Leçon 104 Groupes abéliens et non abéliens fini, exemples et applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Eléments d'analyse et d'algèbre de Pierre Colmez
3. Cours d'algèbre de Daniel Perrin
4. Eléments de théorie des groupes de Josette Calais
5. Représentations linéaires des groupes finis
6. Algèbre discrète de la transformation de Fourier de Gabriel Peyré

Développements.

1. Théorème de structure des groupes abéliens finis
2. Théorèmes de Sylow
3. Table des caractères de S_4

Table des matières

1 Groupes abéliens finis

1.1 Cas des groupes cycliques

(Chapitres 1.4 et 1.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 0.3.1 de Eléments d'analyse et d'algèbre de Pierre Colmez)

On considère G un groupe.

1. Définition : On dit que G est monogène s'il existe $g \in G$ tel que $\langle g \rangle$, si de plus G est fini alors on dit que G est cyclique
2. Exemple : $\mathbb{Z} = \langle 1 \rangle$ n'est pas cyclique
3. Exemple : Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est cyclique
4. Proposition : Si G est cyclique alors G est abélien
5. Théorème : Si $G = \langle g \rangle$ est cyclique d'ordre n alors ses générateurs sont les g^k avec $k \in [\![1, n-1]\!]$ premier avec n
6. Corollaire : Le nombre de générateurs de G est égal à $\varphi(n)$
7. Exemple : Si n premier alors le nombre de générateurs de Γ_n est $n-1$
8. Théorème : Un groupe de cardinal premier est cyclique, et un groupe de cardinal pq avec p, q premiers entre eux est cyclique
9. Remarque : Si p, q ne sont pas premiers entre eux alors G n'est pas nécessairement cyclique
10. Exemple : $|S_3| = 6 = 3 \times 2$ n'est pas cyclique, $(\mathbb{Z}/\mathbb{Z})^2$ n'est pas cyclique
11. Théorème : Si $G = \langle g \rangle$ cyclique alors les sous-groupes de G sont cycliques d'ordre divisant n et pour tout diviseur d de n il existe un unique sous-groupe de G d'ordre d, il s'agit de $\langle a^{\frac{n}{d}} \rangle$
12. Exemple : Si n pair alors $\mathbb{U}_{\frac{n}{2}}$ est un sous-groupe cyclique de $\mathbb{U}_n$ et est engendré par $e^{\frac{4i\pi}{n}}$

1.2 Structure des groupes abéliens finis

(Chapitres 1.5 et 1.9 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 0.3.2 et I.2.5 de Eléments d'analyse et d'algèbre de Pierre Colmez)

On considère un groupe abélien fini G.

1. Théorème de Cauchy : Soit p diviseur premier de n, alors il existe $g \in G$ d'ordre p
2. Remarque : Si G non cyclique et d diviseur quelconque de n alors il n'existe pas nécessairement d'élément d'ordre d dans G
3. Exemple : Dans $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ il n'existe pas d'élément d'ordre 4
4. Définition : L'exposant de G est l'entier $N(G) = PPCM(o(g), g \in G)$
5. Exemple : Si $G = \mathbb{Z}/9\mathbb{Z}$ alors $N(G) = 3$
6. Définition : Un caractère de G est un morphisme de groupe de G dans $\mathbb{C}^*$, et on note $\hat{G}$ l'ensemble des caractères sur G

7. Exemple : Le morphisme $g \in G \longmapsto 1 \in \mathbb{C}^*$ est la caractère trivial
8. Proposition : Soit H sous-groupe de G et χ caractère de H, alors χ peut se prolonger en un caractère sur G
9. Lemme : $\hat{G}$ est un groupe et G et $\hat{\hat{G}}$ sont isomorphismes
10. Proposition : G et $\hat{G}$ ont le même exposant
11. Théorème : Il existe $g \in G$ d'ordre $N(G)$
12. Théorème de structure des groupes abéliens finis : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ...\mathbb{Z}/d_r\mathbb{Z}$ avec $d_{i+1} \mid d_i$

2 Etude de groupes non abéliens finis

2.1 Groupes symétriques et alternées

(Chapitres 0.3.4 de Eléments d'analyse et d'algèbre de Pierre Colmez, 2 d'Algèbre et géométrie de Jean-Etienne Rombaldi et I.8 du Cours d'algèbre de Daniel Perrin)

On considère S_n l'ensemble des permutations de $[\![1, n]\!]$.

