

Cadée: $(G, \cdot)$ un groupe de neutre 1. $H < G$. G' un autre groupe. $\varphi: G \rightarrow G'$ un morphisme de groupes.
Illustration: "descendance" des groupes: se ramener à des groupes de cardinalité plus petits

I. NOTION DE SOUS-GROUPES DISTINGUÉS & GROUPES QUOTIENTS

1. Classe d'équivalence [PER]

Def 1 On appelle classe à gauche de l'élément $a \in G$ relativement à H le sous-ensemble:

$$aH = \{g \in G \mid g = ah, h \in H\}.$$

Rq: on définit de même les classes à droite Ha .
• les classes à gauche (ou à droite) forment une partition de G .

Def 2 L'ensemble des classes à gauche relativement à H est noté G/H . (a priori, ce n'est pas un groupe).

Def 3 Le cardinal de G/H est appelé l'indice de H dans G et est noté $(G:H)$.

Thm 4 Théorème de Lagrange.

soit que G est fini, l'ordre de H et l'indice de H dans G divisent l'ordre de G . Précisément, on a: $|G| = |H| \cdot |G/H|$.
↳ En particulier, l'ordre d'un élément $g \in G$ divise l'ordre de G .

2. Sous-groupes distingués [PER]

Def 5 On dit que H est distingué dans G si:
 $\forall a \in G, \forall h \in H, aha^{-1} \in H$.

On note $H \triangleleft G$.

Ex 6 • $\{1\}$ et G sont toujours des sous-groupes distingués.
Ils sont dits triviaux.

- Si G abélien, tous les sous-groupes sont distingués.
- Le centre de G (ensemble des éléments qui commutent avec tous les autres) est distingué.
↳ il est noté $Z(G)$.

Contre-ex 7. $GL_n(\mathbb{Z})$ n'est pas distingué dans $GL_n(\mathbb{R})$.

$$\text{En effet } a = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$ah a^{-1} = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix} \notin GL_n(\mathbb{Z})$$

Prop 8 soie que H est distingué, on a, $\forall a \in G, aH = Ha$
(égalité des classes à droite et à gauche modulo H)

Prop 9 $\text{Ker } \varphi \triangleleft G$.

Prop 10 Un sous-groupe d'indice 2 est toujours distingué.

Ex 11. $A_n \triangleleft S_n$. (redite après ?)

3. Groupes quotients [PER]

Def / Prop 12 Si $H \triangleleft G$, le quotient G/H est muni d'une structure de groupe et est appelé groupe quotient.

Rq On a alors équivalence dans la prop 9:

$$H \triangleleft G \Leftrightarrow \exists G' \text{ groupe, } f \in \text{Hom}(G, G') \text{ tel que } H = \text{Ker } f$$

Thm 13 Propriété universelle du quotient [ILL]

Si $H \triangleleft G$, $\pi: G \rightarrow G/H$ morphisme canonique.

$$\text{Eql } 1) H \subset \text{Ker } \varphi$$

$$2) \exists ! \text{ morphisme de groupes } \bar{\varphi}: G/H \rightarrow G' \text{ tel que } \bar{\varphi} \circ \pi = \varphi$$

On a le diagramme commutatif:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ \varphi \downarrow & & \swarrow \bar{\varphi} \\ G' & & \end{array}$$

Thm 14 1^{er} théorème d'isomorphisme

Il existe un isomorphisme $\bar{\varphi}: G/\text{Ker } \varphi \xrightarrow{\sim} \text{Im } \varphi$
 $g \text{ Ker } \varphi \mapsto \varphi(g)$.

↳ si φ surjectif $G/\text{Ker } \varphi \xrightarrow{\sim} G'$.

Ex 15 Par l'application det: $GL_n(\mathbb{C}) \rightarrow \mathbb{C}^*$.

$$\text{on a } GL_n(\mathbb{C})/SL_n(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}^*$$

Appel 16 un groupe cyclique fini d'ordre $n \in \mathbb{N}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

II GROUPE ET SOUS-GROUPE REMARQUABLES [PER]

1. Groupe simple

Def 17 $G \neq \{1\}$ est dit simple si ses seuls sous-groupes distingués sont $\{1\}$ et G .

