

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

I. Conjugaison dans un groupe

1. Action de conjugaison [ULM] [ROM]

Action par conjugaison, classe de conjugaison, groupe des automorphismes intérieurs, lien entre $Z(G)$ et classes de conjugaison

2. Sous-groupes distingués [BER]

SGD, exemples, cas du noyau, $SL(E)$, groupe simple

II. Groupes quotients

1. Définition et propriétés [BER]

Classes à gauche, indice, exemple de $\mathbb{Z}/n\mathbb{Z}$, sous-groupe d'indice 2, théorème de Lagrange, groupe quotient, sous-groupes de G/H

2. Théorèmes d'isomorphisme [BER] [ULM]

Théorème de factorisation, les trois théorèmes d'isomorphismes, exemples, groupes cycliques

III. Applications

1. Application aux p -groupes [ULM] [IP]

Formule des classes, p -groupe, formule des classes pour un p -groupe, centre d'un p -groupe
DEV 1 : classification des groupes d'ordre p^2

2. Groupe symétrique et groupe alterné [BER] [ROM]

Décomposition en produit de cycles, générateurs de $\mathcal{S}_n$, conjugaison dans $\mathcal{S}_n$, groupe alterné, générateurs de $\mathcal{A}_n$, DEV 2 : sous-groupes distingués de $\mathcal{S}_n$, $\mathcal{A}_n$ est simple, centre de $\mathcal{S}_n$

3. Matrices semblables [ROM]

Matrices semblables, invariants de similitude, contre-exemple, exemple pour les matrices diagonalisables

Présentation :

- Un sous-groupe est distingué lorsqu'il est stable par conjugaison.
- Pour montrer qu'un sous-groupe est distingué, on peut essayer de l'identifier à un noyau d'un morphisme de groupes.
- La réciproque du théorème de Lagrange est fausse, par exemple $\mathcal{A}_4$ est d'ordre 12 mais n'a pas de sous-groupe d'ordre 6. On a une réciproque partielle avec le théorème de Cauchy.
- La notion de sous-groupe distingué est exactement celle dont on a besoin pour munir G/H d'une structure de groupe tel que la projection π soit un morphisme de groupes.
- L'idée des groupes quotients est de se ramener à l'étude d'un groupe où l'on a regroupé certains éléments ensemble.
- Le premier théorème d'isomorphisme est crucial en algèbre, il est utilisé de nombreuses fois. Par exemple en algèbre linéaire, il permet de démontrer le théorème du rang en quelques lignes.

Développements :

- Classification des groupes d'ordre p^2
 - L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte, p106
- Sous-groupes distingués de $\mathcal{S}_n$
 - Algèbre : le grand combat, Berhuy, p215
 - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p49

Références :

- [ULM] Théorie des Groupes, Ulmer
- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [BER] Algèbre : le grand combat, Berhuy
- [IP] L'oral à l'agrégation de mathématiques - Une sélection de développements , Isenmann-Pecatte

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

Soit G un groupe muni d'une multiplication. Soit H un sous-groupe de G .

I Conjugaison dans un groupe

1) Action de conjugaison [ULM][ROM]

Def 1: Un groupe opère sur lui-même par conjugaison

via: $G \times G \rightarrow G$
 $(g, h) \mapsto ghg^{-1}$

Def 2: L'orbite $\{ghg^{-1} ; g \in G\}$ de $h \in G$ s'appelle la classe de conjugaison de h . Deux éléments de G qui appartiennent à la même classe de conjugaison sont dits conjugués.

Prop 3: Le morphisme de groupes correspondant de G dans $S(G)$ est noté $\text{Int}(g) : G \rightarrow G$. L'image de h par $\text{Int}(g)$ est ghg^{-1} .

Le morphisme est le groupe $\text{Int}(G)$ des automorphismes intérieurs de G .

Prop 4: Un élément est dans le centre du groupe ssi sa classe de conjugaison est réduite à un seul élément. Ainsi $Z(G)$ est l'union des classes de conjugaison de taille 1.

Exemple 5: Dans S_n , tous les p -cycles sont conjugués.

$\bullet$ $G_L(K)$ agit par conjugaison sur $M_n(K)$.

2) Application aux p -groupes [ULM][IP]

Théorème 6 (forme des classes): Soit G un groupe fini et X un ensemble fini. Si $\{x_1, \dots, x_n\}$ est un système de représentants des orbites, alors: $|X| = \sum_{i=1}^n |O_i|$.

