Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotient. Applications

103

I) Conjugaison dans un groupe

G groupe x, d'ordre fini |G|

a) Classes d'un sous-groupe

def 1 : si H ss-groupe de G, H<G, pour a ∈ G, la classe à gauche de a par rapport à H, est aH = {ah, h∈H} (de même à droite)

$G/H_g = \{aH, a \in G\}$ et $[G:H] = |G/H|$ = indice de H dans G

prop 2 : les classes à gauche sont en bijection avec les classes à droite

prop 3 : Les classes à gauche forment une partition de G

ex 4 : H_8, $H = \langle i, -1 \rangle < H_8$. $\{H, iH, jH, kH\}$ sont les classes à gauche / H.

prop 5 : transitivité des indices. si K < H < G, [G:K] = [G:H].[H:K]

Th 6 : Lagrange si H<G, |G| = [G:H].|H|

Ctrex 7 : G/H n'est pas 1 groupe en général : si G = S_3, H = {id, (23)}

G/H ne peut être muni d'une structure de groupe.

def 8 : on dit que H<G est distingué dans G, noté H ◁ G, si on a ∀a∈G, ∀h∈H, $aha^{-1} \in H$

ou de manière équivalente aH = Ha ∀a∈G.

prop 9 : si [G:H] = 2, alors H ◁ G

ex 10 : {e} et G sont distingués dans G

* dans S_n, $[S_n : A_n] = 2$ donc $A_n \triangleleft S_n$
* si G abélien, tous ses ss-gpes sont distingués (△ réciproque fausse)

prop 11 : si f ∈ Hom(G,G'), alors Ker f ◁ G

ex 12 : SO(E) ◁ O(E) pour E ev de dim finie

$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$

b) Action de conjugaison

def/prop 13 : L'automorphisme intérieur $\psi_g : \begin{matrix} G \to G \\ a \to gag^{-1} \end{matrix}$ permet de définir une action de groupe appelée action de conjugaison. $g.a = gag^{-1}$. $\omega(a) = \{gag^{-1}, g \in G\}$ est appelée classe de conjugaison de a.

Rq 14 : G agit également sur ses sous-groupes : H<G $g.H = gHg^{-1}$

ex 15 : si $\sigma \in S_n$, $\sigma = (a_1 \dots a_k)$, $\forall \tau \in S_n$, $\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_k))$

tous les cycles d'ordre $k \leq n$ sont conjugués dans S_n.

Les classes de conjugaison sont en bijection avec les partitions de n.

def 16 : Normalisateur de H<G : $N_G(H) = Stab_H = \{g \in G \mid gHg^{-1} = H\}$

prop 17 : $N_G(H)$ est le plus grand groupe dans lequel H distingué

Ainsi H ◁ G ⟺ $N_G(H) = G$

ex 18 : $U = \left\{\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{F}_p)\right\}$ alors $N_{GL_3}(U) = \left\{\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \in GL_3(\mathbb{F}_p)\right\}$

prop 19 : pour G ↷ X, x' dans l'orbite de x sous G, alors $Stab_{x'}$ et $Stab_x$ sont des sous-groupes conjugués de G.

Ex 20 : (groupe non fini) G = GL(E)

A et B conjugués ssi ∃P∈GL(E) tq $B = P^{-1}AP$

ssi A et B sont semblables

Th 21 structure. si H◁G, il existe une unique structure de groupe sur G/H, telle que la projection $G \xrightarrow{\pi} G/H$ soit un homomorphisme.

II) Exemples de sous-groupes distingués. Morphisme

a) Centre, groupe dérivé

def 22 : centralisateur de a∈G. $C_G(a) = \{g \in G, gag^{-1} = a\}$ | sous-groupes de G

si A ⊂ G, $C_G(A) = \{g \in G, \forall a \in A, gag^{-1} = a\}$

def 23 : Le centre de G, noté $Z(G) = \mathcal{C}_G(G) = \{g \in G, \forall a \in G, ga = ag\}$

prop. 24 $Z(G) \triangleleft G$, et $Z(G)$ est abélien

ex. 25. * si G abélien, $Z(G) = G$ * $Z(GL_n(\mathbb{K})) = \{\lambda I_n, \lambda \in \mathbb{K}^*\}$
* si $G = S_n$, $Z(G) = \{id\}$ * $Z(O_n) = \{\pm I_n\}$
* $Z(\mathbb{H}_8) = \{-1, 1\}$

prop 26 equation aux classes. $G = \bigsqcup w(a)$ où $a \in$ système de représentants
$|G| = \sum |w(a)| = |Z(G)| + \sum_{a \notin Z(G)} |w(a)|$

prop 27 si $G/Z(G)$ est cyclique, alors G est abélien

Appl. 28 : tout groupe d'ordre p^2, p premier, est abélien.

