X \to X$ définie par $(g, x) \mapsto g \cdot x$ telle que :

(i) $\forall\, x \in X,\ e \cdot x = x$

(ii) $\forall\, g_1, g_2 \in G,\ \forall\, x \in X,\ g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$

On dit que G agit sur X.

Proposition 16. *La donnée d'une action de groupe de G sur X est équivalente à la donnée d'un morphisme $G \to S(X)$, où $S(X)$ désigne l'ensemble des bijections de X dans X.*

Exemple 17. *G agit sur lui-même par conjugaison.*

Théorème 18 (Cayley)**.** *Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Définition 19. Si $x \in X$, son orbite est $O_x = \{g \cdot x \,|\, g \in G\}$.

Définition 20. Si $x \in X$, son stabilisateur est $S_x = \{g \in G \,|\, g \cdot x = x\}$.

Proposition 21. *Pour tout $x \in X$, S_x est un sous-groupe de G.*

Proposition 22. *Si G est fini, alors, pour tout $x \in X$, $|G| = |S_x||O_x|$.*

Théorème 23 (Équation aux classes)**.** *On suppose X et G finis. Soit θ une partie X contenant un unique représentant de chaque orbite. Alors :*

$$|X| = \sum_{x \in \theta} |O_x| = \sum_{x \in \theta} \frac{|G|}{|S_x|}$$

Corollaire 24. *Si G est fini, il existe une famille finie $(H_i)_{i \in I}$ de sous-groupes stricts de G telle que :*

$$|G| = |Z(G)| + \sum_{i \in I} \frac{|G|}{|H_i|}$$

où $Z(G)$ est le centre de G.

3) Notion de p-groupe, pour p premier

Définition 25. Un p-groupe est un groupe d'ordre p^α, où $\alpha \in \mathbb{N}^\star$.

Exemple 26. *$|\mathbb{Z}/4\mathbb{Z}| = 2^2$, donc $\mathbb{Z}/4\mathbb{Z}$ est un 2-groupe.*

Proposition 27. *Le centre d'un p-groupe distinct n'est pas trivial.*

Théorème 28 (Cauchy)**.** *Si $p \mid |G|$, alors G a un élément d'ordre p.*

Exemple 29. *$2 \mid 4$, et $\overline{2}$ et d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.*

Définition 30. 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 31. $|GL_n(\mathbb{F}_p)| = p^\alpha m$, *où* $\alpha = \frac{n(n-1)}{2}$ *et* $p \nmid m$, *et* $\{(a_{i,j}) \,|\, a_{i,j} = 0 \text{ si } i > j, a_{i,i} = 1\} \subset GL_n(\mathbb{F}_p)$ *est un p-Sylow.*

Lemme 32. *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 33. *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 34 (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 35. *Soit* $S \in Syl_p(G)$, *alors :* $S \trianglelefteq G \Leftrightarrow |Syl_p(G)| = 1$.

Exemple 36. *Un groupe d'ordre 63 possède un sous-groupe distingué.*

II Groupes remarquables

1) Groupes cycliques

Définition 37. G est monogène s'il existe $a \in G$ tel que $G = \langle a \rangle$.

Définition 38. G est cyclique s'il est monogène et fini.

Proposition 39. *Tout groupe cyclique est abélien.*

Exemple 40. $\mathbb{Z}/n\mathbb{Z}$ *est cyclique.*

Proposition 41. *Si G est cyclique d'ordre n, alors* $G \cong \mathbb{Z}/n\mathbb{Z}$.

Proposition 42. *L'ensemble des racines n-ièmes de l'unité est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Proposition 43. *Si* $|G|$ *est premier, alors G est cyclique, engendré par n'importe quel élément non neutre.*

Proposition 44. *Si G est cyclique, d'ordre n, et engendré par* $a \in G$, *alors :* $G = \langle a^k \rangle \Leftrightarrow k \wedge n = 1$.

Exemple 45. $\overline{1}$, $\overline{5}$, $\overline{7}$ *et* $\overline{12}$ *sont générateurs de* $\mathbb{Z}/12\mathbb{Z}$.

Proposition 46. *Tout sous-groupe d'un groupe cyclique est cyclique.*

2) Groupe symétrique $\mathfrak{S}_n$

Définition 47. On note $\mathfrak{S}_n$ l'ensemble des bijections de $[\![1, n]\!]$ dans $[\![1, n]\!]$. Ses éléments sont appelés permutations.

Proposition 48. $|\mathfrak{S}_n| = n!$

Définition 49. Une transposition est une permutation échangeant deux éléments i et j de $[\![1, n]\!]$ distincts et fixant les autres. On la note $(i\ j)$.

