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

Références : Berhuy, Ulmer, Perrin

I - Conjugaison dans un groupe
1) Action par conjugaison
2) Application aux p-groupes

II - Généralités sur les sous-groupes distingués
1) Sous-groupes distingués
2) Groupes quotient
3) Les théorèmes d'isomorphisme

III - Applications
1) Groupe symétrique et groupe alterné
2) Théorie de Sylow
3) Groupe linéaire

DEV 1 : Wedderburn

DEV 2 : A_n est simple

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

Soit $(G, \times)$ un groupe (noté G par la suite), de neutre e_G.

I - Conjugaison dans un groupe

1) Action par conjugaison [ULM] [BERH]

DEF 1 : Un groupe opère sur lui-même par conjugaison via $\varphi : G \times G \to G$, $(g, h) \mapsto ghg^{-1}$

DEF 2 : L'orbite $\{ghg^{-1} / g \in G\}$ de $h \in G$ sous cette action s'appelle la classe de conjugaison de h. Deux éléments de G dans la même classe de conjugaison sont dits conjugués.

DEF 3 : Le stabilisateur de h : $Stab(h) = \{ghg^{-1} / g \in G\}$ s'appelle le centralisateur de h dans G et est noté $Z_G(h)$.

EX 4 : La classe de conjugaison de e_G est $\{e_G\}$. Si G est abélien, toutes ses classes de conjugaison n'ont qu'un seul élément (il y en a alors autant que d'éléments dans si G est fini).

EX 5 : La classe de conjugaison de $M \in GL_n(K)$ est sa classe de similitude. Diagonaliser une matrice consiste à déterminer une éventuelle matrice diagonale dans sa classe de conjugaison.

2) Application aux p-groupes [BERH]

DEF 6 : Soit p un nombre premier. Un p-groupe est un groupe fini dont l'ordre est une puissance de p.

THM 7 : (Equation aux classes) Si G agit sur un ensemble X fini, on a $\#X = \sum_{x \in S} Orb(x)$ où S est un système de représentants des orbites.

THM 8 : (Sur les p-groupes) Si G est un p-groupe agissant sur X fini, on a $\#X \equiv \#X^G \pmod{p}$ où $X^G = \{x \in X / \forall g \in G, g \cdot x = x\}$

PROP 9 : $g \in G$ est dans le centre $Z(G)$ si et seulement si sa classe de conjugaison est réduite à un élément.

PROP 10 : Si G est un p-groupe agissant sur lui-même par conjugaison, on a :
$$\#G = \#Z(G) + \sum_{x \in S, \#Orb(x) \geq 2} \#Orb(x)$$

COR 11 : Le centre d'un p-groupe n'est pas réduit à $\{e_G\}$.

DEV 1

PROP 12 : Soient $n, d \in \mathbb{N}^*$, $q \geq 2$. On pose r le reste de la division euclidienne de n par d. Alors $q^r - 1$ est le reste de la division euclidienne de $q^n - 1$ par $q^d - 1$. En particulier, $d | n$ si et seulement si $q^d - 1 | q^n - 1$.

THM 13 (Wedderburn) : Tout corps fini est commutatif.

II - Généralités sur les sous-groupes distingués

1) Sous-groupes distingués [BERH] [ULM]

DEF 14 : Soit H un sous-groupe de G. On dit que H est distingué dans G et on note $H \triangleleft G$ lorsque : $\forall g \in G, \forall h \in H, ghg^{-1} \in H$

REM 15 : Autrement dit, $H \triangleleft G$ lorsqu'il est stable par conjugaison.

EX 16 : Si G est abélien, tout sous-groupe de G est distingué dans G. $\{e_G\}$ et G sont distingués dans G.

EX 17 : $Z(G) \triangleleft G$

PROP 18 : L'intersection de sous-groupes distingués est un sous-groupe distingué.

PROP 19 : $H \triangleleft G \Leftrightarrow \forall g \in G, gHg^{-1} \subset H \Leftrightarrow \forall g \in G, gHg^{-1} = H$

PROP 20 : Soit $\varphi : G \to G'$ un morphisme de groupes.
- $\to$ Si $H' \triangleleft G'$, $\varphi^{-1}(H') \triangleleft G$
- $\to$ Si φ est surjectif, si $H \triangleleft G$, $\varphi(H) \triangleleft \varphi(G) = G'$

COR 21 : Si $\varphi : G \to G'$ est un morphisme de groupes, alors $\ker(\varphi) \triangleleft G$.

DEF 22 : Soient $g_1, g_2 \in G$. On appelle commutateur de g_1 et g_2 et on note $[g_1, g_2]$ le nombre $g_1 g_2 g_1^{-1} g_2^{-1}$. On appelle sous-groupe dérivé de G et on note $D(G)$ le sous-groupe engendré par les commutateurs.

