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

RM
2022-2023

On se place dans un groupe G de loi multiplicative de neutre 1, E un ensemble et $n \in \mathbb{N}^*$.

1 Conjugaison dans un groupe

1.1 Action de conjugaison

Définition 1 : On dit que le groupe G opère à gauche sur l'ensemble E si on a une application $(g,x) \in G \times E \mapsto g.x \in E$ telle que pour tout x de E et g, g' de G, alors $1.x = x$ et $g.(g'.x) = (gg').x$.
Cela revient au même que de définir un morphisme de groupe $\varphi : G \to \mathcal{S}(E)$ avec $\varphi(g)(x) = g.x$.

Définition 2 : On appelle alors action par conjugaison une action de G sur lui même avec pour g, h dans G, $g.h = ghg^{-1}$. Le morphisme φ est alors noté Int. On appelle $Int(G)$ l'ensemble des automorphismes intérieurs de G.

Remarque 3 : Si le groupe G est abélien, alors tous les automorphismes intérieurs sont triviales. C'est donc utilisé dans des groupes non abéliens.

Exemple 4 : • $GL_n(\mathbb{C})$ agit par conjugaison sur $M_n(\mathbb{C})$.
• G agit sur tout sous-groupe distingué H par conjugaison.

1.2 Orbites, stabilisateurs et équation aux classes

Définition 5 : Soit G opérant sur lui même par conjugaison, les orbites $O_x = \{g.x | g \in G\}$ pour $x \in G$ sont appelées classes de conjugaison. On dit que deux éléments de G sont conjugués si ils appartiennent à la même classe de conjugaison.

Exemple 6 : • Dans $\mathfrak{S}_n$, tous les cycles d'ordre p sont conjugués.
• Les transvections sont conjuguées dans $GL(E)$.

Définition 7 : Le stabilisateur de $x \in G$, $Stab(x) = \{g \in G, g.x = x\}$ est appelée le centralisateur de x dans G et est noté $Z_G(x)$.

Lemme 8 : Un élément g d'un groupe G est dans le centre $Z(G)$ de G si et seulement si sa classe de conjugaison est réduite à un seul élément. Le centre de $Z(G)$ de G est l'union des classes de conjugaison de taille 1.

Théorème (Équations aux classes) 9 : Soit G un groupe fini agissant sur un ensemble fini E, on a :
i) Si $x_1, ..., x_r$ est un système de représentant des orbites, alors $|E| = \sum_{i=1}^{r} |O_{x_i}|$.
ii) Pour tout $x \in E$, on a $|G| = |O_x||Stab(x)|$.

1.3 Application aux p-groupes

Définition 10 : Si $p \geq 2$ est un nombre premier, on appelle p-groupe tout groupe de cardinal p^α où α est un entier naturel non nul.

Proposition 11 : Soit G un p-groupe opérant sur un ensemble fini E. Alors on a $|E^G| \equiv |E| \pmod p$ avec $E^G = \{x \in E, |O_x| = 1\}$.

Corollaire 12 : Si G opère sur lui même par conjugaison, on a $G^G = Z(G)$ et donc on a $|Z(G)| \equiv |E| \pmod p$.

Corollaire 13 : Le centre d'un p-groupe non trivial est non trivial.

Théorème 14 : Tout groupe d'ordre p^2 avec p premier est abélien.

Application 15 : Soit p un nombre premier. A isomorphisme près, les groupes d'ordre p^2 sont $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

2 Sous-groupes distingués et groupes quotients

2.1 Sous-groupes distingués

Définition 16 : On dit qu'un sous-groupe H de G est distingué (ou normal), si pour tout $g \in G$ et $h \in H$, on a $ghg- ^{-1} \in H$.

Remarque 17 : On a alors que H est distingué si H est stable par automorphisme intérieur.

Exemple 18 : • Les sous-groupes $\{1\}$ et G sont toujours distingués dans G.
• L'intersection de deux sous-groupes distingués de G est distingué.
• Si le groupe G est abélien, tous ses sous-groupes sont alors distingués.

Théorème 19 : Si G, G' sont deux groupes et φ un morphisme de groupe de G dans G', alors $ker(\varphi)$ est un sous-groupe distingué de G.

2.2 Groupes quotients

Théorème 20 : 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 $\pi_H : G \to G/H$ soit un morphisme de groupe.

Remarque 21 : On a donc que G/H est un groupe appelé groupe quotient de G sur H si et seulement si H est distingué dans G. Si G est abélien, alors G/H est toujours un groupe.

Exemple 22 : Comme $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$, on peut munir $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe.