Def 7: Soit p un nombre premier. Un p -groupe est un groupe fini dont l'ordre est une puissance de p .

Prop 8: Soit G un p -groupe agissant sur X . Alors: $|X| \equiv |X^G| \pmod{p}$ où $X^G = \{x \in X ; g \cdot x = x \forall g \in G\}$.

Lemme 9: Soit G un groupe. Si $G/Z(G)$ est métrique, alors

G est abélien.

Prop 10: Le centre d'un p -groupe est non trivial.

Prop 11: Tout groupe d'ordre p^2 est abélien.

Théorème 12: Soit p un nombre premier. Soit G un groupe d'ordre p^2 . Alors $G \cong \mathbb{Z}/p\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

II Généralités sur les sous-groupes distingués.

1) Sous-groupes distingués [BER]

Def 13: On dit que H est distingué dans G si l'on a $ghg^{-1} \in H$ pour tout $h \in H$ et tout $g \in G$.

On note $H \triangleleft G$.

Exemple 14: Si G est abélien, tout sous-groupe est distingué. Les sous-groupes $\{e\}$ et G sont distingués dans G .

Exemple 15: $Z(G) \triangleleft G$.

Prop 16: Soit $\varphi : G \rightarrow G'$ un morphisme de groupes. Alors $\text{Ker}(\varphi)$ est un sous-groupe distingué de G .

Exemple 17: Soit E un K -ev de dimension finie. Alors $\text{SL}(E) \triangleleft \text{GL}(E)$ car il s'agit du noyau du morphisme déterminant $\det : \text{GL}(E) \rightarrow K^*$.

Def 18: On dit que G est simple si $G \neq \{e\}$ et si G n'a pas de sous-groupe propre distingué dans G .

Exemple 19: $\text{GL}(E)$ n'est pas simple.

Un groupe non abélien dont le centre est non-trivial n'est pas simple.

2) Groupes quotients [BER]

Def 20: On définit sur G une relation d'équivalence $\sim$ tel que $x \sim y$ ssi $x^{-1}y \in H$. Les classes d'équivalence sont les classes à gauche modulo H : $\forall x \in G, \bar{x} = xH = \{xh ; h \in H\}$. On note G/H l'ensemble des classes à gauche modulo H .

Def 21: Le nombre de classes à gauche modulo H ,

longueur l est fini, est appelé l'indice de H dans G et est noté $[G:H]$

Exemple 22: Soit $G = \mathbb{Z}$ et $H = m\mathbb{Z}$ alors la relation d'équivalence usuelle $\sim$ sur H est la relation de congruence modulo m et la classe à gauche de $x \in \mathbb{Z}$ est $x + m\mathbb{Z}$.

Si $m > 0$, $[\mathbb{Z} : m\mathbb{Z}] = |\mathbb{Z}/m\mathbb{Z}| = m$.

Prop 23: On a équivalence entre:

1) $H \trianglelefteq G$

2) $\forall x \in G, xH = Hx$

3) $\forall x \in G, xHx^{-1} = H$

Prop 24: Tout sous-groupe d'indice 2 est distingué dans G .

Théorème 25 (de Lagrange): Soit G un groupe fini. Alors:

$|G| = [G:H] \times |H|$. En particulier $|H|$ divise $|G|$.

Prop 26: Soit $H \trianglelefteq G$. Alors la loi interne $(\bar{x}, \bar{y}) \mapsto \overline{xy}$ de G/H est bien définie, le morphisme $\bar{\pi}$ est induit sur G/H

me structure de groupe. De plus, l'application

$\pi: G \rightarrow G/H$ est un morphisme de groupe surjectif de

$\pi^{-1}(\bar{x}) = xH$ noyau H .

Def 27: Soit $H \trianglelefteq G$. Le groupe G/H est appelé groupe quotient

de G par H .

Exemple 28: Soit $n \geq 1$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient de

$\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

Prop 29: Soit $H \trianglelefteq G$. Il y a une correspondance bijective

entre l'ensemble des sous-groupes de G contenant H et

l'ensemble des sous-groupes de G/H .

3) Théorèmes d'isomorphisme [BER] [ULM]

Théorème 30 (de factorisation): Soit $H \trianglelefteq G$. Soit $f: G \rightarrow G'$

un morphisme de groupes tel que $H \subset \ker(f)$. Alors il

existe un unique morphisme de groupes $\bar{f}: G/H \rightarrow G'$

tel que $f = \bar{f} \circ \pi$. On le définit par $\bar{f}(\bar{x}) = f(x)$

$\forall \bar{x} \in G/H$

Théorème 31 (1^{er} théorème d'isomorphisme): Soit $f: G \rightarrow G'$ un

morphisme de groupes. Alors: $G/\ker(f) \cong \text{Im}(f)$.

