Leçon 103 Conjugaison dans un groupe, exemples de sous-groupes distingués et de groupes quotients, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Cours d'algèbre de Daniel Perrin
2. Théorie des groupes de Félix Ulmer
3. Algèbre de Xavier Gourdon
4. Algèbre et géométrie de Jean-Etienne Rombaldi
5. Exercices d'algèbre de Pascal Ortiz
6. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
7. Eléments de théorie des groupes de Josette Calais

Développements.

1. Simplicité du groupe alterné A_n
2. Simplicité de $SO_3(\mathbb{R})$ par une partie génératrice
3. Théorèmes de Sylow

Table des matières

1 Action par conjugaison dans un groupe

1.1 Conjugaison et classe de conjugaison

(Chapitre I.4 du Cours d'algèbre de Daniel Perrin)
On considère une groupe G.

1. Définition : L'action par conjugaison de G sur lui même est définie par $g.a = gag^{-1}$
2. Définition : Les orbites sous cette action s'appellent les classes de conjugaison $Orb_G(a) = Cl(a) = \{gag^{-1}, g \in G\}$
3. Exemple : Si G est abélien alors $Cl(a) = \{a\}$
4. Définition : Les stabilisateurs de cette action s'appellent les centralisateurs $Stab_G(a) = H_a = \{g \in G, gag^{-1} = a\}$
5. Exemple : Si G est abélien alors $\forall a \in G, H_a = G$
6. Définition : Le centralisateur d'une partie $A \subset G$ est $C_G(A) = \{g \in G, \forall a \in A, ga = ag\}$
7. Exemple $C_G(G) = Z(G)$ est le centre de G

1.2 Classes de conjugaison dans le groupe symétrique

(Chapitres I.4 du Cours d'algèbre de Daniel Perrin et 5.1 et 5.2 de Théorie des groupes de Félix Ulmer)

1. Proposition : Soit $\sigma = (i_1, ..., i_p) \in S_n$ un p-cycle et $\tau \in S_n$ alors $\tau\sigma\tau^{-1} = (\tau(i_1), ..., \tau(i_p))$
2. Corollaire : Dans S_n tous les p-cycles sont conjugués ie dans la même classe de conjugaison
3. Lemme : Le groupe A_n agit $n-2$-transitivement sur $[\![1, n]\!]$, ie pour $(a_1, .., a_{n-2})$ distincts et $(b_1, ..., b_{n-2})$ distincts dans $[\![1, n]\!]^{n-2}$, il existe $\sigma \in A_n$ tel que $\forall i \in [\![1, n-2]\!], \sigma(a_i) = b_i$
4. Théorème : Si $n \geq 5$ alors les 3-cycles sont conjugués dans A_n
5. Théorème : Toute permutation peut se décomposer de façon unique (à l'ordre près des facteurs) en produit de cycles à supports disjoint
6. Définition : Soit $\sigma \in S_n$ et $\sigma = \tau_1 \circ ... \circ \tau_r$ sa décomposition en produit de cycles à supports disjoints, alors le type de σ est la liste $[l_1, ..., l_r]$ des cardinaux des orbites dans $[\![1, n]\!]$ de l'action de $\langle\sigma\rangle$ sur $[\![1, n]\!]$ (rangés par ordre croissant)
7. Remarque : Soit $\sigma \in S_n$ de type $[l_1, ..., l_r]$, alors $\sigma = \tau_1 \circ ... \circ \tau_r$ produit de cycles à supports disjoins de longueurs l_i (en comptant les 1-cycles)
8. Exemple : Le type de $(123)(45)$ dans S_6 est $[1, 2, 3]$
9. Théorème : Deux permutations sont conjugués, ie dans la même classe de conjugaison, si et seulement si elles sont de même types
10. Exemple : Dans S_4 on a 5 classes de conjugaison : celle de id, celle de (12), celle de (123), celle de (1234) et celle de $(12)(34)$

1.3 Classes de conjugaison dans $End(E)$

(Chapitre B d'Algèbre de Xavier Gourdon)
On considère E un K-espace vectoriel de dimension finie n et $u \in End(E)$.

