

LE THÉORÈME D^* DE GLAUBERMAN-SOLOMON

C'est un garçon sacrément perspicace.

Il a des choses à nous apprendre.

Wielandt à propos de Thompson (1958)

Les groupes étudiés dans ce texte sont tous finis.

J'ai introduit dans mon précédent travail « Le transfert et ses applications » différents concepts dont ceux de transfert, fusion, p -nilpotence et sous-groupe p -local.

Définition (Sous-groupe p -local) Soient p un nombre premier et G un groupe. On appelle *sous-groupe p -local* de G tout sous-groupe de la forme $N_G(H)$ où H est un p -sous-groupe non trivial de G .

L'analyse p -locale étudie la manière dont les sous-groupes p -locaux d'un groupe contraignent sa structure globale et les premiers résultats de cette branche importante de la théorie des groupes concernent la notion de p -nilpotence.

Définition (Sous-groupe $O_{p'}(G)$ et p -nilpotence) Soient p un nombre premier et G un groupe.

- (i) On note $O_{p'}(G)$ le sous-groupe engendré par tous les p' -sous-groupes distingués de G , qui est aussi le plus grand p' -sous-groupe distingué de G .
- (ii) On dit que G est p -nilpotent si pour tout $P \in \text{Syl}_p(G)$ — ou pour un seul, c'est pareil — $O_{p'}(G)$ est un complément distingué de P dans G , autrement dit : $G = O_{p'}(G)P$.

Le premier théorème d'analyse p -locale a été démontré par Burnside en 1900. Il énonce, dans le cas de p -Sylow abéliens, que la p -nilpotence d'UN UNIQUE sous-groupe p -local suffit à garantir celle du groupe tout entier.

Théorème 1 (Théorème de p -nilpotence de Burnside) Soient p un nombre premier, G un groupe et $P \in \text{Syl}_p(G)$. On suppose P abélien. Les assertions suivantes sont équivalentes :

- 1) G est p -nilpotent.
- 2) $N_G(P)$ est p -nilpotent.
- 3) $P \leq Z(N_G(P))$, ou encore : $N_G(P) = C_G(P)$.

L'assertion 3) de ce théorème peut être négligée dans cette introduction, mais elle nous sera utile en cours de route.

Frobenius a démontré peu de temps après un résultat analogue sans l'hypothèse que les p -Sylow sont abéliens, mais qui requiert en revanche la p -nilpotence de TOUS les sous-groupes p -locaux.

Théorème 2 (Théorème de p -nilpotence de Frobenius) Soient p un nombre premier, G un groupe et $P \in \text{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

- 1) G est p -nilpotent.
- 2) Pour tout sous-groupe non trivial H de P , $N_G(H)$ est p -nilpotent. Cela revient à exiger, d'après les théorèmes de Sylow, que tout sous-groupe p -local de G soit p -nilpotent.

Les choses en sont restées là pendant quelques décennies, et puis Thompson a démontré dans sa thèse en 1959 un résultat majeur, dit *théorème de Thompson*, dont je parlerai brièvement à la fin de cette introduction. Ce résultat n'a pas de rapport direct avec les questions qui vont nous occuper désormais, mais il a conduit Thompson à vouloir affaiblir l'assertion 2) du théorème de p -nilpotence de Frobenius. En lieu et place de « tout sous-groupe non trivial H de P », peut-on se contenter de « tout sous-groupe CARACTÉRISTIQUE non trivial H de P » ?

Ainsi posée, la question a hélas une réponse négative. Le groupe symétrique S_4 , par exemple, a pour 2-Sylow le sous-groupe $P = \langle (1\ 2\ 3\ 4), (1\ 2) \rangle$, isomorphe au groupe diédral D_8 , et les sous-groupes caractéristiques non triviaux de P sont P lui-même, son centre $Z(P) = \langle (1\ 3)(2\ 4) \rangle$ et le sous-groupe cyclique $C = \langle (1\ 2\ 3\ 4) \rangle$. Or il n'est pas dur de vérifier que : $N_{S_4}(P) = N_{S_4}(Z(P)) = N_{S_4}(C) = P$. En particulier, ces trois normalisateurs sont 2-nilpotents. Le groupe S_4 l'est-il pour autant ? Cela signifierait qu'il possède un sous-groupe distingué d'ordre 3, autrement dit un unique 3-Sylow, ce qui est notoirement faux.

Le miracle de la thèse de Thompson, c'est que ce qui vient d'échouer sur un exemple pour $p = 2$ est vrai en toute généralité pour $p \neq 2$. Dans ce cas, l'assertion 2) du théorème de p -nilpotence de Frobenius peut bel et bien être affaiblie et Thompson a même obtenu mieux en introduisant un sous-groupe aujourd'hui incontournable qui porte son nom.

Définition (Sous-groupe de Thompson) Soient p un nombre premier et P un p -groupe.

- On appelle *sous-groupe de Thompson de P* et on note $J(P)$ le sous-groupe de G engendré par les sous-groupes abéliens de G d'ordre maximal.
- On pose en outre : $ZJ(P) = Z(J(P))$.

Par exemple, si P est abélien : $J(P) = P$. Le résultat qui suit généralise ainsi les deux théorèmes de p -nilpotence de Burnside et Frobenius. Publié sous cette forme en 1964, il a fait date dans l'histoire de la théorie des groupes finis et montre que pour $p \neq 2$, la p -nilpotence de DEUX sous-groupes p -locaux prescrits suffit à impliquer la p -nilpotence du groupe tout entier.

Théorème (Théorème de p -nilpotence de Thompson) Soient p un nombre premier IMPAIR, G un groupe et $P \in \text{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

- 1) G est p -nilpotent.
- 2) $N_G(J(P))$ et $C_G(Z(P))$ sont p -nilpotents.

Quelques années plus tard, en 1968, Glauberman est même allé plus loin en montrant qu'UN SEUL sous-groupe p -local suffit. Puissant et surprenant, le résultat signifie qu'il y a dans chaque p -Sylow d'un groupe un sous-groupe caractéristique qui contrôle la p -nilpotence du groupe tout entier.

Théorème (Théorème de p -nilpotence de Glauberman) Soient p un nombre premier IMPAIR, G un groupe et $P \in \text{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

- 1) G est p -nilpotent.
- 2) $N_G(ZJ(P))$ est p -nilpotent.

J'ai démontré complètement les théorèmes de p -nilpotence de Burnside et Frobenius dans mon précédent texte « Le transfert et ses applications ». Nous les tiendrons pour acquis dans le présent travail et les investigations d'analyse p -locale auxquelles nous allons procéder ne requerront pas de nouvelle utilisation du transfert.

Le théorème de p -nilpotence de Glauberman est quant à lui en réalité la conséquence d'un résultat plus général du même auteur, dit *théorème ZJ*. L'énoncé de ce théorème requiert hélas un concept technique, la p -stabilité, que je ne définirai pas dans cette introduction.

Théorème (Théorème ZJ de Glauberman) Soient p un nombre premier IMPAIR et G un groupe p -stable pour lequel : $C_G(O_p(G)) \leq O_p(G)$. Alors pour tout $P \in \text{Syl}_p(G)$: $ZJ(P) \trianglelefteq G$.

On ne se demande plus ici quelle influence les sous-groupes p -locaux d'un groupe ont sur celui-ci, on oblige plutôt un certain p -sous-groupe défini par des conditions universelles à être distingué — et même caractéristique — pour peu qu'un lot d'hypothèses raisonnables soit réuni.

Dernier rebondissement en date, Glauberman et Solomon ont introduit en 2012, pour tout p -groupe P , un sous-groupe caractéristique $D^*(P)$ de P que j'appellerai le *sous-groupe de Glauberman-Solomon de P* et qui paraît pouvoir remplacer

avantageusement le sous-groupe de Thompson $J(P)$ et son centre $ZJ(P)$ dans les énoncés qui précèdent. Avantageusement en quel sens ? Le sous-groupe $D^*(P)$ jouit d'une certaine propriété que les sous-groupes $J(P)$ et $ZJ(P)$ n'ont pas et qui raccourcit substantiellement la preuve du théorème ZJ.

Théorème (Théorème D^* de Glauberman-Solomon) Soient p un nombre premier IMPAIR et G un groupe p -stable pour lequel : $C_G(O_p(G)) \leq O_p(G)$. Alors pour tout $P \in \text{Syl}_p(G)$: $D^*(P) \subseteq G$.

Le voilà donc, l'objectif de ce texte. De ce résultat découlera naturellement un puissant théorème de p -nilpotence.

Théorème (Théorème de p -nilpotence de Glauberman-Solomon) Soient p un nombre premier IMPAIR, G un groupe et $P \in \text{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

- 1) G est p -nilpotent.
- 2) $N_G(D^*(P))$ est p -nilpotent.

Comme annoncé plus haut, la motivation historique du théorème de p -nilpotence de Thompson était un autre *théorème de Thompson* que je me contenterai d'énoncer. Je ne le démontrerai pas pour ne pas alourdir ce texte déjà bien copieux, mais l'essentiel du travail est fait quand on a démontré le théorème de p -nilpotence de Thompson — ou celui de Glauberman, ou celui de Glauberman-Solomon.

Définition (Automorphisme sans point fixe) Soient G un groupe et $\varphi \in \text{Aut}(G)$. On dit que φ est *sans point fixe* si son seul point fixe est l'élément neutre 1.

Théorème 3 (Théorème de Thompson) Soit G un groupe. Si G possède un automorphisme sans point fixe d'ordre premier, alors G est *nilpotent*, i.e. égal au produit de ses sous-groupes de Sylow.

Les groupes nilpotents ne sont pas abéliens en général, mais on peut dire pour fixer les idées que ce sont les groupes les plus abéliens possibles après les groupes abéliens eux-mêmes. Ils sont résolubles en particulier. Le théorème de Thompson énonce donc une contrainte structurelle forte, la présence d'un automorphisme sans point fixe d'ordre premier — situation courante à vrai dire — a un impact considérable sur le groupe concerné.

On formule souvent le théorème de Thompson dans le cadre des *groupes de Frobenius*. Les deux énoncés sont équivalents et je m'épargnerai toute digression à ce sujet. J'en ai parlé un peu dans mon texte « Le transfert et ses applications ».

Ce texte est découpé en cinq parties.

- La première introduit la notion de *groupe p -séparable*. Les groupes p -séparables apparaissent naturellement en analyse p -locale et nous en rencontrerons beaucoup dans ce travail.
- La deuxième partie isole l'une des idées géniales de Thompson qui lui a permis, pour dépasser les exigences trop fortes du théorème de p -nilpotence de Frobenius, de ramener un problème sur des groupes quelconques à un problème sur des groupes p -séparables.
- On commence dans la troisième partie par quelques rappels sur les actions de groupes par automorphismes, puis on introduit rapidement les notions d'*action quadratique* et de *p -stabilité*. Cette partie n'est qu'une introduction et l'on n'y démontre aucun résultat majeur.
- La quatrième partie est entièrement dédiée au sous-groupe de Glauberman-Solomon $D^*(P)$ d'un p -groupe P . On le définit, on l'étudie, et l'on démontre enfin le théorème D^* de Glauberman-Solomon.
- La troisième partie laissait en suspens une question fondamentale — la p -stabilité est-elle une notion contraignante ? On démontre dans la cinquième partie que la p -stabilité est une propriété plutôt ordinaire des groupes. Précisément, il s'avère qu'un groupe p -séparable qui n'est pas p -stable possède forcément une section isomorphe au groupe spécial linéaire $\text{SL}_2(3)$.

Nous terminerons cette introduction par le rappel de quelques notations.