Exemple 32: Grâce à $f: \mathbb{Q}^* \rightarrow \mathbb{R}^*$ on obtient: $\mathbb{Q}^*/\mathbb{Z} \cong \mathbb{R}^*$

Exemple 33: Grâce à $f: \mathbb{R} \rightarrow \mathbb{C}$ on obtient: $\mathbb{R}/2\pi\mathbb{Z} \cong \mathbb{C}^*$.

Application 34: Un groupe cyclique d'ordre n est isomorphe

à $\mathbb{Z}/n\mathbb{Z}$.

Théorème 35 (2^e théorème d'isomorphisme): Soit H et K

deux sous-groupes de G , et $H \trianglelefteq G$. Alors: $H \cap K$ et HK sont

des sous-groupes de G . De plus, $H \trianglelefteq HK$, $H \cap K \trianglelefteq K$ et

donc: $H(K/H) \cong K/(H \cap K)$

Théorème 36 (3^e théorème d'isomorphisme): Soit $H \trianglelefteq G$ et

$K \trianglelefteq G$ avec $K \subset H$. Alors $K \trianglelefteq H$, $H/K \trianglelefteq G/K$ et on a:

$(G/K)/(H/K) \cong G/H$.

Exemple 37: Comme $10\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$, on a que:

$(\mathbb{Z}/10\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$

III Applications

1) Groupe des permutations et groupe alterné [BER] [Lam]

Théorème 38: Soit $\sigma \in S_n$. Alors σ se décompose en produit

de cycles à supports disjoints, et cette décomposition est

unique à l'ordre des facteurs près.

Prop 39: S_n est engendré par les cycles

(i, j) est engendré par les transpositions.

Lemme 40: Soit $\tau \in S_n$. Pour tout p -cycle $(a_1, \dots, a_p)$ on a:

$\tau(a_1, \dots, a_p)\tau^{-1} = (a_1, \dots, a_p)$

Théorème 41: Deux permutations sont conjuguées dans S_n

ssi les listes (avec répétitions) des longueurs des cycles à

soutiens disjoints qui les composent sont les

mêmes

mêmes à l'ordre près.

Déf 42: Le groupe alterné, noté A_n , est l'ensemble des permutations de S_n de signature 1.

Prop 43: A_n est distingué dans S_n et est d'indice 2.

Ainsi $|A_n| = \frac{n!}{2}$.

Prop 44: Si $n \geq 3$, A_n est engendré par chacune des familles suivantes:

1) les produits de deux transpositions.

2) les 3-cycles.

Lemme 45: Si $n \geq 5$, les 3-cycles sont conjugués dans A_n .

Théorème 46: Soit $n \geq 3$. Alors le groupe alterné A_n est simple ssi $n \neq 4$. DEV 2

Lemme 47: Soit $n \geq 3$. Alors le centre de S_n est trivial.

Corollaire 48: Soit $n \geq 2$. Si $n \neq 4$, les sous-groupes distingués de S_n sont: $\{id\}$, A_n et S_n .

2) Matrices semblables [ROM]

Théorème 49: L'application $GL_n(K) \times M_n(K) \rightarrow M_n(K)$
 $(P, A) \mapsto PAP^{-1}$

définit une action par conjugaison de $GL_n(K)$ sur $M_n(K)$.

Déf 50: Deux matrices qui sont dans la même orbite pour cette action sont dites semblables.

Prop 51: Deux matrices semblables sont équivalentes.

Prop 52: Deux matrices semblables ont: même rang, même déterminant, même polynôme caractéristique, même polynôme minimal, même trace.

Centre - ex 53: Les matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ont même déterminant, même trace et même polynôme

caractéristique mais ne sont pas semblables.

Prop 54: Une matrice est diagonalisable (resp triangulable) ssi son orbite pour cette action contient une matrice diagonale (resp triangulaire).

I Conjugaison dans un groupe

1) Action de conjugaison [ULM] [ROM]

2) Sous-groupes distingués [BER]

II Groupes quotient

1) Déf et prop [BER]

2) Théorèmes d'isomorphismes [BER] [ULM]

III Applications

1) Application aux p-groupes [ULM] [IP]

2) Groupe des permutations et groupe alterné [BER] [ROM]

3) Matrices semblables [ROM]