REM 23 : Si G est abélien, $D(G) = \{e_G\}$. $D(G)$ mesure le "défaut de commutativité"

PROP 24 : Les commutateurs vérifient les propriétés :
1) $[g_1, g_2]^{-1} = [g_2, g_1]$ $\forall (g_1, g_2) \in G^2$
2) $h[g_1, g_2]h^{-1} = [hg_1h^{-1}, hg_2h^{-1}]$ $\forall (g_1, g_2, h) \in G^3$
3) $D(G) \triangleleft G$.

DEF 25: On dit que G est simple lorsque $G \neq \{e_G\}$ et lorsque G n'a pas de sous-groupe strict distingué dans G.

EX 26: Pour p premier, $\mathbb{Z}/p\mathbb{Z}$ est simple (voir plus loin)

2) Groupes quotients [BERH]

DEF 27: Soit H un sous-groupe de G. On définit sur G une relation d'équivalence : $x \sim y \iff x^{-1}y \in H$. Les classes d'équivalence pour cette relation sont les classes à gauche modulo H : $\forall x \in G$, $\bar{x} = xH = \{xh \mid h \in H\}$.

DEF 28: On note G/H l'ensemble des classes d'équivalence. On a alors une application surjective $\pi : \begin{array}{l} G \to G/H \\ x \mapsto \bar{x} \end{array}$.

REM 29: On souhaite définir une structure de groupes sur G/H de sorte que π soit un morphisme de groupes. La seule façon serait de poser $\bar{x}\bar{y} = \overline{xy}$ mais il faut que cette loi de composition sur G/H soit bien définie i.e qu'elle ne dépende pas du représentant de chaque classe.

PROP 30: Si une telle loi est bien définie sur G/H, alors $H \triangleleft G$.

PROP 31: Si $H \triangleleft G$, alors la loi interne $\begin{array}{l} G/H \times G/H \to G/H \\ (\bar{x}, \bar{y}) \mapsto \overline{xy} \end{array}$ est bien définie, de neutre $\overline{e_G} = H$ et induit sur G/H une structure de groupes. De plus, π est alors un morphisme de groupes de noyau H.

DEF 32: Le groupe G/H est appelé le groupe quotient de G par H.

DEF 33: Si G et H sont finis, G/H aussi et $\# G/H := [G:H]$ est appelé indice de H dans G.

PROP 34: (Lagrange) On a $\#G = \#H[G:H]$ (si G est fini)

EX 35: $\mathbb{Z}/n\mathbb{Z}$ est le quotient par $n\mathbb{Z} \triangleleft \mathbb{Z}$ ($\mathbb{Z}$ abélien)

PROP 36: Si $G/Z(G)$ est monogène, alors G est abélien

PROP 37: Soit G un groupe d'ordre p^2 avec p premier. Alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

THM 38: Il y a une bijection d'ensembles donnée par :

$$\left\{\begin{array}{c}\text{sous-groupes de } G \\ \text{contenant } H\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{sous-groupes} \\ \text{de } G/H\end{array}\right\} \quad (H \triangleleft G)$$
$$K \longmapsto \pi(K)$$
$$\pi^{-1}(L) \longleftarrow L$$

De même, on a une correspondance bijective donnant les sous groupes de G/H.

DEF 39. Le quotient $G/D(G)$ est abélien, on l'appelle l'abélianisé de G.

PROP 40: $D(G) = \bigcap_{\substack{H \triangleleft G \\ G/H \text{ abélien}}} H$.

3) Les théorèmes d'isomorphisme [BERH]

THM 41: (factorisation) Soit $H \triangleleft G$. Soit $f : G \to G'$ un morphisme de groupes tel que $H \subset \ker(f)$. Alors, il existe un unique morphisme de groupes $\tilde{f} : G/H \to G'$ tel que $\tilde{f} \circ \pi = f$. On le définit par : $\forall \bar{x} \in G/H$, $\tilde{f}(\bar{x}) = f(x)$.

De plus, pour tout groupe G' on a une bijection :

$$\mathrm{Hom}(G/H, G') \longrightarrow \{f \in \mathrm{Hom}(G, G') \mid H \subset \ker(f)\}$$
$$\varphi \longmapsto \varphi \circ \pi$$
$$\tilde{f} \longleftarrow f$$

THM 42 (Premier théorème d'isomorphisme) Soient G, G' deux groupes et $f : G \to G'$ un morphisme de groupes. Alors $G/\ker(f) \simeq \mathrm{Im}(f)$.