$ X $	Cardinal de l'ensemble X
$ X _p$	Plus grande puissance du nombre premier p qui divise $ X $
1	Double notation pour l'élément neutre d'un groupe et le sous-groupe trivial $\{1\}$
$H \leq G$	« H est un sous-groupe du groupe G »
$H < G$	« H est un sous-groupe propre du groupe G »
$H \leq G$	« H est un sous-groupe distingué du groupe G »
$H \sqsubseteq G$	« H est un sous-groupe caractéristique du groupe G »
$ G : H $	Indice du sous-groupe H dans le groupe G
$\langle X \rangle$	Sous-groupe engendré par l'ensemble X dans un groupe donné
x^g	Conjugué $g^{-1}xg$ de l'élément x par l'élément g
x^G	Classe de conjugaison de l'élément x dans le groupe G
x^φ	Image de l'élément x par l'automorphisme φ
$N_G(H)$	Normalisateur dans le groupe G du sous-groupe H
$C_G(H)$	Centralisateur dans le groupe G du sous-groupe H
$[x, y]$	Commutateur $x^{-1}y^{-1}xy$ de x et y dans un groupe donné
$[X, Y]$	Sous-groupe engendré par les commutateurs $[x, y]$, x décrivant X et y décrivant Y
$D(G)$	Sous-groupe dérivé $[G, G]$ du groupe G
$\text{Syl}_p(G)$	Ensemble des p -Sylow du groupe G pour un nombre premier p
$\text{Aut}(G)$	Groupe des automorphismes du groupe G
\mathbb{F}_q	Corps fini de cardinal q où q est une puissance non triviale d'un nombre premier
$\text{GL}_n(q)$	Groupe général linéaire de degré n sur \mathbb{F}_q
$\text{SL}_n(q)$	Groupe spécial linéaire de degré n sur \mathbb{F}_q

1 GROUPES p -SÉPARABLES

Définition-théorème 4 (Sous-groupe $O_\pi(G)$) Soient G un groupe fini et π un ensemble de nombres premiers.

- (i) On note $O_\pi(G)$ le sous-groupe engendré par tous les π -sous-groupes distingués de G . Il est équivalent de dire que $O_\pi(G)$ est le plus grand π -sous-groupe distingué de G , car pour tous π -sous-groupes distingués A et B de G , AB est aussi un π -sous-groupe distingué de G .
- (ii) En réalité : $O_\pi(G) \sqsubseteq G$.
- (iii) En particulier : $O_p(G) = \bigcap_{P \in \text{Syl}_p(G)} P$.

Démonstration

- (i) Le sous-groupe AB a pour ordre : $|AB| = \frac{|A| \times |B|}{|A \cap B|}$, donc en effet c'est un π -groupe.
- (ii) L'ensemble des π -sous-groupes distingués de G est stable par tout automorphisme de G .
- (iii) Le sous-groupe $\bigcap_{S \in \text{Syl}_p(G)} P$ est un p -sous-groupe distingué de G car l'ensemble des p -Sylow de G est stable par conjugaison, donc : $\bigcap_{S \in \text{Syl}_p(G)} P \leq O_p(G)$. Inversement, $O_p(G)$ est inclus dans au moins un p -Sylow de

G , mais comme il est distingué dans G et que les p -Sylow de G sont tous conjugués d'après les théorèmes de Sylow : $O_p(G) \leq \bigcap_{S \in \text{Syl}_p(G)} P$. ■

De même que les groupes résolubles sont des empilements de groupes abéliens, les groupes p -séparables sont des empilements de groupes qui sont soit des p -groupes, soit des p' -groupes. Ces groupes interviennent naturellement en analyse p -locale comme nous allons le découvrir tout au long de ce texte.

Définition (Groupe p -séparable) Soient p un nombre premier et G un groupe. On dit que G est p -séparable s'il existe des sous-groupes H_0, \dots, H_n de G pour lesquels : $1 = H_0 \trianglelefteq \dots \trianglelefteq H_n = G$ et tels que pour tout $i \in \llbracket 0, n-1 \rrbracket$, le quotient $\frac{H_{i+1}}{H_i}$ est soit un p -groupe, soit un p' -groupe.

À l'évidence, tout groupe p -nilpotent est p -séparable.

Théorème 5 (Sous-groupes et quotients d'un groupe p -séparable) Soient p un nombre premier et G un groupe p -séparable.

- (i) Tout sous-groupe de G est p -séparable.
- (ii) Tout quotient de G est p -séparable.

Démonstration Notons H_0, \dots, H_n des sous-groupes de G conformes à la définition de sa p -séparabilité.

- (i) Soit H un sous-groupe de G . Pour commencer : $1 = H \cap H_0 \trianglelefteq \dots \trianglelefteq H \cap H_n = H$. Ensuite, pour tout $i \in \llbracket 0, n-1 \rrbracket$, le morphisme de groupes $x \mapsto (H \cap H_i)x$ de $H \cap H_{i+1}$ dans $\frac{H_{i+1}}{H_i}$ induit par quotient un morphisme injectif de $\frac{H \cap H_{i+1}}{H \cap H_i}$ dans $\frac{H_{i+1}}{H_i}$. En particulier, $\frac{H \cap H_{i+1}}{H \cap H_i}$ est donc soit un p -groupe, soit un p' -groupe. Conclusion : H est p -séparable.
- (ii) Soit N un sous-groupe distingué de G . Nous noterons d'une barre les quotients par N . Pour commencer : $1 = \overline{H_0} \trianglelefteq \dots \trianglelefteq \overline{H_n}$. Ensuite, pour tout $i \in \llbracket 0, n-1 \rrbracket$, le morphisme de groupes $x \mapsto \overline{H_i} \bar{x}$ de H_{i+1} dans $\frac{\overline{H_{i+1}}}{\overline{H_i}}$ induit par quotient un isomorphisme de $\frac{H_{i+1}}{H_{i+1} \cap NH_i}$ sur $\frac{\overline{H_{i+1}}}{\overline{H_i}}$. Comme : $H_i \leq H_{i+1} \cap NH_i$, le quotient $\frac{\overline{H_{i+1}}}{\overline{H_i}}$ est ainsi soit un p -groupe, soit un p' -groupe. Conclusion : $\frac{G}{N}$ est p -séparable. ■

Théorème 6 (Sous-groupes $O_p(G)$ et $O_{p'}(G)$ d'un groupe p -séparable) Soient p un nombre premier et G un groupe p -séparable. Si G est non trivial, alors : $O_p(G) \neq 1$ ou $O_{p'}(G) \neq 1$.

Démonstration Par récurrence sur l'entier n de la définition de la p -séparabilité. Notons H_0, \dots, H_n des sous-groupes de G conformes à cette définition. Le résultat est trivial si : $n = 0$, supposons donc : $n \geq 1$. D'après 5, H_{n-1} est p -séparable, donc par hypothèse de récurrence : $O_p(H_{n-1}) \neq 1$ ou $O_{p'}(H_{n-1}) \neq 1$. Or : $O_p(H_{n-1}) \trianglelefteq H_{n-1} \trianglelefteq H_n = G$ et $O_{p'}(H_{n-1}) \trianglelefteq H_{n-1} \trianglelefteq H_n = G$, donc : $O_p(H_{n-1}) \leq O_p(G)$ et $O_{p'}(H_{n-1}) \leq O_{p'}(G)$ — d'où le résultat. ■

Le résultat qui suit paraîtra anecdotique au premier abord, mais jouera plusieurs fois un rôle essentiel par la suite.

Théorème 7 (Centralisateur de $O_p(G)O_{p'}(G)$ dans un groupe p -séparable) Soient p un nombre premier et G un groupe p -séparable. Alors : $C_G(O_p(G)O_{p'}(G)) \leq O_p(G)O_{p'}(G)$.

Démonstration Posons : $O = O_p(G)O_{p'}(G)$, $C = C_G(O)$ et $Z = Z(O)$, et notons en outre π l'un des deux ensembles suivants — soit $\{p\}$, soit son complémentaire dans l'ensemble des nombres premiers. Notons enfin Π l'unique sous-groupe — distingué — de G contenant Z pour lequel : $\frac{\Pi}{Z} = O_\pi\left(\frac{C}{Z}\right)$. Aussitôt : $Z \leq \Pi \leq C \leq C_G(Z)$, donc : $Z \leq Z(\Pi)$. Par ailleurs, Z étant abélien : $Z = O_p(Z)O_{p'}(Z)$.

- Dans le cas où : $\pi = \{p\}$, soit $P \in \text{Syl}_p(\Pi)$. Le quotient $\frac{\Pi}{Z}$ étant un p -groupe : $\Pi = ZP = O_{p'}(Z)P$, et comme : $Z \leq Z(\Pi)$, alors : $P = O_p(\Pi) \trianglelefteq \Pi \trianglelefteq G$, donc : $P \leq O_p(G)$. De même : $O_{p'}(Z) \leq O_{p'}(G)$, donc : $\Pi = O_{p'}(Z)P \leq O$. Or : $\Pi \leq C_G(O)$, donc : $\Pi \leq Z$, donc enfin : $O_p\left(\frac{C}{Z}\right) = 1$.
- Dans le cas où π est le complémentaire de $\{p\}$ dans l'ensemble des nombres premiers, le quotient $\frac{\Pi}{Z}$ étant un p' -groupe : $O_p(Z) \in \text{Syl}_p(Z)$. Or par ailleurs : $O_p(Z) \leq Z(\Pi)$, donc Π est p -nilpotent d'après le théorème de p -nilpotence de Burnside, de sorte que : $\Pi = O_{p'}(\Pi)O_p(Z)$. Remarquons alors que : $O_{p'}(\Pi) \trianglelefteq \Pi \trianglelefteq G$, donc : $O_{p'}(\Pi) \leq O_{p'}(G)$. De même : $O_p(Z) \trianglelefteq Z \trianglelefteq O \trianglelefteq G$, donc : $O_p(Z) \leq O_p(G)$. A fortiori : $\Pi = O_{p'}(\Pi)O_p(Z) \leq O$, puis : $\Pi \leq Z$, et enfin : $O_{p'}\left(\frac{C}{Z}\right) = 1$.

Au point où nous en sommes : $O_p\left(\frac{C}{Z}\right) = 1$ et $O_{p'}\left(\frac{C}{Z}\right) = 1$. Le quotient $\frac{C}{Z}$ étant p -séparable d'après 5 (ii), le théorème 6 montre que : $\frac{C}{Z} = 1$, et donc : $C = Z \leq O$. ■

2 PAR-DELÀ FROBENIUS, LA RÉDUCTION p -SÉPARABLE DE THOMPSON

Le théorème de p -nilpotence de Frobenius ramène la p -nilpotence d'un groupe à celle de TOUS ses sous-groupes p -locaux. Thompson a montré plus tard que DEUX d'entre eux suffisent, et même UN SEUL d'après Glauberman. Mais de quel sous-groupe p -local parlons-nous ? Nous en parlerons plus facilement après la définition suivante.

Définition (*p -foncteur caractéristique*) Soit p un nombre premier. On appelle *p -foncteur caractéristique* toute application W de la catégorie des p -groupes finis dans elle-même satisfaisant les assertions suivantes :

- pour tout p -groupe P : $W(P) \trianglelefteq P$,
- pour tous p -groupes finis P et P' et pour tout isomorphisme φ de P sur P' : $W(P)^\varphi = W(P')$,
- pour tout p -groupe P : $P \neq 1 \implies W(P) \neq 1$.

L'exemple le plus simple de p -foncteur caractéristique est le foncteur « centre » Z qui associe à tout p -groupe son centre.

D'une manière ou d'une autre, et même s'il ne l'a pas formalisé ainsi, Thompson a cherché un p -foncteur caractéristique W pour lequel, pour tout groupe G et pour tout $P \in \text{Syl}_p(G)$, la p -nilpotence de $N_G(W(P))$ entraîne celle de G . On peut décomposer son travail en deux sous-problèmes.

- **Premier problème** : Que peut-on dire d'un p -foncteur caractéristique pour lequel c'est faux ? Thompson a analysé sous cette hypothèse un contre-exemple G minimal — en un sens à préciser — que nous allons décrire dans cette partie. C'est cette démarche que j'appellerai la *réduction p -séparable de Thompson*.
- **Deuxième problème** : Peut-on concevoir un p -foncteur caractéristique W qui rende toujours contradictoire le contre-exemple minimal G du point précédent ? Cette question nous occupera dans les parties suivantes.

