104 : Groupes abéliens et non abéliens finis. Exemples et applications.

Pandou

22 avril 2022

On fixe G un groupe fini.

1 Outils d'étude de groupes finis

1.1 Ordre d'un groupe, ordre d'un élément

Définition 1. *Le cardinal de G est appelé son ordre. Le cardinal d'un élément $x \in G$ est le cardinal du sous-groupe engendré par x.*

Exemples 2 :

- 1 est le seul élément d'ordre 1.
- Dans un groupe fini, tout élément est d'ordre fini.
- Si tous les éléments de G sont d'ordre au plus 2, alors G est abélien et il existe $n \in \mathbb{N}$ tel que $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

Théorème 3 (Lagrange)**.** *Soit H un sous-groupe de G, alors l'ordre de H divise celui de G.*

Remarque 4 : La réciproque est fausse : $SL_2(\mathbb{Z}/3\mathbb{Z})$ est d'ordre 24, mais n'admet pas de sous-groupe d'ordre 12.

Corollaire 5. *Les groupes d'ordre p premier sont tous isomorphes à $\mathbb{Z}/p\mathbb{Z}$.*

1.2 Groupes cycliques

Définition 6. *On dit que G est cyclique s'il est engendré par un seul élément.*

Remarque 7 : Tout groupe cyclique est abélien. La réciproque est bien sûr fausse : $(\mathbb{Z}/2\mathbb{Z})^2$ n'est pas cyclique.

Proposition 8. *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Corollaire 9. *On suppose que G est d'ordre n. Soit a un générateur de G, alors a^k est un générateur de G si, et seulement si, $k \wedge n = 1$.*

1.3 Actions de groupes

Définition 10. *Une action de G sur X est un morphisme de groupes $G \longrightarrow \mathfrak{S}(X)$.*

Théorème 11 (Cayley)**.** *Tout groupe fini d'ordre n se plonge dans $\mathfrak{S}_n$.*

Application 12 : Tout groupe fini d'ordre n se plonge dans un $GL_n(K)$ (peu importe le corps K).

Définition 13. *Soit $G \curvearrowright X$ une action de groupe et $x \in X$. On note*

1. *$G \cdot x = \{g \cdot x, g \in G\} \subset X$ l'orbite de x.*
2. *$G_x = \{g \in G, g \cdot x = x\} \subset G$ le stabilisateur de x.*
3. *$X^G = \{x \in X, \forall g \in G, g \cdot x = x\}$ les points fixes par G.*

Proposition 14. *On a une bijection naturelle*

$$G/G_x \longrightarrow G \cdot x$$

Corollaire 15. *Soit $\mathcal{X}$ un système de représentants de l'action de G sur X, alors*

$$\mathrm{Card}(X) = \sum_{x \in X} \frac{\mathrm{Card}(G)}{\mathrm{Card}(G_x)}$$

Application 16 : En faisant agir G sur lui-même par conjugaison, il existe un nombre fini de sous-groupes H_i de G tels que

$$\mathrm{Card}(G) = \mathrm{Card}\big(Z(G)\big) + \sum_i \frac{\mathrm{Card}(G)}{\mathrm{Card}(H_i)}$$

Définition 17. *Soit p un nombre premier, on dit que G est un p-groupe si son ordre est une puissance de p.*

Proposition 18. *Soit G un p-groupe qui agit sur X. Alors,*

$$\mathrm{Card}(X) = \mathrm{Card}(X^G) \mod (p)$$

Corollaire 19. *Le centre d'un p-groupe est non trivial.*

Application 20 : Un groupe d'ordre p^2 est abélien.

Théorème 21 (Cauchy). *Soit G un groupe fini et p premier qui divise l'ordre de G. Alors, G admet un élément d'ordre p.*

Définition 22. *On suppose que G est d'ordre $n = p^\alpha m$ avec $p \wedge m = 1$, p premier. Un p-Sylow de G est un sous-groupe de G d'ordre p^α.*

Exemple 23 : Dans $GL_n(\mathbb{F}_p)$, le sous-groupe des matrices unitriangulaires est un p-Sylow.

