103 — Exemples de sous-groupes distingués et de groupes quotients. Applications.

Dans toute la suite, $(G, \cdot)$ est un groupe.

I. Sous-groupe distingué, groupe quotient [CAL]

A. Sous-groupe distingué

Déf 1 : Soit H un sous-groupe de G. On dit que H est distingué dans G et on note $H \lhd G$ si : $\forall g \in G,\ gH = Hg$

Ex 2 : $\langle r \rangle \lhd D_n$ où D_n désigne le groupe diédral, groupe des isométries du n-gone.

Ex 3 : Soit $f \in Hom(G, G')$; • si $H' \lhd G'$ alors $f^{-1}(H') \lhd G$
• si $H \lhd G$ alors $f(H) \lhd f(G)$

En particulier : $A_n \lhd \mathfrak{S}_n$, $Z(G) \lhd G$, $SL_n(K) \lhd GL_n(K)$

Prop 4 : Si G est abélien, tout sous-groupe de G est distingué dans G.

C-Ex 5 : Tous les sous-groupes de $\mathbb{H}_8$ sont distingués mais $\mathbb{H}_8$ n'est pas abélien.

Prop 6 : Tout sous-groupe d'indice 2 est distingué. Plus généralement, tout sous-groupe d'indice le plus petit diviseur premier de $|G|$ est distingué.

Ex 7 : $SO_n(\mathbb{R}) \lhd O_n(\mathbb{R})$

B. Groupe quotient

Déf-prop 8 : Si $H \lhd G$, on peut munir G/H d'une structure de groupe en posant :
$$(gH).(g'H) = (gg')H$$

peu pertinent

Ex 9 : $\mathbb{Z}/n\mathbb{Z}$; $L^p = \mathcal{L}^p/N$ où N est le groupe des fonctions de $\mathcal{L}^p$ nulles presque partout

Prop 10 : La projection canonique $\pi : G \to G/H$ définit un morphisme de groupes surjectif de noyau H.
De plus, si G est fini alors $|G| = |G/H|\,|H|$

Cor 11 : $H \lhd G \iff H$ est le noyau d'un morphisme.

Prop 12 : π induit une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de G/H.

Ex 13 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $k\mathbb{Z}/n\mathbb{Z}$ où $k \mid n$.

Thm 14 [pré univ] : Soit $H \lhd G$, soient Γ un groupe et $\varphi \in Hom(G, \Gamma)$ tel que $H \subset \ker\varphi$.
Alors $\exists !\ \overline{\varphi} \in Hom(G/H, \Gamma)$, $\varphi = \overline{\varphi} \circ \pi$.

manque diagramme

Thm 15 [1er thm d'isomorphie] : Soit $\varphi \in Hom(G, \Gamma)$ alors $G/\ker\varphi \simeq Im\,\varphi$.

Ex 16 : $\mathbb{C}^*/\mathbb{R}_+^* \simeq \mathbb{U}$, $(\mathbb{R}/\mathbb{Z}, +) \simeq \mathbb{U}$, $(\mathbb{C}/\mathbb{Z}, +) \simeq \mathbb{C}^*$
$$GL_n(K)/SL_n(K) \simeq K^*$$

Thm 17 [3e thm d'isomorphie] :
$$(H \lhd G \text{ et } H \subset K \lhd G) \Rightarrow (G/H)/(K/H) \simeq G/K$$

C. Sous-groupes caractéristiques

C-Ex 18 : $H = \langle (12)(34) \rangle \lhd K = \{Id, (12)(34), (13)(24), (14)(23)\}$
$K \lhd A_4$ mais $H \ntriangleleft A_4$.

Déf 19 : Un sous-groupe H est dit caractéristique si H est stable par tout automorphisme de G. On note $H \sqsubset G$.

Ex 20 : $Z(G) \sqsubset G$; $\langle \text{carrés} \rangle \sqsubset G$.

Rq 21 : Si $H \sqsubset G$ alors $H \lhd G$.