EX 43: Via $f : \begin{array}{l} \mathbb{C}^* \to \mathbb{R}_+^* \\ z \mapsto |z| \end{array}$ surjectif, on obtient $\mathbb{C}^*/\mathbb{U} \simeq \mathbb{R}_+^*$

EX 44: Via $f : \begin{array}{l} \mathbb{R} \to \mathbb{U} \\ \theta \mapsto e^{i\theta} \end{array}$ surjectif, on obtient $\mathbb{U} \simeq \mathbb{R}/2\pi\mathbb{Z}$

THM 45: (Deuxième théorème d'isomorphisme) Soient H, K deux sous-groupes. On suppose $H \triangleleft G$. Alors, on a :

(1) $HK = \{hk \mid h \in H, k \in K\}$ et $KH = \{kh \mid k \in K, h \in H\}$ sont des sous-groupes de G, $\langle H, K \rangle = HK = KH$

(2) $H \triangleleft HK$ et $H \cap K \triangleleft K$ de sorte que l'on a un isomorphisme $HK/H \simeq K/(H \cap K)$

III- Applications

1) Groupe symétrique et groupe alterné [BER] [ULM]

THM 46 : Soit $\sigma \in \mathfrak{S}_n$. Alors σ se décompose en produit de cycles à supports disjoints. Cette décomposition est unique à l'ordre près des facteurs.

THM 47 : $\mathfrak{S}_n$ est engendré par les transpositions.

THM 48 : Tous les p-cycles sont conjugués dans $\mathfrak{S}_n$ (pour $p \geq 2$)

DEF 49 : On appelle type d'une permutation $\sigma \in \mathfrak{S}_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux l_i des orbites dans $[\![1;n]\!]$ de l'action de $\langle\sigma\rangle$ sur $[\![1;n]\!]$, rangée en ordre croissant. l_1 est le nombre de points fixes, l_2 le nombre de transpositions, l_3 le nombre de 3-cycles dans la décomposition de σ.

PROP 50 : ρ et $\sigma \in \mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même type.

EX 51 : Dans $\mathfrak{S}_5$, $\sigma = (163)(24)$ et $\rho = (14)(235)$ sont de même type donc conjuguées. On a $\rho = \omega\sigma\omega^{-1}$ avec $\omega = (12)(356)$.

DEF 52 : Pour $\sigma \in \mathfrak{S}_n$, on appelle signature de $\mathfrak{S}_n$ le nombre $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$

PROP 53 : ε est un morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$. Si σ est une transposition, $\varepsilon(\sigma) = -1$. ε est l'unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbb{C}^*$.

DEF 54 : Le noyau de ε est appelé groupe alterné noté $\mathfrak{A}_n$.

PROP 55 : $\mathfrak{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$ donc de cardinal $\frac{n!}{2}$

DEV 2

PROP 56 : $\mathfrak{A}_n$ est engendré par les 3-cycles ~~pour~~

PROP 57 : Tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$.

THM 58 : Pour $n = 3$ ou $n \geq 5$, $\mathfrak{A}_n$ est simple.

REM 59 : $\mathfrak{A}_4$ n'est pas simple car $V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$ est distingué dans $\mathfrak{A}_4$.

2) Théorie de Sylow [BER]

On suppose G fini

DEF 60 : Écrivons $\#G = p^m q$, où $p \nmid q$, $m \geq 0$, p premier. Un p-sous-groupe de Sylow de G (ou p-Sylow) de G est un sous-groupe d'ordre p^m.

EX 61 : Le sous-groupe de $GL_n(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures à diagonale unité est un p-Sylow de G.

LEMME 62 : Soit H un sous-groupe de G. Si G admet un p-Sylow S alors : $\exists g \in G$, $gSg^{-1} \cap H$ est un p-Sylow de H.

THM 63 (1) Il existe des p-Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow

(2) Le conjugué d'un p-Sylow de G est un p-Sylow de G et tous les p-Sylow de G sont conjugués. De plus, si S est un p-Sylow de G, $S \triangleleft G \Leftrightarrow S$ est unique

(3) Si n_p est le nombre de p-Sylow de G, on a $n_p \equiv 1 \mod p$ et $n_p \mid q$.

EX 64 : Un groupe d'ordre 63 n'est pas simple.

3) Groupe linéaire [PER]

Soit E un K-espace vectoriel de dimension finie

THM 65 : Les transvections et dilatations engendrent $GL(E)$. Les transvections engendrent $SL(E)$

COR 66 : $GL_n(\mathbb{C})$, $SL_n(\mathbb{R})$ et $SL_n(\mathbb{C})$ sont connexes par arcs.

PROP 67 : Soit τ une transvection de droite D d'hyperplan H et soit $u \in GL(E)$. Alors $u\tau u^{-1}$ est une transvection de droite $u(D)$ et d'hyperplan $u(H)$.

PROP 68 : Deux dilatations sont conjuguées dans $GL(E)$ ~~si et seulement si~~ elles ssi elles ont même rapport

PROP 69 : Deux transvections sont conjuguées dans $GL(E)$. Pour $\dim(E) \geq 3$, elles le sont aussi dans $SL(E)$.