Lemme 24 (de plongement des p-Sylow). *Soit G un groupe d'ordre $n = p^\alpha m$ avec $p \wedge m = 1$ et H un sous-groupe de G. Si S est un p-Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un p-Sylow de H.*

Théorème 25. *Soit G un groupe d'ordre $n = p^\alpha m$ avec $p \wedge m = 1$. On note n_p le nombre de p-Sylow de G.*

1. *G contient toujours au moins un p-Sylow : $n_p \geqslant 1$.*
2. *Les p-Sylow sont tous conjugués. En particulier, n_p divise n.*
3. *$n_p = 1 \mod (p)$ et $n_p | m$.*

Application 26 : Un groupe d'ordre 63 ou 255 n'est jamais simple car ils possèdent un unique p-Sylow.

2 Quelques groupes remarquables

2.1 Groupes abéliens

On suppose que G est un groupe abélien fini.

Théorème 27. *Les groupes abéliens simples sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.*

Définition 28. *L'exposant de G est le plus grand ordre des éléments de G, noté $e(G)$.*

Remarque 29 : L'exposant de G est aussi le ppcm des ordres des éléments de G.

Application 30 : Soit K un corps commutatif, alors tout sous-groupe fini de K^* est cyclique.

Lemme 31. *Soit a un élément d'ordre $e(G)$. Alors, tout élément de $G/\langle a \rangle$ peut être relevé en un élément de G de même ordre.*

Théorème 32. *Il existe des entiers $d_1 | ... | d_k$ uniques tels que*

$$G \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times ... \times (\mathbb{Z}/d_k\mathbb{Z})$$

La suite $(d_1, ..., d_k)$ est appelée suite des invariants de G.

2.2 Groupe symétrique, groupe alterné

Théorème 33. *Les transpositions engendrent $\mathfrak{S}_n$. On peut même prendre la famille $\begin{pmatrix} 1 & i \end{pmatrix}$ pour $2 \leqslant i \leqslant n$.*

Application 34 : Les morphismes $\mathfrak{S}_n \longrightarrow \mathbb{C}^*$ sont le morphisme trivial et la signature.

DEVELOPPEMENT 1

Lemme 35. *Soit φ un automorphisme de $\mathfrak{S}_n$ tel que l'image de toute transposition est une transposition, alors φ est intérieur.*

Théorème 36. *Si $n \neq 6$, alors tout automorphisme de $\mathfrak{S}_n$ est intérieur.*

Remarque 37 : Il existe un automorphisme non intérieur de $\mathfrak{S}_6$.

Théorème 38. *Toute permutation de $\mathfrak{S}_n$ se décompose de façon unique comme produit de cycles à support disjoints.*

Proposition 39. *Deux permutations de $\mathfrak{S}_n$ si, et seulement s'ils ont le même nombre de cycles de même longueur.*

Proposition 40.

Lemme 41. *Si $n \geqslant 5$, les cycles de longueur 3 sont conjugués dans $\mathfrak{A}_n$.*

Théorème 42. *Si $n \geqslant 5$, $\mathfrak{A}_n$ est simple.*

Corollaire 43. *Si $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont 1, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Corollaire 44. *Soit H un sous-groupe de $\mathfrak{S}_n$ d'indice n, alors H est isomorphe à $\mathfrak{S}_{n-1}$.*

Corollaire 45. *Le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.*

2.3 Groupe diédral

Définition 46. *Soit P_n le polygone régulier à n sommets d'un plan affine euclidien, on note D_n le sous-groupe des isométries du plan qui conservent le polygone.*

On supposera dans la suite sur P_n est inscrit dans le cercle unité dont un sommet est 1.