Théorème 8 (*p -foncteur caractéristique et sous-groupe $O_{p'}(G)$*) Soient p un nombre premier, W un p -foncteur caractéristique et G un groupe. Si on note d'un petit rond en exposant les quotients par $O_{p'}(G)$, alors pour tout $P \in \text{Syl}_p(G)$:

$$N_{G^\circ}(W(P^\circ)) = N_G(W(P))^\circ.$$

Démonstration Il est d'abord clair que : $N_G(W(P))^\circ \leq N_{G^\circ}(W(P^\circ))$. Inversement, soit $n \in G$ pour lequel : $n^\circ \in N_{G^\circ}(W(P^\circ))$. Aussitôt : $(W(P^\circ))^{n^\circ} = W(P^\circ)$, donc : $W(P)^n \leq W(P)O_{p'}(G)$. Or $W(P)$ et $W(P)^n$

sont deux p -Sylow de $W(P)O_{p'}(G)$, donc d'après les théorèmes de Sylow : $W(P)^n = W(P)^\omega$ pour un certain $\omega \in O_{p'}(G)$, donc : $n\omega^{-1} \in N_G(W(P))$. A fortiori : $n^\circ \in N_G(W(P))^\circ$.

Pour finir, l'application $x \mapsto x^\circ$ est un isomorphisme de P sur P° car son noyau $P \cap O_{p'}(G)$ est trivial, donc par définition de W : $W(P)^\circ = W(P^\circ)$. Conclusion : $N_{G^\circ}(W(P^\circ)) = N_{G^\circ}(W(P)^\circ) = N_G(W(P))^\circ$. ■

Théorème 9 (Réduction p -séparable de Thompson) Soient p un nombre premier et W un p -foncteur caractéristique. On note \mathcal{N}_W la catégorie des groupes G pour lesquels, pour un certain $P \in \text{Syl}_p(G)$, $N_G(W(P))$ est p -nilpotent sans que G le soit. Si \mathcal{N}_W est non vide, \mathcal{N}_W contient un groupe G satisfaisant les assertions suivantes :

- pour tout $P \in \text{Syl}_p(G)$: $W(P) \not\trianglelefteq G$,
- G est p -séparable et : $O_{p'}(G) = 1$ — donc d'après 7 : $C_G(O_p(G)) \leq O_p(G)$,
- G est un $\{p, q\}$ -groupe pour un certain nombre premier $q \neq p$ et les q -Sylow de G sont abéliens.

Pour saisir l'importance de ce résultat, il faut bien comprendre que la catégorie \mathcal{N}_W est composée de groupes a priori quelconques. Que Thompson ait réussi à se frayer un chemin dans cette catégorie jusqu'à un groupe p -séparable, c'est cela son premier succès.

Nous aurons besoin en cours de route du petit résultat classique suivant, supposé connu.

Théorème 10 (Normalisateurs dans un p -groupe) Soient p un nombre premier, G un p -groupe et H un sous-groupe propre de G . Dans ces conditions : $H < N_G(H)$ avec inclusion stricte.

Démonstration Raisonnons par l'absurde et donnons-nous une fois pour toutes un contre-exemple G au théorème d'ordre minimal. Le groupe G n'est ainsi pas p -nilpotent, mais $N_G(W(P))$ l'est POUR UN CERTAIN $P \in \text{Syl}_p(G)$. Les p -Sylow de G étant conjugués d'après les théorèmes de Sylow, on peut en fait affirmer par définition de W que $N_G(W(P))$ est p -nilpotent POUR TOUT $P \in \text{Syl}_p(G)$.

- Notons à présent \mathcal{H} l'ensemble des p -sous-groupes non triviaux de G dont le normalisateur dans G n'est pas p -nilpotent. D'après le théorème de p -nilpotence de Frobenius, \mathcal{H} est non vide. Intéressons-nous alors aux éléments H de \mathcal{H} pour lesquels $|N_G(H)|_p$ est maximal, et fixons une fois pour toutes un tel sous-groupe H pour lequel, de plus, $|H|$ est maximal.

C'est cela à proprement parler, la réduction p -séparable de Thompson — un choix judicieux de sous-groupe H grâce auquel nous allons pouvoir dépasser le théorème de p -nilpotence de Frobenius.

Nous pouvons nous donner ensuite un p -Sylow P de G contenant un p -Sylow de $N_G(H)$ contenant lui-même H . Dans ces conditions : $N_p(H) \in \text{Syl}_p(N_G(H))$, ou encore : $|N_G(H)|_p = |N_p(H)|$, et par ailleurs $N_G(W(P))$ est p -nilpotent. Comme G ne l'est pas : $W(P) \not\trianglelefteq G$. Or : $W(P) \subseteq P$, donc : $P \not\trianglelefteq G$. Conclusion : $O_p(G) < P < G$.

- Montrons que $N_G(W(N_p(H)))$ est p -nilpotent. Or les relations : $W(N_p(H)) \subseteq N_p(H) \trianglelefteq N_p(N_p(H))$ montrent que : $N_p(N_p(H)) \leq N_G(W(N_p(H)))$. Aussitôt, de deux choses l'une :
 - si : $N_p(H) = P$, nous savons déjà que $N_G(W(N_p(H))) = N_G(W(P))$ est p -nilpotent,
 - dans le cas contraire : $N_p(H) < N_p(N_p(H))$ d'après 10, donc :

$$|N_G(W(N_p(H)))|_p \geq |N_p(N_p(H))| > |N_p(H)| = |N_G(H)|_p,$$

donc par maximalité de H : $W(N_p(H)) \notin \mathcal{H}$, autrement dit $N_G(W(N_p(H)))$ est p -nilpotent.

- D'après le point précédent, $N_{N_G(H)}(W(N_p(H)))$ est p -nilpotent avec : $N_p(H) \in \text{Syl}_p(N_G(H))$, mais pourtant, par définition de H , $N_G(H)$ n'est pas p -nilpotent. Conclusion : $N_G(H) = G$ par minimalité de G , donc : $H \leq O_p(G)$.

Remarquons à présent que : $O_p(G) \in \mathcal{H}$ car $N_G(O_p(G)) = G$ n'est pas p -nilpotent. Or pourtant : $|N_G(O_p(G))|_p = |G|_p = |N_G(H)|_p$, donc par maximalité de H : $|O_p(G)| \leq |H|$. Conclusion : $H = O_p(G)$.

- Montrons que G est p -séparable. Nous noterons désormais d'une barre les quotients par $O_p(G)$. Notons V l'unique sous-groupe de G pour lequel : $\bar{V} = W(\bar{P})$. L'inclusion stricte : $O_p(G) < P$ s'écrit aussi : $\bar{P} \neq 1$, donc par définition de W : $\bar{V} \neq 1$, ou encore : $H = O_p(G) < V$. Or : $\bar{P} \leq N_{\bar{G}}(W(\bar{P}))$, donc : $P \leq N_G(V)$. En résumé : $|N_G(V)|_p = |G|_p = |N_G(H)|_p$ et $|H| < |V|$, donc par maximalité de H : $V \notin \mathcal{H}$, i.e. $N_G(V)$ est p -nilpotent. Comme : $O_p(G) \leq V$, il en résulte aussitôt que $N_{\bar{G}}(W(\bar{P})) = N_{\bar{G}}(\bar{V}) = \overline{N_G(V)}$ est p -nilpotent, et comme : $O_p(G) = H \neq 1$, la minimalité de G garantit finalement la p -nilpotence de \bar{G} . En particulier, \bar{G} est p -séparable, mais donc G aussi a fortiori.
- Montrons que : $O_{p'}(G) = 1$. D'après **8**, si on note d'un petit rond en exposant les quotients par $O_{p'}(G)$: $N_{G^\circ}(W(P^\circ)) = N_G(W(P))^\circ$, donc $N_{G^\circ}(W(P^\circ))$ est p -nilpotent puisque $N_G(W(P))$ l'est. Par l'absurde, si : $O_{p'}(G) \neq 1$, G° se trouve dès lors p -nilpotent par minimalité de G . Comme : $O_{p'}(G^\circ) = 1$ par définition de $O_{p'}(G)$, il en découle que G° est un p -groupe, donc que G est p -nilpotent — contradiction.
- Montrons que P est maximal dans G . Donnons-nous pour cela un sous-groupe maximal M de G contenant P — donc $O_p(G)$ — et tâchons de montrer que : $M = P$. Comme $O_p(G)$ et $O_{p'}(M)$ sont distingués dans M et d'ordres premiers entre eux : $O_{p'}(M) \leq C_G(O_p(G))$. Or G est p -séparable et : $O_{p'}(G) = 1$, donc d'après **7** : $C_G(O_p(G)) \leq O_p(G)$. Conclusion : $O_{p'}(M) \leq O_p(G) \cap O_{p'}(M) = 1$, i.e. : $O_{p'}(M) = 1$. Pourtant, $N_M(W(P))$ est p -nilpotent puisque $N_G(W(P))$ l'est, donc M lui-même est p -nilpotent par minimalité de G . Comme voulu : $M = O_{p'}(M)P = P$.
- Comme G n'est pas p -nilpotent, G n'est évidemment pas un p -groupe. Donnons-nous donc un diviseur premier $q \neq p$ de $|G|$ et tâchons de montrer que les q -Sylow de G sont abéliens. Or $O_p(G)$ est un q' -groupe et nous avons montré que \bar{G} est p -nilpotent, i.e. que : $\bar{G} = O_{p'}(\bar{G})\bar{P}$. Il nous suffit donc de montrer que $O_{p'}(\bar{G})$ est un q -groupe abélien.

D'après les théorèmes de Sylow, $O_{p'}(\bar{G})$ a un nombre de q -Sylow qui divise $|O_{p'}(\bar{G})|$. L'action par conjugaison de \bar{P} sur $\text{Syl}_q(O_{p'}(\bar{G}))$ possède donc un point fixe d'après l'équation aux classes, disons \bar{Q} avec : $Q \in \text{Syl}_q(G)$. En d'autres termes, \bar{P} normalise \bar{Q} , donc PQ est un sous-groupe de G . Comme : $Q \neq 1$, la maximalité de P montre que : $G = PQ$. Or $\overline{D(Q)}$ est lui aussi normalisé par \bar{P} , donc $D(Q)P$ est un sous-groupe de G avec : $D(Q) < Q$. Par maximalité de P : $D(Q) = 1$, i.e. Q est abélien. ■

3 ACTION QUADRATIQUE ET p -STABILITÉ, UNE INTRODUCTION

Rappelons pour commencer qu'un groupe G agit par automorphismes sur un autre groupe V si pour tous $g \in G$ et $v, v' \in V$: $(vv')^g = v^g v'^g$. On définit dans ces conditions une structure de groupe sur le produit $G \times V$, noté $G \ltimes V$ et appelé le *produit semi-direct de G par V* (pour l'action considérée), en posant pour tous $g, g' \in G$ et $v, v' \in V$: $(g, v)(g', v') = \underbrace{(gg')}_{\in G} \underbrace{(v^g v')}_{\in V}$.

Il est facile de vérifier que les applications $g \mapsto (g, 1)$ et $v \mapsto (1, v)$ sont des morphismes de groupes injectifs, respectivement de G dans $G \ltimes V$ et de V dans $G \ltimes V$, ce qui permet d'identifier G et V à des sous-groupes de $G \ltimes V$. Également, pour tous $g \in G$ et $v \in V$: $(1, v)^{(g, 1)} = (1, v^g)$. Cette relation montre en particulier que : $V \trianglelefteq G \ltimes V$.

