Cadre : On fixe G un groupe et X un ensemble non vide.

I Définitions et premières propriétés

1) Actions de groupes

Définition 1. 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 2. *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 3. *G agit sur lui-même par translation et par conjugaison.*

Théorème 4 (Cayley)**.** *Si G est fini de cardinal n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Définition 5. L'action de G sur X est dite :

(i) fidèle, si seul le neutre fixe tous les points.

(ii) libre, si tout élément non neutre agit sans point fixe.

(iii) transitive, si : $\forall\, x, y \in X, \exists\, g \in G, y = g \cdot x$.

(iv) n fois transitive, si l'action induite de G sur X^n est transitive.

Remarque 6. *Une action libre est fidèle.*

Exemple 7. *L'action du groupe linéaire sur les droites est transitive mais pas fidèle : les homothéties agissent trivialement.*

Exemple 8. *Une action induit une action fidèle du quotient du groupe par le noyau de l'action.*

Application 9. *Soit G un groupe infini et H un sous-groupe de G, distinct de G et d'indice fini. Alors G n'est pas simple.*

Définition 10. On appelle ensemble des points fixes de X sous l'action de G, ou ensemble des élément G-invariants de X, l'ensemble :

$$X^G = \{x \in X \,|\, \forall\, g \in G, g \cdot x = x\}$$

2) Stabilisateur, orbites, fixateur

Définition 11. Si $x \in X$, son stabilisateur est :

$$\mathrm{Stab}_x = \{g \in G \,|\, g \cdot x = x\}$$

Proposition 12. *Pour tout $x \in X$, Stab_x est un sous-groupe de G.*

Définition 13. Si $x \in X$, son orbite est :

$$O_x = \{g \cdot x \,|\, g \in G\}$$

Proposition 14. *Si G est fini, alors pour tout $x \in X$, $|G| = |\,\mathrm{Stab}_x\,||O_x|$.*

Proposition 15. *L'action de G sur X est dite :*

(i) fidèle, si l'intersection des stabilisateurs est triviale.

(ii) libre, si tous les stabilisateurs sont triviaux.

(iii) transitive, s'il n'y a qu'une seule orbite.

Théorème 16 (Équation aux classes)**.** *On suppose X et G finis. Soit θ une partie X contenant un unique représentant de chaque orbite. Alors :*

$$|X| = \sum_{x \in \theta} |O_x| = \sum_{x \in \theta} \frac{|G|}{|\,\mathrm{Stab}_x\,|}$$

Corollaire 17. *On note $Z(G)$ le centre de G. Si G est fini, il existe une famille finie $(H_i)_{i \in I}$ de sous-groupes stricts de G telle que :*

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

Définition 18. Si $g \in G$, son fixateur est :

$$\mathrm{Fix}_g = \{x \in X \,|\, g \cdot x = x\}$$

Théorème 19 (Burnside)**.** *On suppose G et X finis. Soit Ω l'ensemble des orbites distinctes. Alors :*

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_g\,|$$

Application 20. *Le nombre de colliers de 5 perles différents que l'on peut réaliser avec deux couleurs est 8.*

II Actions sur les groupes finis

1) Cas des p-groupes

Définition 21. Un p-groupe est un groupe d'ordre p^α, où $\alpha \in \mathbb{N}^\star$.

Exemple 22. *$|\mathbb{Z}/4\mathbb{Z}| = 2^2$, donc $\mathbb{Z}/4\mathbb{Z}$ est un 2-groupe.*

Proposition 23. *Le centre d'un p-groupe distinct n'est pas trivial.*

Théorème 24 (Cauchy)**.** *Si $p \mid |G|$, alors G a un élément d'ordre p.*

Exemple 25. *$2 \mid 4$, et $\overline{2}$ et d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.*

Définition 26. 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 27. *$|GL_n(\mathbb{F}_p)| = p^\alpha m$, 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 28. *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 29. *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 30 (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 31. *Soit $S \in Syl_p(G)$, alors : $S \trianglelefteq G \Leftrightarrow |Syl_p(G)| = 1$.*

Exemple 32. *Un groupe d'ordre 63 possède un sous-groupe distingué.*

2) Groupe symétrique

Proposition 33. *Le groupe symétrique $\mathfrak{S}_n$ agit sur $[\![1, n]\!]$ par :*

$$\begin{array}{ccc} \mathfrak{S}_n \times [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ (\sigma, i) & \longmapsto & \sigma(i) \end{array}$$