1. Proposition : S_n est un groupe non abélien d'ordre $|S_n| = n!$
2. Exemple : Soit $(12), (13) \in S_3$, alors $(12)(23) = (231) \neq (213) = (23)(12)$
3. Proposition : Soit $\sigma, \sigma' \in S_n$ tels que $Supp(\sigma) \cap Supp(\sigma') = \varnothing$, alors $\sigma \circ \sigma'$
4. Théorème : Soit $\sigma \in S_n \backslash \{id\}$, alors σ se décompose en produits de cycles à supports disjoints et de manière unique à l'ordre près des facteurs
5. Exemple : $(12456)(1579) = (16)(24579) = (24579)(16)$
6. Théorème : Toute permutation se décompose en produit de transpositions
7. Corollaire : Si $n \geq 3$ alors les trois cycles engendrent A_n
8. Théorème : Si $n \geq 5$ alors les sous groupes distingués de S_n sont $\{id\}, A_n, S_n$
9. Remarque : Dans S_4 il y aussi V_4 le groupe des doubles transpositions
10. Théorème : Si $n \geq 5$ alors A_n est simple, ie n'admet pas de sous-groupes distingués non triviaux
11. Théorème de Cayley : Soit G un groupe fini alors G est isomorphe à un sous-groupe de S_n
12. Application : Tout groupe fini est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$

2.2 Groupes diédraux

(Chapitres III.3 de Eléments de théorie des groupes et 3.4.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Définition : On dit que G est de type D_{2n} s'il est dicyclique engendré par un élément r d'ordre n et un élément s d'ordre 2 tel que $rsrs = 1$
2. Théorème : Si G de type D_{2n} alors $G = \{id, r, ..., r^{n-1}\} \cup \{s, sr, ..., sr^{n-1}\}$
3. Corollaire : Les groupes de type D_{2n} sont isomorphes

4. Exemple : Dans le plan la rotation d'angle $\frac{2\pi}{n}$ et la réflexion d'axe $\mathbb{R}e_1$ engendrent un groupe $\langle r, s\rangle$ de type D_{2n}
5. Définition : On note Γ_n l'ensemble des sommets d'un polygone régulier à n côtés et $Is(\Gamma_n)$ le groupe des isométries conservant Γ_n
6. Théorème : Avec les notations de l'exemple précédent, on a $Isom(\Gamma_n) = \langle r, s\rangle$, donc $Isom(\Gamma_n)$ est un groupe de type D_{2n}
7. Exemple : S_3 est isomorphe au groupe du triangle équilatéral, donc S_3 est de type D_6

2.3 Groupe des isométries du cube

(Chapitre 3.4.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi, VIII.2.2 d'Algèbre discrète de la transformation de Fourier de Gabriel Peyré)

1. Définition : On considère C l'enveloppe convexe des sommets $A_1 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, ..., A_8 = -A_2$, ie le cube dans l'espace vectoriel euclidien $\mathbb{R}^3$, et $Isom(C)$ le groupe des isométries de $\mathbb{R}^3$ qui conservent ce cube
2. Théorème : Le groupe $Isom(C)$ est aussi le groupe $Isom(S)$ des isométries qui convervent les sommets de ce cube, il est isomorphe à S_8
3. Proposition : Soit A_k un sommet du cube, alors l'orbite de A_k sous l'action de $Isom^+(S) := Isom(S) \cap SL_3(\mathbb{R})$ est $Orb_{Isom^+(\mathbb{R})}(A_k) = S$, autrement dit l'action de $Isom^+(S)$ sur S est transitive
4. Lemme : Soit une rotation $\varphi \in SO(\mathbb{R}^3)$, alors φ est uniquement déterminée par l'image de deux sommets
5. Proposition : Soit A_k un sommet de C, alors $Stab_{Isom^+(\S)}(A_k)$ est sous-groupe d'ordre 3 de $Isom^+(S)$
6. Exemple : La rotation de matrice $\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$ engendre $Stab_{Isom^+(S)}(A_1)$
7. Théorème : $Isom(S)$ agit transitivement sur S et a 48 éléments
8. Corollaire : $Isom^+(S)$ est isomorphe à S_4 et $Isom(S)$ à $S_4 \times \mathbb{Z}/2\mathbb{Z}$

3 Théorèmes de Sylow et classification des groupes finis

3.1 Théorèmes de Sylow

(Chapitre 1.5 du Cours d'algèbre de Daniel Perrin)

On considère G groupe fini de cardinal $n = p^\alpha m$ avec p diviseur premier de n tel que $p \wedge m = 1$.