Ces remarques justifient qu'on note désormais gv le couple (g, v) pour tous $g \in G$ et $v \in V$. Les deux significations de la notation v^g se trouvent alors coïncider — v^g est à la fois le conjugué de v par g et le résultat de l'action de g sur v . En résumé, toute action par automorphismes peut être vue comme une action par conjugaison dans un produit semi-direct. Le commutateur $[v, g] = v^{-1}v^g$ est quant à lui un élément de V , et on peut dire que v et g commutent quand : $[v, g] = 1$, ou encore : $v^g = v$, autrement dit quand v est un point fixe de l'automorphisme de V induit par l'action de g . On pourra après cette remarque noter $C_G(V)$ le noyau de l'action de G sur V , qui est par définition l'ensemble des éléments de G qui fixent V .

La notation suivante sera très utilisée par la suite. Pour tout groupe G et tous $x, y, z \in G$, on pose : $[x, y, z] = [[x, y], z]$, et pour toutes parties X, Y, Z de G : $[X, Y, Z] = [[X, Y], Z]$.

Entre autres actions par automorphismes, nous nous intéresserons désormais beaucoup, voire exclusivement, aux actions particulières suivantes.

Définition (Action quadratique) Soient G un groupe, V un groupe sur lequel G agit par automorphismes et $x \in G$. On dit que x est quadratique sur V si : $[V, x, x] = 1$.

Dans le cas où V est un \mathbb{F}_p -espace vectoriel de loi notée additivement, l'action par automorphismes de G sur V est de fait déjà \mathbb{F}_p -linéaire — autrement dit G agit \mathbb{F}_p -linéairement sur V — et pour tout $v \in V$:

$$[v, x, x] = [v^x - v, x] = (v^x - v)^x - (v^x - v) = v^{x^2} - 2v^x + v = v^{x^2 - 2x + \text{Id}} = v^{(x - \text{Id})^2}.$$

Dire que l'action de x est quadratique sur V revient alors à dire que l'endomorphisme \mathbb{F}_p -linéaire $(x - \text{Id})^2$ de V est nul, autrement dit que x est annulé comme endomorphisme par le polynôme $(X - 1)^2$. La réduction — de Jordan — des endomorphismes de V annulés par ce polynôme est bien connue. Matriciellement, ces endomorphismes peuvent tous être ramenés à une matrice par blocs de la forme :

$$\begin{pmatrix} I_n & & & \\ & U & & \\ & & \ddots & \\ & & & U \end{pmatrix} \quad \text{avec : } U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Ce cas particulier d'action quadratique sur un \mathbb{F}_p -espace vectoriel n'est qu'un exemple à ce stade, mais il sera davantage à terme et il vaut mieux le garder en mémoire. Le résultat qui suit s'attarde sur la situation plus générale d'une action quadratique sur un p -groupe.

Théorème 11 (Action quadratique sur un p -groupe) Soient G un groupe, V un groupe sur lequel G agit par automorphismes et $x \in G$ quadratique sur V .

- (i) Pour tout $k \in \mathbb{Z}$, x^k est aussi quadratique sur V .
- (ii) Si de plus V est un p -groupe pour un certain nombre premier p , l'image de x dans $\frac{G}{C_G(V)}$ est un p -élément.
Dans le cas d'une action fidèle de G sur V , cela veut simplement dire que x est un p -élément.

Reprenons pour illustrer (ii) le cas d'une action par automorphismes de G sur un \mathbb{F}_p -espace vectoriel V . La matrice

de l'automorphisme \mathbb{F}_p -linéaire de V induit par x est dans une certaine base de la forme : $\begin{pmatrix} I_n & & & \\ & U & & \\ & & \ddots & \\ & & & U \end{pmatrix}$ avec :

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \text{or d'après un calcul classique : } U^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad \text{pour tout } k \in \mathbb{Z}, \text{ donc en particulier : } U^p = I_2.$$

Conclusion : x^p agit trivialement sur V . Cela veut dire que : $x^p \in C_G(V)$, ou encore que l'image de x dans $\frac{G}{C_G(V)}$ est d'ordre 1 ou p .

Démonstration

- (i) Soit $k \in \mathbb{N}^*$ — c'est bien sûr suffisant. Pour tout $v \in V$: $[v, x^k] = [v, x][v, x]^x[v, x]^{x^2} \dots [v, x]^{x^{k-1}}$, donc comme x est quadratique sur V : $[v, x^k] = [v, x]^k \in [V, x]$. Conclusion : $[V, x^k] \leq [V, x]$. Or x commute à $[V, x]$ par hypothèse, donc x^k aussi, donc : $[V, x^k, x^k] = 1$.
- (ii) Faisons dans un premier temps l'hypothèse que x est un q -élément pour un certain nombre premier $q \neq p$ et montrons qu'alors : $x \in C_G(V)$. Fixons pour cela $v \in V$. Comme x est quadratique sur V : $([V, x]v)^x = [V, x]v^x = [V, x][x, v^{-1}]v = [V, x][v^{-1}, x]^{-1}v = [V, x]v$, ce qui signifie que le q -groupe $\langle x \rangle$ agit sur $[V, x]v$. Or V est un p -groupe, donc la classe à gauche $[V, x]v$ de V modulo $[V, x]$ a pour cardinal une puissance de p . Comme : $q \neq p$, l'équation aux classes montre que l'action de $\langle x \rangle$ sur $[V, x]v$ a un point fixe, i.e. que pour un certain $w \in [V, x]$: $(wv)^x = wv$. Or n'oublions pas que x est quadratique sur V , donc : $w^x = w$. Comme voulu : $v^x = v$.

Dans le cas général, notons q_1, \dots, q_r les diviseurs premiers de l'ordre de x autres que p — s'il en existe. Il est connu que x peut être écrit sous la forme : $x = x_0 \dots x_r$, décomposition dans laquelle :

- x_0 est un p -élément et x_i un q_i -élément pour tout $i \in \llbracket 1, r \rrbracket$,
- x_0, \dots, x_r sont des puissances de x — donc sont quadratiques sur V d'après (i).

En particulier, x étant quadratique sur V , x_0, \dots, x_r le sont aussi, alors que d'après le premier point : $x_i \in C_G(V)$ pour tout $i \in \llbracket 1, r \rrbracket$. Conclusion : x a la même image dans $\frac{G}{C_G(V)}$ que le p -élément x_0 — d'où le résultat. ■

Comme nous venons de le voir, l'action quadratique d'un élément x de G sur un p -groupe V contraint fortement l'ordre de x dans le quotient $\frac{G}{C_G(V)}$. La notion de p -stabilité que nous avons évoquée sans la définir en introduction qualifie les actions quadratiques pour lesquelles un peu plus est vrai.

Mais d'abord une notation. Pour tout groupe G , tout sous-groupe distingué N de G et tout nombre premier p , nous noterons $O_p(G/N)$ l'unique sous-groupe — caractéristique — de G contenant N pour lequel : $\frac{O_p(G/N)}{N} = O_p\left(\frac{G}{N}\right)$.

Définition (Action p -stable, groupe p -stable) Soient p un nombre premier et G un groupe.

- Soit V un p -groupe sur lequel G agit par automorphismes. On dit que G est p -stable sur V si pour tout $x \in G$:

$$[V, x, x] = 1 \implies x \in O_p(G/C_G(V)).$$

- On dit que G est p -stable si G est p -stable sur tout p -groupe sur lequel il agit par automorphismes.

Cette définition technique inspire plutôt la méfiance au premier abord mais sera bientôt cruciale. Arrive-t-il si souvent qu'un groupe soit p -stable ? La réponse est OUI pour $p \neq 2$, plutôt souvent, et c'est bien là l'intérêt de la p -stabilité — d'être à la fois facile à garantir et de portée non triviale. Rappelons qu'on appelle *section* d'un groupe n'importe quel quotient de l'un de ses sous-groupes. Nous montrerons plus loin le résultat suivant.

Théorème (Groupes p -séparables non p -stables) Soient p un nombre premier IMPAIR et G un groupe. Si G est p -séparable sans être p -stable, alors d'une part : $p = 3$, et d'autre part G possède une section isomorphe à $SL_2(3)$.

En particulier, si G est p -séparable, G est p -stable dès que l'une des assertions suivantes est vraie :

- 1) $p \geq 5$.
- 2) G est d'ordre impair.
- 3) Les 2-Sylow de G sont abéliens.

À défaut de démontrer ce résultat tout de suite, nous pouvons au moins nous pencher un peu sur le groupe spécial linéaire $SL_2(3)$ et le décrire. Pour commencer, le dénombrement suivant est classique : $|GL_2(3)| = (3^2 - 1)(3^2 - 3) = 48$. On le démontre en remarquant que l'action naturelle de $GL_2(3)$ sur l'ensemble des bases de \mathbb{F}_3^2 est libre et transitive. Or pour construire une telle base, on peut choisir d'abord un vecteur non nul quelconque — $(3^2 - 1)$ possibilités — puis un vecteur quelconque qui ne lui est pas colinéaire — $(3^2 - 3)$ possibilités. Le déterminant étant un morphisme de groupes surjectif de $GL_2(3)$ sur \mathbb{F}_3^* de noyau $SL_2(3)$, il en découle que : $|SL_2(3)| = 24$.

Nous introduisons à présent quatre éléments de $SL_2(3)$: $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $j = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ et $k = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$. Clairement, x est d'ordre 3 et i, j et k d'ordre 4, avec : $i^2 = j^2 = k^2 = -\text{Id}$, $ij = k$ et $ji = -k$. Il n'est dès lors pas dur de se convaincre que $\langle i, j \rangle$ est isomorphe au groupe des quaternions : $\langle i, j \rangle = \{ \pm \text{Id}, \pm i, \pm j, \pm k \}$. Les relations : $j = i^x$ et $k = j^x$ montrent quant à elles que x normalise $\langle i, j \rangle$. Finalement, pour une raison de cardinal : $SL_2(3) = \langle x \rangle \rtimes \langle i, j \rangle$.

Nous pouvons ainsi au moins comprendre pourquoi un groupe p -séparable d'ordre impair ou dont les 2-Sylow sont abéliens est forcément p -stable. Un tel groupe ne saurait en effet posséder une section d'ordre 24, ni une section dont les 2-Sylow sont isomorphes au groupe — non abélien — des quaternions.

Nous pouvons aussi entrevoir de quelle manière la p -stabilité interagit avec la réduction p -séparable de Thompson. Le théorème 9 nous a mis en présence d'un certain $\{p, q\}$ -groupe p -séparable dont les q -Sylow sont abéliens. Un tel groupe est forcément p -stable.

Il est légitime pour finir de se demander ce que le nombre premier 2 a de si particulier dans le contexte de la p -stabilité. Donnons-nous pour le comprendre un groupe G et un 2-groupe abélien élémentaire V sur lequel G opère par automorphismes. Pour toute involution $x \in G$ et pour tout $v \in V$:

$$[v, x]^x = x^{-1}(v^{-1}x^{-1}vx)x^{x^2=1}x^{-1}v^{-1}xv = [x, v] = [v, x]^{-1} \stackrel{[v, x]^2=1}{=} [v, x], \quad \text{donc : } [v, x, x] = 1.$$

En résumé, toute involution de G est quadratique sur V . En particulier, G ne peut être 2-stable sur V que si $O_2(G/C_G(V))$ contient toutes les involutions de G . Or il est possible de choisir V de façon à garantir une action fidèle de G sur V — c'est le cas si V est la représentation régulière de G sur \mathbb{F}_2 par exemple. Pour un tel 2-groupe V : $O_2(G/C_G(V)) = O_2(G)$. Conclusion : pour que G soit 2-stable, il faut que $O_2(G)$ contiennent toutes les involutions de G — condition très contraignante, et même trop contraignante. Nous l'avons dit plus haut, la p -stabilité pour $p \neq 2$ précisément parce qu'elle est à la fois facile à garantir et forte en contenu.

4 LE THÉORÈME D^* DE GLAUBERMAN-SOLOMON

Pour tout groupe G , la notation suivante est classique pour le groupe dérivé : $[G, G] = D(G)$. On a défini aussi $[G, G, G]$ dans la partie précédente. On définit de même : $[G, G, G, G] = [[G, G, G], G]$, etc.

