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

Dans toute cette leçon, G et G' sont des groupes.

I) Conjugaison dans un groupe

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

Le morphisme de groupes correspondant de $(G,\cdot)$ dans $(\mathfrak{S}(G),\circ)$ est noté : $\mathrm{Int}(g) : G \longrightarrow G$, $h \longmapsto ghg^{-1}$.

L'image de ce morphisme est le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G.

Définitions - Proposition 2 : Si $P \subset G$, $\forall g \in G$, on note gPg^{-1} l'image de P par $\mathrm{Int}(g)$.

gPg^{-1} est fini ssi P est fini et dans ce cas $|gPg^{-1}| = |P|$

Définition - Proposition 3 : Soient $x, x' \in G$, x et x' sont conjugués lorsque $\exists g \in G$ tq $x = gx'g^{-1}$. Cela définit une relation d'équivalence sur G dont les classes d'équivalences sont appelées les classes de conjugaison.

Exemple 4 : 1) Les classes de conjugaison dans $GL_n(\mathbb{K})$ sont les classes de similitudes.

2) $\forall x \in G$, on a $\mathrm{Conj}_G(x) = \{x\}$ ssi x commute avec tous les éléments de G.

En particulier, si G est abélien, $\mathrm{Conj}_G(x) = \{x\}$ $\forall x \in G$.

3) Si E est un $\mathbb{K}$-ev de dim ≥ 2, les transvections sont toutes conjuguées dans $GL(E)$, si de plus $n \geq 3$, elles le sont toutes dans $SL(E)$.

4) Si E est un espace euclidien de dim $n \geq 2$. Alors deux réflexions orthogonales sont conjuguées par un élément de $SO(E)$.

En particulier, les réflexions orthogonales sont conjuguées dans $O(E)$.

De même, deux renversements sont conjugués dans $SO(E)$.

Définition - Proposition 5 : Pour $a \in G$, le sous-ensemble de G pour la conjugaison s'appelle le centralisateur :

$$\mathcal{C}_a = \{g \in G,\ gag^{-1} = a\}.$$

Proposition 6 : 1) Si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1, \dots, a_p)$ et si $\tau \in \mathfrak{S}_n$, on a $\tau\sigma\tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$

2) Dans $\mathfrak{S}_n$, tous les cycles d'ordre p sont conjugués.

3) Si $n \geq 5$ les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$.

Contre exemple 7 : Si $n = 3$, A_3 est abélien donc la conjugaison y est triviale.

Si $n = 4$: il y a 8 cycles d'ordre 3 alors que $|A_4| = 12$.

II) Sous groupes distingués et groupes quotients.

1) Préliminaires

Notation 8 : $\forall g \in G$ et $\forall H \subset G$, on note $gH = \{gh, h \in H\}$ et $Hg = \{hg, h \in H\}$

On note $G/H = \{gH, g \in G\}$ et $H\backslash G = \{Hg, g \in G\}$

Proposition 9 : Si H est un sous groupe de G, l'ensemble des classes à gauche (resp à droite) modulo H sont deux-à-deux distinctes et forment une partition de G.

Définition 10 : L'application $\pi_H : G \longrightarrow G/H$, $g \longmapsto gH$ est surjective.

C'est la surjection canonique de G sur G/H.

Théorème 11 : (Lagrange) Si G est fini d'ordre $n \geq 2$ et H sous groupe de G, $\forall g \in G$, $|gH| = |H|$ et $|G| = |G/H||H|$ donc l'ordre de H divise celui de G.

2) Sous groupes distingués.

Définition 12 : On dit qu'un sous groupe H de G est distingué lorsque $gH = Hg$ $\forall g \in G$.

i.e. $\forall h \in H \; \forall g \in G \; / \; ghg^{-1} \in H$.

Remarque 13 : $H \lhd G$ si H est stable par tout automorphisme intérieur.

Exemples 14 : 1) $\{e\}$ et G sont $\lhd G$

2) L'intersection de deux sous groupes distingués est un sous groupe distingué.

3) Si G est commutatif, alors tous ses sous-groupes sont distingués.

Proposition 15 : Si G et G' sont deux groupes et si φ est un morphisme de groupe de G dans G', alors $\ker \varphi \lhd G$.