Déf 22 : Le groupe dérivé de G est :
$$D(G) := \langle \{ xyx^{-1}y^{-1} \mid x, y \in G \} \rangle$$

Prop 23 : $D(G) \sqsubset G$ et $D(G)$ est le plus petit sous-groupe distingué H de G tel que G/H est abélien.

Prop 24 : Si $H \sqsubset K \lhd G$ alors $H \lhd G$
Si $H \sqsubset K \sqsubset G$ alors $H \sqsubset G$.

II - Produits directs et semi-directs [CAL]

A - Produits directs

Déf 25 : Soient G_1, G_2 deux groupes. On peut munir $G_1 \times G_2$ d'une structure de groupe en posant :
$$(g_1, g_2)\cdot(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

Rq 26 : $G_1 \times \{e_2\} \lhd G_1 \times G_2$; $\{e_1\} \times G_2 \lhd G_1 \times G_2$

Thm 27 : Soit G un groupe. Soient G_1, G_2 deux sous-groupes de G avec :
- $G_1 \lhd G$, $G_2 \lhd G$
- $G_1 \cap G_2 = \{e\}$
- $G_1 G_2 = G$

Alors $G \simeq G_1 \times G_2$

App 28 [Thm chinois] : $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z}) \Leftrightarrow (n \wedge m = 1)$

B - Produits semi-directs

Déf 29 : Soient N et H deux groupes, soit $\varphi \in Hom(H, Aut(N))$. On peut munir $N \times H$ d'une structure de groupe en posant :
$$(n,h)\cdot(n',h') = (n\varphi(n')(h), hh')$$
On note ce groupe $N \rtimes_\varphi H$. C'est le produit semi-direct de N par H relativement à φ.

Rq 30 : L'inverse de (n,h) est alors $(\varphi(h^{-1})(n^{-1}), h^{-1})$

Rq 31 : Si on note $\overline{N} = \{(n,1) \mid n \in N\}$, $\overline{H} = \{(1,h) \mid h \in H\}$ alors $\overline{N} \lhd N \rtimes_\varphi H$ mais $\overline{H}$ n'est pas nécessairement distingué dans $N \rtimes_\varphi H$

Prop 32 : Soit $G = N \rtimes_\varphi H$. EQU :
- $\varphi \equiv Id_N$
- $\overline{H} \lhd G$
- $G \simeq N \times H$

Déf 33 : Soient N, H deux sous-groupes de G avec $N \lhd G$. Alors le produit semi-direct intérieur $N \rtimes H$ est donné par $\varphi : h \mapsto (n \mapsto hnh^{-1})$

Thm 34 : Sous les hypothèses précédentes, si de plus $N \cap H = \{e\}$ et $NH = G$ alors
$$G \simeq N \rtimes H$$

Ex 35 :
- $D_n \simeq \langle r \rangle \rtimes \langle s \rangle$
- $\mathfrak{S}_n \simeq A_n \rtimes \langle \tau \rangle$ où τ est une transposition quelconque.

Ces produits sont non directs si $n \geq 3$.

App 36 : Classification des groupes d'ordre 12 [DEV]

III - Groupes simples [PER]

A - Simplicité

Déf 37 : G est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et G

Prop 38 : Les seuls groupes abéliens simples sont les $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Thm 39 : $PSL_n(K) := SL_n(K) / Z(SL_n(K))$ est simple sauf si $(n=2)$ et $((K = \mathbb{F}_2)$ ou $(K = \mathbb{F}_3))$

Thm 40 : $\forall n \geq 5$, A_n est simple.

Cor 41 : Les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{id\}$, A_n et $\mathfrak{S}_n$, si $n \geq 5$.

Cor 42 : $D(\mathfrak{S}_n) = A_n$; $D(A_n) = A_n$.