Théorème 23 : Si G est un groupe fini, alors on a que le groupe G/H est de cardinal $|G/H| = |G|/|H|$.

Corollaire 24 : Un sous-groupe H de G est distingué si et seulement si H est le noyau d'un morphisme de source G.

Théorème 25 : Les sous-groupes de G/H pour H distingué dans G sont les groupes de la forme K/H avec K un sous groupe de G qui contient H.

Remarque 26 : L'idée est ici trouvant H un sous-groupe distingué de G, de "factoriser" G par H et d'étudier le groupe G/H à priori plus simple.

2.3 Les théorèmes d'isomorphismes

Théorème (1er théorème d'isomorphisme) 27 : Soit G, G' deux groupes et $\varphi : G \to G'$ un morphisme de groupes. Alors il existe un isomorphisme $\overline{\varphi} : G/ker(\varphi) \to Im(\varphi)$. Autrement dit, on a $G/ker(\varphi) \cong Im(\varphi)$.

Application 28 : • Un groupe G cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
• Soit G un groupe de centre $Z(G)$, alors $G/Z(G) \cong Int(G)$.

Exemple 29 : Le morphisme det : $GL_n(\mathbb{C}) \to \mathbb{C}^*$ est surjectif de noyau $SL_n(\mathbb{C})$. Donc on a $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \cong \mathbb{C}^*$.

Théorème (2ème théorème d'isomorphisme) 30 : Soit K et H deux sous groupes de G tels que $K \subset N_G(H) = \{g \in G | gHg^{-1} = H\}$. L'ensemble $KH = HK$ est un sous-groupe de G et le groupe H est distingué dans KH. Le groupe $K \cap H$ est distingué dans K et on a l'isomorphisme $KH/H \cong K/(K \cap H)$. De plus, si les groupes K et H sont finis, alors $|KH|.|K \cap H| = |K|.|H|$.

Théorème (3ème théorème d'isomorphisme) 31 : Soit $K \subset H \subset G$ trois groupes. Supposons que H et K soient distingués dans G. Alors les groupes quotients G/H et $(G/H)/(H/K)$ sont isomorphes.

Exemple 32 : On a que $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

3 Simplicité et théorème de Sylow

3.1 Simplicité

Définition 33 : Un groupe G non trivial est dit simple si et seulement si ses seuls sous-groupes distingués sont $\{1\}$ et G.

Exemple 34 : • $\mathbb{Z}/n\mathbb{Z}$ est simple si et seulement si n est premier.
• $\mathcal{A}_n$ est simple pour $n \geq 5$, on le reverra plus tard.

Remarque 35 : Il n'est donc pas possible de "factoriser" les groupes simples. Leur étude est donc particulière. La classification des groupes simples finis à été achevée en 1981.

3.2 Les théorèmes de Sylow

Définition 36 : Soit G un groupe de cardinal $n = p^\alpha m$ avec $\alpha \geq 1$ et $p \not| m$. On appelle p-sous-groupe de Sylow de G un sous-groupe de cardinal p^α.

Exemple 37 : Soit $G = Gl_n(\mathbb{F}_p)$. Alors l'ensemble $P = \{A = (a_{i,j}) | a_{i,j} = 0 \text{ si } i > j \text{ et } a_{i,i} = 1\}$ est un p-sous-groupe de Sylow de G.

Théorème (de Sylow) 38 : Soit G un groupe fini et p un diviseur (premier) de $|G|$, alors G contient au moins un p-sous-groupe de Sylow.

Corollaire 39 : Si $|G| = p^\alpha m, p \not| m$, G contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.

Théorème (de Sylow 2) 40 : Soit G un groupe de cardinal $|G| = p^\alpha m, p \not| m$.
i) Si H est un sous-groupe de G qui est un p-groupe, il existe un p-Sylow S, avec $H \subset S$.
ii) Les p-Sylow sont tous conjugués.
iii) On a $S_p \equiv 1 \pmod p$ et $S_p | m$.

Corollaire 41 : Si S est un p-Sylow de G, on a que S est distingué dans G si et seulement si $S_p = 1$ si et seulement si S est l'unique p-Sylow de G.

Application 42 : • Un groupe d'ordre 63 n'est pas simple.

Développement 43 : Tout groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$. **Dev 1**

4 Application au groupe $\mathfrak{S}_n$ et $GL(E)$

4.1 Le groupe $\mathfrak{S}_n$

Définition 44 : Soit E un ensemble de cardinal n. On appelle groupe des permutations de E notée $\mathcal{S}(E)$ le groupe des bijections de E sur lui même. Si $E = \{1, ..., n\}$, on l'appelle alors groupe symétrique notée $\mathcal{S}_n$.