prop. 29 : Le centre d'un p-groupe est non trivial

def. 30 : commutateur de $x, y \in G$, $[x,y] = xyx^{-1}y^{-1}$
$D(G) = \langle [x,y], x,y \in G \rangle$ est appelé groupe dérivé de G.

prop. 31 : $D(G) \triangleleft G$. De plus, $D(G)$ caractéristique ie stable par tout automorphisme de $G \to G$

rem : caractéristique $\not\Rightarrow$ distingué

prop. 32 : $G/D(G)$ est abélien, c'est le plus grand quotient abélien de G

ex. 33. * $D(S_3) = \{1, \sigma, \sigma^2\}$ où $\sigma = (123)$ * $D(GL_n) = SL_n$
* $D(\mathbb{H}_8) = \{-1, 1\}$ * $D(O_n) = SO_n$
* $D(S_n) = A_n$ si $n \geq 5$
$D(A_n) = A_n$

b) Simplicité

def. 34 : G est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et G

ex. 35 : $\mathbb{Z}/p\mathbb{Z}$ est simple si p premier

prop. 36 : si G simple, $\forall f \in Hom(G, G')$, $Ker f = \{e\}$ ou G

prop 37 : A_n est simple si $n = 3$ ou $n \geq 5$

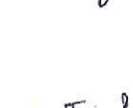
DV 1

ex. 38 : $SO_3(\mathbb{R})$ est simple

c) Morphismes :

prop. 39 : si $f \in Hom(G, G')$. * si $H \triangleleft G$, alors $f(H) \triangleleft f(G)$
* si $K \triangleleft G'$, alors $f^{-1}(K) \triangleleft G$

Th. 40 : factorisation si $H < Ker f$, $\exists ! h \in Hom(G/H \to G')$ tq $f = h \circ \pi_H$



On a $Ker h = Ker f / H$

Th. 41 : On a l'isomorphisme $Im f \simeq G/Ker f$

Ex. 42 : $G = (\mathbb{Z}/p\mathbb{Z})^*$ $\varphi : \begin{matrix} G \to G \\ x \to x^2 \end{matrix}$, $Ker \varphi = \{-1, 1\}$ induit $|Im \varphi| = \frac{p-1}{2}$

Th. 43 d'isomorphismes de Noether. $H \triangleleft G$ et $K \triangleleft G$
* On a $K \cap H \triangleleft H$ et $K/(K \cap H) \simeq KH/H$
* si $K < H < G$, et $K \triangleleft G$, alors $H/K \triangleleft G/K$ et $\frac{G/K}{H/K} \simeq G/H$

Ex. 44 : $(\mathbb{Z}/10\mathbb{Z})/(5\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/5\mathbb{Z}$

III) Applications

a) Théorèmes de Sylow :

def. 45 : si $|G| = p^\alpha m$ avec $p \nmid m$. On appelle p-Sylow un sous-groupe de G, de cardinal p^α

ex. 46 : $|GL_n(\mathbb{F}_p)| = m \cdot p^{n(n-1)/2}$. L'ensemble $\left\{\begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & & * \end{pmatrix} \in GL_n(\mathbb{F}_p)\right\}$ est un p-Sylow

Th. 47 : si $|G| = p^\alpha m$. Alors G contient un p-Sylow (Sylow 1)

Cor. 48 : $\forall i \leq \alpha$, G contient des sous-groupes d'ordre p^i

Th. 49 (Sylow 2) : * si $H < G$, $|H| = p^i$, $i \leq \alpha$, alors il existe S p-Sylow de G, avec $H \subset S$

$|G| = m$

* Les p-Sylow sont conjugués (et leur nombre $N_p \mid m$)

* $N_p \equiv 1 [p]$ (d'où $N_p \mid m$)

Cor. 50 : $\begin{cases} S \lhd G \\ |S| = p^\alpha \end{cases} \iff S$ est l'unique p-Sylow de $G \iff N_p = 1$

App. 51 : Un groupe d'ordre 63 n'est pas simple

Prop 52 : A_5 est le seul groupe simple d'ordre 60.

DV 2

DV 3

b) Produit de groupes :

principe : la connaissance de G/H, $H \lhd G$, aide-t-elle à mieux "comprendre" G ?

Th. 53 Produit direct : si $N < G$, $H < G$ tq $N \cap H = \{e\}$, $G = NH$ et N et H commutent, alors $G \simeq N \times H$

ex. 54 : $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

def/prop 55 Produit semi-direct. $N < G$, $H < G$

$N \times H$ est 1 groupe pour la loi $(n,h).(n',h') = (n \cdot \varphi_h(n'), hh')$ où $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$. On note $N \times_\varphi H$

Th. 56 : Critère de déscente. Si $G = NH$, $N \cap H = \{e\}$, $N \lhd G$, alors $G \simeq N \times_\varphi H$ où $\varphi : \begin{array}{ccc} H & \to & \mathrm{Aut}(N) \\ h & \to & n \to hnh^{-1} \end{array}$

