

[Ber]
[Ulm]
[R]

103- Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications

I- Conjugaison dans un groupe [Ber] 131-132 [Ulm] 24-25
126 33-34 19

- def conjugaison, action, classe de conjugaison, centralisateur
- ex groupes abéliens, A, B semblables
- def centre
- automorphisme intérieur
- def classe à gauche
- Th Lagrange
- applications: $\alpha(g) | G|$
- $|G| = |Z(G)| + \sum_{i=1}^r |G/H_i|$
- app: G p groupe $Z(G) \neq \{e\}$

II- Sous-groupes distingués, Groupe quotients

1) Sous-groupes distingués [Ber] 135-136
139-140

- def
- ex $Z(G) \trianglelefteq G, D(G)$
- Th $\text{Ker } \varphi \trianglelefteq G$ + ex $S_n(K), A_n$
- def simple

2) Groupes quotients [Ulm] 58 63 [Ber] 241

- Th structure groupe G/H
- ex $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ donc $(\mathbb{Z}/n\mathbb{Z}, +)$ groupe
- Th d'isomorphisme + ex $G/Z(G) \cong \text{Int}(G), \mathbb{R}/2\pi\mathbb{Z} \cong U$

III- Applications

1) Caractérisation des groupes produits [Ber] 291

- def produit direct et loi produit
- Th: $H \trianglelefteq G, H \cap K = \{e\}, HK = G \Rightarrow G \cong H \times K$
- app: classification des groupes d'ordre p^2

2) Groupe symétrique et alterné [Ber] 189 202

• def + def orbite + def cyclique 203 211 213

• Th conjugaison cycle

• Th conjugaison permutations

• def signature

• def/prop ϵ_n

DEV 1

{ • Lemme 37: pour $n \geq 5$, les 3-cycles sont conjugués dans A_n
• Pour $n = 3$ et $n \geq 5$ A_n simple

3) Commutativité dans un groupe

DEV 2

• Th Dixon

• Rombaldi Algèbre et géométrie

• Berkuy

• Ulmer

103: Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications

I - Conjugaison dans un groupe

[Ber] 131 Définition 1. Soit G un groupe, deux éléments x et x' de G sont dits conjugués s'il existe $g \in G$ tel que $x' = gxg^{-1}$

[Um] 33 Proposition 2. Le groupe G agit sur lui-même par:
 $G \times G \rightarrow G$
 $(g, R) \mapsto gRg^{-1}$

Cette action est appelée action par conjugaison de G sur lui-même.

34 Définition 3. On appelle classe de conjugaison d'un élément R de G l'orbite de R pour l'action par conjugaison de G sur lui-même. On la note $O(R)$. Deux éléments de G sont dits conjugués s'ils appartiennent à la même classe de conjugaison. On appelle centralisateur d'un élément g de G , noté C_g , le stabilisateur de g pour cette action.

[Ber] 132 Exemples 4. • Dans un groupe abélien, les classes de conjugaison sont réduites à des singletons et les centralisateurs sont égaux au groupe G .
 • Soit $\mathbb{K}$ un corps. Soient $A, B \in GL_n(\mathbb{K})$
 A, B conjugués $\Leftrightarrow A, B$ semblables

Définition 5 On appelle centre de G , noté $Z(G)$, l'ensemble des éléments de G qui commutent avec tous les éléments de G .

[Um] 19
[Ber] 136

Proposition 6 Pour tout $R \in G$, l'application $\text{Int}_R: G \rightarrow G$ définie par $\text{Int}_R(g) = RgR^{-1}$ est un automorphisme de G .
 L'application $\varphi: G \rightarrow \text{Int}(G)$ est un morphisme de groupe de noyau $Z(G)$.

Définition 7 Soit H un sous-groupe d'un groupe G , on appelle classe à gauche de $a \in G$ relativement à H le sous-ensemble. $aH = \{g \in G \mid g = aR, R \in H\}$

[Um] 24

On définit de même les classes à droite Ha . Les classes à gauche forment une partition de G . Leur ensemble est noté G/H . Le cardinal de G/H est appelé indice de H dans G et noté $[G:H]$.

Théorème 8. (Lagrange)

25

Soient G un groupe fini d'ordre $n \geq 2$ et H un sous-groupe de G . On a $|G| = [G:H] |H|$ donc l'ordre de H divise l'ordre de G .