Proposition 47. *D_n est fini et d'ordre $2n$. Il est engendré par la rotation r d'angle $\frac{2\pi}{n}$ et s la symétrie par rapport à (Ox).*

Corollaire 48. *Si $n \geqslant 3$, D_n n'est pas abélien.*

Remarque 49 : D_n contient un sous-groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et à $\mathbb{Z}/2\mathbb{Z}$. Mais, si $n \geqslant 3$, D_n n'est pas isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Théorème 50. *Soit G un groupe engendré par deux éléments r, s tels que*

1. *r est d'ordre n et s est d'ordre 2.*
2. *rs est d'ordre 2.*

Alors, G est isomorphe à D_n.

Remarque 51 : Il y a, à isomorphisme près, 2 groupes d'ordre 8 non abéliens :

$$D_4 \qquad \text{et} \qquad \mathbb{H}_8$$

où Q_8 est le groupe quaternionique.

3 Les groupes linéaires

3.1 Le groupe $PSL_n(k)$

Soit E un k-espace vectoriel de dimension n.

Lemme 52. *Soit $u \in GL(E)$. Si u laisse invariant toutes les droites de E, alors u est une homothétie.*

Proposition 53. *Le centre de $GL(E)$ est l'ensemble des homothéties qui est isomorphe à k^*.*
Le centre de $SL(E)$ est isomorphe à $\mu_n(k)$: l'ensemble des racines n-ième de l'unité.

Théorème 54.
- *$SL_n(k)$ est engendré par les transvections.*
- *$GL_n(k)$ est engendré par les transvections et les dilatations.*

Proposition 55. *Si $n \geqslant 3$, deux transvections sont conjuguées dans $SL(E)$.*

Théorème 56. *Si $n \geqslant 3$, alors $PSL_n(k)$ est simple.*

Proposition 57. *Dans $SL_2(k)$, toute transvection est conjugué à une matrice $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ avec $\lambda \in k^*$.*
$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjugués dans $SL_2(k)$ si, et seulement si, $\dfrac{\lambda}{\mu}$ est un carré dans k^*.

Lemme 58. *Soit N un sous-groupe distingué de $SL_2(k)$ contenant $\mu_2(k)$. Alors, il existe $g \in N$ qui admet une valeur propre.*

Théorème 59. *$PSL_2(k)$ est simple sauf si $k = \mathbb{F}_2$ et si $k = \mathbb{F}_3$.*

3.2 Étude approfondie de $SL_2(\mathbb{F}_3)$

DEVELOPPEMENT 2

Théorème 60. *On a les isomorphismes suivants :*
1. *$GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.*
2. *$PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ et $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$.*
3. *$PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$.*
4. *$PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ et $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.*

Proposition 61. *L'unique 2-Sylow de $SL_2(\mathbb{F}_3)$ est isomorphe à $\mathbb{H}_8$.*

Application 62 : $\mathrm{Aut}(\mathbb{H}_8) \simeq \mathfrak{S}_4 \simeq PGL_2(\mathbb{F}_3)$.

Proposition 63.

$$GL_2(\mathbb{F}_3)/\mathbb{H}_8 \simeq \mathfrak{S}_3$$

Théorème 64.

$$\mathrm{Aut}\big(SL_2(\mathbb{F}_3)\big) \simeq \mathfrak{S}_4 \qquad \textit{et} \qquad \mathrm{Aut}\big(GL_2(\mathbb{F}_3)\big) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$$

4 Représentation d'un groupe fini

4.1 Généralités

Définition 65. *Une représentation linéaire de G est un morphisme $\rho : G \longrightarrow GL(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension finie.*
La dimension de V est le degré de la représentation.

Exemples 62 : Soit ρ_V et ρ_W deux représentations de G.
- Alors on a une représentation sur $V \oplus W$ définie par
$$g \cdot (v, w) = g \cdot v + g \cdot w$$
- Alors, on a une représentation sur $\mathrm{End}(V, W)$ définie par
$$\forall x \in V, g \cdot f(x) = g \cdot \big(f(g^{-1} \cdot x)\big)$$
- On a une représentation sur $V^* = \mathrm{End}(V, K)$.

