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

I Action par conjugaison dans un groupe.

A Conjugaison et classe de conjugaison. Per 1.4

Définition 1 : On peut faire opérer un groupe G sur lui-même par automorphisme intérieur en posant $g.a = gag^{-1}$.

Définition 2 : Les orbites sous cette action sont appelées classes de conjugaison $O(a) = \{gag^{-1}, g \in G\}$ pour tout $a \in G$.

Exemple 3 : si G est abélien, pour tout $a \in G$, $O(a) = \{a\}$.

Définition 4 : Les stabilisateurs de cette action s'appellent les centralisateurs
$$Stab(a) = H_a = \{g \in G, gag^{-1} = a\} = \{g \in G, ga = ag\}$$

Exemple 5 : si G est abélien, pour tout $a \in G$, $H_a = G$.

Remarque 6 : On étend la définition 4 à une partie A de G :
$$C_G(A) = \{g \in G \mid \forall a \in A,\ ga = ag\}.$$
En particulier $C_G(G) = Z(G)$ est le centre de G.

B Classes de conjugaison dans le groupe symétrique. Per 1.4

Proposition 7 : i) Si $\sigma \in S_n$ est un cycle d'ordre p, $\sigma = (a_1, \dots, a_p)$ et si $\tau \in S_n$ on a $\tau \sigma \tau^{-1} = (\tau(a_1), \dots, \tau(a_p))$
ii) Dans S_n, tous les cycles d'ordre p sont conjugués.
iii) Si $n \geq 5$ les cycles d'ordres 3 sont conjugués dans A_n.

Lemme 8 : Le groupe A_n est $n-2$ fois transitif sur $\{1, \dots, n\}$ i.e si on a $a_1, \dots, a_{n-2}$ distincts et $b_1, \dots, b_{n-2}$ distincts, il existe $\sigma \in A_n$ tel que $\sigma(a_i) = b_i$

Exemple 9 : C'est faux si $n = 3$ ou 4. En effet pour $n = 3$, A_3 est abélien donc la conjugaison est triviale. Pour $n = 4$ il y a 8 cycles d'ordre 3 et donc peuvent être tous conjugués dans A_4 sinon ils formeraient une orbite dont le cardinal devrait diviser 12.

Exemple 10 : Soit $\mathbb{K}$ un corps commutatif, $GL(n, \mathbb{K})$ le groupe des matrices carrées d'ordre n inversibles à coefficients dans $\mathbb{K}$. Alors pour $A, B \in GL_n(\mathbb{K})$:
A, B conjugués $\Leftrightarrow \exists P \in GL_n(\mathbb{K}), B = P^{-1}AP \Leftrightarrow A, B$ semblables.

C Classes de conjugaison dans $End(E)$.

Soit E un $\mathbb{K}$-ev, $f \in End(E)$
X-G Annexe B.

Notation 11 : On note π_f le polynôme minimal de f, et $\mathcal{L}_f$ l'ensemble $\{P(f) \mid P \in \mathbb{K}[X]\}$. Si $x \in E$, on note P_x le polynôme unitaire engendrant l'idéal $\{P \in \mathbb{K}[X] \mid P(f)(x) = 0\}$ et E_x l'ensemble $\{P(f)(x) \mid P \in \mathbb{K}[X]\}$.

Proposition 12 : Si $k = \deg \pi_f$, l'ensemble $\mathcal{L}_f$ est un sev de $\mathcal{L}(E)$ de dimension k, dont une base est $(id_E, f, \dots, f^{k-1})$. Si l est le degré de P_x, l'ensemble E_x est un sev de E de dimension l dont une base est $(x, \dots, f^{l-1}(x))$.

Proposition 13 : Il existe $x \in E$ tel que $P_x = \pi_f$.

Définition 14 : On dit que f est cyclique s'il existe $x \in E$ tel que $E_x = E$.
D'après les propositions précédentes, cela équivaut à dire $\deg \pi_f = n$ (ou encore que $\pi_f = \chi_f$ où χ_f désigne le polynôme caractéristique de f).

Définition 15 : Soit $P = X^p + a_{p-1}X^{p-1} + \dots + a_0 \in \mathbb{K}[X]$. On appelle matrice compagnon de P la matrice
$$C(P) = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{p-2} \\ 0 & & 1 & -a_{p-1} \end{pmatrix} \in M_p(\mathbb{K})$$

Proposition 16 : Soit $P \in \mathbb{K}[X]$, alors $\pi_{C(P)} = \chi_{C(P)} = P$.

Proposition 17 : Soit $f \in \mathcal{L}(E)$ un endomorphisme cyclique. Il existe une base de E dans laquelle la matrice de f est égale à $C(\pi_f)$.

