Etude de groupes finis : Théorème de Chermak-Delgado et applications.

Matthieu MEUNIER

Table des matières

1 Introduction

Lorsque se pose la question de l'ordre d'un sous-groupe d'un groupe fini, le théorème de Lagrange nous assure que les valeurs possibles ne sont pas quelconques. On rapelle

Théorème 1. *Soit G un groupe fini. Tout sous-groupe H de G vérifie $|H| \,|\, |G|$.*

Cependant, rien ne nous assure que pour tout diviseur de l'ordre du groupe, on dispose d'un sous-groupe d'ordre ce diviseur. Ce constat est le point de départ du travail exposé ici, l'objectif étant d'obtenir plus d'informations sur les ordres des sous-groupes d'un groupe fini. Le pilier de l'étude est un théorème démontré par Andrew Chermak et Alberto Delgado en 1989, que nous présentons dans un premier temps, pour ensuite établir des propriétés sur certains groupes finis.

Notations

- Dans tout le texte, $(G, \cdot)$ désigne un groupe fini noté multiplicativement.
- L'ordre d'un élément $x \in G$ sera noté $\omega(x)$ (ainsi $\omega(x) \mid |G|$).
- "$H \leq G$" désigne la proposition "*H est un sous-groupe de G*".
- Pour $H \leq G$, on notera $[G : H] = |G/H|$ l'indice de H dans G.
- "$H \triangleleft G$" signifie "*H est un sous-groupe distingué de G*".
- Pour $A \subset G$, on note $C_G(A) = \{\, g \in G \mid \forall a \in A, ga = ag \,\}$. On vérifie aisément que $C_G(A) \leq G$.

2 Le théorème de Chermak-Delgado

On énonce

Théorème 2. *Soit G un groupe fini. G possède un sous-groupe abélien distingué I tel que, pour tout $A \leq G$ abélien*

$$[G : I] \leq [G : A]^2$$

soit, de façon équivalente

$$|A|^2 \leq |G| \times |I|$$

2.1 Préliminaires

Le point de départ est une application du lemme du berger.

Lemme 1. *Pour tous* $H, K \leq G$, $|HK| = \dfrac{|H| \times |K|}{|H \cap K|}$.

En particulier, $\dfrac{|H| \times |K|}{|H \cap K|} \leq | < H \cup K > |$.

L'idée principale de Chermak et Delgado a été d'introduire une mesure sur l'ensemble des sous-groupes de G, qui traduit un équilibre entre l'ordre d'un sous-groupe H de G et celui de $C_G(H)$. Nous utiliserons une version simplifiée de cette mesure, qui nous suffit pour l'étude.

Définition 1. *Pour* $H \leq G$, *on définit* $\mu(H) = |H| \times |C_G(H)|$.

Du lemme 1, on tire

$$\forall H, K \leq G,\ \ \mu(H)\mu(K) \leq \mu(H \cap K)\mu(< H \cup K >)$$

On peut alors se poser la question des sous-groupes de G qui maximisent μ. A cet effet, on pose $m = max\{\mu(H) \mid H \leq G\}$ et $\mathcal{E} = \{H \leq G \mid \mu(H) = m\}$.

Lemme 2. $(\mathcal{E}, \subset)$ *possède un minimum pour l'inclusion, noté* I. *C'est le sous-groupe de Chermak-Delgado de* G.

Démonstration. Il suffit de poser $I = \bigcap_{H \in \mathcal{E}} H$. Cette intersection est non vide par définition de $\mathcal{E}$ et elle est finie. L'inégalité précédente (qui devient une égalité pour $H, K \in \mathcal{E}$) permet de conclure. □

