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

Ulmer
Rombaldi

Dans toute cette leçon, G est un groupe et H un sous-groupe de G.

I - Généralités

1. Notion de conjugaison

Proposition - Définition 1.1 Un groupe agit sur lui-même avec $\varphi : G \times G \longrightarrow G$, $(g,h) \longmapsto g.h = ghg^{-1}$.

On appelle cette action l'action de G sur lui-même par conjugaison.

Définition 1.2 L'orbite $\{ghg^{-1} \mid g \in G\}$ de $h \in G$ s'appelle la classe de conjugaison de h. Deux éléments de G dans la même classe de conjugaison sont dits conjugués.

Le stabilisateur $\{g \in G \mid ghg^{-1} = h\}$ de $h \in G$ s'appelle le centralisateur de h dans G et est noté $C(h)$.

Remarque 1.3 L'action par conjugaison n'est jamais libre. En effet, on a $C(e) = G \neq \{e\}$.

De plus, si G est non trivial alors l'action n'est pas transitive.

Proposition 1.4 Soit $g \in G$. Alors $g \in Z(G)$ si et seulement si la classe de conjugaison est $\{g\}$.

Exemples 1.5

- si G est abélien, il s'agit de l'action triviale
- dans S_n, deux permutations sont conjuguées si et seulement si dans leurs décompositions en produit de permutations à supports disjoints, elles admettent le même nombre de permutations de même longueur :

  $(1\ 2)(3\ 4\ 5)(7\ 9)$ et $(4\ 10)(3\ 6)(1\ 2\ 7)$ sont conjugués dans S_{10}

  $(1\ 2)(3\ 4\ 5)(7\ 9)$ et $(4\ 10)(3\ 6)(1\ 2\ 7\ 8)$ ne sont pas conjugués

Application

Lemme 1.6 Soient $q, d, n \in \mathbb{N}^*$ avec $q \geq 2$. Alors $q^d - 1 \mid q^n - 1$ si et seulement si $d \mid n$. Le cas échéant, si d est un diviseur strict de n, $\Phi_n(q) \mid \frac{q^n - 1}{q^d - 1}$.

Théorème 1.7 (Wedderburn) Soit A un anneau intègre vérifiant $A^* = A \setminus \{0\}$. Si A est fini alors A est commutatif (et donc un corps).

ajouter les isomorphismes exceptionnels !

2. Notion de sous-groupe distingué

Définition 1.8 Le sous-groupe H est dit distingué (ou normal) s'il vérifie pour tout $g \in G$, $gH = Hg$. On note $H \lhd G$.

Remarque 1.9 Cette notion apparaît naturellement pour que la relation d'équivalence de classe à gauche, définie par $g_1 \mathcal{R}_H g_2$ si $g_1^{-1} g_2 \in H$, soit compatible avec la loi de G i.e. $g_1 \mathcal{R} g_2 \iff g_1 g \mathcal{R} g g_2$ et $g g_1 \mathcal{R} g_2 g$.

Exemples 1.10

- les sous-groupes $\{1\}$ et G sont toujours distingués dans G
- l'intersection de sous-groupes distingués est un sous-groupe distingué
- si G est commutatif, tout sous-groupe est distingué

développement 1

Exemple 1.11
Dans S_4, le sous-groupe des bi-transpositions est distingué.

Proposition 1.12 Si H est d'indice 2 alors H est distingué dans G.

Définition 1.13 Un groupe dont les seuls sous-groupes distingués sont $\{1\}$ et G est dit simple.

Proposition 1.14 Soit $n \geq 5$ alors $\mathcal{A}_n$ est simple.

Lemme 1.15 Les 3-cycles sont conjugués dans $\mathcal{A}_n$ et engendrent $\mathcal{A}_n$.

II - Groupes quotient

Théorème 2.1 Un sous-groupe H est distingué dans G, 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 $\pi_H : G \longrightarrow G/H$ soit un morphisme de groupes.

Théorème 2.2 (Premier théorème d'isomorphisme) Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes. Il existe alors un unique isomorphisme de groupes $\overline{\varphi} : G/\ker\varphi \to \operatorname{Im}\varphi$ tel que $\varphi = i \circ \overline{\varphi} \circ \pi$ où $i : \operatorname{Im}\varphi \longrightarrow G'$ injection canonique.

Corollaire 2.3 Sous les hypothèses précédentes, si G est un groupe fini, on obtient : $|G| = |\ker\varphi| \cdot |\operatorname{Im}\varphi|$.

Corollaire 2.4 Si G est fini cyclique d'ordre n alors $G \simeq \mathbb{Z}_n$.

Exemples 2.5

$GL_n(\mathbb{C})/SL_n(\mathbb{C}) \simeq \mathbb{C}^*$ $\qquad$ $S_n/\mathcal{A}_n \simeq \mathbb{Z}_2 \simeq \{-1, 1\}$

Théorème 2.6 Soit $\mathcal{D}(G)$ le groupe dérivé et soit H un sous-groupe de G. Alors :

- $G/\mathcal{D}(G)$ est un groupe abélien
- $\mathcal{D}(G) \subset H$ si et seulement si $H \lhd G$ et G/H est abélien

Définition 2.7 Le groupe $G/\mathcal{D}(G)$ est appelé l'abélianisé de G.

Théorème 2.8 (Troisième théorème d'isomorphisme) Soient $K \subset H \subset G$ trois groupes, avec H et K distingués dans G. Alors : $(G/K)/(H/K) \simeq G/H$.

Exemples 2.9

- $10\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$ et ils sont abéliens donc $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$
- $V_4 \subset \mathcal{A}_4 \subset S_4$, avec V_4 le groupe des bitranspositions de S_4, on obtient alors : $S_4/\mathcal{A}_4 \simeq (S_4/V_4)/(\mathcal{A}_4/V_4)$

III - Applications aux groupes de la conjugaison

1. Notion de p-groupe

Définition 3.1 Soit p un nombre premier. Un p-groupe est un groupe fini d'ordre une puissance de p.

Proposition 3.2 Soit G un p-groupe. Alors $Z(G)$ est non trivial.
En particulier, si G est un p-groupe d'ordre non premier alors G n'est pas simple.

Corollaire 3.3 Un groupe d'ordre p^2 est abélien.

Exemple 3.4
pour $n \geq 3$, p premier et K un corps à p^m éléments, les matrices triangulaires supérieures dont la diagonale est constituée de 1 forment un sous-groupe non abélien de $GL_n(K)$ d'ordre $p^{m.n(n-1)/2}$

2. Théorie de Sylow

Dans ce paragraphe, p est un nombre premier et $m \geq 1$ un nombre premier à p.

Définition 3.5 Soit G d'ordre $p^r m$. Un p-Sylow est un sous-groupe de G d'ordre p^r.

Théorème 3.6 Un groupe d'ordre $p^r m$ admet un p-sous groupe de Sylow.

Théorème 3.7 (de Sylow) Soit G un groupe d'ordre $p^r m$.

Alors :

- les p-Sylows sont tous conjugués
- notons n_p le nombre de p-Sylows de G alors $n_p \mid m$ et $n_p \equiv 1 \pmod p$

Exemple 3.8

si $|G| = 36$, G admet un 3-Sylow H

On a donc $|H| = 9$ et $[G : H] = 4$.

Application 3.9 Un groupe simple G d'ordre 60 est isomorphe à A_5. devrait 2