Ex. 57 : D_{2n} = groupe des isométries conservant un n-gone

$D_{2n} = \{\langle r \rangle \times \langle s \rangle, r^n = s^2 = srsr = e\} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

prop 58 : si $|G| = pq$, p, q premiers, $p < q$ DV4

* si $q \not\equiv 1 [p]$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ $(\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})$

* si $q \equiv 1 [p]$, alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \times_\alpha \mathbb{Z}/p\mathbb{Z}$, α non triviale

Ex. 59 : $|G| = 21$. $G \simeq \mathbb{Z}/21\mathbb{Z}$ ou $G \simeq \mathbb{Z}/7\mathbb{Z} \times_\alpha \mathbb{Z}/3\mathbb{Z}$

Ex. 60 : $S_n \simeq A_n \times_\alpha \mathbb{Z}/2\mathbb{Z}$

103-104-105-108
190

Si $n=3$ ou $n \geq 5$, A_n est simple

Perrin, alg.
Lang, alg.
Szpirglas, L3 Alg.

Lemme 1 : si $\sigma = (a_1 - a_p)$ p-cycle de S_n et $\tau \in S_n$, alors
$\tau \sigma \tau^{-1} = (\tau(a_1) - \tau(a_p))$

démo : si $x = \tau(a_i)$, $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$
si $\forall i$, $x \neq \tau(a_i)$, $a_i \neq \tau^{-1}(x)$ donc $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$
d'où $\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$

Lemme 2 : (i) si $(a_i - a_{n-2})$ distincts, $(b_1 - b_{n-2})$ aussi $\exists\, \sigma \in A_n$, $\sigma(a_i) = b_i$

démo : pour $\{1-n\} = \{a_1 - a_n\} = \{b_1 - b_n\}$, on pose $\sigma(a_i) = b_i \in S_n$.
Si σ paire c'est ok, sinon, $\sigma \circ (a_{n-1}\, a_n) \in A_n$ → ok.

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

démo : $\sigma = (a_1 a_2 a_3)$ et $\tau = (b_1 b_2 b_3)$ le lemme 2 nous fournit $g \in A_n$, $b_i = g(a_i)$. D'après lemme 1, $\tau = (g(a_1)\, g(a_2)\, g(a_3))$ fournit $\tau = g\sigma g^{-1}$ donc σ et τ sont conjugués.

Lemme 4 : Les 3-cycles engendrent A_n

démo : tout élt de A_n est un produit pair de transposition.
mq 2 transpositions sont un produit de 3-cycles : soit $(ij)(rs)$
si i,j et r,s distincts : $(ij)(rs) = (isr)(ijr)$
sinon : $i=r$; $i=s$ ou $j=r$ ou $j=s$, on obtient un 3-cycle
$(ij) = (rs) \Rightarrow$ id.

c'est bon.

Démo du th: on prend $N \lhd A_n$ non trivial.

si N contient un 3-cycle σ, $\forall \tau$ 3-cycle de A_n, $\tau = g\sigma g^{-1}$, $g \in A_n$.

comme $N \lhd A_n$, on a $\tau \in N$. Et comme A_n engendré par les 3-cycles, on obtient $N = A_n$.

Si on trouve un σ 3-cycle dans N, on a donc fini.

Pour cela on s'intéresse au σ ayant le max. de points fixes (il existe évidemment, (hors id))

On décompose $\{1-n\} = W_1 \cup \dots \cup W_k$, orbites disjointes de $\langle\sigma\rangle$.

$\sigma \neq id$ donc certaines orbites ont au moins 2 elts.

ABS: si toutes les orbites non singleton ont 2 éléments.

il y en a 2 au moins car σ paire. $\sigma = (ij)(rs).\gamma$, γ disjoint de i,j,r,s

soit $\tau = (rsk)$, $k \neq i,j,r,s$ alors $\sigma' = \underbrace{\tau\sigma\tau^{-1}}_{\in \tau N \tau = N}\underbrace{\sigma^{-1}}_{\in N} \in N$

$\sigma'(i) = i$
$\sigma'(j) = j$ donc σ' fixe 2 elts de + que σ (_ éventuellement k).

donc σ' a + de pts fixes que σ CONTRADiction.
et $\sigma' \neq id$ car $\tau\sigma\tau^{-1} \neq \sigma^{-1}$

Ainsi au moins 1 orbite de σ a 3 elts : $\sigma = (ijk)\dots$ (ou +...)

ABS: si $\sigma \neq (ijk)$, comme elle est paire, elle déplace 2 pts en + $\sigma = (ijk)(\dots)(\dots)$
r et s : si $\tau = (krs)$ et $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$

$\sigma'(j) = j$ donc σ' fixe j et tous les pts fixes de σ.

$\tau\sigma\tau^{-1} \neq \sigma'$ (se vérifie facilement)

donc contradict°.

σ est un 3-cycle (ijk) donc N est engendré par les 3-cycles $\Rightarrow N = A_n$