Définition-théorème 12 (Groupe nilpotent, classe de nilpotence) Soit G un groupe.

- On dit que G est *nilpotent* s'il existe un entier $n \in \mathbb{N}^*$ pour lequel : $\overbrace{[G, G, \dots, G]}^{n+1 \text{ fois}} = 1$. Dans ce cas, le plus petit entier n pour lequel l'égalité est vraie est appelé la *classe de nilpotence de G* et notée $\text{cl}(G)$.

Par convention, si G n'est pas nilpotent, on pose : $\text{cl}(G) = +\infty$.

- De manière immédiate, G est nilpotent de classe 1 si et seulement si G est abélien, et nilpotent de classe au plus 2 si et seulement si : $D(G) \leq Z(G)$.

La notion de nilpotence mériterait qu'on s'y attarde et qu'on l'étudie pour elle-même, mais nous irons ici à l'économie. Pour information, les groupes — finis — nilpotents sont plutôt faciles à expliciter, ce sont exactement les groupes qui possèdent un et un seul p -Sylow pour tout nombre premier p . Il revient au même de dire que les groupes — finis — nilpotents sont les groupes qui sont le produit direct de leurs différents sous-groupes de Sylow. En particulier, les p -groupes sont nilpotents.

Pour un groupe G — fini — la nilpotence est aussi équivalente à l'assertion suivante : $\forall H \leq G, H < N_G(H)$. Le théorème 10 s'avère sous cet angle moins une propriété des p -groupes qu'une propriété des groupes nilpotents.

Le petit résultat qui suit nous permettra bientôt de relier le *sous-groupe de Glauberman-Solomon* à la notion de p -stabilité.

Théorème 13 (Un lien entre action quadratique et classe de nilpotence au plus 2) Soient G un groupe, A un sous-groupe abélien et $x \in N_G(A)$. Les assertions suivantes sont équivalentes :

- 1) $\text{cl}(\langle A, x \rangle) \leq 2$.
- 2) x est quadratique sur A .

Démonstration Posons : $B = \langle A, x \rangle$.

1) \implies 2) Par hypothèse : $\text{cl}(B) \leq 2$, donc : $[A, x, x] \leq [B, B, B] = 1$.

2) \implies 1) Faisons l'hypothèse que : $[A, x, x] = 1$, i.e. que : $[A, x] \leq C_G(x)$. Comme x normalise A et comme A est abélien : $[A, x] \leq A \leq C_B(A)$, donc : $[A, x] \leq C_B(x) \cap C_B(A) = C_B(B) = Z(B)$, ce qui veut dire que \bar{A} et \bar{x} commutent si nous notons d'une barre les quotients par $Z(B)$. Il en découle que \bar{B} est abélien, et donc finalement : $D(B) \leq Z(B)$, ou encore : $\text{cl}(B) \leq 2$. ■

Ça y est, nous pouvons enfin définir le sous-groupe novateur que Glauberman et Solomon ont déniché en 2012 et qui détrône un peu l'incontournable sous-groupe $J(P)$ de Thompson et son petit frère $ZJ(P)$.

Définition-théorème 14 (Sous-groupe de Glauberman-Solomon) Soient p un nombre premier et P un p -groupe. On note $\mathcal{D}^*(P)$ l'ensemble des sous-groupes abéliens A de P pour lesquels pour tout $x \in P$: $\text{cl}(\langle A, x \rangle) \leq 2$.

Il est équivalent d'exiger pour tout $x \in P$ l'implication : $\text{cl}(\langle A, x \rangle) \leq 2 \implies [A, x] = 1$.

- (i) L'ensemble $\mathcal{D}^*(P)$ est stable par tout automorphisme de P .
- (ii) Pour tous $A, A' \in \mathcal{D}^*(P)$, si A et A' se normalisent mutuellement : $AA' \in \mathcal{D}^*(P)$.
- (iii) L'ensemble $\mathcal{D}^*(P)$ possède un maximum pour l'inclusion. On le note $D^*(P)$ et on l'appelle le *sous-groupe de Glauberman-Solomon* de P .
En particulier, $D^*(P)$ est abélien et : $D^*(P) \subseteq P$. En outre : $D^*(P) = \langle A \rangle_{A \in \mathcal{D}^*(P)}$.
- (iv) $Z(P) \leq D^*(P)$. En particulier, si $P \neq 1$: $D^*(P) \neq 1$.
- (v) Pour tout sous-groupe P' de P contenant $D^*(P)$: $D^*(P) \leq D^*(P')$.

Dans le cas où x normalise A , le lemme 13 montre que l'implication : $\text{cl}(\langle A, x \rangle) \leq 2 \implies \text{cl}(\langle A, x \rangle) = 1$ est équivalente à celle-ci : $[A, x, x] = 1 \implies [A, x] = 1$.

Démonstration

- (i) Soient $A \in \mathcal{D}^*(P)$ et $\varphi \in \text{Aut}(P)$. Alors : $A^\varphi \in \mathcal{D}^*(P)$, car pour tout $x \in P$:

$$\text{cl}(\langle A^\varphi, x \rangle) = \text{cl}(\langle A, x^{\varphi^{-1}} \rangle^\varphi) = \text{cl}(\langle A, x^{\varphi^{-1}} \rangle) \quad \text{et} \quad [A^\varphi, x] = [A, x^{\varphi^{-1}}]^\varphi.$$

- (ii) Soient $A, A' \in \mathcal{D}^*(P)$. On suppose que A et A' se normalisent mutuellement. Cela fait au moins de AA' un sous-groupe de P , mais cela montre aussi que : $[A, A'] \leq A'$. Or A' est abélien, donc pour tout $x \in A'$: $[A, x, x] \leq [A, A', A'] \leq [A', A'] = 1$, puis d'après 13 : $\text{cl}(\langle A, x \rangle) \leq 2$. Par définition de A enfin : $[A, x] = 1$ pour tout $x \in A'$, donc AA' est abélien.

Soit $x \in P$ pour lequel : $\text{cl}(\langle AA', x \rangle) \leq 2$. A fortiori : $\text{cl}(\langle A, x \rangle) \leq 2$ et $\text{cl}(\langle A', x \rangle) \leq 2$, donc par définition de A et A' : $[A, x] = [A', x] = 1$, autrement dit x centralise à la fois A et A' , et enfin : $[AA', x] = 1$. Conclusion : $AA' \in \mathcal{D}^*(P)$.

- (iii) Soit M un élément maximal de $\mathcal{D}^*(P)$. Soit $x \in N_p(N_p(M))$. Alors d'une part : $M \trianglelefteq N_p(M)$, mais d'autre part : $M^x \trianglelefteq N_p(M)^x = N_p(M)$, donc M et M^x se normalisent mutuellement. Or d'après (i) : $M^x \in \mathcal{D}^*(P)$, donc d'après (ii) : $MM^x \in \mathcal{D}^*(P)$. Ainsi, par maximalité de M : $M^x = M$, i.e. : $x \in N_p(M)$. Conclusion : $N_p(N_p(M)) = N_p(M)$, donc d'après 10 : $N_p(M) = P$, autrement dit : $M \trianglelefteq P$.

Donnons-nous à présent deux éléments maximaux M et M' de $\mathcal{D}^*(P)$. Distingués dans P , ils se normalisent mutuellement, donc d'après (ii) : $MM' \in \mathcal{D}^*(P)$, puis par maximalité de M : $M = M'$. Conclusion : $\mathcal{D}^*(P)$ possède un maximum, lequel contient donc tous les éléments de $\mathcal{D}^*(P)$ tout en étant l'un d'eux, ce qui montre bien que $D^*(P)$ est le sous-groupe de P engendré par les éléments de $\mathcal{D}^*(P)$.

Le fait que $D^*(P)$ soit caractéristique dans P est une conséquence immédiate de (i).

- (iv) Pour tout $x \in P$: $[Z(P), x] = 1$, donc : $Z(P) \in \mathcal{D}^*(P)$, donc d'après (ii) : $Z(P) \leq D^*(P)$.

- (v) Soit P' un sous-groupe de P contenant $D^*(P)$. D'après (iii), il s'agit seulement de montrer l'inclusion : $\mathcal{D}^*(P) \subset \mathcal{D}^*(P')$, laquelle est évidente. ■

Théorème 15 (Foncteur p -caractéristique D^*) Soit p un nombre premier. L'application D^* qui associe à tout p -groupe P son sous-groupe de Glauberman-Solomon $D^*(P)$ est un p -foncteur caractéristique.

Démonstration Le théorème 14 montre une bonne partie du résultat. Pour le reste, soient P et P' deux p -groupes et φ un isomorphisme de P sur P' . Clairement, φ induit une bijection de l'ensemble des sous-groupes abéliens de P sur l'ensemble des sous-groupes abéliens de P' . En outre, pour tout sous-groupe abélien A de P et pour tout $x \in P$: $\text{cl}(\langle A, x \rangle)^\varphi = \text{cl}(\langle A^\varphi, x^\varphi \rangle)$, donc : $\mathcal{D}^*(P)^\varphi = \mathcal{D}^*(P')$. A fortiori, par unicité du maximum : $D^*(P)^\varphi = D^*(P')$. ■

Autre moment important de ce texte, nous pouvons enfin démontrer le théorème D^* de Glauberman-Solomon. Ce qui est fort dans le travail de Glauberman et Solomon, c'est que deux pages suffisent à définir le sous-groupe de Glauberman-Solomon ET démontrer le théorème éponyme. C'est très peu. Le théorème ZJ de Glauberman demandait en 1968 beaucoup plus de travail.

Théorème 16 (Théorème D^* de Glauberman-Solomon) Soient p un nombre premier et G un groupe p -stable pour lequel : $C_G(O_p(G)) \leq O_p(G)$. Alors pour tout $P \in \text{Syl}_p(G)$: $D^*(P) \trianglelefteq G$.

Démonstration Soit $P \in \text{Syl}_p(G)$. Il nous suffit de montrer que : $D^*(P) \trianglelefteq G$, car pour tout $\varphi \in \text{Aut}(G)$: $P^\varphi = P^g$ pour un certain $g \in G$ d'après les théorèmes de Sylow, donc :

$$D^*(P)^\varphi = D^*(P^\varphi) = D^*(P^g) = D^*(P)^g.$$

Notons N le sous-groupe — distingué — de G engendré par les conjugués de $D^*(P)$ dans G . Pour montrer que : $D^*(P) \trianglelefteq G$, il nous suffit de montrer que : $N \leq D^*(P)$, mais donc aussi que : $N \in \mathcal{D}^*(P)$.

- Montrons d'abord que N est un sous-groupe abélien de P . Or : $O_p(G) \leq P$ et $D^*(P) \trianglelefteq P$, donc : $[O_p(G), D^*(P)] \leq D^*(P)$, et comme $D^*(P)$ est abélien : $[O_p(G), D^*(P), D^*(P)] \leq [D^*(P), D^*(P)] = 1$. Aussitôt, par p -stabilité de G : $D^*(P) \leq O_p(G/C_G(O_p(G)))$.

Ensuite, par hypothèse : $C_G(O_p(G)) \leq O_p(G)$, donc $C_G(O_p(G))$ est un p -groupe. Par définition de $O_p(G)$, il en découle que : $O_p(G/C_G(O_p(G))) = O_p(G)$.

Conclusion : $D^*(P) \leq O_p(G)$, puis d'après 14 (v) : $D^*(P) \leq D^*(O_p(G))$. Remarquons alors que : $D^*(O_p(G)) \trianglelefteq O_p(G) \trianglelefteq G$. Ainsi : $N \leq D^*(O_p(G)) \leq O_p(G) \leq P$, donc N est comme voulu un sous-groupe abélien de P .

- Montrons que pour tout $x \in P$: $\text{cl}(\langle N, x \rangle) \leq 2 \implies [N, x] = 1$.