Théorème 45 : Toute permutation $\sigma \in \mathcal{S}_n$ non trivial se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre près.

Exemple 46 : On a $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 1 & 3 & 4 & 7 \end{pmatrix} = (1, 2, 6, 4).(3, 5).(7)$.

Remarque 47 : Les cycles sont des générateurs de $\mathcal{S}_n$.

Théorème 48 : Le groupe $\mathcal{S}_n$ est engendré par les transpositions.

Lemme 49 : Soit r tel que $2 \leq r \leq n$. Le conjugué dans $\mathcal{S}_n$ d'un r-cycle est encore un r-cycle. Plus précisément, pour tout r-cycle $\sigma = (x_1, x_2, ..., x_r)$ et toute permutation τ, on a :

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), ..., \tau(x_r))$$

Corollaire 50 : Réciproquement, deux cycles de même longueur sont conjugués dans $\mathcal{S}_n(E)$, i.e que si σ et σ' sont deux cycles de même longueur r, il existe alors une permutation τ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$.

Remarque 51 : Le résultat précédent signifie que pour tout $r \in [\![2\,;n]\!]$, le groupe $\mathcal{S}_n$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

Définition 52 : Le groupe alterné notée $\mathcal{A}_n$ est le sous-ensemble de $\mathcal{S}_n$ formé des permutations paires. C'est le noyau du morphisme signature.

Proposition 53 : On a $|\mathcal{A}_n| = n!/2$.

Théorème 54 : Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.
Théorème 55 : $\mathcal{A}_n$ est simple pour $n \geq 5$. **Dev 2**

4.2 Le groupe $GL(E)$

Soit E un $\mathbb{K}$-espace vectoriel de dimension n.

Définition 56 : Soit φ une forme linéaire non nulle sur E. On appelle transvection d'hyperplan $ker(\varphi)$ toute application linéaire $u \in \mathcal{L}(E)$ définie par $u(x) = x + \varphi(x)a$ pour tout x de E où $a \in ker(\varphi)$.

Théorème 57 : Soit $u \in \mathcal{L}(E)$ non trivial. Alors sont équivalents :
i) u est une transvection.
ii) Il existe une base de E dans laquelle la matrice de u est de la forme $T_n = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.
iii) il existe une base dans laquelle la matrice de u est $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ avec $\lambda \in \mathbb{K}^*$.
iv) $rg(u - Id) = 1$ et le polynôme caractéristique de u est $(X - 1)^n$.

Définition 58 : Soit φ une forme linéaire non nulle sur E. On appelle dilatation d'hyperplan $ker(\varphi)$ toute application linéaire $u \in \mathcal{L}(E)$ définie par $u(x) = x + \phi(x)$ pour tout x dans E et $a \in E \setminus ker(\varphi)$.

Théorème 59 : Une dilatation $\delta_{\varphi,a}$ est dans $GL(E)$ si et seulement si $\lambda = 1+\varphi(a) \neq 0$. On appelle alors λ le rapport de dilatation.

Théorème 60 : Pour $u \in GL(E)$, sont équivalents :
i) u est une dilatation de rapport λ.
ii) Il existe une base de E dans laquelle u est de la forme $D_n(\lambda) = \begin{pmatrix} I_{n-1} & 0 \\ 0 & \lambda \end{pmatrix} = I_n + (\lambda - 1)E_{n,n}$ avec $\lambda = det(u) \in \mathbb{K} \setminus \{0, 1\}$.

Théorème 61 : • Le centre Z de $GL(E)$ est formé des homothéties $x \mapsto \lambda x$ avec $\lambda \in \mathbb{K}^*$. Il est donc isomorphe à $\mathbb{K}^*$.
• Le centre de $SL(E)$ est $Z \cap SL(E)$, il est isomorphe à $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K} | \lambda^n = 1\}$.

Théorème 62 : • Les transvections engendrent $SL(E)$.
• Les transvections et les dilatations engendrent $GL(E)$.

Proposition 63 : Deux dilatations sont conjuguées dans $GL(E)$ si et seulement si elles ont le même rapport.
• Deux transvections quelconques sont conjuguées dans $GL(E)$. Pour $n \geq 3$, elles le sont aussi dans $SL(E)$.

Références :

1. Algèbre Gourdon
2. Cours d'algèbre Perrin
3. Algèbre et géométrie Rombaldi
4. Théorie des groupes Ulmer
5. isenmann (rip)