1. Définition : Soit $x \in E$, alors π_x est le polynôme unitaire tel que $(\pi_x) = \{P \in K[X], P(u)(x) = 0\}$ et $E_x = \{P(u)(x), P \in K[X]$
2. Proposition : Soit $x \in E$, alors E_x est sous-espace de E de dimension $deg(\pi_x)$ et de base $(x, ..., u^{deg(\pi_x)-1})$
3. Théorème : Il existe $x \in E$ tel que $\pi_x = \pi_u$
4. Définition : On dit que u est cyclique s'il existe $x \in E$ tel que $E_x = E$
5. Définition : Soit $P = X^p + a_{p-1}X^{p-1} + ... + a_0 \in K[X]$, alors on note $C(P)$ sa matrice compagnon
6. Proposition : Soit $P \in K[X]$, alors $\pi_{C(P)} = \chi_{C(P)} = P$
7. Théorème : Si u cyclique alors il existe une base b de E tel que $Mat_b(u) = C(\pi_u)$
8. Théorème : Il existe $F_1, ..., F_r$ sous-espaces de E stables par u tels que $E = F_1 \otimes ... \otimes F_r$, $u_i := u_{|F_i}$ cyclique et $P_i := \pi_{u_i} \mid P_{i-1}$
9. Remarque : La suite des polynômes P_i ne dépend que de u, et est est appelée les invariants de similitude de u
10. Théorème de réduction de Frobenius : Il existe une base b de E telle que $Mat_b(u) = diag(C(P_1), ..., C(P_r))$
11. Corollaire : Deux endomorphismes sont semblables, ie dans la même classe d'équivalence, si et seulement s'ils ont les mêmes invariants de similitude

2 Sous-groupes stables par conjugaison

2.1 Les sous-groupes distingués

(Chapitres I.2 du Cours d'algèbre de Daniel Perrin, Exercices I.B du Cours d'algèbre de Daniel Perrin, 1.1 d'Algèbre et géométrie de Jean-Etienne Rombaldi et 6 de Théorie des groupes de Félix Ulmer)
On considère H un sous-groupe de G.

1. Définition : On dit que H est distingué (ou normal) si $\forall g \in G, \forall h \in H, ghg^{-1} \in H$, dans ce cas on le note $H \triangleleft G$
2. Remarque : Autrement dit H est stable par l'action par conjugaison
3. Exemple : $\{1\}, G$ sont distingués dans G
4. Proposition : Si G est abélien alors $H \triangleleft G$
5. Proposition : Soit $H' \triangleleft G$, si $H \triangleleft G$ alors $H \cap H' \triangleleft G$
6. Théorème : Soit $f : G \longrightarrow G'$ morphisme de groupes et $H' \triangleleft G'$ alors $f^{-1}(H') \triangleleft G$
7. Corollaire : En particulier $ker(f) \triangleleft G$
8. Exemple : $SL_n(K) = ker(det) \triangleleft GL_n(K), A_n = ker(\varepsilon) \triangleleft S_n$

9. Proposition : Si $K < H < G$ et $K \triangleleft G$ alors $K \triangleleft H$
10. Remarque : Si $K \triangleleft H \triangleleft G$ alors on a non nécessairement $K \triangleleft G$
11. Exemple : $\{id, (12)(34)\} \triangleleft V_4 \triangleleft S_4$ mais $\{id, (12)(34)\}$ n'est pas distingué dans S_4

2.2 Exemples du centre d'un groupe et du groupe dérivé

(Chapitre I.3 du Cours d'algèbre de Daniel Perrin)

1. Définition : Le centre de G est $Z(G) := \{a \in G, \forall g \in G, ag = ga\}$
2. Proposition : $Z(G) \triangleleft G$
3. Remarque : $Z(G)$ est même un sous-groupe caractéristique de G, ie invariant pour tout automorphisme de G
4. Exemple : Si G est abélien alors $Z(G) = G$
5. Exemple : Si $G = S_n$ et $n \geq 3$ alors $Z(G) = \{id\}$
6. Définition : Un commutateur est un élément de la forme $xyx^{-1}y^{-1}$ avec $x, y \in G$
7. Définition : Le groupe dérivé de G est $D(G)$ le sous-groupe de G engendré par les commutateurs de G
8. Proposition : $D(G) \triangleleft G$
9. Remarque : $D(G)$ est même un sous-groupe caractéristique de G
10. Exemple : Si G est abélien alors $D(G) = \{1\}$
11. Exemple : Si $G = S_3$ alors $D(G) = \{1, \sigma, \sigma^2\}$

2.3 Lien avec les groupes quotients

(Chapitre 6 de Théorie des groupes de Félix Ulmer)