Soit $x \in P$ pour lequel : $\text{cl}(\langle N, x \rangle) \leq 2$. Comme : $N \trianglelefteq G$, alors d'après 13 : $[N, x, x] = 1$. Posons : $C = C_G(N)$ et $O = O_p(G/C)$. L'égalité : $[N, x, x] = 1$ montre par p -stabilité de G que : $x \in O$.

À présent, pour montrer que : $[N, x] = 1$, il nous suffit de prouver que : $[D^*(P)^g, x] = 1$ pour tout $g \in G$. Soit $g \in G$. Comme : $O \trianglelefteq G$, alors : $P^g \cap O \in \text{Syl}_p(O)$, donc : $O = C(P^g \cap O)$. Nous pouvons ainsi écrire que : $x = cy$ avec : $c \in C$ et $y \in P^g \cap O$. Il en découle que : $[N, x] = [N, y] \leq N$, puis que : $[D^*(P)^g, y, y] \leq [N, y, y] = [N, x, x] = 1$. Or il se trouve que : $D^*(P)^g = D^*(P^g) \in \mathcal{D}^*(P^g)$ et $y \in P^g$, donc par définition de $\mathcal{D}^*(P^g)$: $[D^*(P)^g, y] = 1$. Comme voulu : $[D^*(P)^g, x] = 1$ puisque : $D^*(P)^g \leq N$ et $c \in C = C_G(N)$. ■

5 GROUPES p -STABLES

Le concept de p -stabilité a été défini et utilisé dans les parties précédentes, mais nous ne savons toujours pas quels groupes sont p -stables et lesquels ne le sont pas. Nous allons nous demander dans cette partie ce qui peut être dit d'un groupe qui n'est PAS p -stable. L'analyse d'un tel groupe sera menée grâce à une série de réductions plus ou moins fastidieuses.

Le résultat qui suit, notre point de départ, donne a posteriori au concept d'action quadratique une motivation naturelle.

Théorème 17 (Action p -stable sur un quotient) Soient p un nombre premier, G un groupe, V un p -groupe sur lequel G agit par automorphismes et W un sous-groupe distingué G -stable de V

- (i) Tout élément de $C_G(W) \cap C_G\left(\frac{V}{W}\right)$ est quadratique sur V .
- (ii) Si G est p -stable sur W et $\frac{V}{W}$, il l'est aussi sur V .

En résumé, l'assertion (ii) stipule qu'un élément qui agit trivialement à la fois sur W et sur $\frac{V}{W}$ est quadratique sur V .

Démonstration

- (i) Soient $x \in C_G(W) \cap C_G\left(\frac{V}{W}\right)$ et $v \in V$. Montrons que : $[v, x, x] = 1$. Or : $(Wv)^x = Wv$ car : $x \in C_G\left(\frac{V}{W}\right)$, donc en particulier : $v^x = wv$ pour un certain $w \in W$. Aussitôt : $[w, x] = 1$ car : $x \in C_G(W)$, donc finalement : $[v, x, x] = [w, x] = 1$.
- (ii) Notons W' le quotient de V par W . Soit $x \in G$ pour lequel : $[V, x, x] = 1$. Aussitôt : $[W, x, x] = 1$ et $[W', x, x] = 1$, donc par p -stabilité : $x \in O_p(G/C_G(W)) \cap O_p(G/C_G(W'))$. Montrer la relation : $x \in O_p(G/C_G(V))$ revient dès lors à montrer l'inclusion suivante :

$$O_p(G/C_G(W)) \cap O_p(G/C_G(W')) \leq O_p(G/C_G(V)).$$

- Le morphisme de groupes $g \mapsto (C_G(W)g, C_G(W')g)$ de G dans $\frac{G}{C_G(W)} \times \frac{G}{C_G(W')}$ a pour noyau l'intersection $C_G(W) \cap C_G(W')$ et envoie $O_p(G/C_G(W)) \cap O_p(G/C_G(W'))$ dans $O_p\left(\frac{G}{C_G(W)}\right) \times O_p\left(\frac{G}{C_G(W')}\right)$, lui-même inclus dans le p -sous-groupe distingué $O_p\left(\frac{G}{C_G(W)} \times \frac{G}{C_G(W')}\right)$. Conclusion :

$$O_p(G/C_G(W)) \cap O_p(G/C_G(W')) \leq O_p(G/C_G(W) \cap C_G(W')).$$

- Ensuite, d'après (i) et 11 (ii), $\frac{C_G(W) \cap C_G(W')}{C_G(V)}$ est un p -sous-groupe distingué de $\frac{G}{C_G(V)}$. Par ailleurs : $\frac{O_p(G/C_G(W) \cap C_G(W'))}{C_G(W) \cap C_G(W')} = O_p\left(\frac{G}{C_G(W) \cap C_G(W')}\right)$, donc $\frac{O_p(G/C_G(W) \cap C_G(W'))}{C_G(V)}$ est un p -sous-groupe distingué de $\frac{G}{C_G(V)}$. Conclusion : $O_p(G/C_G(W) \cap C_G(W')) \leq O_p(G/C_G(V))$ et le résultat en découle. ■

Théorème 18 (Réduction de la non- p -stabilité à une action linéaire diagonalisable) Soient p un nombre premier, G un groupe NON p -stable et q une puissance de p pour laquelle le polynôme $X^{|G|} - 1$ est scindé sur \mathbb{F}_q . Il existe alors un \mathbb{F}_q -espace vectoriel de dimension finie V pour lequel :

- 1) G agit \mathbb{F}_q -linéairement sur V ,
- 2) G n'est PAS p -stable sur V ,
- 3) les automorphismes \mathbb{F}_q -linéaires de V induits par G sont diagonalisables sur \mathbb{F}_q .

Démonstration Comme G n'est pas p -stable, nous pouvons nous donner un p -groupe V sur lequel G n'est pas p -stable, minimal pour cette propriété. Par hypothèse, pour un certain $x \in G$: $[V, x, x] = 1$ mais : $x \notin O_p(G/C_G(V))$. En particulier : $C_G(V) \neq G$, donc : $V \neq 1$, donc comme V est un p -groupe : $Z(V) \neq 1$.

- Soit W un sous-groupe distingué G -stable de V . Parce qu'il n'est pas p -stable sur V , G ne peut l'être à la fois sur W et sur $\frac{V}{W}$ d'après 17 (ii). Par minimalité de V , on a donc soit : $W = 1$, soit : $W = V$. Conclusion : V ne possède aucun sous-groupe propre non trivial à la fois distingué et G -stable.
- En particulier : $Z(V) = V$, i.e. V est abélien. De ce fait, l'ensemble des éléments d'ordre p de V est un sous-groupe distingué G -stable non trivial de V , donc est égal à V tout entier. Conclusion : V est abélien p -élémentaire. Il est dès lors possible de voir V comme un \mathbb{F}_p -espace vectoriel de dimension finie sur lequel G agit \mathbb{F}_p -linéairement. Dans le vocabulaire des représentations linéaires, il est équivalent d'affirmer que V est une représentation \mathbb{F}_p -linéaire de G .
- Les automorphismes \mathbb{F}_p -linéaires de V issus de G n'ont a priori aucune raison d'être diagonalisables, mais tous sont annulés par le polynôme $X^{|G|} - 1$ d'après le théorème de Lagrange, par hypothèse scindé sur \mathbb{F}_q — forcément à racines simples. Donnons-nous alors une base (v_1, \dots, v_n) de V sur \mathbb{F}_p et V_q un \mathbb{F}_q -espace vectoriel quelconque de dimension n dont nous notons aussi (v_1, \dots, v_n) une base sur \mathbb{F}_q . L'action de G sur V s'étend naturellement en une action \mathbb{F}_q -linéaire de G sur V_q , avec pour tous $g \in G$ et $\lambda_1, \dots, \lambda_n \in \mathbb{F}_q$ par : $g \cdot \left(\sum_{k=1}^n \lambda_k v_k \right) = \sum_{k=1}^n \lambda_k (g \cdot v_k)$. Pour les lecteurs que le produit tensoriel n'effraie pas, il paraîtra

plus élégant de poser : $V_q = \mathbb{F}_q \otimes_{\mathbb{F}_p} V$ et de définir l'action \mathbb{F}_q -linéaire de G sur V_q par prolongement \mathbb{F}_p -linéaire des relations : $g \cdot (\lambda \otimes v) = \lambda \otimes (g \cdot v)$ pour tous $g \in G, \lambda \in \mathbb{F}_q$ et $v \in V$. Quelque définition qu'on choisisse pour V_q , les automorphismes \mathbb{F}_q -linéaires de V_q issus de G ont à présent le mérite d'être tous diagonalisables.

- Pour finir, il n'est pas dur de se convaincre que $[V_q, x, x]$ est le sous- \mathbb{F}_q -espace vectoriel de V_q engendré par $[V, x, x]$, de sorte que : $[V_q, x, x] = 1$. Également : $C_G(V_q) = C_G(V) = 1$, donc a fortiori : $x \notin O_p(G/C_G(V)) = O_p(G/C_G(V_q))$. ■

Le théorème qui précède montre que la non- p -stabilité d'un groupe peut toujours être imputée si l'on veut à sa non- p -stabilité sur un espace vectoriel sur lequel il agit linéairement par des automorphismes diagonalisables. Le théorème qui suit, important en soi, va nous permettre de ramener de tels contre-exemples à des espaces vectoriels de dimension 2.

Théorème 19 (Théorème de Baer) Soient p un nombre premier, G un groupe et $x \in G$. Les assertions suivantes sont équivalentes :

- 1) $x \in O_p(G)$.
- 2) Pour tout $g \in G, \langle x, x^g \rangle$ est un p -groupe.

Démonstration

- 1) \implies 2) Si : $x \in O_p(G)$, alors pour tout $g \in G : x^g \in O_p(G)$ car : $O_p(G) \trianglelefteq G$, donc $\langle x, x^g \rangle$ est un sous-groupe de $O_p(G)$, a fortiori un p -groupe.
- 2) \implies 1) Supposons réciproquement que $\langle x, x^g \rangle$ est un p -groupe pour tout $g \in G$ et raisonnons par récurrence sur $|G|$ en supposant l'implication : 2) \implies 1) vraie de tout groupe d'ordre strictement inférieur. On peut supposer sans perte de généralité que G n'est pas un p -groupe. En particulier : $G \neq \langle x \rangle$, donc x est inclus dans au moins un sous-groupe maximal de G .

Se peut-il que x appartienne à un seul sous-groupe maximal M de G ? Supposons que ce soit le cas. Pour tout $g \in G, \langle x, x^g \rangle$ étant un p -groupe alors que G ne l'est pas, $\langle x, x^g \rangle$ est inclus dans un sous-groupe maximal de G contenant x , forcément M , donc : $\langle x^G \rangle \leq M$. Or par ailleurs, pour tous $g \in G$ et $m \in M, \langle x^g, x^{gm} \rangle = \langle x, x^{gmg^{-1}} \rangle^g$ est un p -groupe, donc par hypothèse de récurrence : $x^g \in O_p(M)$. Ainsi $\langle x^G \rangle$ est un p -sous-groupe distingué de G , donc : $x \in \langle x^G \rangle \leq O_p(G)$.

Nous pouvons supposer désormais que x n'appartient pas à un seul sous-groupe maximal de G . Donnons-nous-en deux, disons M et M' , pour lesquels $|M \cap M'|_p$ est maximal, et notons I un p -Sylow de $M \cap M'$ contenant x . Si : $I \trianglelefteq G, \langle x^G \rangle$ est un sous-groupe de I , donc un p -sous-groupe distingué de G , donc : $x \in \langle x^G \rangle \leq O_p(G)$.

Supposons : $I \not\trianglelefteq G$. Dans ces conditions, $N_G(I)$ est inclus dans un sous-groupe maximal M'' de G , qui bien sûr contient x . Soit $P \in \text{Syl}_p(M)$ contenant I . Aussitôt : $N_p(I) = P \cap N_G(I) \leq M \cap M''$, donc : $|M \cap M'|_p = |I| \leq |N_p(I)| \leq |M \cap M''|_p$, d'où l'égalité : $N_p(I) = I$ grâce à notre choix des sous-groupes M et M' . Il en découle d'après 10 que : $I = P$, autrement dit que : $I \in \text{Syl}_p(M)$, et pour la même raison : $I \in \text{Syl}_p(M')$. Retenons-en que : $O_p(M) \leq I$ et $O_p(M') \leq I$.