Proposition 18 : Soit $f \in \mathcal{L}(E)$. Il existe une suite $F_1, F_2, \dots, F_n$ de sev de E, tous stables par f telle que : i) $E = F_1 \oplus \dots \oplus F_n$
ii) $\forall i \in \{1, \dots, n\}$, la restriction $f_i = f_{|F_i}$ est un endomorphisme de F_i cyclique.
iii) si P_i désigne le polynôme minimal de f_i, on a $P_{i+1} | P_i \quad \forall i \in [\![1, n-1]\!]$

Remarque 19 : La suite $P_1, \dots, P_n$ ne dépend que de f et non du choix de la décomposition. On l'appelle suite des invariants de similitude de f.

Théorème 20 : (Réduction de Frobenius) Si $P_1, \dots, P_n$ désigne la suite des invariants de similitude de $f \in \mathcal{L}(E)$, il existe une base B de E telle que $[f]_B = \begin{pmatrix} C(P_1) & & 0 \\ & \ddots & \\ 0 & & C(P_n) \end{pmatrix}$
On a d'ailleurs $P_1 = \pi_f$ et $P_1 \cdots P_n = \chi_f$.

Corollaire 21 : Deux endomorphismes f et $g \in \mathcal{L}(E)$ sont semblables si et seulement s'ils ont les même invariants de similitude.

Application/développement : déterminant circulant.

II Sous groupes stables par conjugaison

A Les sous groupes distingués Par 1.2 + exo et Ulm 6.

Soit H un sous groupe de G.

Définition 22 : On dit que H est distingué dans G et on note $H \triangleleft G$ s'il est invariant par automorphisme intérieur ie si on a :
$$\forall a \in G, \forall h \in H, \ a h a^{-1} \in H.$$

Exemple 23 : 1) $\{1\}$ et G sont toujours distingués dans G (dits triviaux)
2) Si G est abélien tout sous groupe de G est distingué.

Remarque 24 : Si $f : G \to G'$ est un homomorphisme, alors $\ker f \triangleleft G$.

Proposition 25 : Soit $H' \triangleleft G$, si $H \triangleleft G$ alors $H \cap H' \triangleleft G$.

Proposition 26 : Si $K < H < G$ et $K \triangleleft G$ alors $K \triangleleft H$

Remarque 27 : Si $K \triangleleft H \triangleleft G$ alors on a pas forcément $K \triangleleft G$. Par exemple $\{id, (12)(34)\} \triangleleft V_4 \triangleleft S_4$ mais $\{id, (12)(34)\} \not\triangleleft S_4$.

B Exemples du centre d'un groupe et du groupe dérivé Par 1.3

Définition 28 : Le centre du groupe G est le sous groupe de G formé des éléments qui commutent avec tous les autres : $Z(G) = \{a \in G \mid \forall g \in G, ag = ga\}$

Proposition 29 : On a $Z(G) \triangleleft G$.

Exemple 30 : Si G est abélien, $Z(G) = G$

Si $G = S_n$ avec $n \geq 3$, on a $Z(G) = \{1\}$.

Définition 31 : Le groupe dérivé $D(G)$ est le sous groupe engendré par les commutateurs de G ie les éléments de la forme $xyx^{-1}y^{-1}$ avec $x, y \in G$.

Proposition 32 : On a $D(G) \triangleleft G$.

Exemple 33 : Si G est abélien on a $D(G) = \{1\}$.
Si $G = S_3$ on a $D(G) = \{1, \sigma, \sigma^2\}$

C Lien avec les groupes quotients. Ulm 6

Déf-prop 34 : Soit G un groupe. Un sous groupe H de G est distingué dans G si et seulement si la formule $g_1 H * g_2 H = (g_1 g_2) H$ définit sur lui même la loi de groupe $*$ sur l'ensemble quotient G/H telle que l'application canonique
$\pi : G \to G/H$, $g \mapsto gH$ soit un morphisme de groupe. Ces propriétés déterminent la loi $*$ de manière unique et le groupe $(G/H, *)$ est appelé groupe quotient de G par H.

Proposition 35 : Si $H \triangleleft G$ alors $\pi : G \to G/H$ est un morphisme surjectif de noyau H.

Proposition 36 : $|G/H| = [G : H]$ et si G est fini alors $|G/H| = \frac{|G|}{|H|}$.

Exemples 37 : i) $n\mathbb{Z} \triangleleft \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique d'ordre n.
ii) $A_n = \ker(\varepsilon) \triangleleft S_n$ et $S_n/A_n \simeq S_2 \simeq \mathbb{Z}/2\mathbb{Z}$.