$\boxed{\text{Prop 43 : Tout groupe simple d'ordre 60 est isomorphe à } \mathcal{A}_5 \text{. [DEV]}}$

Thm 44 [Feit-Thompson] : Tout groupe simple non banal est d'ordre pair. [ADM15]

B - Théorèmes de Sylow · Outils

Déf 45 : Soit G un groupe d'ordre $p^\alpha m$ où p est premier, $\alpha \geq 1$ et $p \nmid m$. Un p-Sylow de G est un sous-groupe d'ordre p^α.

Rq 46 : Un p-sous-groupe H de G est un p-Sylow si et seulement si $[G:H] \wedge p = 1$.

Thm 47 [Sylow] : Soit G un groupe fini, soit p un facteur premier de $|G|$. Alors :

- G contient un p-Sylow,
- Deux p-Sylow sont toujours conjugués,
- Le nombre n_p de p-Sylow vérifie :

$$n_p \equiv 1 \, [p]$$

Cor 48 : Si S est un p-Sylow de G alors

$$(S \triangleleft G) \iff (n_p = 1)$$

App 49 : Tout groupe d'ordre
$\begin{cases} p^\alpha q & \text{avec } p > q \text{ premiers, } \alpha \geq 1 \\ pqr & \text{avec } p,q,r \text{ premiers distincts} \end{cases}$
n'est pas simple.

Par exemple : si $|G| \in \{18, 30, 42, 50, 54, 70\}$, G n'est pas simple.

IV - Représentations linéaires et sous-groupes distingués [ULM]

Déf 50 : Le caractère d'une représentation (ρ, V) d'un groupe G est l'application :

$$\chi : \begin{array}{l} G \longrightarrow \mathbb{C} \\ g \longmapsto \mathrm{Tr}(\rho(g)) \end{array}$$

Un caractère est dit irréductible s'il est associé à une représentation irréductible.

Déf 51 : Soit χ un caractère de G. On appelle noyau de χ l'ensemble défini par :

$$\mathrm{Ker}\,\chi := \{g \in G \mid \chi(g) = \chi(e)\}$$

Prop 52 : Soit G un groupe fini. Tout sous-groupe distingué H est de la forme $\bigcap_{j \in J} \mathrm{Ker}\,\chi_j$ où les $(\chi_i)_{i \in I}$ sont les caractères irréductibles et $J \subset I$.

Ex 53 : V_4 est le seul sous-groupe distingué non trivial de $\mathcal{A}_4$.

App 54 : Sous-groupes distingués de $\mathbb{D}_6$ (cf annexe) [RAU]

Cor 55 : Un groupe est simple si et seulement si tous ses caractères non triviaux ont un noyau trivial.

App 56 : $\mathcal{A}_5$ est simple (cf annexe) [RAU]

Références :
- [CAL] : J. Calais, Éléments de théorie des groupes.
- [PER] : D. Perrin, Cours d'algèbre
- [ULM] : F. Ulmer, Théorie des groupes
- [RAU] : G. Rauch, Les groupes finis et leurs représentations.

ANNEXE.

A_5	$1_{(1)}$	$C_{3\,(20)}$	$\tau\tau'_{(15)}$	$C_{5\,(12)}$	$C'_{5\,(12)}$
$\mathbb{1}$	1	1	1	1	1
χ_3	3	0	-1	φ	$1-\varphi$
χ'_3	3	0	-1	$1-\varphi$	φ
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

où $\varphi = \frac{1+\sqrt{5}}{2}$

D_6	$1_{(1)}$	$r_{(2)}$	$r^2_{(2)}$	$r^3_{(1)}$	$s_{(3)}$	$sr_{(3)}$
$\mathbb{1}$	1	1	1	1	1	1
ε_1	1	1	1	1	-1	-1
ε_2	1	-1	1	-1	1	-1
ε_3	1	-1	1	-1	-1	1
χ_2	2	1	-1	-2	0	0
χ'_2	2	-1	-1	2	0	0

Classification des groupes d'ordre 12

Référence : • Ramis-Warusfel, *Cours de mathématiques pures et appliquées, Volume 1*, p.27

Théorème 1 *A isomorphisme près, les seuls groupes d'ordre 12 sont :*

$$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z},\ \mathfrak{A}_4,\ \mathbb{D}_6 \text{ et } G_{12} := \mathbb{Z}/3\mathbb{Z}\rtimes_\varphi\mathbb{Z}/4\mathbb{Z}$$

abelien non ab.