Ex 18 $\mathbb{Z}/p\mathbb{Z}$ est simple si p est premier.

Prop 19 les seuls groupes simples abéliens sont les groupes cycliques d'ordre premier.

2. Produit direct [PER]

Def / Prop 20 G_1, G_2 deux groupes. Le produit direct $G_1 \times G_2$ est le produit cartésien de G_1 et G_2 . Il est un groupe avec la loi produit $(g_1, g_2)(g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$.

Rq le produit direct n'est jamais simple (prendre $G_1 \times \{e_2\} \triangleleft G_1 \times G_2$)

Prop 21 Lemme chinois

Si $p, q \neq 1$, on a $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Rq l'assertion est fausse si $p, q \neq 1$.

Ex 22 $\mathbb{Z}/4\mathbb{Z}$ et $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes

3. p-groupes et thm de Sylow

Def 23 Si p est un nombre premier, on appelle p -groupe un groupe dont le cardinal est une puissance de p .

Def 24 G fini de cardinal n , p un diviseur premier de n . Si $n = p^\alpha m$ avec $p \nmid m$. On appelle p -sous-groupe de Sylow de G un sous-groupe de cardinal p^α .

Thm 25 Théorème de Sylow.

Soit G défini comme dans la def 24.

- 1) G contient au moins un p -sous-groupe de Sylow.
- 2) Si $H < G$ qui est un p -groupe, il existe un p -sylow S avec $H \subset S$.
- 3) Les p -sylows sont tous conjugués (et leur nombre $k_p(n)$)
- 4) $k_p \equiv 1 \pmod{p}$ (donc $k_p \mid m$)

Coro 26 Si S est un p -sylow de G , on a:

$S \trianglelefteq G \Leftrightarrow S$ est l'unique p -sylow de $G \Leftrightarrow k_p = 1$.

Appl 27 Un groupe d'ordre 63 n'est pas simple.

III. RESOLUBILITÉ

1. Groupe dérivé et groupes résolubles [PER] p13

Def 28 Le groupe dérivé $D(G)$ est le sous-groupe engendré par les commutateurs de G i.e les éléments de la forme $xyx^{-1}y^{-1} = [x, y]$ avec $x, y \in G$.

Rq $D(G) \trianglelefteq G$

• $G/D(G)$ est abélien

Ex 29 G abélien $\Leftrightarrow D(G) = \{1\}$

Def 30 On définit itérativement la suite dérivée de G par $G^{(0)} = G$; $G^{(1)} = D(G)$ et $\forall i \geq 1$ $G^{(i+1)} = D(G^{(i)}) = D^{(i+1)}(G)$

Def 31 G est dit résoluble s'il existe $n \in \mathbb{N}$ tq $G^{(n)} = D^{(n)}(G) = \{1\}$.

Ex 32 • un groupe abélien est résoluble

• un groupe simple et non abélien n'est jamais résoluble

Thm 33 Sont équivalents.

1) G résoluble

2) il existe une suite finie stationnaire en $\{1\}$ de sous-groupes distingués $H_i \trianglelefteq G$ avec $H_0 = G \supseteq H_1 \supseteq \dots \supseteq H_n = \{1\}$ tq les quotients H_i/H_{i+1} soient abéliens.

3) il existe une suite finie stationnaire en $\{1\}$ de sous-groupes $H_i \trianglelefteq G$ avec $H_0 = G \supseteq H_1 \supseteq \dots \supseteq H_n = \{1\}$ tq $H_{i+1} \trianglelefteq H_i$ et les quotients H_i/H_{i+1} soient abéliens.

Thm 34 Soit $N \trianglelefteq G$.