1. Définition : Soit H sous-groupe de G, alors on dit que H est un p-sous groupe de Sylow de G si $|H| = p^\alpha$

2. Autrement dit H est un p-groupe est $[G : H]$ est premier avec p
3. Exemple : Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $G = GL_n(\mathbb{F}_p)$, alors $|GL_n(\mathbb{F}_p)| = (p^n - 1)...(p^n - p^{n-1}) = mp^{\frac{n(n-1)}{2}}$ avec $p \wedge m = 1$, et le sous-groupes des matrices triangulaires supérieures de diagonale unitaire est un p-sous groupe de Sylow de G
4. Lemme : Soit H un sous-groupe de G et S un p-sous groupe de Sylow de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-sous groupe de Sylow de H
5. Théorème de Sylow (premier) : G contient au moins un p-sous groupe de Sylow
6. Théorème de Sylow (second) : Soit H p-sous-groupe de G, alors H est inclus dans un p-sous groupe de Sylow de G, de plus les p-sous groupes de Sylow sont tous conjugués et leur nombre k vérifie $k \mid n, k \equiv 1[p]$
7. Corollaire : Soit S un p-sous groupe de Sylow de G, alors $S \triangleleft G$ si et seulement si S est l'unique p-sous groupe de Sylow de G

3.2 Conséquences sur les groupes finis d'un cardinal donné

(Chapitre VI.2 de Eléments de théorie des groupes de Josette Calais)

1. Théorème : Si $|G| = pq$ avec p, q premiers distincts tels que $q \neq 1[p]$ alors G admet un unique p-sous groupe de Sylow
2. Exemple : S_3 admet un unique 3-sous groupe de Sylow, il s'agit du groupes des 3-cycles
3. Théorème : Si G simple non abélien et p diviseur premier de $|G|$ alors le nombre k de p-sous groupes de Sylow de G vérifie $k > 1$
4. Corollaire : Si G simple et p diviseur premier de $|G|$ tel que G admette un unique p-sous-groupe de Sylow alors G est abélien
5. Proposition : Si $|G| = pq$ avec p, q premiers distincts, alors G n'est pas simple
6. Proposition : Si $|G| = pq$ avec p, q premiers distincts tels que $p \neq 1[q], q \neq 1[p]$ alors G est cylique
7. Théorème : Soit p nombre premier impair, si $|G| = 2p$ alors $G \simeq \mathbb{Z}/2p\mathbb{Z}$ ou $G \simeq D_{2p}$

4 Représentations et caractères linéaires des groupes finis

4.1 Définitions et résultats importants

(Chapitre 6 d'Algèbre et géométrie de Rombaldi)

1. Définition : Une représentation linéaire de G est un couple (ρ, V) avec V un $\mathbb{C}$-espace vectoriel de dimension finie et $\rho : G \longrightarrow GL(V)$ un morphisme de groupes, et un caractère linéaire est une application de la forme $\chi = tr \circ \rho$
2. Exemple : $(1, \mathbb{C})$ est la représentation triviale de G et $\chi_1 = 1$
3. Exemple : La représentation régulière de G est $(\rho_r, \mathbb{C}^n)$ avec $\rho_r(g)(e_k) = e_{gk}$ et $(e_k)_{k \in G}$ base de $\mathbb{C}^n$

4. Définition : On dit que (ρ, V) est une représentation irréductible si les seuls sous-espaces de V invariants par l'action de G sont $\{0\}$ et V
5. Exemple : $(1, \mathbb{C})$ est irréductible et $(\rho_r, \mathbb{C}^n)$ ne l'est pas car $Vect\left(\sum_{k\in G} e_k\right)$ est G-invariant
6. Lemme de Schur : Soit (ρ_1, V_1) et (ρ_2, V_2) deux représentations irréductibles de G, alors si V_1 et V_2 ne sont pas isomorphes alors il n'existe pas de morphismes u de V_1 dans V_2 tels que $u \circ \rho_1(g) = \rho_2(g) \circ u$, et sinon l'espace vectoriel de tels morphismes est de dimension 1
7. Proposition : Un caractère prend les mêmes valeurs dans une classe de conjugaison
8. Théorème de Mashke : Soit (ρ, V) une représentation de G, alors (ρ, V) est somme de sous-représentations irréductibles
9. Théorème : Les caractères irréductibles de G forment une base orthonormée des fonctions centrales muni de $\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\varphi(g)}\psi(g)$, de plus leur nombre est égal au nombre de classes de conjugaison de G
10. Théorème : Un caractère linéaire est irréductible si et seulement si $\langle \chi, \chi \rangle = 1$

4.2 Conséquences sur les caractéristiques des groupes finis

(Chapitre 6 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Théorème : $|G| = \sum_{k=1}^{p} (dim(V_k))^2$ avec $V_1, ..., V_p$ les représentations des caractéres irréductibles de G
2. Théorème : G est abélien si et seulement si toutes ses caractères irréductibles sont de degré 1
3. Définition : Le noyau d'un caractère χ de degré d est $ker(\chi) = \{g \in G, \chi(g) = d\}$
4. Proposition : Les sous-groupes distingués de G sont des intersections de noyaux de caractères linéaires irréducibles
5. Théorème : La table de caractères de S_4 est donnée en annexe
6. Application : On peut observer en annexe la table de caractères irréductibles de S_4 et en déduire que les sous-groupes distingués de S_4 sont $\{id\}, V_4, A_4, S_4$, et aussi que S_4 n'est pas abélien