Remarque 34. *Le stabilisateur d'un point est isomorphe à $\mathfrak{S}_n$.*

Application 35. *Soit $\sigma \in \mathfrak{S}_n$, alors $\langle\sigma\rangle$ agit aussi sur $[\![1, n]\!]$. Soient $F_1, \dots, F_r$ les orbites de $[\![1, n]\!]$ sur l'action de $\langle\sigma\rangle$. On pose :*

$$\sigma_i : \left| \begin{array}{ccc} [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ x & \longmapsto & \begin{cases} x & \text{si } x \notin F_i \\ \sigma(x) & \text{si } x \in F_i \end{cases} \end{array} \right.$$

Les σ_i sont des cycles à support disjoints, d'ordre $|F_i|$, qui commutent et on a $\sigma = \sigma_1 \cdots \sigma_r$.

Exemple 36. *$\mathfrak{S}_n$ agit sur $\mathbb{K}[X_1, \dots, X_n]$, avec $\mathbb{K}$ un corps, par :*

$$\begin{array}{ccc} \mathfrak{S}_n \times \mathbb{K}[X_1, \dots, X_n] & \longrightarrow & \mathbb{K}[X_1, \dots, X_n] \\ (\sigma, P) & \longmapsto & P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) \end{array}$$

Remarque 37. *Ici, $\mathbb{K}[X_1, \dots, X_n]$ n'est pas fini, on ne peut donc pas utiliser l'équation de Burnside. Il y a un nombre infini d'orbites.*

Définition 38. 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 39. *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 40. *Deux permutation de $\mathfrak{S}_n$ sont conjuguées si, et seulement si, elles ont le même type.*

Proposition 41. *$\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.*

Proposition 42. *Les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$ pour $n \geqslant 5$.*

Théorème 43. *$\mathfrak{A}_n$ est simple pour $n \geqslant 5$.*

III Applications

1) Théorie des représentations

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

Définition 44. 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 45. 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 46. *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 47. *$\rho : g \mapsto Id_V$ est une représentation de G sur V.*

Définition 48. 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 49. *Les caractères irréductibles forment une base orthonormale de l'espace vectoriel des fonctions centrales sur G.*

Théorème 50. *Le nombre des représentations irréductibles de G (à isomorphisme près) est égal au nombre classes de conjugaison de G.*

Théorème 51. *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 52. *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

2) Applications aux corps finis

Fixons $\mathbb{K}$ un corps et $n \in \mathbb{N}^\star$.

Définition 53. On pose $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \,|\, \zeta^n = 1\}$ le groupe des racines n-ièmes de l'unité.

Proposition 54. *Tout sous-groupe de $\mathbb{K}^\star$ est cyclique.*

Définition 55. On pose $\mathbb{K}_n$ un corps de décomposition de $X^n - 1 \in \mathbb{K}[X]$. Le groupe $\mu_n(\mathbb{K})$ est cyclique d'ordre n. On note $\mu_n^\star(\mathbb{K})$ l'ensemble des générateurs de $\mu_n(\mathbb{K})$, ses éléments sont les racines primitives n-ièmes de l'unité.

Remarque 56. $|\mu_n^\star(\mathbb{K}_n)| = \varphi(n)$

Définition 57. On définit le n-ième polynôme cyclotomique par :

$$\Phi_{n,\mathbb{K}} = \prod_{\zeta \in \mu_n^\star(\mathbb{K}_n)} (X - \zeta) \in \mathbb{K}[X]$$

Proposition 58. $X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}}$

Proposition 59. *On a $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. De plus, pour $\sigma : \mathbb{Z} \to \mathbb{K}$ le morphisme canonique, on a $\Phi_{n,\mathbb{K}}(X) = \sigma(\Phi_{n,\mathbb{Q}}(X))$. En particulier, $\Phi_{n,\mathbb{F}_p}$ s'obtient à partir de $\Phi_{n,\mathbb{Q}}$ par réduction modulo p.*

Théorème 60 (Wedderburn)**.** *Tout corps fini est commutatif.*

Développements

- Simplicité de $\mathfrak{A}_n$ pour $n \geqslant 5$ (41,42,43) [Per96]
- Table de caractères de $\mathfrak{S}_4$ et isométries du tétraèdre (51,52) [Ser70]

Références

[Per96] D. Perrin. *Cours d'Algèbre.* Ellipses
[Gou94] X. Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e édition
[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