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

I) Conjugaison

a) Généralités

Déf 1 : Soit G un groupe et soient deux parties P et P' de G. On dit que P et P' sont conjuguées dans G s'il existe $g \in G$ tel que $P' = gPg^{-1}$. Deux éléments x et x' de G sont conjugués dans G s'il existe $g \in G$ tel que $x' = gxg^{-1}$. On note $\mathrm{Int}_g : G \to G$, $x \mapsto gxg^{-1}$ l'application automorph. intérieure.

Déf 2 : Soit G un groupe. La classe de conjugaison de $x \in G$ est :

$$\mathrm{Conj}_G(x) = \{gxg^{-1} ; g \in G\}$$

Rq 3 : La relation « être conjugués dans G » est une relation d'équivalence dont les classes d'équivalence sont les classes d'éléments de G.

Ex 4 : Deux permutations dans $\mathfrak{S}(E)$ si et seulement si, les listes des longueurs des cycles à supports disjoints qui les composent sont les mêmes à l'ordre près.

Ex 5 : Si G est un groupe et si $x \in G$, on a $\mathrm{Conj}_G(x) = \{x\}$ si et seulement si x commute avec tout élément de G.

b) Application à la réduction des endomorphismes

Déf 6 : Deux matrices sont semblables si et seulement si elles sont dans la même orbite de conjugaison sous l'action de $GL_n(\mathbb{C})$ - L'orbite d'une matrice A sous l'action de $GL_n(\mathbb{C})$ par conjugaison, aussi appelée classe de similitude est :

$$\mathrm{Conj}(A) = \{PAP^{-1}, P \in GL_n(\mathbb{C})\}.$$

Déf 7 : Une matrice A de $M_n(\mathbb{C})$ est diagonalisable si et seulement si elle est semblable à une matrice diagonalisable.

Déf 8 : Une matrice A de $M_n(\mathbb{C})$ est trigonalisable si et seulement si elle est semblable à une matrice triangulaire supérieure.

Rq 9 : Une matrice diagonale est un représentant « simple » de sa classe de conjugaison.

Prop 10 : Le polynôme caractéristique et le spectre (= valeurs propres comptées avec multiplicités) sont des invariants totaux de similitude pour les matrices diagonalisables.

Prop 11 : Le polynôme minimal, le déterminant, la trace sont des invariants (non totaux) de similitude).

Ex 12 : $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ ont même polynôme minimal mais ne sont pas semblables.

c) Un résultat de commutativité

Déf 13 : Soit G un groupe. Le centre d'un groupe $\cdot$ est l'ensemble :

$$Z(G) = \{z \in G, zg = gz \text{ pour tout } g \in G\}$$

Rq 14 : $Z(G) = G$ si et seulement si G est abélien.

Déf 15 : Soit G un groupe et soit $g \in G$. Le centralisateur de g, noté Z_g ou $C(g)$, est l'ensemble des éléments de G commutant avec g :

$$C(g) = \{g' \in G, gg' = g'g\}$$

Ex 16 : On a bien sûr $C(1_G) = G$

Thm 17 : Soit G un groupe fini non abélien. (Théorème de Dixon) La probabilité $p(G)$ pour que deux éléments tirés uniformément et indépendamment commutent est majorée par $5/8$.

Thm 18 : Formule de Burnside

Soit G un groupe fini opérant sur un ensemble fini E. Pour tout $g \in G$, on note $\mathrm{Fix}(g) = \{x \in E, g \cdot x = x\}$. Le cardinal du nombre d'orbites, noté $\mathcal{C}$, vérifie :

$$\mathcal{C} = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Coro 19 : En utilisant les notations du théorème 17, on a $p(G) = \frac{k}{n}$ où k est le nombre de classes de conjugaison de G.

Rq 20 : L'inégalité trouvée au théorème 17 est maximale : en considérant D_4 le groupe diédral à 8 éléments, on a

$$p(D_8) = \frac{5}{8}$$

DEV. 1

II) Sous-groupes distingués et groupes quotients

a) Sous-groupe distingué

Déf 21 : Soit G un groupe. Soit H un sous-groupe de G. On dit que H est distingué dans G si l'on a :

$$\forall h \in H, \forall g \in G, ghg^{-1} \in H$$

Autrement dit, H est distingué dans G s'il est stable par tout automorphisme intérieur (cf définition 1) de G.

Nota 22 : Si H est distingué dans G on note $H \lhd G$

Ex 23 :
- si G est abélien, tout sous-groupe de G est distingué dans G
- $\{1_G\} \lhd G$ et $G \lhd G$
- $Z(G) \lhd G$

Prop 24 : Soit $f : G \to G'$ un morphisme de groupes. Alors, $\ker(f)$ est un sous-groupe distingué de G.

Rq 25 : Réciproquement, tout sous-groupe distingué pourra être vu comme le noyau d'un certain morphisme de projection (cf II b) 2c)

Ex 26 : Soit E un K-espace vectoriel de dimension finie. On note $SL(E) = \{u \in \mathcal{L}(E), \det u = 1\}$. On a $SL(E) \lhd GL(E)$ car c'est le noyau du morphisme déterminant $\det : GL(E) \to K^\times$

Ex 27 : Pour tout $n \geq 2$, le groupe alterné $\mathfrak{A}_n$ est un sous-groupe distingué du groupe symétrique $\mathfrak{S}_n$, puisque c'est le noyau du morphisme signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$

Déf 28 : On dit qu'un groupe G est simple si $G \neq \{1_G\}$ et si G n'a pas de sous-groupe propre qui soit distingué dans G.