À présent, $\langle y, y^m \rangle$ est un p -groupe pour tout $y \in x^G \cap M$, donc de nouveau, par hypothèse de récurrence : $x^G \cap M \subset O_p(M) \leq I \leq M'$, ou encore : $x^G \cap M \subset x^G \cap M'$. Par symétrie : $x^G \cap M = x^G \cap M'$. En outre, $\langle x^G \cap M \rangle$ est un sous-groupe de $O_p(M)$, donc un p -groupe. Si : $\langle x^G \cap M \rangle \trianglelefteq G$, il en découle que : $x \in \langle x^G \cap M \rangle \leq O_p(G)$, et il en va de même si : $\langle x^G \cap M' \rangle \trianglelefteq G$. Le cas contraire n'est pas possible, car on aurait par maximalité de M et M' : $M = N_G(\langle x^G \cap M \rangle) = N_G(\langle x^G \cap M' \rangle) = M'$. ■

Nous aurons besoin de deux lemmes encore pour poursuivre notre étude des groupes non p -stables.

Théorème 20 (Action p -stable et fidélité) Soient p un nombre premier, G un groupe et V un p -groupe sur lequel G agit par automorphismes. Alors G est p -stable sur V si et seulement si $\frac{G}{C_G(V)}$ l'est.

Démonstration Notons d'une barre les quotients par $C_G(V)$ dans G . L'action de \overline{G} sur V est fidèle, autrement dit : $C_{\overline{G}}(V) = 1$. Or pour tout $x \in G$: $[V, \overline{x}, \overline{x}] = [V, x, x]$, et de plus : $\frac{\overline{G}}{C_{\overline{G}}(V)} = \overline{G} = \frac{G}{C_G(V)}$. Le résultat en découle par définition de la p -stabilité. ■

Théorème 21 (p -Sylow de $SL_2(q)$) Soient p un nombre premier et q une puissance non triviale de p .

- (i) Les p -Sylow de $SL_2(q)$ sont abéliens p -élémentaires d'ordre q .
- (ii) Tout p -sous-groupe non trivial de $SL_2(q)$ est inclus dans un unique p -Sylow.

Démonstration Le groupe $SL_2(q)$ agit \mathbb{F}_q -linéairement sur \mathbb{F}_q^2 , mais aussi transitivement sur $\mathbb{F}_q^2 \setminus \{(0, 0)\}$. Ensuite, l'égalité suivante est classique : $|SL_2(q)| = (q-1)q(q+1)$ et montre que les p -Sylow de $SL_2(q)$ sont d'ordre q .

- (i) Notons i le vecteur $(1, 0)$ de \mathbb{F}_q^2 . Il n'est pas dur de comprendre que $C_{SL_2(q)}(i)$ est l'ensemble des matrices $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, α décrivant \mathbb{F}_q . Or l'application $\alpha \mapsto \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ est un morphisme de groupes injectif du groupe additif \mathbb{F}_q dans $SL_2(\mathbb{F}_q)$. Pour une raison de cardinal, $C_{SL_2(q)}(i)$ est donc un p -Sylow de $SL_2(q)$, qui plus est abélien p -élémentaire.

Pour tout $s \in SL_2(q)$, $C_{SL_2(q)}(i^s) = C_{SL_2(q)}(i)^s$ est à son tour un p -Sylow de $SL_2(q)$, et nous avons trouvé là en réalité tous les p -Sylow de $SL_2(q)$ puisqu'ils sont conjugués d'après les théorèmes de Sylow. En résumé, l'action de $SL_2(q)$ étant transitive sur $\mathbb{F}_q^2 \setminus \{(0, 0)\}$, les p -Sylow de $SL_2(q)$ sont exactement les sous-groupes $C_{SL_2(q)}(x)$, x décrivant $\mathbb{F}_q^2 \setminus \{(0, 0)\}$ — attention, cette description occasionne des répétitions.

- (ii) Tout p -sous-groupe de $SL_2(q)$ est inclus dans un p -Sylow, donc fixe au moins un vecteur de $\mathbb{F}_q^2 \setminus \{(0, 0)\}$, mais peut-il être inclus dans deux p -Sylow distincts ? Il fixerait dans ce cas deux vecteurs non colinéaires de \mathbb{F}_q^2 , donc \mathbb{F}_q^2 tout entier, assertion à que seule la matrice identité I_2 satisfait. Comme voulu, tout p -sous-groupe non trivial de $SL_2(q)$ est inclus dans un et un seul p -Sylow. ■

Théorème 22 (Irruption du groupe $SL_2(q)$ en cas de non- p -stabilité) Soient p un nombre premier, G un groupe NON p -stable et q une puissance de p pour laquelle le polynôme $X^{|G|} - 1$ est scindé sur \mathbb{F}_q . Le groupe G possède alors une section isomorphe à un sous-groupe Γ de $SL_2(q)$ pour lequel :

- 1) $\Gamma = \langle x, y \rangle$ avec : $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et où $y \in \Gamma$ est d'ordre p ,
- 2) $O_p(\Gamma) = 1$.

Démonstration Ce n'est pas vraiment G qui nous intéresse ici, mais seulement l'une de ses sections. Nous pourrions ainsi nous permettre dans la preuve qui suit de remplacer sans perte de généralité G par n'importe laquelle de ses sections.

D'après 18, nous pouvons nous donner un \mathbb{F}_q -espace vectoriel de dimension finie V sur lequel G agit \mathbb{F}_q -linéairement, sur lequel G n'est pas p -stable, et qui induit des automorphismes \mathbb{F}_q -linéaires de V tous diagonalisables sur \mathbb{F}_q . Nous choisissons de plus V de dimension minimale pour ces propriétés. Par hypothèse, pour un certain $x \in G$: $[V, x, x] = 1$ mais : $x \notin O_p(G/C_G(V))$.

- On peut montrer grâce à 17 (ii), de même que dans la preuve du théorème 18, que V ne possède pas de sous- \mathbb{F}_q -espace vectoriel G -stable propre non trivial. Dans le vocabulaire des représentations linéaires, cela revient à dire que V est une représentation \mathbb{F}_q -linéaire irréductible de G .
- Ensuite, d'après 20, $\frac{G}{C_G(V)}$ n'est pas p -stable sur V , donc nous pouvons supposer sans perte de généralité que l'action de G sur V est fidèle, i.e. que : $C_G(V) = 1$. L'action \mathbb{F}_q -linéaire de G sur V identifie dès lors G à un sous-groupe de $GL(V)$. En outre, d'après 11 (ii), x est un p -élément.
- Maintenant que : $C_G(V) = 1$, la définition de x montre que : $x \notin O_p(G)$. D'après le théorème de Baer, G contient donc un élément g pour lequel $\langle x, y \rangle$ n'est pas un p -groupe avec : $y = x^g$. Il découle aisément de l'égalité : $[V, x, x] = 1$ que : $[V, y, y] = 1$. Nous supposons désormais, sans perte de généralité, que : $G = \langle x, y \rangle$. En particulier, G n'est pas un p -groupe.

- L'automorphisme xy^{-1} de V étant diagonalisable sur \mathbb{F}_q , nous pouvons nous en donner une valeur propre λ et un vecteur propre associé e . Clairement : $\lambda \neq 0$ et $e^{xy^{-1}} = \lambda e$, mais aussitôt : $e^x = \lambda e^y$.

Se peut-il que x stabilise la droite $\mathbb{F}_q e$? Supposons que ce soit le cas. L'élément y stabilise dans ce cas lui aussi $\mathbb{F}_q e$ car : $e^x = \lambda e^y$, mais donc $G = \langle x, y \rangle$ également. Ainsi, par minimalité de E : $E = \mathbb{F}_q e$, ce qui fait de G un sous-groupe du groupe linéaire $GL(\mathbb{F}_q e)$, lequel est isomorphe à \mathbb{F}_q^* . Or \mathbb{F}_q^* est cyclique alors que, d'une part x est un p -élément, d'autre part : $x \notin O_p(G)$ — contradiction. Conclusion : les vecteurs e et e^x sont \mathbb{F}_q -linéairement indépendants.

Comme nous l'avons vu juste après la définition des action quadratiques, l'égalité : $[V, x, x] = 1$ s'écrit aussi : $(x - \text{Id})^2 = 0$ en termes plus linéaires. En particulier : $(e^x)^x = 2e^x - e$, donc x stabilise le sous- \mathbb{F}_q -espace vectoriel $\mathbb{F}_q e + \mathbb{F}_q e^x$ de V . De même : $[V, y, y] = 1$, donc y commute à $[e, y] = e^y - e$, donc : $(e^x)^y - e^x = (\lambda e^y)^y - \lambda e^y = \lambda(e^y - e)^y = \lambda(e^y - e) = e^x - \lambda e$, et enfin : $(e^x)^y = 2e^x - \lambda e$. Conclusion : y stabilise lui aussi le sous- \mathbb{F}_q -espace vectoriel $\mathbb{F}_q e + \mathbb{F}_q e^x$, mais c'est finalement le groupe $G = \langle x, y \rangle$ tout entier qui le stabilise, donc par irréductibilité de V : $V = \mathbb{F}_q e + \mathbb{F}_q e^x$. En résumé, V est un \mathbb{F}_q -espace vectoriel de dimension 2.

- Notons à présent (a, b) la base $(e^x - e, e)$ de V . D'après les calculs qui précèdent, l'automorphisme x de V a pour matrice : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans (a, b) car : $(e^x - e)^x = e^x - e$ et $e^x = (e^x - e) + e$. Aussitôt : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = I_2$, donc x est d'ordre p , et par ailleurs : $\det(x) = 1$. Les éléments x et y jouant des rôles identiques dans cette preuve, y est lui aussi d'ordre p et : $\det(y) = 1$. L'action \mathbb{F}_q -linéaire de G sur V identifie ainsi $G = \langle x, y \rangle$ à un sous-groupe de $SL(V)$, et même de $SL_2(q)$ grâce à la base (a, b) , avec : $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et y d'ordre p .
- Se peut-il pour finir qu'on ait : $O_p(G) \neq 1$? Supposons que ce soit le cas. D'après 21, $O_p(G)$ est alors inclus dans un unique p -Sylow P de $SL_2(q)$. Or $O_p(G)\langle x \rangle$ et $O_p(G)\langle y \rangle$ sont eux-mêmes des p -sous-groupes non triviaux de $SL(E)$, donc sont inclus dans P . A fortiori : $G = \langle x, y \rangle \leq P$, ce que contredit le fait que G n'est pas un p -groupe. Comme voulu : $O_p(G) = 1$. ■

Théorème 23 (Un lemme de calcul matriciel dans $SL_2(q)$) Soient p un nombre premier IMPAIR, q une puissance non triviale de p , $x \in SL_2(q)$ un élément d'ordre p et $\omega \in SL_2(q)$ un p' -élément. Si ω et ω^x commutent, alors : $\omega = I_2$ ou $\omega = -I_2$.

Une remarque en passant. Toute involution de $SL_2(q)$ est annulée par le polynôme $X^2 - 1 = (X - 1)(X + 1)$, donc est diagonalisable à valeurs propres dans $\{1, -1\}$, mais cela ne peut concerner dans $SL_2(q)$ que les matrices I_2 et $-I_2$. En particulier, $-I_2$ est donc la seule involution de $SL_2(q)$.