2.2 Preuve du résultat

Pour tout $H \leq G$, on a

$$\mu(H) \leq \mu(I) \leq |I| \times |G|$$

En particulier, si $A \leq G$ est abélien, alors $A \leq C_G(A)$, donc

$$|A|^2 \leq |I| \times |G|$$

soit

$$[G : I] \leq [G : A]^2$$

Il reste à montrer que I est abélien et distingué. Le caractère abélien résulte de l'inégalité suivante

$$\forall H \leq G,\ \ \mu(H) \leq \mu(C_G(H))$$

inégalité qui découle immédiatement de l'inclusion $P \subset C_G(C_G(P))$, valable pour toute partie P de G ; par μ-maximalité de I, on a $\mu(I) = \mu(C_G(I))$, et I étant minimal au sens de $(\mathcal{E}, \subset)$, on en déduit que $I \subset C_G(I)$, et que I est abélien.
Pour le caractère distingué, on va montrer une propriété plus forte sur I, à savoir que I est un sous-groupe caractéristique de G, c'est-à-dire que I est stable par tout automorphisme de G. Soit alors $\sigma \in Aut(G)$. σ étant bijective on a $|\sigma(I)| = |I|$, et d'autre part (on ne détaille pas la preuve) $\sigma(C_G(I)) = C_G(\sigma(I))$

(en particulier on obtient l'égalité des ordres). Ainsi, il vient $\mu(I) = \mu(\sigma(I))$, puis $I \subset \sigma(I)$. Par égalité des ordres, $I = \sigma(I)$, ce qui prouve que I est un sous-groupe caractéristique de G. En particulier, I est stable par les automorphismes intérieurs, donc I est distingué, ce qui achève la preuve du théorème de Chermak-Delgado.
On a finalement démontré un résultat plus général, que l'on consigne en un nouveau théorème.

Théorème 3. *Soit G un groupe fini. Il existe I sous-groupe abélien distingué de G tel que*

$$\forall\, H \leq G, \quad |H| \times |C_G(H)| \leq |I| \times |G|$$

3 Applications du théorème de Chermak-Delgado

On peut à présent se poser la question de l'efficacité d'une telle majoration. Pour un groupe abélien par exemple, la majoration est sans intérêt (car $I = G$ dans ce cas). Un cas plus pertinent est celui des groupes simples non abéliens, car pour ces groupes on a automatiquement $I = \{1_G\}$. On en déduit un corollaire sur l'ordre des éléments de tels groupes.

Corollaire 1. *Soit G un groupe fini simple non abélien. Alors tout $x \in G$ vérifie*

$$\omega(x)^2 \leq |G|$$

Démonstration. On applique le théorème 1 à $A = < x >$ (il s'agit bien d'un sous-groupe abélien de G) et $I = \{1_G\}$ (le seul sous-groupe abélien distingué de G). □

3.1 Quelques résultats utiles

Nous commençons par établir un lemme de Cauchy.

Lemme 3. *Soit G un groupe fini d'ordre n, et p premier tel que $p \mid n$. Alors G possède un élément d'ordre p.*

Démonstration. On pose $E = \{(x_1, ..., x_p) \in G^p, x_1...x_p = 1_G\}$, et on définit la relation $\sim$ sur E de sorte que, pour $x, y \in E$, $x \sim y$ si et seulement si $(y_1, ..., y_p)$ s'obtient par permutation circulaire de $(x_1, ..., x_p)$. On vérifie que $\sim$ est une relation d'équivalence, et on note, pour $x \in E$, $\gamma(x)$ la classe d'équivalence de x. Soit alors $x = (x_1, ..., x_p) \in E$ et calculons $|\gamma(x)|$.

- Si $x_1 = ... = x_p$, alors $|\gamma(x)| = 1$.
- Sinon, montrons que $|\gamma(x)| = p$. On a clairement $|\gamma(x)| \leq p$, et supposons par l'absurde que $|\gamma(x)| < p$. On dispose alors de $k \in \{2, ..., p\}$ tel que $(x_k, ..., x_p, x_1, ..., x_{k-1}) = (x_1, ..., x_p)$, de sorte que $x_k = x_1 = x_{1+(p-k+1 \ mod\, p)}$ et plus généralement

  $$\forall\, l \in \mathbb{N}, \ x_{1+(l(p-k+1) \ mod\, p)} = x_k$$

  Or, $p - k + 1$ est premier avec p, donc c'est un générateur de $(\mathbb{Z}/p\mathbb{Z}, +)$, donc $l(p - k + 1)$ décrit tous les entiers modulo p, quand l parcourt $\mathbb{N}$, d'où $x_1 = ... = x_p$, ce qui est absurde.

Or, on a clairement $|E| = n^{p-1}$, donc en partitionnant E selon ses classes d'équivalence, on obtient, en notant $C = |\{x \in G, x^p = 1_G\}|$

$$n^{p-1} = C \ mod\, p$$

p divise n, donc $C = 0 \ mod\, p$, et comme $C \geq 1$, on en déduit $C \geq 2$, donc G possède un élément d'ordre p.