Exemples 16 : 1) $Z(G) \lhd G$

2) $\forall n \in \mathbb{N}^*$, $\mathcal{D}_n \lhd \mathcal{C}_n$

3) $\forall n \in \mathbb{N}^*$, $SO_n \lhd O_n$.

Définition 17 : Un groupe $G \neq \{1\}$ est dit simple lorsque ses seuls sous groupes distingués sont $\{1\}$ et G.

Exemples 18 : 1) $\mathbb{Z}/p\mathbb{Z}$ est simple si p est premier

2) $SO_3(\mathbb{R})$ est simple. dev 1

3) Construisons les groupes quotients !

Théorème 19 : Un sous groupe H de G est distingué si $\exists!$ structure de groupe sur l'ensemble quotient G/H telle que la surjection canonique $\pi_H : G \longrightarrow G/H$ soit un morphisme de groupes.

Théorème 20 : (de factorisation) Soit $H \lhd G$. Soit $f : G \longrightarrow G'$ un morphisme de groupes tel que $H \subset \ker(f)$.
Alors $\exists!$ morphisme de groupe $\overline{f} : G/H \longrightarrow G'$ tq $f = \overline{f} \circ \pi$

Lemme 21 : Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors le morphisme de groupes $\overline{f} : G/\ker f \longrightarrow G'$ est injectif.

Théorème 22 : (1er th d'isomorphisme) Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors le morphisme de groupe $\overline{f} : G/\ker f \longrightarrow G'$ induit un isomorphisme de groupes $G/\ker(f) \simeq \operatorname{Im} f$.

Exemple 23 : 1) $\mathbb{C}^*/\mathbb{U} \simeq \mathbb{R}_+^*$ via $f : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$, $z \longmapsto |z|$

2) $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$ via $f : \mathbb{R} \longrightarrow \mathbb{U}$, $\theta \longmapsto e^{i\theta}$.

Théorème 24 : (2e th d'isomorphisme) Soient H et K deux sous groupes de G. On suppose $H \lhd G$. Alors :

1) HK et KH sont des sous groupes de G et $HK = KH$.

2) $H \lhd HK$ et $H \cap K \lhd K$.

3) On a $HK/H \simeq K/H\cap K$

Théorème 25 : (3e th d'isomorphisme) Soient H et K deux sous groupes de G. On suppose que H et K sont $\lhd$ dans G et que K est un sous groupe de H.

Alors 1) $K \lhd H$

2) $H/K \lhd G/K$

3) $(G/K)/(H/K) \simeq G/H$

III) Pour aller plus loin : Théorème de Sylow

1) Théorème de Sylow.

Définition 26 : Si G est fini et si p est premier.
G est un p groupe lorsque $|G| = p^\alpha$ pour un certain α.

Définition 27 : Si $|G| = p^\alpha m$ avec $p \nmid m$, un p-Sylow de G est un sous groupe de G d'ordre p^α.

Lemme 28 : $|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$

Lemme 29 : Si G est fini et $|G| = p^m q$ avec $p \nmid q$
Soit H un sous groupe de G. Si G admet un p-Sylow S.
Alors, $\exists g \in G$ tq $gSg^{-1} \cap H$ soit un p-Sylow de H.

Théorème 30 : (Sylow) Si G est fini et si p est premier tq $|G| = p^m q$ avec $p \nmid q$
Alors 1) $\exists$ des p-Sylow de G et tout p-sous groupe de G est contenu dans un p-Sylow.

deux 2

2) Le conjugué d'un p-Sylow de G est un p-Sylow de G et tous les p-Sylow de G sont conjugués.
En particulier, si S est un p-Sylow de G, alors S est distingué dans G ssi S est l'unique p-Sylow de G.

3) Si N_p est le nombre de p-Sylow de G, on a :
$N_p \equiv 1 [p]$ et $N_p \mid q$.

Application 31 : Un groupe d'ordre 33 est cyclique

Application 32 : Un groupe d'ordre 63 n'est pas simple.

2) Application : Simplicité de A_n.

Lemme 33 : Pour $n \geq 5$, A_n est engendré par les 3 cycles.

Lemme 34 : Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n

Lemme 35 : Les doubles transpositions sont conjugués dans A_5.

Théorème 36 : Pour $n \geq 5$, A_n est simple

Contre-exemple 37 : A_4 n'est pas simple car $V_4 \lhd A_4$
où $V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$.

deux possible