Théorème 50. *Les transpositions engendrent* $\mathfrak{S}_n$.

Définition 51. Un cycle de longueur k est une permutation, notée $\sigma = (a_1\ a_2\ \dots\ a_k)$, où $\sigma(a_i) = \sigma(a_{i+1})$ pour $i \in [\![1, k-1]\!]$, $\sigma(a_k) = a_1$ et qui fixe les autres éléments de $[\![1, n]\!]$.

Corollaire 52. *On a les engendrements suivants :*

(i) $(1\ 2)$, $(1\ 3)$, $\dots$, $(1\ n)$ *engendrent* $\mathfrak{S}_n$.

(ii) $(1\ 2)$, $(2\ 3)$, $\dots$, $((n-1)\ n)$ *engendrent* $\mathfrak{S}_n$.

(iii) $(1\ 2)$ *et* $(1\ 2\ \dots\ n)$ *engendrent* $\mathfrak{S}_n$.

Définition 53. On appelle support d'une permutation σ, noté $\text{supp}(\sigma)$, l'ensemble des éléments de $[\![1, n]\!]$ qui ne sont pas fixés par σ.

Proposition 54. *Deux permutations à support disjoints commutent.*

Proposition 55. *Si* σ *est un cycle de longueur k, alors* $\sigma^k = Id$.

Théorème 56. *Toute permutation se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près.*

Exemple 57. $\left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right) = (1\ 2)(3\ 4) = (3\ 4)(1\ 2)$

Proposition 58. *Soient* $\sigma = (a_1\ a_2\ \dots\ a_k)$ *un cycle d'ordre k et* $\tau \in \mathfrak{S}_n$. *Alors* $\tau\sigma\tau^{-1} = (\tau(a_1)\ \dots\ \tau(a_k))$.

Définition 59. Soit $\sigma \in \mathfrak{S}_n$. On définit la signature de σ par :

$$\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Proposition 60. *La signature possède les propriétés suivantes :*

(i) $\forall\, \sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) \in \{\pm 1\}$

(ii) $\forall\, \sigma, \sigma' \in \mathfrak{S}_n,\ \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$

(iii) Si σ *est un cycle d'ordre k, alors* $\varepsilon(\sigma) = (-1)^{k-1}$.

Définition 61. $\mathfrak{A}_n = \varepsilon^{-1}(\{1\})$ est le groupe alterné.

Définition 62. Un groupe est dit simple si ses seuls sous-groupes distingués sont le sous-groupe trivial et lui-même.

Définition 63. On appelle type de $\sigma \in \mathfrak{S}_n$, notée $[l_1, \dots, l_m]$, la liste des cardinaux des orbites de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ dans l'ordre décroissant.

Exemple 64. *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* $[5]$.

Proposition 65. $\mathfrak{A}_n$ *est engendré par les 3-cycles de* $\mathfrak{S}_n$.

Proposition 66. *Les cycles d'ordre 3 sont conjugués dans* $\mathfrak{A}_n$ *pour* $n \geqslant 5$.

Théorème 67. $\mathfrak{A}_n$ *est simple pour* $n \geqslant 5$.

Remarque 68. *Pour* $n = 4$, $\{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq \mathfrak{A}_n$.

III Théorie des représentations

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

Définition 69. 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 70. 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 71. *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 72. $\rho : g \mapsto Id_V$ *est une représentation de* G *sur* V.

Définition 73. 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 74. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur* G.

Théorème 75. *Le nombre des représentations irréductibles de* G *(à isomorphisme près) est égal au nombre classes de conjugaison de* G.

Théorème 76. *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 77. *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

Proposition 78. *L'application* $\iota : G \to \widehat{\widehat{G}}$ *définie pour* $g \in G$ *par* $\iota(g) : \chi \mapsto \chi(g)$ *est un isomorphisme.*

Proposition 79. G *et* $\widehat{G}$ *ont même exposant.*

Théorème 80. *Il existe un unique entier* ℓ *et une unique suite* $d_\ell | \cdots | d_2 | d_1$ *d'entiers supérieurs à 2 tels que* d_1 *est l'exposant de* G *et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Développements

- Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (65,67) [Per96]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (76,77) [Ser70]
- Structure des groupes abéliens finis (78,79,80) [Col09]

Références

[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Ser70] J.-P. Serre. *Représentations linéaires des groupes finis.* Hermann
[Col09] P. Colmez. *Éléments d'analyse et d'algèbre.* Les éditions de l'École Polytechnique