1. Définition : L'ensemble quotient G/H est l'ensemble des classes d'équivalences pour la relation $g \sim g'$ si $gg'^{-1} \in H$
2. Proposition : Si $H \triangleleft G$ alors G/H est un groupe pour la loi $gH \times g'H = gg'H$
3. Corollaire : $\pi : G \longrightarrow G/H$ est un morphisme de groupes surjectif de noyau H
4. Corollaire : $|G/H| = [G : H]$ et si G est fini alors $|G/H| = \frac{|G|}{|H|}$
5. Exemple : $n\mathbb{Z} \triangleleft \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ groupe cyclique d'ordre n
6. Exemple : $A_n = ker(\varepsilon) \triangleleft S_n$ (et d'indice 2), $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$
7. Théorème : Propriété universelle du quotient : Soit G' un groupe et $\varphi; G \longrightarrow G'$ un morphisme de groupes, si $H \triangleleft G$ alors les assertions suivantes sont équivalentes :
   — $H \subset ker(\varphi)$
   — $\varphi(H) = \{1\}$
   — Le morpphisme φ se factorise à travers G/H, ie il existe un morphisme de groupes $\overline{\varphi} : G/H \longrightarrow G'$ tel que $\varphi = \overline{\varphi} \circ \pi$

   Dans ce cas $\overline{\varphi}$ est unique, donné par $\overline{\varphi}(gH) = \varphi(g)$, $Im(\overline{\varphi}) = Im(\varphi)$ et $ker(\overline{\varphi}) = ker(\varphi)/H$

8. Théorème : $G/D(G)$ est abélien, appelé abélianisé de G
9. Théorème : $D(G) \subset H$ si et seulement si $H \triangleleft G$ et G/H abélien
10. Théorème : Premier théorème d'isomorphisme : Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes, alors il existe un isomorphisme $\overline{\varphi} : G/ker(\varphi) \longrightarrow Im(\varphi)$
11. Corollaire : Si G cyclique d'ordre n alors $G \simeq \mathbb{Z}/n\mathbb{Z}$
12. Théorème : Troisième théorème d'isomorphisme : Soit $K \subset H \subset G$ trois groupes tels que $K, H \triangleleft G$, alors $(G/K)/(K/H) \simeq G/H$
13. Exemple : $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$

3 Groupes remarquables sans sous-groupes distingués

3.1 Les groupes simples

(Chapitre 5.3 de Théorie des groupes de Félix Ulmer et II.3 et II.4 de H2G2 tome 1 de Caldero et Germoni)

1. Définition : On dit que G est un groupe simple si $\forall H \triangleleft G, H \in \{\{1\}, G\}$
2. Exemple : Soit $p \in \mathbb{N}$ premier, alors $\mathbb{Z}/p\mathbb{Z}$ est simple
3. Lemme : Soit $N \triangleleft A_n$, si N contient un 3-cycles alors $N = A_n$
4. Théorème : Si $n \geq 5$ alors A_n est un groupe simple
5. Remarque : A_1, A_2, A_3 sont simples
6. Remarque : A_4 n'est pas simple car $V_4 \triangleleft A_4$
7. Lemme : $SO_3(\mathbb{R})$ est connexe
8. Lemme : Soit $N \triangleleft SO_3(\mathbb{R})$, si N contient un renversement alors $N = SO_3(\mathbb{R})$
9. Théorème : $SO_3(\mathbb{R})$ est un groupe simple

3.2 Outil pour le déterminer : les théorèmes de Sylow

(Chapitres I.4 et I.5 du Cours d'algèbre de Daniel Perrin et VI.2 de Eléments de théorie des groupes de Josette Calais)

1. Définition : On dit que G est un p-groupe si $|G| = p^\alpha$ et p premier
2. Lemme : Si G est un p-groupe agissant sur un ensemble X et X^G l'ensemble des points fixes de cette action alors $|X| \equiv |X^G|[p]$
3. Théorème : Si G p-groupe alors $Z(G) \neq \{1\}$
4. Définition : Soit $H < G$, alors on dit que H est un p-Sylow de G si $|H| = p^\alpha$ avec $|G| = p^\alpha m$ et $m \wedge p = 1$
5. Exemple : $T_n^{+1}(\mathbb{F}_|)$ est un p-Sylow de $GL_n(\mathbb{F}_p)$
6. Lemme : Si $|G| = p^\alpha m$, $H < G$ et S un p-Sylow de G alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H
7. Théorème de Sylow (premier) : G contient au moins un p-sous groupe de Sylow

8. 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 $k \mid n, k \equiv 1[p]$
9. 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
10. Proposition : Un groupe d'ordre 63 n'est pas simple
11. Proposition : Si $|G| = pq$ avec p, q premiers distincts, alors G n'est pas simple