Applications 9: • Si $g \in G$, alors l'ordre de g divise l'ordre $|G|$ de G .

• Les sous-groupes de S_3 sont: $\{id\}$, $\{id, (12)\}$, $\{id, (13)\}$, $\{id, (23)\}$, $\{id, (123), (132)\}$, S_3
 de cardinaux respectifs: 1, 2, 3 et 6.

[R] 22 Théorème 10 Soit G un groupe fini que l'on fait agir sur lui-même par conjugaison on note $R_1, \dots, R_r$ des éléments de G tels que $(R_1), \dots, (R_r)$ soient disjoints 2 à 2.

$$\text{Alors } |G| = |Z(G)| + \sum_{1 \leq i \leq r} |O(R_i)|$$

Application 11: Soit G un p -groupe non trivial avec p premier. Alors $Z(G) \neq \{e\}$

II- Sous-groupes distingués, Groupes quotients

1) Sous-groupes distingués

[Br] 135 Définition 12: On dit qu'un sous-groupe H de G est distingué, si on a $gH = Hg$ pour tout $g \in G$. On note $H \triangleleft G$.

Exemples 13: • Pour G un groupe, $Z(G) \triangleleft G$

136 • On note $D(G) = \langle [a, b], a, b \in G \rangle$ le sous-groupe engendré par les commutateurs, appelé le groupe dérivé. $D(G) \triangleleft G$

139 Théorème 14: Si G, G' deux groupes et φ un morphisme de groupe de G dans G' . Alors $\text{Ker } \varphi \triangleleft G$.

Exemples 15: Soit K corps. $SL_n(K) \triangleleft GL_n(K)$ car $SL_n(K) = \ker(\det)$ avec $\det: GL_n(K) \rightarrow K \setminus \{0\}$ morphisme. • $A_n \triangleleft S_n$ (voir III)

140 Définition 16 Soit G un groupe. On dit que G est simple si G n'a pas de sous-groupes distingués non trivial

2) Groupes quotients.

Théorème 17: Un sous-groupe H de G est distingué si et seulement si, il existe une unique structure de groupe sur l'ensemble quotient G/H des classes à gauche modulo H telle que la surjection canonique $\pi_H: G \rightarrow G/H$ soit un morphisme de groupe. [Ulm] 58

Exemple 18: Pour tout $n \in \mathbb{N}^*$, $n\mathbb{Z} \triangleleft \mathbb{Z}$ donc $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe.

Théorème 19: (1^{er} Théorème d'isomorphisme)

Soit $\varphi: G \rightarrow H$ un morphisme de groupes. Alors, il existe un isomorphisme $\bar{\varphi}: G/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi)$ 63

$$g\text{Ker}(\varphi) \mapsto \varphi(g)$$

Si φ est surjectif, on a: $G/\text{Ker}(\varphi) \cong H$. 63

Exemple 20: • Soit $\varphi: t \in \mathbb{R} \mapsto e^{it} \in \mathbb{C}^*$. $\text{Im}(\varphi) = \mathbb{U}$ et $\text{Ker}(\varphi) = 2\pi\mathbb{Z}$ donc $\mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{U}$.

• $G/Z(G) \cong \text{Int}(G)$ par le morphisme de la proposition 6.

Théorème 21: (2^{ème} Théorème d'isomorphisme).

Soit G un groupe, H, K sous-groupes de G tel que $K \triangleleft G$. Alors: • $H \cap K \triangleleft H$

$$\bullet H/(H \cap K) \cong HK/K$$

Théorème 22: (3^{ème} Théorème d'isomorphisme)

Soit $H \subseteq K$ deux sous-groupes de G tel que $H \triangleleft G, K \triangleleft G$. Alors $K/H \triangleleft G/H$ et $(G/H)/(K/H) \cong G/K$.

Exemple 23: $m, n \in \mathbb{N}$ $(\mathbb{Z}/mn\mathbb{Z})/(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$.

III - Applications

1) Caractérisation des groupes produits.

Définition 24: Soient H, K deux sous-groupes de G .
Leur produit direct interne est $HK := \{hk, h \in H, k \in K\}$.
On dit que H et K commutent si $HK = KH$.

Définition 25: Soient H, K deux groupes.

On munit $G = H \times K$ de loi produit définie par :

$$\forall (h, k), (h', k') \in H \times K, (h, k) \cdot (h', k') = (hh', kk')$$

G muni de cette loi est un groupe appelé produit direct de H et K .