Définition 63. *On dit que (ρ, V) et (ρ', V') sont isomorphes s'il existe un isomorphisme $\tau : V \longrightarrow V'$ tel que pour tout $g \in G$, le diagramme suivant est commutatif :*

$$\begin{array}{ccc} V & \xrightarrow{\ \tau\ } & V' \\ \downarrow{\scriptstyle \rho(g)} & & \downarrow{\scriptstyle \rho'(g)} \\ GL(V) & \longrightarrow & GL(V') \end{array}$$

Un endomorphisme u tel que le diagramme est commutatif est appelé morphisme de représentations, on note $\mathrm{Hom}_G(V, W)$ l'ensemble des morphismes de représentations.

Définition 64. *Une sous-représentation de (ρ, V) est la donnée d'un sous-espace W stable par l'action de G.*
On dit que (ρ, V) est irréductible si les seuls sous-représentations de V sont $\{0\}$ et V.

Proposition 65. *Soit N un sous-groupe distingué de G. Soit ρ une représentation de G/N sur U. Alors, il existe une représentation canonique de G telle que les sous-représentations de U sous l'action de G/N soit exactement celles de U.*

Théorème 66. *Toute représentation est somme directe de représentations irréductibles.*

Lemme 67 (Schur). *Soit (ρ, V) et (ρ', W) deux représentations et $f \in \mathrm{Hom}_G(V, W)$.*
- *Si V et W ne sont pas isomorphes, alors $f = 0$.*
- *Si $f \neq 0$, alors f est un isomorphisme et les deux représentations sont isomorphes.*

4.2 Tables de caractères

Définition 68. *Soit (ρ, V) une représentation de G, on définit son caractère par :*

$$\chi_V : g \in G \longmapsto \mathrm{Tr}\big(\rho(g)\big)$$

Proposition 69. *Soit (ρ, V) une représentation.*
- $\chi_V(g) = \dim(V) \Longleftrightarrow g = 1$.
- $\forall g \in G, \chi_V(g^{-1}) = \overline{\chi_V(g)}$.
- $\chi_{V\oplus W} = \chi_V + \chi_W$.
- $\chi_{\mathrm{End}(V,W)} = \overline{\chi_V}\chi_W$.

Définition 70. *Soit $(\chi_i)_{1\leqslant i\leqslant p}$ l'ensemble des caractères irréductibles associé à des représentations distinctes et $(\mathcal{C}_j)_{1\leqslant j\leqslant q}$ l'ensemble des classes de conjugaison de G.*
La table de caractères est un tableau $\big(\chi_i(\mathcal{C}_j)\big)_{i,j}$.

Théorème 71 (Admis)**.** *La table de caractères est carrée : $p = q$.*

Proposition 72. *Les colonnes de la table de caractères sont orthogonales. Plus précisément :*

$$\sum_i \chi_i(\mathcal{C}_j)\chi_i(\mathcal{C}_k) = \begin{cases} \dfrac{|G|}{|\mathcal{C}_j|} & si\ \mathcal{C}_j = \mathcal{C}_k \\ 0 & sinon \end{cases}$$

Définition 73. *Soit (ρ, V) une représentation de caractère χ_V. Le noyau de la représentation est le sous-groupe distingué de G défini par*

$$K_V = \{g \in G, \chi_V(g) = \chi_V(1)\}$$

Théorème 74. *Les sous-groupes distingués de G sont exactement de la forme $\bigcap_{i\in I} K_{\chi_i}$ où les χ_i est une famille de représentations irréductibles non isomorphes.*

Corollaire 75. *G est simple si, et seulement si, $\forall i \neq 1, \forall g \in G, \chi_i(g) \neq \chi_i(1)$, où χ_1 est la représentation triviale.*

Références :

- Gourdon, Algèbre.
- FGN Algèbre 2.
- Mneimé, Éléments de géométrie.
- Calais, Éléments de théorie des groupes.
- Combes, Algèbre et géométrie.
- Serre, Représentations linéaires des groupes finis.
- Perrin, Cours d'algèbre.
- Peyré, L'algèbre de la transformation de Fourier discrète.