□

On admet le résultat suivant, et on rappelle que G désigne un groupe fini.

Lemme 4. *Soit $x, y \in G$ tels que $\omega(x)$ et $\omega(y)$ sont premiers entre eux et $xy = yx$. Alors $\omega(xy) = \omega(x)\omega(y)$.*

On pose, pour $d \in \mathbb{N}^*$, $\Omega_d = \{x \in G, \omega(x) = d\}$.

Lemme 5. *Soit p premier tel que $p \mid |G|$, et $d \in \mathbb{N}^*$ tel que p ne divise pas d. On suppose que G n'a pas d'élément d'ordre dp. Alors $p \mid |\Omega_d|$.*

Démonstration. D'après le lemme de Cauchy, on dispose de H sous-groupe cyclique de G d'ordre p. On considère alors, pour $x \in \Omega_d$,

$$C(x) := \{hxh^{-1}, h \in H\} \subset \Omega_d$$

$C(x)$ est alors de cardinal au plus p, et s'il existe $h, h' \in H$ tel que $h \neq h'$ et $hxh^{-1} = h'xh'^{-1}$, alors $xh^{-1}h' = h^{-1}h'x$ et par le lemme 4, cet élément est d'ordre dp ce qui est absurde. Donc $|C(x)| = p$, puis en écrivant Ω_d comme réunion disjointe des classes de conjugaison, il vient $p \mid |\Omega_d|$.

□

3.2 Etude de l'ordre d'un groupe fini simple non abélien

Dans cette partie on suppose que G est un groupe fini simple non abélien.

Proposition 1. *$|G|$ n'est pas de la forme pq où p et q sont des nombres premiers distincts.*

Démonstration. Raisonnons par l'absurde et supposons $|G| = pq$ avec $p < q$. D'après le lemme de Cauchy, on dispose de $x \in G$ tel que $\omega(x) = q$. Alors $\omega(x)^2 = q^2 > |G|$, ce qui contredit le corollaire 1. □

Proposition 2. *$|G|$ n'est pas de la forme pqr où p, q et r sont des nombres premiers deux à deux distincts.*

Démonstration. Raisonnons par l'absurde et supposons $|G| = pqr$ avec $p < q < r$. Pour $x \in G$, le théorème de Lagrange fournit $\omega(x) \in \{1, p, q, r, pq, pr, qr, pqr\}$. Le lemme de Cauchy assure l'existence d'un élément d'ordre r, et le corollaire 1 amène alors $r < pq$. Donc

$$\{\omega(x), x \in G\} = \{1, p, q, r\}$$

D'après le lemme 5, on a alors $r \mid |\Omega_p|$ et $q \mid |\Omega_p|$, et enfin $p - 1 \mid |\Omega_p|$, car un groupe cyclique d'ordre p possède $p-1$ générateurs. Ainsi on dispose de $A \in \mathbb{N}^*$

tel que $|\Omega_p| = Aqr(p-1)$. En raisonnant de façon analogue avec Ω_q et Ω_r, on dispose de $B, C \in \mathbb{N}^*$ tels que

$$|G| = |\Omega_p| + |\Omega_q| + |\Omega_r| + |\Omega_1|$$

i.e

$$\begin{aligned} pqr &= Aqr(p-1) + Br(q-1) + C(r-1) + 1 \\ &\geq pqr - qr + qr - r + r - 1 + 1 \\ &= pqr \end{aligned}$$

Cela impose $C = 1$, soit $|\Omega_r| = r - 1$, mais le lemme 5 nous donne $pq \,|\, |\Omega_r|$, donc $|\Omega_r| \geq pq > r$, ce qui est absurde.

□

3.3 Etude d'un groupe alterné

Dans cette partie nous donnons des éléments de preuve pour montrer que $(A_5, \circ)$ (groupe des permutations paires de $\{1,2,3,4,5\}$) est le seul groupe fini simple non abélien de cardinal inférieur ou égal à 119.