Commençons par un lemme utile dont la démonstration est immédiate :

Lemme : *Soient A et B deux groupes, et φ, $\psi \in Hom(B, Aut(A))$ tels que $\exists\,\alpha \in Aut(B)$, $\varphi = \psi\circ\alpha$. Alors $A\rtimes_\varphi B \cong A\rtimes_\psi B$ via* $\Phi : \begin{cases} A\rtimes_\varphi B \to A\rtimes_\psi B \\ (a,b)\mapsto(a,\alpha(b)) \end{cases}$

Démonstration du théorème :

Soit G un groupe d'ordre $12 = 2^2\times 3$. Alors son nombre n_3 de 3-Sylow vérifie : $\begin{cases} n_3 \equiv 1[3] \\ n_3 | 4 \end{cases}$

Donc $n_3 \in \{1,4\}$.

• Premier cas : $n_3 = 4$.

Notons $S = \{S_1, S_2, S_3, S_4\}$ ses 3-Sylows. Alors G agit transitivement sur S par conjugaison :

$$f : \begin{cases} G \to \mathrm{Bij}(S) \\ g \mapsto (S_i \mapsto gS_ig^{-1}) \end{cases}$$

On a $\mathrm{Ker}(f) = \bigcap_i \mathrm{Stab}(S_i)$. Or pour tout i, $\mathrm{Stab}(S_i)$ contient S_i et est d'ordre $\frac{|G|}{\#\mathrm{Orb}(S_i)} = 3$, donc $\mathrm{Stab}(S_i) = S_i$, et donc $\mathrm{Ker}(f) = \{e\}$ en tant qu'intersection de sous-groupes cycliques distincts. G est donc isomorphe à un sous-groupe de $\mathfrak{S}_4$ qui est d'indice deux. Donc $\boxed{G \cong \mathfrak{A}_4}$

• Second cas : $n_3 = 1$.

Soit H son unique 3-Sylow, et K un 2-Sylow quelconque. Alors :
- H est distingué dans G
- $H \cap K = \{e\}$ car les éléments de H sont d'ordre 1 ou 3, et ceux de K d'ordre 1, 2 ou 4.
- $|H|.|K| = |G|$ donc $G = HK$

Donc $G \cong H \rtimes K$. Donc $G \cong \mathbb{Z}/3\mathbb{Z}\rtimes_\varphi N$, où $N = \mathbb{Z}/4\mathbb{Z}$ ou V_4, et $\varphi \in \mathrm{Hom}(N, \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}))$. Tout d'abord, notons que $\mathbb{Z}/3\mathbb{Z}$ possède un seul automorphisme non trivial : $k \mapsto 2.k$ Donc $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Il s'agit donc maintenant de chercher les morphismes $\varphi : N \to \mathbb{Z}/2\mathbb{Z}$.

— Premier sous-cas : $N = \mathbb{Z}/4\mathbb{Z}$.

Alors φ est déterminé par l'image d'un générateur. Il n'y a donc qu'un seul morphisme non trivial : $N \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$. On peut donc former deux groupes. Tout d'abord $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, associé au morphisme $\varphi \equiv id$, et qui est isomorphe à $\boxed{\mathbb{Z}/12\mathbb{Z}}$. Puis le groupe dicyclique $\boxed{G_{12} := \mathbb{Z}/3\mathbb{Z}\rtimes_\varphi\mathbb{Z}/4\mathbb{Z}}$, associé à l'unique φ non trivial.

— Second sous-cas : $N = (\mathbb{Z}/2\mathbb{Z})^2$.