• G résoluble $\Rightarrow N$ résoluble

• G résoluble $\Rightarrow G/N$ résoluble

• G résoluble $\Leftrightarrow N$ et G/N résolubles.

• N, H résolubles $\Rightarrow HN$ résoluble

Appl 35 Tout p -groupe G d'ordre fini est résoluble.

2. Application aux groupes symétriques et alterné [CHA]

Def 36 $\mathcal{S}_n$ est le groupe des permutations de l'ensemble $\{1, \dots, n\}$. Il est de cardinal $n!$.

Prop 37 Les transpositions sont toutes conjuguées entre elles. Il en est de même pour les 3-cycles.

Def 38 La signature d'une permutation σ est
$$E(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \quad |E: \mathcal{S}_n \rightarrow \{-1, 1\} \text{ est un morphisme}$$

Def 39 Une permutation est dite paire (resp impaire) si $E(\sigma) = 1$ (resp -1).

Def 40 L'ensemble des permutations paires forme un sous-groupe $\mathcal{A}_n$ de $\mathcal{S}_n$. Il est appelé groupe alterné.

Prop 41 $\mathcal{A}_n \triangleleft \mathcal{S}_n$. (car noyau de E) $\uparrow$??
• $[\mathcal{S}_n: \mathcal{A}_n] = 2$.

Prop 42 Les 3-cycles engendrent $\mathcal{A}_n$. Pour $n \geq 5$, ils sont conjugués dans $\mathcal{A}_n$.

Thm 43 Si $n \geq 5$, $\mathcal{A}_n$ est simple. [PER]

Coro 44 $\forall n \geq 5 \quad D(\mathcal{A}_n) = \mathcal{A}_n$.
 $\forall n \geq 2 \quad D(\mathcal{S}_n) = \mathcal{A}_n$.

Coro 45 Pour $n \geq 5$, les sous-groupes distingués de $\mathcal{S}_n$ sont $\{1\}$, $\mathcal{A}_n$, $\mathcal{S}_n$.

Coro 46 Si $n \geq 5$, $\mathcal{S}_n$ et $\mathcal{A}_n$ ne sont pas résolubles.

3. Groupe nilpotent et groupe de matrices [CHA]

Def 47 On dit qu'un groupe G est nilpotent s'il possède une suite distinguée $\{1\} = G_0 \subset G_1 \subset \dots \subset G_{n-1} \subset G_n = G$.

$$\text{tq } \forall i \in \{0, \dots, n-1\} : G_i \triangleleft G \quad \bullet \quad G_{i+1}/G_i \subset Z(G/G_i)$$

Rq nilpotent $\Rightarrow$ résoluble.

Ex 48 $\mathcal{S}_3$ est résoluble mais non nilpotent.

Soit K un corps. On se place sur $GL_n(K)$.

Def 49 On note T le sous-groupe des matrices diagonales, B celui des matrices triangulaires supérieures et U celui des matrices triangulaires supérieures n'ayant que des 1 sur la diagonale.

Prop 50 U est nilpotent.
• $D(B) \subset U$.
• B est résoluble.

Lem 51 Toute famille de matrices qui commutent 2 à 2 peut être mise sous forme triangulaire dans une base convenable.

En particulier, tout sous-groupe commutatif de $GL_n(K)$ est conjugué à un sous-groupe de B .

Lem 52 Soit G un sous-groupe connexe de $GL_n(K)$. Alors son sous-groupe dérivé est connexe.

Thm 53 Théorème de Lie-Kolchin.

Tout sous-groupe connexe résoluble de $GL_n(K)$ est conjugué à un sous-groupe de B .

Références

- [PER] Daniel Perron, Cours d'Algèbre, Ellipses
- [ULN] Felix Ulmer, Théorie des Groupes, Ellipses
- [CHA] Antoine Chambert-Loir, Algèbre corporelle.
- [CAL] Joëlle Cabré, Elements de Théorie des groupes, 2ème édition.

Tauvel, Algèbre 2ème édition peut être bien