Théorème 38 : Soit G et Γ deux groupes, H distingué dans G, $\pi : G \to G/H$ le morphisme canonique et $\varphi : G \to \Gamma$ un morphisme de groupes. On a équivalence entre :
i) $H \subset \ker(\varphi)$
ii) $\varphi(H) = \{e_\Gamma\}$
iii) Le morphisme φ se "factorise" à travers G/H ie il existe un morphisme de groupes $\overline{\varphi} : G/H \to \Gamma$ tel que $\varphi = \overline{\varphi} \circ \pi$
Dans ce cas $\overline{\varphi}$ est unique, donné par $\overline{\varphi}(gH) = \varphi(g)$, $\mathrm{Im}(\varphi) = \mathrm{Im}(\overline{\varphi})$ et $\ker(\overline{\varphi}) = \ker(\varphi)/H$.

Théorème 39 : Le groupe dérivé $D(G)$ et $H \lhd G$, alors :
i) $G/D(G)$ est un groupe abélien appelé l'abélianisé de G.
ii) $D(G) \subset H \iff H \lhd G$ et G/H est abélien.

Théorème 40 (d'isomorphisme 1) : Soit $\varphi : G \to \Gamma$ un morphisme de groupes. Alors il existe un isomorphisme
$\overline{\varphi} : G/\ker(\varphi) \to \mathrm{Im}(\varphi)$, $g\ker(\varphi) \mapsto \varphi(g)$.
En particulier si φ est surjectif alors $\overline{\varphi}$ fournit un isomorphisme entre $G/\ker(\varphi)$ et Γ.

Corollaire 41 : Un groupe cyclique fini G d'ordre $m \in \mathbb{N}$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Théorème 42 (d'isomorphisme 3) Soient $K \subset H \subset G$ trois groupes. On suppose que $H \lhd G$ et $K \lhd G$. Alors $(G/K)/(H/K) \cong G/H$.

Exemple 43 : $(\mathbb{Z}/10\mathbb{Z})/(2\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

III Groupes remarquables sans sous groupes distingués

A Les groupes simples Ulm 5.3.

Définition 44 : Un groupe $G \neq \{e\}$ est appelé un groupe simple si les seuls sous groupes distingués de G sont les groupes triviaux G et $\{e\}$.

Exemple 45 : Soit $p \in \mathcal{P}$, alors $\mathbb{Z}/p\mathbb{Z}$ est simple

Lemme 46 : Soit $N \lhd A_m$, si N contient un 3 cycle alors $N = A_m$.

Développement : Soit $m \geq 5$, alors A_m est simple.

Remarque 47 : A_1, A_2, A_3 sont simples
A_4 n'est pas simple car $V_4 \lhd A_4$ (V_4 groupe de Klein).

B p groupes et théorèmes de Sylows. Per 1.4 et 1.5

Définition 48 : Si $p \in \mathcal{P}$ on appelle p groupe un groupe dont le cardinal est une puissance de p.

Proposition 49 : Le centre d'un p groupe distinct de $\{1\}$ n'est pas réduit à $\{e\}$.

Lemme 50 : Soit G un p groupe opérant sur un ensemble X et soit X^G l'ensemble des points fixes de X sous G. Alors on a $|X| \equiv |X^G| \ [p]$

Soit G un groupe d'ordre $m = p^\alpha m$, $p \nmid m$, $\alpha \in \mathbb{N}$.

Définition 51 : On appelle p sous groupe de Sylow de G un sous groupe d'ordre p^α

Exemple 52 : $T_m^{+1}(\mathbb{F}_p)$ est un p Sylow de $GL_m(\mathbb{F}_p)$.

Lemme 53 : Soit H un sous groupe de G et S un p Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p Sylow de H.

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

Corollaire 54 : Si $|G| = p^\alpha m$, $p \nmid m$, G contient des sous groupes d'ordre p^i pour tout $i \leq \alpha$.

Théorème 55 (Sylow 2) : i) Si $H < G$ qui est un p groupe, il existe S un p Sylow avec $H \subset S$.
ii) Les p Sylow sont tous conjugués (et donc leur nombre k divise m).
iii) On a $k \equiv 1 \ [p]$ (donc k divise m).

Corollaire 56 : Si S est un p Sylow de G on a :
$S \lhd G \iff S$ est l'unique p Sylow de $G \iff k = 1$

Application 57 : Un groupe d'ordre 63 n'est pas simple

Références :

- D. Perrin Cours d'Algèbre. Per
- Théorie des groupes Ulmer. Ulm
- Xavier Gourdon Algèbre X.G