On dénombre trois morphismes non triviaux : $\varphi_1 : \begin{cases} (1,0) \mapsto 1 \\ (0,1) \mapsto 0 \end{cases}$, $\varphi_2 : \begin{cases} (1,0) \mapsto 0 \\ (0,1) \mapsto 1 \end{cases}$, $\varphi_2 : \begin{cases} (1,0) \mapsto 1 \\ (0,1) \mapsto 1 \end{cases}$. Mais pour tout i, j, il existe $\alpha \in \mathrm{Aut}(V_4), \varphi_i = \varphi_j \circ \alpha$. En effet, on peut par exemple voir que $\mathrm{Aut}(V_4) \cong \mathfrak{S}_3$. Donc d'après le lemme, il n'y a que deux groupes cette forme : le groupe abélien $\mathbb{Z}/3\mathbb{Z} \times V_4$, qui est isomorphe à $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}}$, et un groupe non abélien $\boxed{\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi V_4}$.

• Montrons enfin que ce dernier groupe est isomorphe à $\mathbb{D}_6$. $\mathbb{D}_6$ est un groupe d'ordre 12, donc isomorphe à l'un des groupes précédemment trouvés. Il n'est pas abélien et possède un sous-groupe d'ordre 3 distingué $H =< r^2 >$. Donc $\mathbb{D}_6$ est soit G_{12}, soit $\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi V_4$. Mais on vérifie aisément que $\mathbb{D}_6/H$ n'est pas cyclique car tous ses éléments sont d'ordre 1 ou 2. Donc $\boxed{\mathbb{D}_6 \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\varphi V_4}$ □

$\mathfrak{A}_5$ est le seul groupe simple d'ordre 60

Références : • D. Perrin, *Cours d'Algèbre* (pour les deux lemmes et le théorème 1)
• M. Savoyant, *Le groupe simple d'ordre 60*, RMS novembre-décembre 1999

Théorème 1 *$\mathfrak{A}_5$ est simple*

Commençons par énoncer les deux lemmes suivants.

Lemme : *Les 3-cycles sont conjugués dans $\mathfrak{A}_5$, et engendrent $\mathfrak{A}_5$.*

Démonstration :

• Soient (abc) et $(a'b'c')$ deux trois-cycles. Il existe $\sigma \in \mathfrak{S}_5$ telle que $\sigma(abc)\sigma^{-1} = (a'b'c')$.
Si $\sigma \in \mathfrak{A}_5$, c'est gagné.
Sinon, posons $\tau = (d'e')$, puis $\sigma' = \tau\sigma$. Alors on a toujours $\sigma'(abc)\sigma'^{-1} = \tau(a'b'c')\tau = (a'b'c')$, et $\sigma' \in \mathfrak{A}_5$, ce qui prouve que (abc) et $(a'b'c')$ sont conjugués dans $\mathfrak{A}_5$.

• $\mathfrak{A}_5$ est engendré par les produits pairs de transpositions. Il suffit alors d'observer que :

$$(ab)(bc) = (abc), (ab)(ac) = (acb) \text{ et } (ab)(cd) = (abc)(bcd)$$

Donc $\mathfrak{A}_5$ est aussi engendré par les 3-cycles.

Lemme : *Les doubles-transpositions sont conjuguées dans $\mathfrak{A}_5$*

Démonstration :

Soient $(ab)(cd)(e)$ et $(a'b')(c'd')(e')$ deux doubles transpositions. Il existe $\sigma \in \mathfrak{S}_5$ telle que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$. On a alors $\sigma(\{c,d\}) = \{c',d'\}$. Il y a en fait deux permutations ayant cette propriété, mais elles n'ont pas la même parité (pas le même nombre d'inversions). On peut donc supposer $\sigma \in \mathfrak{A}_5$. On a alors $\sigma(ab)(cd)(e)\sigma^{-1} = (a'b')(c'd')(e')$

Démonstration du théorème :
Commençons par remarquer que $\mathfrak{A}_5$ contient 15 éléments d'ordre 2 (les doubles transpositions), 20 éléments d'ordre 3 (les 3-cycles) et 24 éléments d'ordre 5 (les 5-cycles).