Proposition 3. *$(A_5, \circ)$ est un groupe fini simple non abélien de cardinal 60.*

Démonstration. Le caractère non abélien ne pose pas de difficulté. On classe les éléments de A_5 selon leur décomposition en produit de cycles (en omettant les cycles de longueur 1), et on s'intéresse à leur classe de conjugaison dans A_5 :

- $C_1 := \{Id\}$
- $C_2 := \{(a\ b) \circ (c\ d),\ a, b, c, d \textit{ distincts}\}$. On a $|C_2| = 15$, et les éléments de C_2 sont conjugués deux à deux (*i.e* ils font tous partie de la même classe de conjugaison).
- $C_3 := \{(a\ b\ c),\ a, b, c \textit{ distincts}\}$. On a $|C_3| = 20$ et les élément de C_3 sont deux à deux conjugués.
- $C_4 := \{(a\ b\ c\ d\ e),\ a, b, c, d, e \textit{ distincts}\}$. On a $|C_4| = 24$ et l'on peut montrer que ces éléments sont conjugués à (1 2 3 4 5) ou à (2 1 3 4 5) (mais pas aux deux à la fois, les classes de conjugaison étant distinctes et étant chacune de cardinal 12).

On retrouve bien $|A_5| = \sum_{i=1}^{4} |C_i| = 60$. Supposons alors par l'absurde que A_5 n'est pas simple. On se donne $H \triangleleft A_5$ non trivial, c'est donc une réunion de classes de conjugaison. On dispose alors de $A, B, C, D \in \{0,1\}$ tels que

$$|H| = 1 + 15A + 20B + 12C + 12D$$

D'autre part, le théorème de Lagrange nous assure que $|H| \in \{2,3,4,6,10,15,20,30\}$, ce qui est incompatible avec la relation précédente, car

$$\{1+15A+20B+12C+12D, A, B, C, D \in \{0,1\}\} = \{1, 13, 16, 21, 25, 28, 33, 36, 40, 48, 60\}$$

Donc A_5 est simple. □

Nous montrons enfin une propriété sur les groupes d'ordre 72 (afin de donner un aperçu de la preuve du résultat annoncé plus haut). Nous énonçons d'abord un lemme que nous admettons (il repose sur la notion de plongement dans un

groupe alterné que nous n'abordons pas ici). On rappelle que G est un groupe fini simple non abélien et on note, pour $H \leq G$, $c(H) := \{gHg^{-1},\ g \in G\}$, et

$$\mathcal{D}(G) := \{|c(H)|,\ H \leq G \text{ cyclique non trivial}\}$$

$$\Delta(G) := \{n \in \mathbb{N}^*,\ n \mid |G| \text{ et } 2|G| \mid n!\}$$

On note enfin $d(G)$ le pgcd des éléments de $\mathcal{D}(G)$.

Lemme 6. *On a $\mathcal{D}(G) \subset \Delta(G)$ ainsi que $d(G) = 1$.*

Proposition 4. *Il n'existe pas de groupe fini simple non abélien d'ordre 72.*

Démonstration. Par l'absurde, soit un tel groupe G d'ordre 72. Alors

$$\Delta(G) = \{6,\ 8,\ 9,\ 12,\ 18,\ 24,\ 36,\ 72\}$$

En particulier $8 \in \mathcal{D}(G)$, sinon $d(G) \geq 3$. On dispose ainsi de $H \leq G$ cyclique tel que $|c(H)| = 8$. On vérifie alors que $N(H) := \{g \in G,\ gHg^{-1} = H\}$ est d'ordre 9 et qu'il est abélien (car de la forme p^2 où p est premier). Or $81 > 72$, cela contredit le théorème 2. □

Conclusion

Ainsi, le théorème de Chermak-Delgado nous a permis d'obtenir une majoration de l'ordre des sous-groupes d'un groupe fini, qui, conjointement avec le théorème de Lagrange, nous permettent dans certains cas de déterminer plus précisément les ordres possibles des sous-groupes que la simple majoration par l'ordre du groupe. D'autre part, il nous aura permis de montrer que certains groupes aux propriétés spécifiques (les groupes finis simples non abéliens ici) ne peuvent être d'ordre quelconque.

Références

1 Josette CALAIS : *Eléments de théorie des groupes* : Puf, 2016.

2 Christophe BERTAULT : *Le théorème de Chermak-Delgado* : RMS129-4, 2018, p.22-33.