Démonstration On peut supposer sans perte de généralité, quitte à conjuguer x et ω , c'est-à-dire à changer de base, que : $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Écrivons : $\omega = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ avec $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ et notons n l'ordre de ω . Après calcul, l'égalité : $\omega^x \omega = \omega \omega^x$ implique que : $2\beta^2 = 0$, donc : $\beta = 0$ car p est impair, mais aussi du coup que : $\alpha = \delta$. Conclusion : $\omega = \begin{pmatrix} \alpha & \gamma \\ 0 & \alpha \end{pmatrix}$, puis : $\begin{pmatrix} \alpha^n & n\alpha^{n-1}\gamma \\ 0 & \alpha^n \end{pmatrix} = \omega^n = I_2$ d'après le théorème de Lagrange. En particulier : $n\alpha^{n-1}\gamma = 0$, et comme n et p sont premiers entre eux et : $\alpha \neq 0$, finalement : $\gamma = 0$. Conclusion : ω est une homothétie, et comme : $\omega \in SL(E)$, forcément : $\omega = I_2$ ou $\omega = -I_2$. ■

Théorème 24 (Groupes p -séparables non p -stables) Soient p un nombre premier IMPAIR et G un groupe. Si G est p -séparable sans être p -stable, alors d'une part : $p = 3$, et d'autre part G possède une section isomorphe à $SL_2(3)$.

En particulier, si G est p -séparable, G est p -stable dès que l'une des assertions suivantes est vraie :

- 1) $p \geq 5$.
- 2) G est d'ordre impair.
- 3) Les 2-Sylow de G sont abéliens.

Démonstration D'après 22, si on note q une puissance de p pour laquelle le polynôme $X^{|G|} - 1$ est scindé sur \mathbb{F}_q , G possède une section isomorphe à un sous-groupe Γ de $\mathrm{SL}_2(q)$ pour lequel : $\Gamma = \langle x, y \rangle$ avec : $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $y \in \Gamma$ d'ordre p , et : $O_p(\Gamma) = 1$. Posons en outre : $Z = Z(\mathrm{SL}_2(q)) = \langle -I_2 \rangle = \{I_2, -I_2\}$.

- D'après 6, G étant p -séparable : $O_{p'}(\Gamma) \neq 1$, donc nous pouvons nous donner un diviseur premier r de $|O_{p'}(\Gamma)|$. Parce qu'il normalise $O_{p'}(\Gamma)$, x agit par conjugaison sur $\mathrm{Syl}_q(O_{p'}(\Gamma))$, dont le cardinal est premier à p car il divise $|O_{p'}(\Gamma)|$ d'après les théorèmes de Sylow. D'après l'équation aux classes, x étant d'ordre p , x normalise donc au moins un r -Sylow de $O_{p'}(\Gamma)$, disons R . A fortiori, x normalise $Z(R)$. Or pour tout $\omega \in Z(R)$, ω et ω^x commutent, donc d'après 23 : $\omega \in Z$. Comme : $R \neq 1$, cela montre que : $Z(R) = Z$. En particulier : $r = 2$ et $O_{p'}(\Gamma) = R$ est un 2-groupe.

Ensuite, d'après 7, Γ étant p -séparable : $C_\Gamma(O_{p'}(\Gamma)) \leq O_{p'}(\Gamma)$. Or : $Z = Z(\mathrm{SL}_2(q))$, donc : $R = O_{p'}(\Gamma) \neq Z$.

- Intéressons-nous à présent au 2-groupe quotient non trivial $\frac{R}{Z}$. Son centre est lui-même non trivial et ses involutions forment un sous-groupe caractéristique de $\frac{R}{Z}$ dont nous notons Q la pré-image dans R . Caractéristique dans R , Q est en particulier normalisé par x . En outre, pour tout $\chi \in Q \setminus Z$: $\chi^2 \in Z$ par définition de Q , mais comme $-I_2$ est la seule involution de G : $\chi^2 = -I_2$.
- Fixons enfin $i \in Q \setminus Z$ et posons : $j = i^x$ et $k = i^{x^2}$, eux aussi éléments de $Q \setminus Z$. En particulier : $i^2 = j^2 = k^2 = -I_2$.

Comme : $i \notin Z$, le théorème 23 montre que i et $j = i^x$ ne commutent pas. En particulier : $ij \notin Z$, donc : $ij \in Q \setminus Z$, et ainsi : $(ij)^2 = -I_2$. Aussitôt : $ijij = i^2$, donc : $jij = i$, et enfin : $ji = j^2ij = -ij$. Après conjugaison par x , on obtient donc aussi : $kj = -jk$. Le même argument, appliqué aux éléments i et $k = i^{x^2}$, montre que : $ki = -ik$.

Finalement : $(ijk)^2 = ij(ki)jk = -ij(ik)jk = -i(ji)(kj)k = -i(ij)(jk)k = -i^2j^2k^2 = I_2$, et comme $-I_2$ est la seule involution de $\mathrm{SL}_2(q)$: $ijk \in Z$. En particulier : $(ijk)^x = (ijk)^i$, ce qui nous donne : $jki^{x^3} = jki$, et enfin : $i^{x^3} = i$. En d'autres termes, i et x^3 commutent alors que i et x ne commutent pas — sans quoi i et i^x commuteraient à leur tour, ce qui est faux — donc x est d'ordre divisible par 3. Comme x est d'ordre p , nous venons donc de montrer que : $p = 3$.

Comme : $ijk \in Z$, alors : $jk = \pm i$, donc : $\langle i, j \rangle^x = \langle j, k \rangle = \langle j, jk \rangle = \langle i, j \rangle$, autrement dit le sous-groupe $\langle i, j \rangle$ de Q est normalisé par x . Grâce à la relation : $ji = -ij$, il apparaît en outre que : $\langle i, j \rangle = \{ \pm I_2, \pm i, \pm j, \pm k \}$, et il est bien clair à présent que Q est isomorphe au groupe des quaternions. Le produit semi-direct $\langle x \rangle Q$ est enfin d'ordre $3 \times 8 = 24 = |\mathrm{SL}_2(3)|$. Conclusion : $\Gamma = \langle x \rangle Q = \mathrm{SL}_2(3)$. ■

Les pièces du puzzle sont maintenant en place, le théorème de p -nilpotence de Glauberman-Solomon est enfin à notre portée.

Théorème 25 (Théorème de p -nilpotence de Glauberman-Solomon) Soient p un nombre premier IMPAIR, G un groupe et $P \in \mathrm{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

- 1) G est p -nilpotent.
- 2) $N_G(D^*(P))$ est p -nilpotent.

Démonstration Pour commencer, D^* est un p -foncteur caractéristique d'après 15. Ensuite, tout groupe p -séparable dont les 2-Sylow sont abéliens est p -stable d'après 24, donc d'après le théorème D^* , tout groupe p -séparable G pour lequel : $C_G(O_p(G)) \leq O_p(G)$ et dont les 2-Sylow sont abéliens satisfait la proposition : $\forall P \in \mathrm{Syl}_p(G), D^*(P) \subseteq G$. La réduction p -séparable de Thompson fournit la conclusion souhaitée. ■

Nous achèverons ce texte sur une application simple et efficace du théorème de p -nilpotence de Glauberman-Solomon.

Théorème 26 (Sous-groupes de Sylow maximaux) Soient p un nombre premier IMPAIR et G un groupe. Si les p -Sylow de G sont maximaux dans G , alors G est résoluble.

En raffinant un peu — mais à peine — on peut montrer que si G possède un sous-groupe nilpotent d'ordre impair, alors G est résoluble.

Démonstration Par récurrence sur $|G|$, faisons l'hypothèse que le théorème est vrai dans tout groupe d'ordre strictement à $|G|$. Soit $P \in \text{Syl}_p(G)$, maximal dans G par hypothèse. On peut supposer sans perte de généralité que : $P \neq 1$, et G n'est pas un p -groupe puisque : $G \neq P$. Par maximalité de P dans G , en tout cas : $N_G(D^*(P)) = G$ ou $N_G(D^*(P)) = P$.

- Si : $N_G(D^*(P)) = G$, alors : $D^*(P) \trianglelefteq G$. Or : $P \neq 1$ donc : $D^*(P) \neq 1$, donc si nous notons d'une barre les quotients par $D^*(P)$, \overline{P} est un p -Sylow maximal dans \overline{G} , donc \overline{G} est résoluble par hypothèse de récurrence. A fortiori, $D^*(P)$ étant un p -groupe, G lui-même est résoluble.
- Supposons désormais que : $N_G(D^*(P)) = P$. En particulier, $N_G(D^*(P))$ est p -nilpotent, donc G aussi d'après le théorème de p -nilpotence de Glauberman-Solomon : $G = O_{p'}(G)P$ avec : $O_{p'}(G) \neq 1$. Donnons-nous alors un diviseur premier q de $|O_{p'}(G)|$. L'action par conjugaison de P sur $\text{Syl}_q(O_{p'}(G))$ possède un point fixe Q d'après l'équation aux classes, car $|O_{p'}(G)|$ est premier à p . Or dans ces conditions, PQ est un sous-groupe de G , donc par maximalité de P : $PQ = G$, autrement dit : $O_{p'}(G) = Q$. Comme voulu, G est résoluble puisque P et $O_{p'}(G) = Q$ le sont. ■

On s'oblige à exiger que p soit impair en utilisant le théorème de p -nilpotence de Glauberman-Solomon, mais est-il possible tout de même qu'un 2-Sylow soit maximal dans un groupe NON résoluble ? La réponse est OUI avec le groupe linéaire $G = \text{GL}_3(2)$ comme contre-exemple. Ce groupe, pour commencer, est d'ordre $(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$. Ensuite, parce qu'on travaille sur le corps \mathbb{F}_2 : $G = \text{GL}_3(2) = \text{SL}_3(2) = \text{PSL}_3(2)$, donc en vertu d'un résultat de simplicité

bien connu, G est simple, non abélien donc non résoluble. Il a pour 2-Sylow, par exemple, le sous-groupe $P = \begin{pmatrix} 1 & \cdot & \cdot \\ 0 & 1 & \cdot \\ 0 & 0 & 1 \end{pmatrix}$ —

dans lequel le symbole « \cdot » désigne un élément quelconque de \mathbb{F}_2 . Ce 2-Sylow est isomorphe au groupe des quaternions avec pour seule involution la matrice $\tau = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. En particulier : $P \leq N_G(P) \leq C_G(\tau)$, or après calcul : $C_G(\tau) = P$,

donc : $N_G(P) = C_G(\tau) = P$. L'égalité : $C_G(\tau) = P$ montre aussi que P est le seul 2-Sylow de G qui contient τ , mais comme τ est la seule involution de P , cela signifie que P intersecte trivialement tout autre 2-Sylow. Plus généralement, les 2-Sylow de G étant conjugués d'après les théorèmes de Sylow, l'intersection de deux 2-Sylow distincts est toujours triviale.

À présent, pour montrer que P est maximal dans G , donnons-nous un sous-groupe maximal M de G contenant P — d'ordre 8, 24 ou 56.

- **Cas où $|M| = 56$** : L'action de G sur l'ensemble G/M des classes à droite de G modulo M nous fournit dans ce cas un morphisme de groupes non nul de G dans le groupe symétrique $S_{G/M}$. Or l'existence d'un tel morphisme contredit la simplicité de G car : $|S_{G/M}| = 6$ alors que : $|G| = 168$.

- **Cas où $|M| = 24$** : D'après les théorèmes de Sylow, dans ce cas : $|\text{Syl}_2(M)| = |M : N_M(P)| = |M : P| = 3$, donc M contient $3 \times (8 - 1) = 21$ 2-éléments non triviaux, ce qui ne laisse de place qu'à un seul 3-Sylow d'ordre 3 —

forcément distingué — disons : $\{1, \sigma, \sigma^{-1}\}$ où σ est d'ordre 3. Or si nous posons : $\theta = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, alors :

$\sigma^\theta \in \{\sigma, \sigma^{-1}\}$, donc : $\sigma^{\theta^2} = \sigma$, et comme : $\theta^2 = \tau$, alors : $\sigma \in C_G(\tau) = P$ — contradiction.

Conclusion : $|M| = 8$, autrement dit : $M = P$, donc le 2-Sylow P est maximal dans G .