Soit $H \triangleleft \mathfrak{A}_5$ avec $H \neq \{id\}$.

- Si H contient un 3-cycle, comme ceux-ci sont conjugués, et engendrent $\mathfrak{A}_5$, alors $H = \mathfrak{A}_5$
- Si H contient une double transposition, alors il les contient toutes
- Si H contient un 5-cycle, alors H contient le 5-Sylow engendré par celui-ci. Les 5-Sylow étant conjugués, H les contient tous, et donc contient tous les 5-cycles.

Donc $|H| \in \{16, 25, 40, 60\}$. Or $|H|$ divise $|\mathfrak{A}_5| = 60$ donc nécessairement, $|H| = 60$, ie $H = \mathfrak{A}_5$, ce qui conclut la démonstration. □

Théorème 2 *Tout groupe simple d'ordre 60 est isomorphe à* $\mathfrak{A}_5$

Démonstration :
Soit G un groupe d'ordre $60 = 2^2 \times 3 \times 5$. Alors $n_5 \equiv 1[5]$ et $n_5|12$, donc $n_5 = 6$.
Notons $S = \{S_1, \dots, S_6\}$ l'ensemble des 5-Sylow de G.

L'action de G sur S par conjugaison est transitive, donc le morphisme $f : \begin{cases} G \to \mathrm{Bij}(S) \\ g \mapsto (S_i \mapsto gS_ig^{-1}) \end{cases}$ n'est pas trivial. Donc $\mathrm{Ker}(f)$, qui est distingué dans G est donc nécessairement réduit à $\{e\}$. G est donc isomorphe à un sous groupe H de $\mathfrak{S}_6$.

• Comme H n'est pas abélien, et que $D(H) \triangleleft H$, alors $D(H) = H$. Donc $H = D(H) \subset D(\mathfrak{S}_6) \subset \mathfrak{A}_6$

• Montrons que H n'est pas distingué dans $\mathfrak{A}_6$:
H étant d'ordre 60, il contient un élément d'ordre 5, donc un 5-Sylow. Si H était distingué, il contiendrait tous les 5-Sylow donc tous les 5-cycles. Or il y a $6 \times 4! = 144$ 5-cycles dans $\mathfrak{A}_6$, donc H ne peut être distingué.

• On fait agir H sur $\mathfrak{A}_6/H$ par translation : $\phi : \begin{cases} H \to \mathrm{Bij}(\mathfrak{A}_6/H) \\ g \mapsto (xH \mapsto (gx)H) \end{cases}$, avec $|\mathfrak{A}_6/H| = 6$, donc $\mathrm{Bij}(\mathfrak{A}_6/H) \cong \mathfrak{S}_6$

$\mathrm{Ker}(\phi) \triangleleft H$ donc $\mathrm{Ker}(\phi) = \{id\}$ ou $\mathrm{Ker}(\phi) = H$.

$$\begin{aligned} \text{Or :}\quad \mathrm{Ker}(\phi) = H &\Leftrightarrow \forall h \in H, \forall \sigma \in \mathfrak{A}_6, \sigma H = (h\sigma)H \\ &\Rightarrow \forall h \in H, \forall \sigma \in \mathfrak{A}_6, h\sigma \in \sigma H \\ &\Rightarrow \forall \sigma \in \mathfrak{A}_6, H \subset \sigma H \sigma^{-1} \\ &\Rightarrow H \triangleleft \mathfrak{A}_6 \end{aligned}$$

Donc ϕ est injective. Notons enfin que $\forall h \in H, \phi(h)(H) = H$ donc toutes les permutations $\phi(h)$ ont un point fixe commun. Cela montre que H est alors isomorphe à un sous-groupe de $\mathfrak{S}_5$, qui est d'indice deux. C'est donc nécessairement $\mathfrak{A}_5$. □