Ex 29 : $\mathfrak{S}_n$ n'est pas simple pour $n \geq 3$, puisque $\mathfrak{A}_n$ est un sous-groupe propre distingué dans $\mathfrak{S}_n$.

Thm 30 : Soit E un ensemble fini à n ($n \geq 3$) éléments. Alors, le groupe alterné $\mathfrak{A}_n$ est simple si et seulement si $n \neq 4$.

Ex 31 : On a $Z(GL(E)) = K^\times \cdot id$ donc en général $GL(E)$ n'est pas simple.

b) Groupe quotient

Prop 32 : Soit $H \lhd G$. Alors la loi interne

$$\begin{aligned} G/H \times G/H &\to G/H \\ (\bar{x}, \bar{y}) &\longmapsto \overline{xy} \end{aligned}$$

est bien définie, de neutre $\bar{1}_G$ et induit sur G/H une structure de groupes. De plus, l'application $\pi : G \to G/H$, $x \mapsto \bar{x}$ est un morphisme de groupes.

Déf 33 : Soit G un groupe et soit $H \lhd G$. Le groupe G/H est appelé le groupe quotient de G par H.

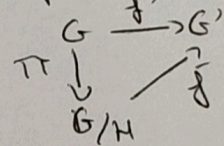
Rq 34 : Pour tout $x \in G$, on a $\bar{x} = \bar{1}_G$ si et seulement si $x \in H$.

Prop 35 : (Théorème de Lagrange) Soient G un groupe et $H \lhd G$. On a $|G/H| = [G : H] = \frac{|G|}{|H|}$

Ex 36 :
- $G/G = \{\bar{1}_G\}$
- $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

c) Théorèmes de factorisation

Thm 37 : Soit G un groupe et soit $H \lhd G$. Soit $f : G \to G'$ un morphisme de groupes tels que $H \subset \ker(f)$. Alors, il existe un unique morphisme de groupes $\bar{f} : G/H \to G'$ tel que $f = \bar{f} \circ \pi$



Rq 38 : Comme mentionné dans la remarque 25, tout sous-groupe distingué peut être vu comme $\ker(\pi)$ où $\pi : G \to G/H$ est la projection canonique (cf remarque 34).

Lemme 39 : Soit $f : G \to G'$ un morphisme de groupes. Alors, le morphisme de groupes $\bar{f} : G/\ker(f) \to G'$ est injective.

Coro 40 : (Premier théorème d'isomorphisme) Soient G, G' deux groupes. Alors, le morphisme de groupes $f : G/\ker(f) \to G'$ induit un isomorphisme de groupes $G/\ker(f) \xrightarrow{\sim} \mathrm{Im}(f)$

Ex 44 : En considérant le morphisme de groupes surjectif

$$f : \mathbb{R} \to \mathbb{U}, \quad \theta \mapsto e^{i\theta}$$

on obtient $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$

d) Application aux théorèmes de Sylow

Déf 42 : Soit p un nombre premier. On dit que G est un p-groupe si $|G| = p^\alpha$ où $\alpha \geq 0$.

Déf 43 : Soit G un groupe fini, et soit p un nombre premier. Un p-sous-groupe de G est un sous-groupe de G qui est un p-groupe. Ecrivons $|G| = p^m q$ où $p \nmid q$ et $m \geq 0$. Un p-Sylow de G est un p-sous-groupe de G d'ordre p^m. Autrement dit, un sous-groupe S est un p-Sylow du groupe G si et seulement si S est un p-groupe et $p \nmid [G : S]$

Thm 44 : (Bayley) Tout groupe G s'identifie à un sous-groupe de $\mathfrak{S}_n$, où $n = |G|$

Lemme 45 : Soit G un groupe fini avec $|G| = m = p^m q$ où $p \nmid q$ $m \geq 0$. Soit H un sous-groupe de G. Supposons que G admette un p-Sylow S. Alors, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.

Prop 46 : Soit G un groupe opérant sur E. Si G est fini, pour tout $x \in G$, l'ensemble Gx (orbite de x sous l'action de G) est fini et son cardinal vérifie :

$$|Gx| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$$

Thm 47 : Soit G un p-groupe agissant sur un ensemble fini E. Alors, on a $|E| \equiv |E^G| \ (p)$ où E^G est l'ensemble des éléments fixés par l'action.

Thm 48 : Théorèmes de Sylow

Soit G un groupe fini, et soit p un nombre premier. Ecrivons $|G| = p^m q$ avec $m \geq 0$ et $p \nmid q$. Alors

(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. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si et seulement si, 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 $n_p \mid q$.

Ex 49 : Un groupe d'ordre 63 n'est pas simple.

Appli 50 : $\mathfrak{A}_5$ est l'unique groupe simple d'ordre 60 à isomorphisme près.