Théorème 26: Soient H, K deux sous-groupes de G tels que

$$H \triangleleft G, K \triangleleft G; \quad H \cap K = \{e_G\}; \quad HK = G.$$

Alors $G \cong H \times K$.

Application 27: Classification des groupes d'ordre p^2 avec p premier.

$$|G| = p^2 \Rightarrow G \cong \mathbb{Z}/p^2\mathbb{Z} \text{ ou } G \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

2) Groupe symétrique et alterné.

Définition 28: Soit $E = \{1, \dots, n\}$ un ensemble fini avec $n \in \mathbb{N}^*$.

L'ensemble des bijections de E sur lui-même est un groupe pour la composition des applications, appelé groupe symétrique noté S_n .
On appelle $\sigma \in S_n$ une permutation. On a $|S_n| = n!$.

Définition 29: Soit $\sigma \in S_n$ et $x \in E$.

On définit la σ -orbite de x comme : $O(x) = \{\sigma^k(x) \mid k \in \mathbb{Z}\}$.

Définition 30: On dit que $\sigma \in S_n$ est un cycle s'il n'existe qu'une seule σ -orbite non réduite à un singleton.

Théorème 31: Pour tout cycle $(a_1 \dots a_n) \in S_n$ et $\sigma \in S_n$,
 $\sigma(a_1 \dots a_n) \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_n))$.

Corollaire 32: Les conjugués d'un cycle dans S_n sont les cycles de même longueur. 209

Définition 33: Le type de $\sigma \in S_n$ est $(\ell_1, \dots, \ell_k)$ avec $\ell_1 \leq \ell_2 \leq \dots \leq \ell_k$ où ℓ_i est la longueur de γ_i avec $\sigma = \gamma_1 \dots \gamma_k$ une décomposition en cycles à support disjoints. 211

Proposition 34: Deux permutations dans S_n sont conjugués si et seulement si elles sont de même type.

Définition 35: On définit le morphisme de groupe signature tel que $\varepsilon: (S_n, \circ) \rightarrow (\{-1, 1\}, \times)$
 $\sigma \mapsto (-1)^{(\ell_1 + \dots + \ell_k) - k}$ où $\text{type}(\sigma) = (\ell_1, \dots, \ell_k)$. 213

Définition / Proposition 36: $A_n = \text{Ker}(\varepsilon)$ est appelé le groupe alterné. On a donc $A_n \triangleleft S_n$ et $|A_n| = \frac{n!}{2}$.

Lemme 37: Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n .

Théorème 38: Pour $n = 3$ et $n \geq 5$, A_n est simple. DEV 1

3) Commutativité dans un groupe.

Théorème 39: Théorème de Dixon.

Soit G un groupe fini d'ordre n , non abélien.

On note k le nombre de classes de conjugaison dans G .

$p(G)$ la probabilité que 2 éléments de G tirés uniformément et indépendamment commutent.

$$\text{Alors } p(G) = \frac{k}{n} \leq \frac{5}{8}.$$

DEV 2.

Références: • Mathématiques pour l'agrégation, Algèbre et géométrie
• Algèbre : le grand combat - BERTHUY
• Théorie des groupes - ULMER

PQ Étudier les groupes quotients?

↳ utilités en théorie des groupes?

simplifier des groupes

ex: si G un groupe infini
on essaie de se ramener
à l'étude d'un groupe +
petit et + simple à
comprendre.

$(\mathbb{Z}, +)$

$\mathbb{Z}/n\mathbb{Z}$

↳ n elms

On note par

$H < G$

G/H

Cas concrets

↳ groupes produits

↳ S_n et A_n : nbreuses prop

A_n simple

DEV 1

103: Conjugaison dans un
groupe. Ex de ss groupes
distingués et groupes quotients

Cent muni G/H d'une structure de
groupe?

↳ loi interne

↳ H doit être distingué dans G

=

stable par conjugaison

1er Th d'iso

Ouh! Is
Cent savoir si un
groupe est distingué?

↳ indice 2 ex S_3 et A_3

↳ $H = \ker \varphi$ φ morphisme ex $S_n = \ker(\det)$

Exemples de sous groupes
distingués

↳ centre et groupe dérivée

lien avec action de groupe
 $G \curvearrowright G$ par conjugaison

↳ équation aux classes

↳ centre ↳ taille classe

App: Th de Dixon

DEV 2